# Configuration Reference

/ Directory Services 7

Latest update: 7.0.2

ForgeRock AS.
201 Mission St., Suite 2900
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

## Abstract

Configuration settings accessible through the **dsconfig** command.

# Table of Contents

# About This Reference

This reference describes server configuration settings that you can view and edit with the **dsconfig** command. The **dsconfig** command is the primary tool for managing the server configuration, which follows an object-oriented configuration model. Each configuration object has its own properties. Configuration objects can be related to each other by inheritance and by reference.

The server configuration model exposes a wide range of configurable features. As a consequence, the **dsconfig** command has many subcommands. Subcommands exist to create, list, and delete configuration objects, and to get and set properties of configuration objects. Their names reflect these five actions:

- **create-*object***
- **list-*objects***
- **delete-*object***
- **get-*object*-prop**
- **set-*object*-prop**

Each configuration *object* has a user-friendly name, such as `Connection Handler`. Subcommand names use lower-case, hyphenated versions of the friendly names, as in `create-connection-handler`.

Chapter 1
# Subcommands

The following lists show **dsconfig** subcommands by category:

## *Core Server*

### Administration Connector

- get-administration-connector-prop
- set-administration-connector-prop

### Alert Handler

- create-alert-handler
- delete-alert-handler
- get-alert-handler-prop
- list-alert-handlers
- set-alert-handler-prop

### Connection Handler

- create-connection-handler
- delete-connection-handler
- get-connection-handler-prop
- list-connection-handlers
- set-connection-handler-prop

### Extended Operation Handler

- create-extended-operation-handler
- delete-extended-operation-handler
- get-extended-operation-handler-prop
- list-extended-operation-handlers

- set-extended-operation-handler-prop

**Global Configuration**

- get-global-configuration-prop
- set-global-configuration-prop

**Group Implementation**

- create-group-implementation
- delete-group-implementation
- get-group-implementation-prop
- list-group-implementations
- set-group-implementation-prop

**HTTP Endpoint**

- create-http-endpoint
- delete-http-endpoint
- get-http-endpoint-prop
- list-http-endpoints
- set-http-endpoint-prop

**Plugin**

- create-plugin
- delete-plugin
- get-plugin-prop
- list-plugins
- set-plugin-prop

**Plugin Root**

- get-plugin-root-prop
- set-plugin-root-prop

**Root DSE Backend**

- get-root-dse-backend-prop

- set-root-dse-backend-prop

**Schema Provider**

- create-schema-provider
- delete-schema-provider
- get-schema-provider-prop
- list-schema-providers
- set-schema-provider-prop

**Virtual Attribute**

- create-virtual-attribute
- delete-virtual-attribute
- get-virtual-attribute-prop
- list-virtual-attributes
- set-virtual-attribute-prop

**Work Queue**

- get-work-queue-prop
- set-work-queue-prop

### *Caching and Backends*

**Backend**

- create-backend
- delete-backend
- get-backend-prop
- list-backends
- set-backend-prop

**Backend Index**

- create-backend-index
- delete-backend-index

- get-backend-index-prop
- list-backend-indexes
- set-backend-index-prop

**Backend VLV Index**

- create-backend-vlv-index
- delete-backend-vlv-index
- get-backend-vlv-index-prop
- list-backend-vlv-indexes
- set-backend-vlv-index-prop

**Entry Cache**

- create-entry-cache
- delete-entry-cache
- get-entry-cache-prop
- list-entry-caches
- set-entry-cache-prop

**Root DSE Backend**

- get-root-dse-backend-prop
- set-root-dse-backend-prop

### *Logging*

**Access Log Filtering Criteria**

- create-access-log-filtering-criteria
- delete-access-log-filtering-criteria
- get-access-log-filtering-criteria-prop
- list-access-log-filtering-criteria
- set-access-log-filtering-criteria-prop

**Debug Target**

- create-debug-target

- delete-debug-target
- get-debug-target-prop
- list-debug-targets
- set-debug-target-prop

**Log Publisher**

- create-log-publisher
- delete-log-publisher
- get-log-publisher-prop
- list-log-publishers
- set-log-publisher-prop

**Log Retention Policy**

- create-log-retention-policy
- delete-log-retention-policy
- get-log-retention-policy-prop
- list-log-retention-policies
- set-log-retention-policy-prop

**Log Rotation Policy**

- create-log-rotation-policy
- delete-log-rotation-policy
- get-log-rotation-policy-prop
- list-log-rotation-policies
- set-log-rotation-policy-prop

*Directory Proxy*

**Service Discovery Mechanism**

- create-service-discovery-mechanism
- delete-service-discovery-mechanism

- get-service-discovery-mechanism-prop
- list-service-discovery-mechanisms
- set-service-discovery-mechanism-prop

### *Replication*

#### Replication Domain

- create-replication-domain
- delete-replication-domain
- get-replication-domain-prop
- list-replication-domains
- set-replication-domain-prop

#### Replication Server

- create-replication-server
- delete-replication-server
- get-replication-server-prop
- list-replication-server
- set-replication-server-prop

#### Synchronization Provider

- create-synchronization-provider
- delete-synchronization-provider
- get-synchronization-provider-prop
- list-synchronization-providers
- set-synchronization-provider-prop

### *Authentication and Authorization*

#### Access Control Handler

- create-access-control-handler
- delete-access-control-handler

- get-access-control-handler-prop
- list-access-control-handler
- set-access-control-handler-prop

**Certificate Mapper**

- create-certificate-mapper
- delete-certificate-mapper
- get-certificate-mapper-prop
- list-certificate-mappers
- set-certificate-mapper-prop

**Crypto Manager**

- get-crypto-manager-prop
- set-crypto-manager-prop

**Global Access Control Policy**

- create-global-access-control-policy
- delete-global-access-control-policy
- get-global-access-control-policy-prop
- list-global-access-control-policies
- set-global-access-control-policy-prop

**HTTP Authorization Mechanism**

- create-http-authorization-mechanism
- delete-http-authorization-mechanism
- get-http-authorization-mechanism-prop
- list-http-authorization-mechanisms
- set-http-authorization-mechanism-prop

**Identity Mapper**

- create-identity-mapper

- delete-identity-mapper
- get-identity-mapper-prop
- list-identity-mappers
- set-identity-mapper-prop

**Key Manager Provider**

- create-key-manager-provider
- delete-key-manager-provider
- get-key-manager-provider-prop
- list-key-manager-providers
- set-key-manager-provider-prop

**Password Policy**

- create-password-policy
- delete-password-policy
- get-password-policy-prop
- list-password-policies
- set-password-policy-prop

**SASL Mechanism Handler**

- create-sasl-mechanism-handler
- delete-sasl-mechanism-handler
- get-sasl-mechanism-handler-prop
- list-sasl-mechanism-handlers
- set-sasl-mechanism-handler-prop

**Trust Manager Provider**

- create-trust-manager-provider
- delete-trust-manager-provider
- get-trust-manager-provider-prop

- list-trust-manager-providers
- set-trust-manager-provider-prop

### *Service Discovery Mechanism*

#### Service Discovery Mechanism

- create-service-discovery-mechanism
- delete-service-discovery-mechanism
- get-service-discovery-mechanism-prop
- list-service-discovery-mechanisms
- set-service-discovery-mechanism-prop

### *User Management*

#### Account Status Notification Handler

- create-account-status-notification-handler
- delete-account-status-notification-handler
- get-account-status-notification-handler-prop
- list-account-status-notification-handlers
- set-account-status-notification-handler-prop

#### Certificate Mapper

- create-certificate-mapper
- delete-certificate-mapper
- get-certificate-mapper-prop
- list-certificate-mappers
- set-certificate-mapper-prop

#### Identity Mapper

- create-identity-mapper
- delete-identity-mapper
- get-identity-mapper-prop

- list-identity-mappers
- set-identity-mapper-prop

**Password Generator**

- create-password-generator
- delete-password-generator
- get-password-generator-prop
- list-password-generators
- set-password-generator-prop

**Password Policy**

- create-password-policy
- delete-password-policy
- get-password-policy-prop
- list-password-policies
- set-password-policy-prop

**Password Storage Scheme**

- create-password-storage-scheme
- delete-password-storage-scheme
- get-password-storage-scheme-prop
- list-password-storage-schemes
- set-password-storage-scheme-prop

**Password Validator**

- create-password-validator
- delete-password-validator
- get-password-validator-prop
- list-password-validators
- set-password-validator-prop

**Help.** list-properties

# create-access-control-handler

Creates Access Control Handlers.

The **dsconfig create-access-control-handler** command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Access Control Handler which should be created. The value for TYPE can be one of: custom | dsee-compat | policy-based.

Properties used in options depend on the type of object to configure.

For details about available properties, see Access Control Handler.

# create-access-log-filtering-criteria

Creates Access Log Filtering Criteria.

The **dsconfig create-access-log-filtering-criteria** command takes the following options:

`--criteria-name {name}`

The name of the new Access Log Filtering Criteria.

`--publisher-name {name}`

The name of the Access Log Publisher.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Access Log Filtering Criteria.

# create-account-status-notification-handler

Creates Account Status Notification Handlers.

The **dsconfig create-account-status-notification-handler** command takes the following options:

`--handler-name {name}`

The name of the new Account Status Notification Handler.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Account Status Notification Handler which should be created. The value for TYPE can be one of: custom | error-log | smtp.

Properties used in options depend on the type of object to configure.

For details about available properties, see Account Status Notification Handler.

# create-alert-handler

Creates Alert Handlers.

The **dsconfig create-alert-handler** command takes the following options:

`--handler-name {name}`

The name of the new Alert Handler.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Alert Handler which should be created. The value for TYPE can be one of: custom | jmx | smtp.

Properties used in options depend on the type of object to configure.

For details about available properties, see Alert Handler.

# create-backend

Creates Backends.

The **dsconfig create-backend** command takes the following options:

`--backend-name {STRING}`

The name of the new Backend which will also be used as the value of the "backend-id" property: Specifies a name to identify the associated backend.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Backend which should be created. The value for TYPE can be one of: custom | je | ldif | memory | monitor | null | proxy | schema | task.

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend.

# create-backend-index

Creates Backend Indexes.

The **dsconfig create-backend-index** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

`--index-name {OID}`

The name of the new Backend Index which will also be used as the value of the "attribute" property: Specifies the name of the attribute for which the index is to be maintained.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend Index.

# create-backend-vlv-index

Creates Backend VLV Indexes.

The **dsconfig create-backend-vlv-index** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

`--index-name {STRING}`

The name of the new Backend VLV Index which will also be used as the value of the "name" property: Specifies a unique name for this VLV index.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend VLV Index.

# create-certificate-mapper

Creates Certificate Mappers.

The **dsconfig create-certificate-mapper** command takes the following options:

`--mapper-name {name}`

The name of the new Certificate Mapper.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Certificate Mapper which should be created. The value for TYPE can be one of: custom | fingerprint | subject-attribute-to-user-attribute | subject-dn-to-user-attribute | subject-equals-dn.

Properties used in options depend on the type of object to configure.

For details about available properties, see Certificate Mapper.

# create-connection-handler

Creates Connection Handlers.

The **dsconfig create-connection-handler** command takes the following options:

`--handler-name {name}`

The name of the new Connection Handler.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Connection Handler which should be created. The value for TYPE can be one of: custom | http | jmx | ldap | ldif | snmp.

Properties used in options depend on the type of object to configure.

For details about available properties, see Connection Handler.

# create-debug-target

Creates Debug Targets.

The **dsconfig create-debug-target** command takes the following options:

`--publisher-name {name}`

The name of the Debug Log Publisher.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`--target-name {STRING}`

The name of the new Debug Target which will also be used as the value of the "debug-scope" property: Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp).

Properties used in options depend on the type of object to configure.

For details about available properties, see Debug Target.

# create-entry-cache

Creates Entry Caches.

The **dsconfig create-entry-cache** command takes the following options:

`--cache-name {name}`

The name of the new Entry Cache.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Entry Cache which should be created. The value for TYPE can be one of: custom | fifo | soft-reference.

Properties used in options depend on the type of object to configure.

For details about available properties, see Entry Cache.

# create-extended-operation-handler

Creates Extended Operation Handlers.

The **dsconfig create-extended-operation-handler** command takes the following options:

`--handler-name {name}`

The name of the new Extended Operation Handler.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Extended Operation Handler which should be created. The value for TYPE can be one of: cancel | custom | get-connection-id | get-symmetric-key | password-modify | password-policy-state | start-tls | who-am-i.

Properties used in options depend on the type of object to configure.

For details about available properties, see Extended Operation Handler.

# create-global-access-control-policy

Creates Global Access Control Policies.

The **dsconfig create-global-access-control-policy** command takes the following options:

`--policy-name {name}`

The name of the new Global Access Control Policy.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Global Access Control Policy.

# create-group-implementation

Creates Group Implementations.

The **dsconfig create-group-implementation** command takes the following options:

`--implementation-name {name}`

The name of the new Group Implementation.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Group Implementation which should be created. The value for TYPE can be one of: custom | dynamic | static | virtual-static.

Properties used in options depend on the type of object to configure.

For details about available properties, see Group Implementation.

# create-http-authorization-mechanism

Creates HTTP Authorization Mechanisms.

The **dsconfig create-http-authorization-mechanism** command takes the following options:

`--mechanism-name {name}`

The name of the new HTTP Authorization Mechanism.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of HTTP Authorization Mechanism which should be created. The value for TYPE can be one of: http-anonymous-authorization-mechanism | http-basic-authorization-mechanism | http-oauth2-cts-authorization-mechanism | http-oauth2-file-authorization-mechanism | http-oauth2-openam-authorization-mechanism | http-oauth2-token-introspection-authorization-mechanism.

Properties used in options depend on the type of object to configure.

For details about available properties, see HTTP Authorization Mechanism.

# create-http-endpoint

Creates HTTP Endpoints.

The **dsconfig create-http-endpoint** command takes the following options:

`--endpoint-name {STRING}`

The name of the new HTTP Endpoint which will also be used as the value of the "base-path" property: All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of HTTP Endpoint which should be created (Default: generic). The value for TYPE can be one of: admin-endpoint | alive-endpoint | crest-metrics-endpoint | generic | healthy-endpoint | prometheus-endpoint | rest2ldap-endpoint.

Default: generic

Properties used in options depend on the type of object to configure.

For details about available properties, see HTTP Endpoint.

# create-identity-mapper

Creates Identity Mappers.

The **dsconfig create-identity-mapper** command takes the following options:

`--mapper-name {name}`

The name of the new Identity Mapper.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Identity Mapper which should be created. The value for TYPE can be one of: custom | exact-match | regular-expression.

Properties used in options depend on the type of object to configure.

For details about available properties, see Identity Mapper.

# create-key-manager-provider

Creates Key Manager Providers.

The **dsconfig create-key-manager-provider** command takes the following options:

`--provider-name {name}`

The name of the new Key Manager Provider.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Key Manager Provider which should be created. The value for TYPE can be one of: custom | file-based | ldap | pkcs11.

Properties used in options depend on the type of object to configure.

For details about available properties, see Key Manager Provider.

# create-log-publisher

Creates Log Publishers.

The **dsconfig create-log-publisher** command takes the following options:

`--publisher-name {name}`

The name of the new Log Publisher.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Log Publisher which should be created. The value for TYPE can be one of: console-error | csv-file-access | csv-file-http-access | custom-access | custom-debug | custom-error | custom-http-access | external-access | external-http-access | file-based-access | file-based-audit | file-based-debug | file-based-error | file-based-http-access | json-file-access | json-file-http-access.

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Publisher.

# create-log-retention-policy

Creates Log Retention Policies.

The **dsconfig create-log-retention-policy** command takes the following options:

`--policy-name {name}`

The name of the new Log Retention Policy.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Log Retention Policy which should be created. The value for TYPE can be one of: custom | file-count | free-disk-space | size-limit.

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Retention Policy.

# create-log-rotation-policy

Creates Log Rotation Policies.

The **dsconfig create-log-rotation-policy** command takes the following options:

`--policy-name {name}`

The name of the new Log Rotation Policy.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Log Rotation Policy which should be created. The value for TYPE can be one of: custom | fixed-time | size-limit | time-limit.

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Rotation Policy.

# create-mail-server

Creates Mail Servers.

The **dsconfig create-mail-server** command takes the following options:

`--server-name {name}`

The name of the new Mail Server.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Mail Server.

# create-password-generator

Creates Password Generators.

The **dsconfig create-password-generator** command takes the following options:

`--generator-name {name}`

The name of the new Password Generator.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Password Generator which should be created. The value for TYPE can be one of: custom | random.

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Generator.

# create-password-policy

Creates Authentication Policies.

The **dsconfig create-password-policy** command takes the following options:

`--policy-name {name}`

The name of the new Authentication Policy.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Authentication Policy which should be created. The value for TYPE can be one of: ldap-pass-through | password-policy.

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Policy.

# create-password-storage-scheme

Creates Password Storage Schemes.

The **dsconfig create-password-storage-scheme** command takes the following options:

`--scheme-name {name}`

The name of the new Password Storage Scheme.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Password Storage Scheme which should be created. The value for TYPE can be one of: aes | base64 | bcrypt | blowfish | clear | crypt | custom | md5 | pbkdf2 | pbkdf2-hmac-sha256 | pbkdf2-hmac-sha512 | pkcs5s2 | rc4 | salted-md5 | salted-sha1 | salted-sha256 | salted-sha384 | salted-sha512 | scram-sha256 | scram-sha512 | sha1 | triple-des.

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Storage Scheme.

# create-password-validator

Creates Password Validators.

The **dsconfig create-password-validator** command takes the following options:

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Password Validator which should be created. The value for TYPE can be one of: attribute-value | character-set | custom | dictionary | length-based | repeated-characters | similarity-based | unique-characters.

`--validator-name {name}`

The name of the new Password Validator.

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Validator.

# create-plugin

Creates Plugins.

The **dsconfig create-plugin** command takes the following options:

`--plugin-name {name}`

The name of the new Plugin.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Plugin which should be created. The value for TYPE can be one of: attribute-cleanup | change-number-control | custom | entry-uuid | fractional-ldif-import | graphite-monitor-reporter | last-mod | ldap-attribute-description-list | password-policy-import | referential-integrity | samba-password | seven-bit-clean | unique-attribute.

Properties used in options depend on the type of object to configure.

For details about available properties, see Plugin.

# create-replication-domain

Creates Replication Domains.

The **dsconfig create-replication-domain** command takes the following options:

`--domain-name {name}`

The name of the new Replication Domain.

`--provider-name {name}`

The name of the Replication Synchronization Provider.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Replication Domain.

# create-replication-server

Creates Replication Servers.

The **dsconfig create-replication-server** command takes the following options:

`--provider-name {name}`

The name of the Replication Synchronization Provider.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Replication Server.

# create-sasl-mechanism-handler

Creates SASL Mechanism Handlers.

The **dsconfig create-sasl-mechanism-handler** command takes the following options:

`--handler-name {name}`

The name of the new SASL Mechanism Handler.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of SASL Mechanism Handler which should be created. The value for TYPE can be one of: anonymous | cram-md5 | custom | digest-md5 | external | gssapi | plain | scram-sha256 | scram-sha512.

Properties used in options depend on the type of object to configure.

For details about available properties, see SASL Mechanism Handler.

# create-schema-provider

Creates Schema Providers.

The **dsconfig create-schema-provider** command takes the following options:

`--provider-name {name}`

The name of the new Schema Provider.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Schema Provider which should be created (Default: generic). The value for TYPE can be one of: core-schema | generic | json-equality-matching-rule | json-ordering-matching-rule | json-query-equality-matching-rule.

Default: generic

Properties used in options depend on the type of object to configure.

For details about available properties, see Schema Provider.

# create-service-discovery-mechanism

Creates Service Discovery Mechanisms.

The **dsconfig create-service-discovery-mechanism** command takes the following options:

`--mechanism-name {name}`

The name of the new Service Discovery Mechanism.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Service Discovery Mechanism which should be created. The value for TYPE can be one of: custom | replication | static.

Properties used in options depend on the type of object to configure.

For details about available properties, see Service Discovery Mechanism.

# create-synchronization-provider

Creates Synchronization Providers.

The **dsconfig create-synchronization-provider** command takes the following options:

`--provider-name {name}`

The name of the new Synchronization Provider.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Synchronization Provider which should be created. The value for TYPE can be one of: custom | replication.

Properties used in options depend on the type of object to configure.

For details about available properties, see Synchronization Provider.

# create-trust-manager-provider

Creates Trust Manager Providers.

The **dsconfig create-trust-manager-provider** command takes the following options:

`--provider-name {name}`

The name of the new Trust Manager Provider.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Trust Manager Provider which should be created. The value for TYPE can be one of: admin-data | blind | custom | file-based | ldap | pkcs11.

Properties used in options depend on the type of object to configure.

For details about available properties, see Trust Manager Provider.

# create-virtual-attribute

Creates Virtual Attributes.

The **dsconfig create-virtual-attribute** command takes the following options:

`--name {name}`

The name of the new Virtual Attribute.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`-t | --type {type}`

The type of Virtual Attribute which should be created. The value for TYPE can be one of: collective-attribute-subentries | custom | entity-tag | entry-dn | entry-uuid | governing-structure-

rule | has-subordinates | is-member-of | member | num-subordinates | password-expiration-time | password-policy-subentry | structural-object-class | subschema-subentry | user-defined.

Properties used in options depend on the type of object to configure.

For details about available properties, see Virtual Attribute.

# delete-access-control-handler

Deletes Access Control Handlers.

The **dsconfig delete-access-control-handler** command takes the following options:

`-f | --force`

Ignore non-existent Access Control Handlers.

Default: false

Properties used in options depend on the type of object to configure.

For details about available properties, see Access Control Handler.

# delete-access-log-filtering-criteria

Deletes Access Log Filtering Criteria.

The **dsconfig delete-access-log-filtering-criteria** command takes the following options:

`--criteria-name {name}`

The name of the Access Log Filtering Criteria.

`-f | --force`

Ignore non-existent Access Log Filtering Criteria.

Default: false

`--publisher-name {name}`

The name of the Access Log Publisher.

Properties used in options depend on the type of object to configure.

For details about available properties, see Access Log Filtering Criteria.

# delete-account-status-notification-handler

Deletes Account Status Notification Handlers.

The **dsconfig delete-account-status-notification-handler** command takes the following options:

`-f | --force`

Ignore non-existent Account Status Notification Handlers.

Default: false

`--handler-name {name}`

The name of the Account Status Notification Handler.

Properties used in options depend on the type of object to configure.

For details about available properties, see Account Status Notification Handler.

# delete-alert-handler

Deletes Alert Handlers.

The **dsconfig delete-alert-handler** command takes the following options:

`-f | --force`

Ignore non-existent Alert Handlers.

Default: false

`--handler-name {name}`

The name of the Alert Handler.

Properties used in options depend on the type of object to configure.

For details about available properties, see Alert Handler.

# delete-backend

Deletes Backends.

The **dsconfig delete-backend** command takes the following options:

`--backend-name {name}`

The name of the Backend.

`-f | --force`

Ignore non-existent Backends.

Default: false

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend.

# delete-backend-index

Deletes Backend Indexes.

The **dsconfig delete-backend-index** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

`-f | --force`

Ignore non-existent Backend Indexes.

Default: false

`--index-name {name}`

The name of the Backend Index.

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend Index.

# delete-backend-vlv-index

Deletes Backend VLV Indexes.

The **dsconfig delete-backend-vlv-index** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

`-f | --force`

Ignore non-existent Backend VLV Indexes.

Default: false

`--index-name {name}`

The name of the Backend VLV Index.

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend VLV Index.

# delete-certificate-mapper

Deletes Certificate Mappers.

The **dsconfig delete-certificate-mapper** command takes the following options:

`-f | --force`

Ignore non-existent Certificate Mappers.

Default: false

`--mapper-name {name}`

The name of the Certificate Mapper.

Properties used in options depend on the type of object to configure.

For details about available properties, see Certificate Mapper.

# delete-connection-handler

Deletes Connection Handlers.

The **dsconfig delete-connection-handler** command takes the following options:

`-f | --force`

Ignore non-existent Connection Handlers.

Default: false

`--handler-name {name}`

The name of the Connection Handler.

Properties used in options depend on the type of object to configure.

For details about available properties, see Connection Handler.

# delete-debug-target

Deletes Debug Targets.

The **dsconfig delete-debug-target** command takes the following options:

`-f | --force`

Ignore non-existent Debug Targets.

Default: false

`--publisher-name {name}`

The name of the Debug Log Publisher.

`--target-name {name}`

The name of the Debug Target.

Properties used in options depend on the type of object to configure.

For details about available properties, see Debug Target.

# delete-entry-cache

Deletes Entry Caches.

The **dsconfig delete-entry-cache** command takes the following options:

`--cache-name {name}`

The name of the Entry Cache.

`-f | --force`

Ignore non-existent Entry Caches.

Default: false

Properties used in options depend on the type of object to configure.

For details about available properties, see Entry Cache.

# delete-extended-operation-handler

Deletes Extended Operation Handlers.

The **dsconfig delete-extended-operation-handler** command takes the following options:

`-f | --force`

Ignore non-existent Extended Operation Handlers.

Default: false

`--handler-name {name}`

The name of the Extended Operation Handler.

Properties used in options depend on the type of object to configure.

For details about available properties, see Extended Operation Handler.

# delete-global-access-control-policy

Deletes Global Access Control Policies.

The **dsconfig delete-global-access-control-policy** command takes the following options:

`-f | --force`

Ignore non-existent Global Access Control Policies.

Default: false

`--policy-name {name}`

The name of the Global Access Control Policy.

Properties used in options depend on the type of object to configure.

For details about available properties, see Global Access Control Policy.

# delete-group-implementation

Deletes Group Implementations.

The **dsconfig delete-group-implementation** command takes the following options:

`-f | --force`

Ignore non-existent Group Implementations.

Default: false

`--implementation-name {name}`

The name of the Group Implementation.

Properties used in options depend on the type of object to configure.

For details about available properties, see Group Implementation.

# delete-http-authorization-mechanism

Deletes HTTP Authorization Mechanisms.

The **dsconfig delete-http-authorization-mechanism** command takes the following options:

`-f | --force`

Ignore non-existent HTTP Authorization Mechanisms.

Default: false

`--mechanism-name {name}`

The name of the HTTP Authorization Mechanism.

Properties used in options depend on the type of object to configure.

For details about available properties, see HTTP Authorization Mechanism.

# delete-http-endpoint

Deletes HTTP Endpoints.

The **dsconfig delete-http-endpoint** command takes the following options:

`--endpoint-name {name}`

The name of the HTTP Endpoint.

`-f | --force`

Ignore non-existent HTTP Endpoints.

Default: false

Properties used in options depend on the type of object to configure.

For details about available properties, see HTTP Endpoint.

# delete-identity-mapper

Deletes Identity Mappers.

The **dsconfig delete-identity-mapper** command takes the following options:

`-f | --force`

Ignore non-existent Identity Mappers.

Default: false

`--mapper-name {name}`

The name of the Identity Mapper.

Properties used in options depend on the type of object to configure.

For details about available properties, see Identity Mapper.

# delete-key-manager-provider

Deletes Key Manager Providers.

The **dsconfig delete-key-manager-provider** command takes the following options:

`-f | --force`

Ignore non-existent Key Manager Providers.

Default: false

`--provider-name {name}`

The name of the Key Manager Provider.

Properties used in options depend on the type of object to configure.

For details about available properties, see Key Manager Provider.

# delete-log-publisher

Deletes Log Publishers.

The **dsconfig delete-log-publisher** command takes the following options:

`-f | --force`

Ignore non-existent Log Publishers.

Default: false

`--publisher-name {name}`

The name of the Log Publisher.

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Publisher.

# delete-log-retention-policy

Deletes Log Retention Policies.

The **dsconfig delete-log-retention-policy** command takes the following options:

`-f | --force`

Ignore non-existent Log Retention Policies.

Default: false

`--policy-name {name}`

The name of the Log Retention Policy.

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Retention Policy.

# delete-log-rotation-policy

Deletes Log Rotation Policies.

The **dsconfig delete-log-rotation-policy** command takes the following options:

`-f | --force`

Ignore non-existent Log Rotation Policies.

Default: false

`--policy-name {name}`

The name of the Log Rotation Policy.

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Rotation Policy.

# delete-mail-server

Deletes Mail Servers.

The **dsconfig delete-mail-server** command takes the following options:

`-f | --force`

Ignore non-existent Mail Servers.

Default: false

`--server-name {name}`

The name of the Mail Server.

Properties used in options depend on the type of object to configure.

For details about available properties, see Mail Server.

# delete-password-generator

Deletes Password Generators.

The **dsconfig delete-password-generator** command takes the following options:

`-f | --force`

Ignore non-existent Password Generators.

Default: false

`--generator-name {name}`

The name of the Password Generator.

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Generator.

# delete-password-policy

Deletes Authentication Policies.

The **dsconfig delete-password-policy** command takes the following options:

`-f | --force`

Ignore non-existent Authentication Policies.

Default: false

`--policy-name {name}`

The name of the Authentication Policy.

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Policy.

# delete-password-storage-scheme

Deletes Password Storage Schemes.

The **dsconfig delete-password-storage-scheme** command takes the following options:

`-f | --force`

Ignore non-existent Password Storage Schemes.

Default: false

`--scheme-name {name}`

The name of the Password Storage Scheme.

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Storage Scheme.

# delete-password-validator

Deletes Password Validators.

The **dsconfig delete-password-validator** command takes the following options:

`-f | --force`

Ignore non-existent Password Validators.

Default: false

`--validator-name {name}`

The name of the Password Validator.

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Validator.

# delete-plugin

Deletes Plugins.

The **dsconfig delete-plugin** command takes the following options:

`-f | --force`

Ignore non-existent Plugins.

Default: false

`--plugin-name {name}`

The name of the Plugin.

Properties used in options depend on the type of object to configure.

For details about available properties, see Plugin.

# delete-replication-domain

Deletes Replication Domains.

The **dsconfig delete-replication-domain** command takes the following options:

`--domain-name {name}`

The name of the Replication Domain.

`-f | --force`

Ignore non-existent Replication Domains.

Default: false

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Properties used in options depend on the type of object to configure.

For details about available properties, see Replication Domain.

# delete-replication-server

Deletes Replication Servers.

The **dsconfig delete-replication-server** command takes the following options:

`-f | --force`

Ignore non-existent Replication Servers.

Default: false

`--provider-name {name}`

The name of the Replication Synchronization Provider.

Properties used in options depend on the type of object to configure.

For details about available properties, see Replication Server.

# delete-sasl-mechanism-handler

Deletes SASL Mechanism Handlers.

The **dsconfig delete-sasl-mechanism-handler** command takes the following options:

`-f | --force`

Ignore non-existent SASL Mechanism Handlers.

Default: false

`--handler-name {name}`

The name of the SASL Mechanism Handler.

Properties used in options depend on the type of object to configure.

For details about available properties, see SASL Mechanism Handler.

# delete-schema-provider

Deletes Schema Providers.

The **dsconfig delete-schema-provider** command takes the following options:

`-f | --force`

Ignore non-existent Schema Providers.

Default: false

`--provider-name {name}`

The name of the Schema Provider.

Properties used in options depend on the type of object to configure.

For details about available properties, see Schema Provider.

# delete-service-discovery-mechanism

Deletes Service Discovery Mechanisms.

The **dsconfig delete-service-discovery-mechanism** command takes the following options:

`-f | --force`

Ignore non-existent Service Discovery Mechanisms.

Default: false

`--mechanism-name {name}`

The name of the Service Discovery Mechanism.

Properties used in options depend on the type of object to configure.

For details about available properties, see Service Discovery Mechanism.

# delete-synchronization-provider

Deletes Synchronization Providers.

The **dsconfig delete-synchronization-provider** command takes the following options:

`-f | --force`

Ignore non-existent Synchronization Providers.

Default: false

`--provider-name {name}`

The name of the Synchronization Provider.

Properties used in options depend on the type of object to configure.

For details about available properties, see Synchronization Provider.

# delete-trust-manager-provider

Deletes Trust Manager Providers.

The **dsconfig delete-trust-manager-provider** command takes the following options:

`-f | --force`

Ignore non-existent Trust Manager Providers.

Default: false

`--provider-name {name}`

The name of the Trust Manager Provider.

Properties used in options depend on the type of object to configure.

For details about available properties, see Trust Manager Provider.

# delete-virtual-attribute

Deletes Virtual Attributes.

The **dsconfig delete-virtual-attribute** command takes the following options:

`-f | --force`

Ignore non-existent Virtual Attributes.

Default: false

`--name {name}`

The name of the Virtual Attribute.

Properties used in options depend on the type of object to configure.

For details about available properties, see Virtual Attribute.

# get-access-control-handler-prop

Shows Access Control Handler properties.

The **dsconfig get-access-control-handler-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Access Control Handler.

# get-access-log-filtering-criteria-prop

Shows Access Log Filtering Criteria properties.

The **dsconfig get-access-log-filtering-criteria-prop** command takes the following options:

`--criteria-name {name}`

The name of the Access Log Filtering Criteria.

`--property {property}`

The name of a property to be displayed.

`--publisher-name {name}`

The name of the Access Log Publisher.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Access Log Filtering Criteria.

# get-account-status-notification-handler-prop

Shows Account Status Notification Handler properties.

The **dsconfig get-account-status-notification-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the Account Status Notification Handler.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Account Status Notification Handler.

# get-administration-connector-prop

Shows Administration Connector properties.

The **dsconfig get-administration-connector-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Administration Connector.

# get-alert-handler-prop

Shows Alert Handler properties.

The **dsconfig get-alert-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the Alert Handler.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Alert Handler.

# get-backend-index-prop

Shows Backend Index properties.

The **dsconfig get-backend-index-prop** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

`--index-name {name}`

The name of the Backend Index.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend Index.

# get-backend-prop

Shows Backend properties.

The **dsconfig get-backend-prop** command takes the following options:

`--backend-name {name}`

The name of the Backend.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend.

# get-backend-vlv-index-prop

Shows Backend VLV Index properties.

The **dsconfig get-backend-vlv-index-prop** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

`--index-name {name}`

The name of the Backend VLV Index.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend VLV Index.

# get-certificate-mapper-prop

Shows Certificate Mapper properties.

The **dsconfig get-certificate-mapper-prop** command takes the following options:

`--mapper-name {name}`

The name of the Certificate Mapper.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Certificate Mapper.

# get-connection-handler-prop

Shows Connection Handler properties.

The **dsconfig get-connection-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the Connection Handler.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Connection Handler.

# get-crypto-manager-prop

Shows Crypto Manager properties.

The **dsconfig get-crypto-manager-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Crypto Manager.

# get-debug-target-prop

Shows Debug Target properties.

The **dsconfig get-debug-target-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--publisher-name {name}`

The name of the Debug Log Publisher.

`--record`

Modifies the display output to show one property value per line.

Default: false

`--target-name {name}`

The name of the Debug Target.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Debug Target.

# get-entry-cache-prop

Shows Entry Cache properties.

The **dsconfig get-entry-cache-prop** command takes the following options:

`--cache-name {name}`

The name of the Entry Cache.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Entry Cache.

# get-extended-operation-handler-prop

Shows Extended Operation Handler properties.

The **dsconfig get-extended-operation-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the Extended Operation Handler.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Extended Operation Handler.

# get-global-access-control-policy-prop

Shows Global Access Control Policy properties.

The **dsconfig get-global-access-control-policy-prop** command takes the following options:

`--policy-name {name}`

The name of the Global Access Control Policy.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Global Access Control Policy.

# get-global-configuration-prop

Shows Global Configuration properties.

The **dsconfig get-global-configuration-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Global Configuration.

# get-group-implementation-prop

Shows Group Implementation properties.

The **dsconfig get-group-implementation-prop** command takes the following options:

`--implementation-name {name}`

The name of the Group Implementation.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Group Implementation.

# get-http-authorization-mechanism-prop

Shows HTTP Authorization Mechanism properties.

The **dsconfig get-http-authorization-mechanism-prop** command takes the following options:

`--mechanism-name {name}`

The name of the HTTP Authorization Mechanism.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see HTTP Authorization Mechanism.

# get-http-endpoint-prop

Shows HTTP Endpoint properties.

The **dsconfig get-http-endpoint-prop** command takes the following options:

`--endpoint-name {name}`

The name of the HTTP Endpoint.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see HTTP Endpoint.

# get-identity-mapper-prop

Shows Identity Mapper properties.

The **dsconfig get-identity-mapper-prop** command takes the following options:

`--mapper-name {name}`

The name of the Identity Mapper.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Identity Mapper.

# get-key-manager-provider-prop

Shows Key Manager Provider properties.

The **dsconfig get-key-manager-provider-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--provider-name {name}`

The name of the Key Manager Provider.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Key Manager Provider.

# get-log-publisher-prop

Shows Log Publisher properties.

The **dsconfig get-log-publisher-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--publisher-name {name}`

The name of the Log Publisher.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Publisher.

# get-log-retention-policy-prop

Shows Log Retention Policy properties.

The **dsconfig get-log-retention-policy-prop** command takes the following options:

`--policy-name {name}`

The name of the Log Retention Policy.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Retention Policy.

# get-log-rotation-policy-prop

Shows Log Rotation Policy properties.

The **dsconfig get-log-rotation-policy-prop** command takes the following options:

`--policy-name {name}`

The name of the Log Rotation Policy.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Rotation Policy.

# get-mail-server-prop

Shows Mail Server properties.

The **dsconfig get-mail-server-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`--server-name {name}`

The name of the Mail Server.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Mail Server.

# get-password-generator-prop

Shows Password Generator properties.

The **dsconfig get-password-generator-prop** command takes the following options:

`--generator-name {name}`

The name of the Password Generator.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Generator.

# get-password-policy-prop

Shows Authentication Policy properties.

The **dsconfig get-password-policy-prop** command takes the following options:

`--policy-name {name}`

The name of the Authentication Policy.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Policy.

# get-password-storage-scheme-prop

Shows Password Storage Scheme properties.

The **dsconfig get-password-storage-scheme-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`--scheme-name {name}`

The name of the Password Storage Scheme.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Storage Scheme.

# get-password-validator-prop

Shows Password Validator properties.

The **dsconfig get-password-validator-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

`--validator-name {name}`

The name of the Password Validator.

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Validator.

# get-plugin-prop

Shows Plugin properties.

The **dsconfig get-plugin-prop** command takes the following options:

`--plugin-name {name}`

The name of the Plugin.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Plugin.

# get-plugin-root-prop

Shows Plugin Root properties.

The **dsconfig get-plugin-root-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Plugin Root.

# get-replication-domain-prop

Shows Replication Domain properties.

The **dsconfig get-replication-domain-prop** command takes the following options:

`--domain-name {name}`

The name of the Replication Domain.

`--property {property}`

The name of a property to be displayed.

`--provider-name {name}`

The name of the Replication Synchronization Provider.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Replication Domain.

# get-replication-server-prop

Shows Replication Server properties.

The **dsconfig get-replication-server-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--provider-name {name}`

The name of the Replication Synchronization Provider.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Replication Server.

# get-root-dse-backend-prop

Shows Root DSE Backend properties.

The **dsconfig get-root-dse-backend-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Root DSE Backend.

# get-sasl-mechanism-handler-prop

Shows SASL Mechanism Handler properties.

The **dsconfig get-sasl-mechanism-handler-prop** command takes the following options:

`--handler-name {name}`

The name of the SASL Mechanism Handler.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see SASL Mechanism Handler.

# get-schema-provider-prop

Shows Schema Provider properties.

The **dsconfig get-schema-provider-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--provider-name {name}`

The name of the Schema Provider.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Schema Provider.

# get-service-discovery-mechanism-prop

Shows Service Discovery Mechanism properties.

The **dsconfig get-service-discovery-mechanism-prop** command takes the following options:

`--mechanism-name {name}`

The name of the Service Discovery Mechanism.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Service Discovery Mechanism.

# get-synchronization-provider-prop

Shows Synchronization Provider properties.

The **dsconfig get-synchronization-provider-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--provider-name {name}`

The name of the Synchronization Provider.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Synchronization Provider.

# get-trust-manager-provider-prop

Shows Trust Manager Provider properties.

The **dsconfig get-trust-manager-provider-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--provider-name {name}`

The name of the Trust Manager Provider.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Trust Manager Provider.

# get-virtual-attribute-prop

Shows Virtual Attribute properties.

The **dsconfig get-virtual-attribute-prop** command takes the following options:

`--name {name}`

The name of the Virtual Attribute.

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Virtual Attribute.

# get-work-queue-prop

Shows Work Queue properties.

The **dsconfig get-work-queue-prop** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--record`

Modifies the display output to show one property value per line.

Default: false

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Work Queue.

# list-access-control-handler

Lists existing Access Control Handler.

The **dsconfig list-access-control-handler** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Access Control Handler.

# list-access-log-filtering-criteria

Lists existing Access Log Filtering Criteria.

The **dsconfig list-access-log-filtering-criteria** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--publisher-name {name}`

The name of the Access Log Publisher.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Access Log Filtering Criteria.

# list-account-status-notification-handlers

Lists existing Account Status Notification Handlers.

The **dsconfig list-account-status-notification-handlers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Account Status Notification Handler.

# list-alert-handlers

Lists existing Alert Handlers.

The **dsconfig list-alert-handlers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Alert Handler.

# list-backend-indexes

Lists existing Backend Indexes.

The **dsconfig list-backend-indexes** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend Index.

# list-backend-vlv-indexes

Lists existing Backend VLV Indexes.

The **dsconfig list-backend-vlv-indexes** command takes the following options:

`--backend-name {name}`

The name of the Pluggable Backend.

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend VLV Index.

# list-backends

Lists existing Backends.

The **dsconfig list-backends** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend.

# list-certificate-mappers

Lists existing Certificate Mappers.

The **dsconfig list-certificate-mappers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Certificate Mapper.

# list-connection-handlers

Lists existing Connection Handlers.

The **dsconfig list-connection-handlers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Connection Handler.

# list-debug-targets

Lists existing Debug Targets.

The **dsconfig list-debug-targets** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--publisher-name {name}`

The name of the Debug Log Publisher.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Debug Target.

# list-entry-caches

Lists existing Entry Caches.

The **dsconfig list-entry-caches** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Entry Cache.

# list-extended-operation-handlers

Lists existing Extended Operation Handlers.

The **dsconfig list-extended-operation-handlers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Extended Operation Handler.

# list-global-access-control-policies

Lists existing Global Access Control Policies.

The **dsconfig list-global-access-control-policies** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Global Access Control Policy.

# list-group-implementations

Lists existing Group Implementations.

The **dsconfig list-group-implementations** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Group Implementation.

# list-http-authorization-mechanisms

Lists existing HTTP Authorization Mechanisms.

The **dsconfig list-http-authorization-mechanisms** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see HTTP Authorization Mechanism.

# list-http-endpoints

Lists existing HTTP Endpoints.

The **dsconfig list-http-endpoints** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see HTTP Endpoint.

# list-identity-mappers

Lists existing Identity Mappers.

The **dsconfig list-identity-mappers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Identity Mapper.

# list-key-manager-providers

Lists existing Key Manager Providers.

The **dsconfig list-key-manager-providers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Key Manager Provider.

# list-log-publishers

Lists existing Log Publishers.

The **dsconfig list-log-publishers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Publisher.

# list-log-retention-policies

Lists existing Log Retention Policies.

The **dsconfig list-log-retention-policies** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Retention Policy.

# list-log-rotation-policies

Lists existing Log Rotation Policies.

The **dsconfig list-log-rotation-policies** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Rotation Policy.

# list-mail-servers

Lists existing Mail Servers.

The **dsconfig list-mail-servers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Mail Server.

# list-password-generators

Lists existing Password Generators.

The **dsconfig list-password-generators** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Generator.

# list-password-policies

Lists existing Password Policies.

The **dsconfig list-password-policies** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Policy.

# list-password-storage-schemes

Lists existing Password Storage Schemes.

The **dsconfig list-password-storage-schemes** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Storage Scheme.

# list-password-validators

Lists existing Password Validators.

The **dsconfig list-password-validators** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Validator.

# list-plugins

Lists existing Plugins.

The **dsconfig list-plugins** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Plugin.

# list-properties

Describes managed objects and their properties.

The **dsconfig list-properties** command takes the following options:

`-c | --category {category}`

The category of components whose properties should be described.

`--inherited`

Modifies the display output to show the inherited properties of components.

Default: false

`--property {property}`

The name of a property to be displayed.

`-t | --type {type}`

The type of components whose properties should be described. The value for TYPE must be one of the component types associated with the CATEGORY specified using the "--category" option.

# list-replication-domains

Lists existing Replication Domains.

The **dsconfig list-replication-domains** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--provider-name {name}`

The name of the Replication Synchronization Provider.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Replication Domain.

# list-replication-server

Lists existing Replication Server.

The **dsconfig list-replication-server** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`--provider-name {name}`

The name of the Replication Synchronization Provider.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Replication Server.

# list-sasl-mechanism-handlers

Lists existing SASL Mechanism Handlers.

The **dsconfig list-sasl-mechanism-handlers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see SASL Mechanism Handler.

# list-schema-providers

Lists existing Schema Providers.

The **dsconfig list-schema-providers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Schema Provider.

# list-service-discovery-mechanisms

Lists existing Service Discovery Mechanisms.

The **dsconfig list-service-discovery-mechanisms** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Service Discovery Mechanism.

# list-synchronization-providers

Lists existing Synchronization Providers.

The **dsconfig list-synchronization-providers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Synchronization Provider.

# list-trust-manager-providers

Lists existing Trust Manager Providers.

The **dsconfig list-trust-manager-providers** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Trust Manager Provider.

# list-virtual-attributes

Lists existing Virtual Attributes.

The **dsconfig list-virtual-attributes** command takes the following options:

`--property {property}`

The name of a property to be displayed.

`-z | --unit-size {unit}`

Display size data using the specified unit. The value for UNIT can be one of b, kb, mb, gb, or tb (bytes, kilobytes, megabytes, gigabytes, or terabytes).

`-m | --unit-time {unit}`

Display time data using the specified unit. The value for UNIT can be one of ms, s, m, h, d, w, or y (milliseconds, seconds, minutes, hours, days, weeks, or years).

Properties used in options depend on the type of object to configure.

For details about available properties, see Virtual Attribute.

# set-access-control-handler-prop

Modifies Access Control Handler properties.

The **dsconfig set-access-control-handler-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Access Control Handler.

# set-access-log-filtering-criteria-prop

Modifies Access Log Filtering Criteria properties.

The **dsconfig set-access-log-filtering-criteria-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--criteria-name {name}`

The name of the Access Log Filtering Criteria.

`--publisher-name {name}`

The name of the Access Log Publisher.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Access Log Filtering Criteria.

# set-account-status-notification-handler-prop

Modifies Account Status Notification Handler properties.

The **dsconfig set-account-status-notification-handler-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--handler-name {name}`

The name of the Account Status Notification Handler.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Account Status Notification Handler.

# set-administration-connector-prop

Modifies Administration Connector properties.

The **dsconfig set-administration-connector-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Administration Connector.

# set-alert-handler-prop

Modifies Alert Handler properties.

The **dsconfig set-alert-handler-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--handler-name {name}`

The name of the Alert Handler.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Alert Handler.

# set-backend-index-prop

Modifies Backend Index properties.

The **dsconfig set-backend-index-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--backend-name {name}`

The name of the Pluggable Backend.

`--index-name {name}`

The name of the Backend Index.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend Index.

# set-backend-prop

Modifies Backend properties.

The **dsconfig set-backend-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--backend-name {name}`

The name of the Backend.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend.

# set-backend-vlv-index-prop

Modifies Backend VLV Index properties.

The **dsconfig set-backend-vlv-index-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--backend-name {name}`

The name of the Pluggable Backend.

`--index-name {name}`

The name of the Backend VLV Index.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Backend VLV Index.

# set-certificate-mapper-prop

Modifies Certificate Mapper properties.

The **dsconfig set-certificate-mapper-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--mapper-name {name}`

The name of the Certificate Mapper.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Certificate Mapper.

# set-connection-handler-prop

Modifies Connection Handler properties.

The **dsconfig set-connection-handler-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--handler-name {name}`

The name of the Connection Handler.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Connection Handler.

# set-crypto-manager-prop

Modifies Crypto Manager properties.

The **dsconfig set-crypto-manager-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Crypto Manager.

# set-debug-target-prop

Modifies Debug Target properties.

The **dsconfig set-debug-target-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--publisher-name {name}`

The name of the Debug Log Publisher.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`--target-name {name}`

The name of the Debug Target.

Properties used in options depend on the type of object to configure.

For details about available properties, see Debug Target.

# set-entry-cache-prop

Modifies Entry Cache properties.

The **dsconfig set-entry-cache-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--cache-name {name}`

The name of the Entry Cache.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Entry Cache.

# set-extended-operation-handler-prop

Modifies Extended Operation Handler properties.

The **dsconfig set-extended-operation-handler-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--handler-name {name}`

The name of the Extended Operation Handler.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Extended Operation Handler.

# set-global-access-control-policy-prop

Modifies Global Access Control Policy properties.

The **dsconfig set-global-access-control-policy-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--policy-name {name}`

The name of the Global Access Control Policy.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Global Access Control Policy.

# set-global-configuration-prop

Modifies Global Configuration properties.

The **dsconfig set-global-configuration-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Global Configuration.

# set-group-implementation-prop

Modifies Group Implementation properties.

The **dsconfig set-group-implementation-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--implementation-name {name}`

The name of the Group Implementation.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Group Implementation.

# set-http-authorization-mechanism-prop

Modifies HTTP Authorization Mechanism properties.

The **dsconfig set-http-authorization-mechanism-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--mechanism-name {name}`

The name of the HTTP Authorization Mechanism.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see HTTP Authorization Mechanism.

# set-http-endpoint-prop

Modifies HTTP Endpoint properties.

The **dsconfig set-http-endpoint-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--endpoint-name {name}`

The name of the HTTP Endpoint.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see HTTP Endpoint.

# set-identity-mapper-prop

Modifies Identity Mapper properties.

The **dsconfig set-identity-mapper-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--mapper-name {name}`

The name of the Identity Mapper.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Identity Mapper.

# set-key-manager-provider-prop

Modifies Key Manager Provider properties.

The **dsconfig set-key-manager-provider-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--provider-name {name}`

The name of the Key Manager Provider.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Key Manager Provider.

# set-log-publisher-prop

Modifies Log Publisher properties.

The **dsconfig set-log-publisher-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--publisher-name {name}`

The name of the Log Publisher.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Publisher.

# set-log-retention-policy-prop

Modifies Log Retention Policy properties.

The **dsconfig set-log-retention-policy-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--policy-name {name}`

The name of the Log Retention Policy.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Retention Policy.

# set-log-rotation-policy-prop

Modifies Log Rotation Policy properties.

The **dsconfig set-log-rotation-policy-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--policy-name {name}`

The name of the Log Rotation Policy.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Log Rotation Policy.

# set-mail-server-prop

Modifies Mail Server properties.

The **dsconfig set-mail-server-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--server-name {name}`

The name of the Mail Server.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Mail Server.

# set-password-generator-prop

Modifies Password Generator properties.

The **dsconfig set-password-generator-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--generator-name {name}`

The name of the Password Generator.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Generator.

# set-password-policy-prop

Modifies Authentication Policy properties.

The **dsconfig set-password-policy-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--policy-name {name}`

The name of the Authentication Policy.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Policy.

# set-password-storage-scheme-prop

Modifies Password Storage Scheme properties.

The **dsconfig set-password-storage-scheme-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--scheme-name {name}`

The name of the Password Storage Scheme.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Storage Scheme.

# set-password-validator-prop

Modifies Password Validator properties.

The **dsconfig set-password-validator-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

`--validator-name {name}`

The name of the Password Validator.

Properties used in options depend on the type of object to configure.

For details about available properties, see Password Validator.

# set-plugin-prop

Modifies Plugin properties.

The **dsconfig set-plugin-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--plugin-name {name}`

The name of the Plugin.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Plugin.

# set-plugin-root-prop

Modifies Plugin Root properties.

The **dsconfig set-plugin-root-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Plugin Root.

# set-replication-domain-prop

Modifies Replication Domain properties.

The **dsconfig set-replication-domain-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--domain-name {name}`

The name of the Replication Domain.

`--provider-name {name}`

The name of the Replication Synchronization Provider.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Replication Domain.

# set-replication-server-prop

Modifies Replication Server properties.

The **dsconfig set-replication-server-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--provider-name {name}`

The name of the Replication Synchronization Provider.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Replication Server.

# set-root-dse-backend-prop

Modifies Root DSE Backend properties.

The **dsconfig set-root-dse-backend-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Root DSE Backend.

# set-sasl-mechanism-handler-prop

Modifies SASL Mechanism Handler properties.

The **dsconfig set-sasl-mechanism-handler-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--handler-name {name}`

The name of the SASL Mechanism Handler.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see SASL Mechanism Handler.

# set-schema-provider-prop

Modifies Schema Provider properties.

The **dsconfig set-schema-provider-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--provider-name {name}`

The name of the Schema Provider.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Schema Provider.

# set-service-discovery-mechanism-prop

Modifies Service Discovery Mechanism properties.

The **dsconfig set-service-discovery-mechanism-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--mechanism-name {name}`

The name of the Service Discovery Mechanism.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Service Discovery Mechanism.

# set-synchronization-provider-prop

Modifies Synchronization Provider properties.

The **dsconfig set-synchronization-provider-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--provider-name {name}`

The name of the Synchronization Provider.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Synchronization Provider.

# set-trust-manager-provider-prop

Modifies Trust Manager Provider properties.

The **dsconfig set-trust-manager-provider-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--provider-name {name}`

The name of the Trust Manager Provider.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Trust Manager Provider.

# set-virtual-attribute-prop

Modifies Virtual Attribute properties.

The **dsconfig set-virtual-attribute-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--name {name}`

The name of the Virtual Attribute.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Virtual Attribute.

# set-work-queue-prop

Modifies Work Queue properties.

The **dsconfig set-work-queue-prop** command takes the following options:

`--add {PROP:VALUE}`

Adds a single value to a property where PROP is the name of the property and VALUE is the single value to be added.

`--remove {PROP:VALUE}`

Removes a single value from a property where PROP is the name of the property and VALUE is the single value to be removed.

`--reset {property}`

Resets a property back to its default values where PROP is the name of the property to be reset.

`--set {PROP:VALUE}`

Assigns a value to a property where PROP is the name of the property and VALUE is the single value to be assigned. Specify the same property multiple times in order to assign more than one value to it.

Properties used in options depend on the type of object to configure.

For details about available properties, see Work Queue.

Chapter 2
# Objects

The following lists show **dsconfig** configuration objects by their inheritance relationships:

**Core Server.**

- Administration Connector
- Alert Handler
  - JMX Alert Handler
  - SMTP Alert Handler
- Connection Handler
  - HTTP Connection Handler
  - JMX Connection Handler
  - LDAP Connection Handler
  - LDIF Connection Handler
  - SNMP Connection Handler
- Extended Operation Handler
  - Cancel Extended Operation Handler
  - Get Connection ID Extended Operation Handler
  - Get Symmetric Key Extended Operation Handler
  - Password Modify Extended Operation Handler
  - Password Policy State Extended Operation Handler
  - StartTLS Extended Operation Handler
  - Who Am I Extended Operation Handler
- Global Configuration
- Group Implementation

  - Dynamic Group Implementation
  - Static Group Implementation
  - Virtual Static Group Implementation
- HTTP Endpoint
  - Admin Endpoint
  - Alive HTTP endpoint
  - Common REST Metrics HTTP Endpoint
  - Healthy HTTP endpoint
  - Prometheus HTTP Endpoint
  - Rest2LDAP Endpoint
- Plugin
  - Attribute Cleanup Plugin
  - Change Number Control Plugin
  - entryUUID Plugin
  - Fractional LDIF Import Plugin
  - Graphite Monitor Reporter Plugin
  - Last Mod Plugin
  - LDAP Attribute Description List Plugin
  - Password Policy Import Plugin
  - Referential Integrity Plugin
  - Samba Password Plugin
  - Seven Bit Clean Plugin
  - Unique Attribute Plugin
- Plugin Root
- Root DSE Backend
- Schema Provider

- Core Schema
- JSON Equality Matching Rule
- JSON Ordering Matching Rule
- JSON Query Equality Matching Rule

- Virtual Attribute
  - Collective Attribute Subentries Virtual Attribute
  - Entity Tag Virtual Attribute
  - entryDN Virtual Attribute
  - entryUUID Virtual Attribute
  - Governing Structure Rule Virtual Attribute
  - Has Subordinates Virtual Attribute
  - Is Member Of Virtual Attribute
  - Member Virtual Attribute
  - Num Subordinates Virtual Attribute
  - Password Expiration Time Virtual Attribute
  - Password Policy Subentry Virtual Attribute
  - Structural Object Class Virtual Attribute
  - Subschema Subentry Virtual Attribute
  - User Defined Virtual Attribute
- Work Queue
  - Traditional Work Queue

**Caching and Backends.**

- Backend
  - Local Backend
    - LDIF Backend
    - Memory Backend

    - Monitor Backend
    - Null Backend
    - Pluggable Backend
      - JE Backend
    - Schema Backend
    - Task Backend
  - Proxy Backend
- Backend Index
- Backend VLV Index
- Entry Cache
  - FIFO Entry Cache
  - Soft Reference Entry Cache
- Root DSE Backend

**Logging.**

- Access Log Filtering Criteria
- Debug Target
- Log Publisher
  - Access Log Publisher
    - Common Audit Access Log Publisher
      - CSV File Access Log Publisher
      - External Access Log Publisher
      - JSON File Based Access Log Publisher
    - File Based Access Log Publisher
    - File Based Audit Log Publisher
  - Debug Log Publisher
    - File Based Debug Log Publisher

- Error Log Publisher
  - Console Error Log Publisher
  - File Based Error Log Publisher
- HTTP Access Log Publisher
  - CSV File HTTP Access Log Publisher
  - External HTTP Access Log Publisher
  - File Based HTTP Access Log Publisher
  - JSON File Based HTTP Access Log Publisher
- Log Retention Policy
  - File Count Log Retention Policy
  - Free Disk Space Log Retention Policy
  - Size Limit Log Retention Policy
- Log Rotation Policy
  - Fixed Time Log Rotation Policy
  - Size Limit Log Rotation Policy
  - Time Limit Log Rotation Policy

**Directory Proxy.**

- Service Discovery Mechanism
  - Replication Service Discovery Mechanism
  - Static Service Discovery Mechanism

**Replication.**

- Replication Domain
- Replication Server
- Synchronization Provider
  - Replication Synchronization Provider

**Authentication and Authorization.**

- Access Control Handler
  - DSEE Compatible Access Control Handler
  - Policy Based Access Control Handler
- Certificate Mapper
  - Fingerprint Certificate Mapper
  - Subject Attribute To User Attribute Certificate Mapper
  - Subject DN To User Attribute Certificate Mapper
  - Subject Equals DN Certificate Mapper
- Crypto Manager
- Global Access Control Policy
- HTTP Authorization Mechanism
  - HTTP Anonymous Authorization Mechanism
  - HTTP Basic Authorization Mechanism
  - HTTP OAuth2 Authorization Mechanism
    - HTTP OAuth2 CTS Authorization Mechanism
    - HTTP OAuth2 File Based Authorization Mechanism
    - HTTP OAuth2 OpenAM Authorization Mechanism
    - HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism
- Identity Mapper
  - Exact Match Identity Mapper
  - Regular Expression Identity Mapper
- Key Manager Provider
  - File Based Key Manager Provider
  - LDAP Key Manager Provider
  - PKCS#11 Key Manager Provider
- SASL Mechanism Handler

- Anonymous SASL Mechanism Handler
- CRAM-MD5 SASL Mechanism Handler
- DIGEST-MD5 SASL Mechanism Handler
- External SASL Mechanism Handler
- GSSAPI SASL Mechanism Handler
- Plain SASL Mechanism Handler
- SCRAM-SHA-256 SASL Mechanism Handler
- SCRAM-SHA-512 SASL Mechanism Handler

- Trust Manager Provider
  - cn=admin data Trust Manager Provider
  - Blind Trust Manager Provider
  - File Based Trust Manager Provider
  - LDAP Trust Manager Provider
  - PKCS#11 Trust Manager Provider

**Service Discovery Mechanism.**

- Service Discovery Mechanism
  - Replication Service Discovery Mechanism
  - Static Service Discovery Mechanism

**User Management.**

- Account Status Notification Handler
  - Error Log Account Status Notification Handler
  - SMTP Account Status Notification Handler
- Authentication Policy
  - LDAP Pass Through Authentication Policy
  - Password Policy
- Certificate Mapper

- Fingerprint Certificate Mapper
- Subject Attribute To User Attribute Certificate Mapper
- Subject DN To User Attribute Certificate Mapper
- Subject Equals DN Certificate Mapper

- Identity Mapper
  - Exact Match Identity Mapper
  - Regular Expression Identity Mapper
- Password Generator
  - Random Password Generator
- Password Storage Scheme
  - AES Password Storage Scheme
  - Base64 Password Storage Scheme
  - Bcrypt Password Storage Scheme
  - Blowfish Password Storage Scheme
  - Clear Password Storage Scheme
  - Crypt Password Storage Scheme
  - MD5 Password Storage Scheme
  - PBKDF2 Password Storage Scheme
    - PBKDF2-HMAC-SHA256 Password Storage Scheme
    - PBKDF2-HMAC-SHA512 Password Storage Scheme
  - PKCS#5 V2.0 Scheme 2 Password Storage Scheme
  - RC4 Password Storage Scheme
  - Salted MD5 Password Storage Scheme
  - Salted SHA-1 Password Storage Scheme
  - Salted SHA-256 Password Storage Scheme
  - Salted SHA-384 Password Storage Scheme

- Salted SHA-512 Password Storage Scheme
- SCRAM-SHA-256 Password Storage Scheme
- SCRAM-SHA-512 Password Storage Scheme
- SHA-1 Password Storage Scheme
- Triple-DES Password Storage Scheme

- Password Validator
  - Attribute Value Password Validator
  - Character Set Password Validator
  - Dictionary Password Validator
  - Length Based Password Validator
  - Repeated Characters Password Validator
  - Similarity Based Password Validator
  - Unique Characters Password Validator

# Access Control Handler

*This is an abstract object type that cannot be instantiated.*

Access Control Handlers manage the application-wide access control. The OpenDJ access control handler is defined through an extensible interface, so that alternate implementations can be created. Only one access control handler may be active in the server at any given time.

Note that OpenDJ also has a privilege subsystem, which may have an impact on what clients may be allowed to do in the server. For example, any user with the bypass-acl privilege is not subject to access control checking regardless of whether the access control implementation is enabled.

## Access Control Handlers

The following Access Control Handlers are available:

- DSEE Compatible Access Control Handler
- Policy Based Access Control Handler

These Access Control Handlers inherit the properties described below.

# Access Control Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| enabled<br>java-class |

## Basic Properties

enabled

| | |
| --- | --- |
| *Synopsis* | Indicates whether the Access Control Handler is enabled. If set to FALSE, then any client (including unauthenticated or anonymous clients) is allowed to bind to the server and any connection with the "bypass-acl" privilege is allowed to perform any operation. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
| --- | --- |
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Access Control Handler implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.AccessControlHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# Access Log Filtering Criteria

A set of rules which together determine whether a log record should be logged or not.

## Dependencies

The following objects have Access Log Filtering Criteria:

- Access Log Publisher

## Access Log Filtering Criteria Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| connection-client-address-equal-to<br>connection-client-address-not-equal-to<br>connection-port-equal-to<br>connection-protocol-equal-to<br>log-record-type<br>request-target-dn-equal-to<br>request-target-dn-not-equal-to<br>response-etime-greater-than<br>response-etime-less-than<br>response-result-code-equal-to<br>response-result-code-not-equal-to<br>search-response-is-indexed<br>search-response-nentries-greater-than<br>search-response-nentries-less-than<br>user-dn-equal-to<br>user-dn-not-equal-to<br>user-is-member-of<br>user-is-not-member-of |

## Basic Properties

connection-client-address-equal-to

| | |
| --- | --- |
| *Synopsis* | Filters log records associated with connections which match at least one of the specified client host names or address masks. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. |
| *Default Value* | None |
| *Allowed Values* | An IP address mask. |

| | |
|---|---|
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

connection-client-address-not-equal-to

| | |
|---|---|
| *Synopsis* | Filters log records associated with connections which do not match any of the specified client host names or address masks. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. |
| *Default Value* | None |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

connection-port-equal-to

| | |
|---|---|
| *Synopsis* | Filters log records associated with connections to any of the specified listener port numbers. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br>Lower limit: 1.<br>Upper limit: 65535. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

connection-protocol-equal-to

| | |
|---|---|
| *Synopsis* | Filters log records associated with connections which match any of the specified protocols. |

| | |
|---|---|
| *Description* | Typical values include "ldap", "ldaps", or "jmx". |
| *Default Value* | None |
| *Allowed Values* | The protocol name as reported in the access log. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-record-type

| | |
|---|---|
| *Synopsis* | Filters log records based on their type. |
| *Default Value* | None |
| *Allowed Values* | abandon: Abandon operations<br>add: Add operations<br>bind: Bind operations<br>compare: Compare operations<br>connect: Client connections<br>delete: Delete operations<br>disconnect: Client disconnections<br>extended: Extended operations<br>modify: Modify operations<br>rename: Rename operations<br>search: Search operations<br>unbind: Unbind operations |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

request-target-dn-equal-to

| | |
|---|---|
| *Synopsis* | Filters operation log records associated with operations which target entries matching at least one of the specified DN patterns. |

| | |
|---|---|
| *Description* | Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com). |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

request-target-dn-not-equal-to

| | |
|---|---|
| *Synopsis* | Filters operation log records associated with operations which target entries matching none of the specified DN patterns. |
| *Description* | Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com). |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

response-etime-greater-than

| | |
|---|---|
| *Synopsis* | Filters operation response log records associated with operations which took longer than the specified number of milli-seconds to complete. |
| *Description* | It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

response-etime-less-than

| | |
|---|---|
| *Synopsis* | Filters operation response log records associated with operations which took less than the specified number of milli-seconds to complete. |
| *Description* | It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

response-result-code-equal-to

| | |
|---|---|
| *Synopsis* | Filters operation response log records associated with operations which include any of the specified result codes. |
| *Description* | It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

response-result-code-not-equal-to

| | |
|---|---|
| *Synopsis* | Filters operation response log records associated with operations which do not include any of the specified result codes. |
| *Description* | It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

search-response-is-indexed

| | |
|---|---|
| *Synopsis* | Filters search operation response log records associated with searches which were either indexed or unindexed. |
| *Description* | It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

search-response-nentries-greater-than

| | |
|---|---|
| *Synopsis* | Filters search operation response log records associated with searches which returned more than the specified number of entries. |
| *Description* | It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages. |
| *Default Value* | None |
| *Allowed Values* | An integer. |

| | |
|---|---|
| | Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

search-response-nentries-less-than

| | |
|---|---|
| *Synopsis* | Filters search operation response log records associated with searches which returned less than the specified number of entries. |
| *Description* | It is recommended to only use this criteria in conjunction with the "combined" output mode of the access logger, since this filter criteria is only applied to response log messages. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

user-dn-equal-to

| | |
|---|---|
| *Synopsis* | Filters log records associated with users matching at least one of the specified DN patterns. |
| *Description* | Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com). |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

user-dn-not-equal-to

| | |
|---|---|
| *Synopsis* | Filters log records associated with users which do not match any of the specified DN patterns. |
| *Description* | Valid DN filters are strings composed of zero or more wildcards. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com). |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

user-is-member-of

| | |
|---|---|
| *Synopsis* | Filters log records associated with users which are members of at least one of the specified groups. |
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

user-is-not-member-of

| | |
|---|---|
| *Synopsis* | Filters log records associated with users which are not members of any of the specified groups. |
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Access Log Publisher

*This is an abstract object type that cannot be instantiated.*

Access Log Publishers are responsible for distributing access log messages from the access logger to a destination.

Access log messages provide information about the types of operations processed by the server.

## Access Log Publishers

The following Access Log Publishers are available:

- Common Audit Access Log Publisher
- File Based Access Log Publisher
- File Based Audit Log Publisher

These Access Log Publishers inherit the properties described below.

## Parent

The Access Log Publisher object inherits from Log Publisher.

## Dependencies

The following objects belong to Access Log Publishers:

- Access Log Filtering Criteria

## Access Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>filtering-policy<br>java-class | suppress-internal-operations<br>suppress-synchronization-operations |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filtering-policy

| | |
|---|---|
| *Synopsis* | Specifies how filtering criteria should be applied to log records. |
| *Default Value* | no-filtering |
| *Allowed Values* | exclusive: Records must not match any of the filtering criteria in order to be logged.<br>inclusive: Records must match at least one of the filtering criteria in order to be logged.<br>no-filtering: No filtering will be performed, and all records will be logged. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the Access Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.AccessLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

suppress-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

suppress-synchronization-operations

| | |
|---|---|
| *Synopsis* | Indicates whether access messages that are generated by synchronization operations should be suppressed. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Account Status Notification Handler

*This is an abstract object type that cannot be instantiated.*

Account Status Notification Handlers are invoked to provide notification to users in some form (for example, by an email message) when the status of a user's account has changed in some way. The Account Status Notification Handler can be used to notify the user and/or administrators of the change.

## Account Status Notification Handlers

The following Account Status Notification Handlers are available:

- Error Log Account Status Notification Handler
- SMTP Account Status Notification Handler

These Account Status Notification Handlers inherit the properties described below.

## Dependencies

The following objects depend on Account Status Notification Handlers:

- Password Policy

## Account Status Notification Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| enabled<br>java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Account Status Notification Handler implementation. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.AccountStatusNotificationHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# cn=admin data Trust Manager Provider

The cn=admin data trust manager provider determines whether to trust a presented certificate based on whether that certificate exists in cn=admin data in the server.

## Parent

The cn=admin data Trust Manager Provider object inherits from Trust Manager Provider.

## cn=admin data Trust Manager Provider Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicate whether the Trust Manager Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the cn=admin data Trust Manager Provider implementation. |
| *Default Value* | org.opends.server.extensions.AdminDataTrustManagerProvider |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.TrustManagerProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## Admin Endpoint

The Admin Endpoint provides RESTful access to OpenDJ's monitoring and configuration backends.

### Parent

The Admin Endpoint object inherits from HTTP Endpoint.

### Admin Endpoint Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| authorization-mechanism<br>base-path<br>enabled | java-class |

### Basic Properties

authorization-mechanism

| | |
|---|---|
| *Synopsis* | The HTTP authorization mechanisms supported by this HTTP Endpoint. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing HTTP Authorization Mechanism .<br><br>The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-path

| | |
|---|---|
| *Synopsis* | All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Endpoint is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Admin Endpoint implementation. |
| *Default Value* | org.opends.server.protocols.http.rest2ldap.AdminEndpoint |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.HttpEndpoint |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Administration Connector

The Administration Connector is used to interact with administration tools using LDAP.

It is a dedicated entry point for administration.

## Dependencies

Administration Connectors depend on the following objects:

- Key Manager Provider
- Trust Manager Provider

## Administration Connector Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| advertised-listen-address<br>allowed-client<br>denied-client<br>key-manager-provider<br>listen-address<br>listen-port<br>restricted-client<br>restricted-client-connection-limit<br>ssl-cert-nickname |

| Basic Properties |
| --- |
| ssl-cipher-suite<br>ssl-protocol<br>trust-manager-provider |

## Basic Properties

advertised-listen-address

| | |
| --- | --- |
| *Synopsis* | The advertised address(es) which clients should use for connecting to this Administration Connector. |
| *Description* | Multiple addresses may be provided as separate values for this attribute. The meta-address 0.0.0.0 is not permitted. |
| *Default Value* | None |
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

allowed-client

| | |
| --- | --- |
| *Synopsis* | A set of clients who will be allowed to establish connections to this Administration Connector. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

denied-client

| | |
|---|---|
| *Synopsis* | A set of clients who are not allowed to establish connections to this Administration Connector. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

key-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the key manager that is used with the Administration Connector . |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Key Manager Provider .<br><br>The referenced key manager provider must be enabled. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | Restart the server for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

listen-address

| | |
|---|---|
| *Synopsis* | The network interface(s) on which this Administration Connector should listen for incoming client connections. |
| *Description* | Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the directory server will listen on all interfaces. |
| *Default Value* | 0.0.0.0 |

| | |
|---|---|
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | Restart the server for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

listen-port

| | |
|---|---|
| *Synopsis* | Specifies the port number on which the Administration Connector will listen for connections from clients. |
| *Description* | Only a single port number may be provided. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br>Lower limit: 1.<br>Upper limit: 65535. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be limited to the maximum number of connections specified by the "restricted-client-connection-limit" property. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | No restrictions are imposed on the number of connections a client can open. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

restricted-client-connection-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of connections a restricted client can open at the same time to this Administration Connector. |
| *Description* | Once Directory Server accepts the specified number of connections from a client specified in restricted-client, any additional connection will be rejected. The number of connections is maintained by IP address. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | 100 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cert-nickname

| | |
|---|---|
| *Synopsis* | Specifies the nicknames (also called the aliases) of the keys or key pairs that the Administration Connector should use when performing SSL communication. |
| *Description* | The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Administration Connector is configured to use SSL. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | Restart the server for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cipher-suite

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL cipher suites that are allowed for use in SSL communication. |
| *Default Value* | Uses the default set of SSL cipher suites provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-protocol

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication. |
| *Default Value* | Uses the default set of SSL protocols provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

trust-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name(s) of the trust manager(s) that is used with the Administration Connector . |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Trust Manager Provider .<br><br>The referenced trust manager provider must be enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | Restart the server for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# AES Password Storage Scheme

The AES Password Storage Scheme provides a mechanism for encoding user passwords using the AES reversible encryption mechanism.

This scheme contains only an implementation for the user password syntax, with a storage scheme name of "AES".

## Parent

The AES Password Storage Scheme object inherits from Password Storage Scheme.

## AES Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the AES Password Storage Scheme implementation. |

| | |
|---|---|
| *Default Value* | org.opends.server.extensions.AESPasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Alert Handler

*This is an abstract object type that cannot be instantiated.*

Alert Handlers are used to notify administrators of significant problems or notable events that occur in the OpenDJ directory server.

## Alert Handlers

The following Alert Handlers are available:

- JMX Alert Handler
- SMTP Alert Handler

These Alert Handlers inherit the properties described below.

## Alert Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| disabled-alert-type<br>enabled<br>enabled-alert-type<br>java-class |

## Basic Properties

disabled-alert-type

| | |
|---|---|
| *Synopsis* | Specifies the names of the alert types that are disabled for this alert handler. |
| *Description* | If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed. |
| *Default Value* | If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Alert Handler is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled-alert-type

| | |
|---|---|
| *Synopsis* | Specifies the names of the alert types that are enabled for this alert handler. |
| *Description* | If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed. |
| *Default Value* | All alerts with types not included in the set of disabled alert types are allowed. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Alert Handler implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.AlertHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# Alive HTTP endpoint

The Alive HTTP endpoint provides a way to check whether the server is facing serious problems that need administrative actions to recover.

This endpoint responds 200 without content when the server is alive or 503 with a JSON containing an array of serious errors in the field "alive-errors".

## Parent

The Alive HTTP endpoint object inherits from HTTP Endpoint.

## Alive HTTP endpoint Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| authorization-mechanism<br>base-path<br>enabled | java-class |

## Basic Properties

authorization-mechanism

| | |
|---|---|
| *Synopsis* | The HTTP authorization mechanisms supported by this HTTP Endpoint. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing HTTP Authorization Mechanism .<br><br>The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-path

| | |
|---|---|
| *Synopsis* | All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Endpoint is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Alive HTTP endpoint implementation. |
| *Default Value* | org.opends.server.protocols.http.AliveEndpoint |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.HttpEndpoint |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Anonymous SASL Mechanism Handler

The ANONYMOUS SASL mechanism provides the ability for clients to perform an anonymous bind using a SASL mechanism.

The only real benefit that this provides over a normal anonymous bind (that is, using simple authentication with no password) is that the ANONYMOUS SASL mechanism also allows the client to include a trace string in the request. This trace string can help identify the application that performed the bind (although since there is no authentication, there is no assurance that some other client did not spoof that trace string).

## Parent

The Anonymous SASL Mechanism Handler object inherits from SASL Mechanism Handler.

## Anonymous SASL Mechanism Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the SASL mechanism handler is enabled for use. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation. |
| *Default Value* | org.opends.server.extensions.AnonymousSASLMechanismHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.SASLMechanismHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Attribute Cleanup Plugin

A pre-parse plugin which can be used to remove and rename attributes in ADD and MODIFY requests before being processed.

This plugin should be used in order maintain interoperability with client applications which attempt to update attributes in a way which is incompatible with LDAPv3 or OpenDJ. For example, this plugin may be used in order to remove changes to operational attributes such as modifiersName, creatorsName, modifyTimestamp, and createTimestamp (Sun DSEE chaining does this).

### Parent

The Attribute Cleanup Plugin object inherits from Plugin.

# Attribute Cleanup Plugin Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>java-class<br>remove-inbound-attributes<br>rename-inbound-attributes | invoke-for-internal-operations<br>plugin-type |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the plug-in implementation. |
| *Default Value* | org.opends.server.plugins.AttributeCleanupPlugin |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.plugin.DirectoryServerPlugin |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

remove-inbound-attributes

| | |
|---|---|
| *Synopsis* | A list of attributes which should be removed from incoming add or modify requests. |
| *Default Value* | No attributes will be removed |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

rename-inbound-attributes

| | |
|---|---|
| *Synopsis* | A list of attributes which should be renamed in incoming add or modify requests. |
| *Default Value* | No attributes will be renamed |
| *Allowed Values* | An attribute name mapping. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

invoke-for-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in should be invoked for internal operations. |
| *Description* | Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

plugin-type

| | |
|---|---|
| *Synopsis* | Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked. |
| *Default Value* | preparseadd<br><br>preparsemodify |
| *Allowed Values* | initialization: Invoked at the initialization of the directory server.<br><br>intermediateresponse: Invoked before sending an intermediate repsonse message to the client.<br><br>ldifimport: Invoked for each entry read during an LDIF import.<br><br>ldifimportbegin: Invoked at the beginning of an LDIF import session.<br><br>ldifimportend: Invoked at the end of an LDIF import session.<br><br>postconnect: Invoked whenever a new connection is established to the server.<br><br>postdisconnect: Invoked whenever an existing connection is terminated (by either the client or the server).<br><br>postoperationabandon: Invoked after completing the abandon processing.<br><br>postoperationadd: Invoked after completing the core add processing but before sending the response to the client.<br><br>postoperationbind: Invoked after completing the core bind processing but before sending the response to the client.<br><br>postoperationcompare: Invoked after completing the core compare processing but before sending the response to the client.<br><br>postoperationdelete: Invoked after completing the core delete processing but before sending the response to the client.<br><br>postoperationextended: Invoked after completing the core extended processing but before sending the response to the client.<br><br>postoperationmodify: Invoked after completing the core modify processing but before sending the response to the client.<br><br>postoperationmodifydn: Invoked after completing the core modify DN processing but before sending the response to the client.<br><br>postoperationsearch: Invoked after completing the core search processing but before sending the response to the client.<br><br>postoperationunbind: Invoked after completing the unbind processing.<br><br>postresponseadd: Invoked after sending the add response to the client.<br><br>postresponsebind: Invoked after sending the bind response to the client. |

postresponsecompare: Invoked after sending the compare response to the client.

postresponsedelete: Invoked after sending the delete response to the client.

postresponseextended: Invoked after sending the extended response to the client.

postresponsemodify: Invoked after sending the modify response to the client.

postresponsemodifydn: Invoked after sending the modify DN response to the client.

postresponsesearch: Invoked after sending the search result done message to the client.

postsynchronizationadd: Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete: Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify: Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn: Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd: Invoked prior to performing the core add processing.

preoperationbind: Invoked prior to performing the core bind processing.

preoperationcompare: Invoked prior to performing the core compare processing.

preoperationdelete: Invoked prior to performing the core delete processing.

preoperationextended: Invoked prior to performing the core extended processing.

preoperationmodify: Invoked prior to performing the core modify processing.

preoperationmodifydn: Invoked prior to performing the core modify DN processing.

preoperationsearch: Invoked prior to performing the core search processing.

preparseabandon: Invoked prior to parsing an abandon request.

preparseadd: Invoked prior to parsing an add request.

preparsebind: Invoked prior to parsing a bind request.

preparsecompare: Invoked prior to parsing a compare request.

preparsedelete: Invoked prior to parsing a delete request.

preparseextended: Invoked prior to parsing an extended request.

preparsemodify: Invoked prior to parsing a modify request.

| | |
|---|---|
| | preparsemodifydn: Invoked prior to parsing a modify DN request.<br><br>preparsesearch: Invoked prior to parsing a search request.<br><br>preparseunbind: Invoked prior to parsing an unbind request.<br><br>searchresultentry: Invoked before sending a search result entry to the client.<br><br>searchresultreference: Invoked before sending a search result reference to the client.<br><br>shutdown: Invoked during a graceful directory server shutdown.<br><br>startup: Invoked during the directory server startup process.<br><br>subordinatedelete: Invoked in the course of deleting a subordinate entry of a delete operation.<br><br>subordinatemodifydn: Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Attribute Value Password Validator

The Attribute Value Password Validator attempts to determine whether a proposed password is acceptable for use by determining whether that password is contained in any attribute within the user's entry.

It can be configured to look in all attributes or in a specified subset of attributes.

## Parent

The Attribute Value Password Validator object inherits from Password Validator.

## Attribute Value Password Validator Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| check-substrings<br>enabled | java-class |

| Basic Properties | Advanced Properties |
|---|---|
| match-attribute<br>min-substring-length<br>test-reversed-password | |

## Basic Properties

### check-substrings

| | |
|---|---|
| *Synopsis* | Indicates whether this password validator is to match portions of the password string against attribute values. |
| *Description* | If "false" then only match the entire password against attribute values otherwise ("true") check whether the password contains attribute values. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the password validator is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### match-attribute

| | |
|---|---|
| *Synopsis* | Specifies the name(s) of the attribute(s) whose values should be checked to determine whether they match the provided password. If no values are provided, then the server checks if the proposed password matches the value of any attribute in the user's entry. |
| *Default Value* | All attributes in the user entry will be checked. |

| | |
|---|---|
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

min-substring-length

| | |
|---|---|
| *Synopsis* | Indicates the minimal length of the substring within the password in case substring checking is enabled. |
| *Description* | If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords. |
| *Default Value* | 5 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

test-reversed-password

| | |
|---|---|
| *Synopsis* | Indicates whether this password validator should test the reversed value of the provided password as well as the order in which it was given. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the password validator implementation. |
| *Default Value* | org.opends.server.extensions.AttributeValuePasswordValidator |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordValidator |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Authentication Policy

*This is an abstract object type that cannot be instantiated.*

Authentication Policies define the policies which should be used for authenticating users and managing the password and other account related state.

## Authentication Policies

The following Authentication Policies are available:

- LDAP Pass Through Authentication Policy
- Password Policy

These Authentication Policies inherit the properties described below.

## Dependencies

The following objects depend on Authentication Policies:

- Global Configuration

## Authentication Policy Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties |
| --- |
| java-class |

## Basic Properties

java-class

| | |
| --- | --- |
| *Synopsis* | Specifies the fully-qualified name of the Java class which provides the Authentication Policy implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.AuthenticationPolicyFactory |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# Backend

*This is an abstract object type that cannot be instantiated.*

Backends are responsible for providing access to the underlying data presented by the server.

The data may be stored locally in an embedded database, remotely in an external system, or generated on the fly (for example, calculated from other information that is available).

## Backends

The following Backends are available:

- Local Backend
- Proxy Backend

These Backends inherit the properties described below.

## Backend Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties |
| --- |
| backend-id<br>enabled<br>java-class |

## Basic Properties

### backend-id

| | |
| --- | --- |
| *Synopsis* | Specifies a name to identify the associated backend. |
| *Description* | The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

### enabled

| | |
| --- | --- |
| *Synopsis* | Indicates whether the backend is enabled in the server. |
| *Description* | If a backend is not enabled, then its contents are not accessible when processing operations. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### java-class

| | |
| --- | --- |
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the backend implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements: |

| | |
|---|---|
| | • org.opends.server.api.Backend |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# Backend Index

Backend Indexes are used to store information that makes it possible to locate entries very quickly when processing search operations.

Indexing is performed on a per-attribute level and different types of indexing may be performed for different kinds of attributes, based on how they are expected to be accessed during search operations.

## Dependencies

The following objects have Backend Indexes:

- Pluggable Backend

## Backend Index Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute<br>confidentiality-enabled<br>index-extensible-matching-rule<br>index-type<br>ttl-age<br>ttl-enabled | index-entry-limit<br>substring-length |

## Basic Properties

attribute

| | |
|---|---|
| *Synopsis* | Specifies the name of the attribute for which the index is to be maintained. |
| *Default Value* | None |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

confidentiality-enabled

| | |
|---|---|
| *Synopsis* | Specifies whether contents of the index should be confidential. |
| *Description* | Setting the flag to true will hash keys for equality type indexes using SHA-1 and encrypt the list of entries matching a substring key for substring indexes. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>If the index for the attribute must be protected for security purposes and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate. The property cannot be set on a backend for which confidentiality is not enabled. |
| *Advanced* | No |
| *Read-Only* | No |

index-extensible-matching-rule

| | |
|---|---|
| *Synopsis* | The extensible matching rule in an extensible index. |
| *Description* | An extensible matching rule must be specified using either LOCALE or OID of the matching rule. |
| *Default Value* | No extensible matching rules will be indexed. |
| *Allowed Values* | A Locale or an OID. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>The index must be rebuilt before it will reflect the new value. |
| *Advanced* | No |
| *Read-Only* | No |

index-type

| | |
|---|---|
| *Synopsis* | Specifies the type(s) of indexing that should be performed for the associated attribute. |
| *Description* | For equality, presence, and substring index types, the associated attribute type must have a corresponding matching rule. |
| *Default Value* | None |
| *Allowed Values* | approximate: This index type is used to improve the efficiency of searches using approximate matching search filters.<br><br>equality: This index type is used to improve the efficiency of searches using equality search filters.<br><br>extensible: This index type is used to improve the efficiency of searches using extensible matching search filters.<br><br>ordering: This index type is used to improve the efficiency of searches using "greater than or equal to" or "less then or equal to" search filters.<br><br>presence: This index type is used to improve the efficiency of searches using the presence search filters.<br><br>substring: This index type is used to improve the efficiency of searches using substring search filters. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None<br><br>If any new index types are added for an attribute, and values for that attribute already exist in the database, the index must be rebuilt before it will be accurate. |
| *Advanced* | No |
| *Read-Only* | No |

ttl-age

| | |
|---|---|
| *Synopsis* | The age when timestamps are considered to have expired. |
| *Default Value* | 0s |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 0 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

ttl-enabled

| | |
|---|---|
| *Synopsis* | Enable TTL for this generalized time index. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

index-entry-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of entries that are allowed to match a given index key before that particular index key is no longer maintained. |
| *Description* | This is analogous to the ALL IDs threshold in the Sun Java System Directory Server. If this is specified, its value overrides the JE backend-wide configuration. For no limit, use 0 for the value. Changing the index entry limit significantly can result in serious performance degradation. Please read the documentation before changing this setting. |
| *Default Value* | 4000 |
| *Allowed Values* | An integer.<br>Lower limit: 0.<br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br>If any index keys have already reached this limit, indexes must be rebuilt before they will be allowed to use the new limit. |
| *Advanced* | Yes |
| *Read-Only* | No |

substring-length

| | |
|---|---|
| *Synopsis* | The length of substrings in a substring index. |
| *Default Value* | 6 |

| | |
|---|---|
| *Allowed Values* | An integer.<br><br>Lower limit: 3. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>The index must be rebuilt before it will reflect the new value. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Backend VLV Index

Backend VLV Indexes are used to store information about a specific search request that makes it possible to efficiently process them using the VLV control.

A VLV index effectively notifies the server that a virtual list view, with specific query and sort parameters, will be performed. This index also allows the server to collect and maintain the information required to make using the virtual list view faster.

## Dependencies

The following objects have Backend VLV Indexes:

- Pluggable Backend

## Backend VLV Index Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| base-dn<br>filter<br>name<br>scope<br>sort-order |

## Basic Properties

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DN used in the search query that is being indexed. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None<br>The index must be rebuilt after modifying this property. |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the LDAP filter used in the query that is being indexed. |
| *Default Value* | None |
| *Allowed Values* | A valid LDAP search filter. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None<br>The index must be rebuilt after modifying this property. |
| *Advanced* | No |
| *Read-Only* | No |

name

| | |
|---|---|
| *Synopsis* | Specifies a unique name for this VLV index. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None<br>The VLV index name cannot be altered after the index is created. |
| *Advanced* | No |
| *Read-Only* | Yes |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope of the query that is being indexed. |
| *Default Value* | None |
| *Allowed Values* | base-object: Search the base object only. |

| | |
|---|---|
| | single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None<br><br>The index must be rebuilt after modifying this property. |
| *Advanced* | No |
| *Read-Only* | No |

sort-order

| | |
|---|---|
| *Synopsis* | Specifies the names of the attributes that are used to sort the entries for the query being indexed. |
| *Description* | Multiple attributes can be used to determine the sort order by listing the attribute names from highest to lowest precedence. Optionally, + or - can be prefixed to the attribute name to sort the attribute in ascending order or descending order respectively. |
| *Default Value* | None |
| *Allowed Values* | Valid attribute types defined in the schema, separated by a space and optionally prefixed by + or -. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None<br><br>The index must be rebuilt after modifying this property. |
| *Advanced* | No |
| *Read-Only* | No |

# Base64 Password Storage Scheme

The Base64 Password Storage Scheme provides a mechanism for encoding user passwords using the BASE64 encoding mechanism.

This scheme contains only an implementation for the user password syntax, with a storage scheme name of "BASE64". The Base64 Password Storage Scheme merely obscures the password so that the clear-text password is not available to casual observers. However, it offers no real protection and should only be used if there are client applications that specifically require this capability.

## Parent

The Base64 Password Storage Scheme object inherits from Password Storage Scheme.

## Base64 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Base64 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.Base64PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Bcrypt Password Storage Scheme

The Bcrypt Password Storage Scheme provides a mechanism for encoding user passwords using the bcrypt message digest algorithm.

This scheme contains an implementation for the user password syntax, with a storage scheme name of "BCRYPT".

## Parent

The Bcrypt Password Storage Scheme object inherits from Password Storage Scheme.

## Bcrypt Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| bcrypt-cost<br>enabled<br>rehash-policy | java-class |

## Basic Properties

bcrypt-cost

| | |
|---|---|
| *Synopsis* | The cost parameter specifies a key expansion iteration count as a power of two. A default value of 12 (2^12 iterations) is considered in 2016 as a reasonable balance between responsiveness and security for regular users. |
| *Description* | By default, changes to this setting impact only newly created and updated passwords. However, if the rehash-policy is set to always or only-increase, it causes the server to recalculate each user's password hash on their next authentication, and write the new hash to the user's entry on disk. Changing the number of iterations therefore leads to a short-term spike in CPU and disk use as the server updates each user's password when they next authenticate. Longer term, increasing this settings results in more secure passwords at the expense of longer response times and lower throughput. |
| *Default Value* | 12 |

| | |
|---|---|
| *Allowed Values* | An integer.<br>Lower limit: 4.<br>Upper limit: 30. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

rehash-policy

| | |
|---|---|
| *Synopsis* | Indicates whether the server should rehash passwords after the cost has been changed. |
| *Description* | Passwords will be rehashed when a user successfully authenticates. Note that rehashing will increase the write load on the server. |
| *Default Value* | never |
| *Allowed Values* | always: Rehash passwords when the cost is increased or decreased.<br>never: Never rehash passwords.<br>only-increase: Only rehash passwords when the cost has been increased (do not downgrade the security of the hashed password). |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Bcrypt Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.BcryptPasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## Blind Trust Manager Provider

The blind trust manager provider always trusts any certificate that is presented to it, regardless of its issuer, subject, and validity dates.

Use the blind trust manager provider only for testing purposes, because it allows clients to use forged certificates and authenticate as virtually any user in the server.

### Parent

The Blind Trust Manager Provider object inherits from Trust Manager Provider.

### Blind Trust Manager Provider Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

### Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicate whether the Trust Manager Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the Blind Trust Manager Provider implementation. |
| *Default Value* | org.opends.server.extensions.BlindTrustManagerProvider |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.TrustManagerProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## Blowfish Password Storage Scheme

The Blowfish Password Storage Scheme provides a mechanism for encoding user passwords using the Blowfish reversible encryption mechanism.

This scheme contains only an implementation for the user password syntax, with a storage scheme name of "BLOWFISH".

### Parent

The Blowfish Password Storage Scheme object inherits from Password Storage Scheme.

# Blowfish Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Blowfish Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.BlowfishPasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Cancel Extended Operation Handler

The Cancel Extended Operation Handler provides support for the LDAP cancel extended operation as defined in RFC 3909.

It allows clients to cancel operations initiated from earlier requests. The property ensures that both the cancel request and the operation being canceled receives response messages.

## Parent

The Cancel Extended Operation Handler object inherits from Extended Operation Handler.

## Cancel Extended Operation Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server). |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Cancel Extended Operation Handler implementation. |
| *Default Value* | org.opends.server.extensions.CancelExtendedOperation |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.ExtendedOperationHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Certificate Mapper

*This is an abstract object type that cannot be instantiated.*

Certificate Mappers are responsible for establishing a mapping between a client certificate and the entry for the user that corresponds to that certificate.

## Certificate Mappers

The following Certificate Mappers are available:

- Fingerprint Certificate Mapper
- Subject Attribute To User Attribute Certificate Mapper
- Subject DN To User Attribute Certificate Mapper
- Subject Equals DN Certificate Mapper

These Certificate Mappers inherit the properties described below.

## Dependencies

The following objects depend on Certificate Mappers:

- External SASL Mechanism Handler

## Certificate Mapper Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties |
| --- |
| enabled<br>issuer-attribute<br>java-class |

## Basic Properties

### enabled

| | |
| --- | --- |
| *Synopsis* | Indicates whether the Certificate Mapper is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### issuer-attribute

| | |
| --- | --- |
| *Synopsis* | Specifies the name or OID of the attribute whose value should exactly match the certificate issuer DN. |
| *Description* | Certificate issuer verification should be enabled whenever multiple CAs are trusted in order to prevent impersonation. In particular, it is possible for different CAs to issue certificates having the same subject DN. |
| *Default Value* | The certificate issuer DN will not be verified. |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### java-class

| | |
| --- | --- |
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Certificate Mapper implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements: |

| | |
|---|---|
| | • org.opends.server.api.CertificateMapper |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# Change Number Control Plugin

The Change Number Control Plugin returns the change number generated by the replication subsystem.

The Change Number Control Plugin returns the change number generated by the Multi-Master Replication subsystem when : - the Multi-Master Replication is configured and enabled - the request is a write operation (add, delete, modify, moddn) - the control is part of a request. If all of the above are true, the response contains a control response with a string representing the change number. The implementation for the chnage number control plug-in is contained in the org.opends.server.plugins.ChangeNumberControlPlugin class. It must be configured with the postOperationAdd, postOperationDelete, postOperationModify and postOperationModifyDN plug-in types, but it does not have any other custom configuration.

## Parent

The Change Number Control Plugin object inherits from Plugin.

## Change Number Control Plugin Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | invoke-for-internal-operations<br>java-class<br>plugin-type |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true |

| | |
|---|---|
| | false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

invoke-for-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in should be invoked for internal operations. |
| *Description* | Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the plug-in implementation. |
| *Default Value* | org.opends.server.plugins.ChangeNumberControlPlugin |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.plugin.DirectoryServerPlugin |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

plugin-type

| | |
|---|---|
| *Synopsis* | Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked. |
| *Default Value* | postOperationAdd<br><br>postOperationDelete<br><br>postOperationModify<br><br>postOperationModifyDN |
| *Allowed Values* | initialization: Invoked at the initialization of the directory server.<br><br>intermediateresponse: Invoked before sending an intermediate repsonse message to the client.<br><br>ldifimport: Invoked for each entry read during an LDIF import.<br><br>ldifimportbegin: Invoked at the beginning of an LDIF import session.<br><br>ldifimportend: Invoked at the end of an LDIF import session.<br><br>postconnect: Invoked whenever a new connection is established to the server.<br><br>postdisconnect: Invoked whenever an existing connection is terminated (by either the client or the server).<br><br>postoperationabandon: Invoked after completing the abandon processing.<br><br>postoperationadd: Invoked after completing the core add processing but before sending the response to the client.<br><br>postoperationbind: Invoked after completing the core bind processing but before sending the response to the client.<br><br>postoperationcompare: Invoked after completing the core compare processing but before sending the response to the client.<br><br>postoperationdelete: Invoked after completing the core delete processing but before sending the response to the client.<br><br>postoperationextended: Invoked after completing the core extended processing but before sending the response to the client.<br><br>postoperationmodify: Invoked after completing the core modify processing but before sending the response to the client.<br><br>postoperationmodifydn: Invoked after completing the core modify DN processing but before sending the response to the client.<br><br>postoperationsearch: Invoked after completing the core search processing but before sending the response to the client.<br><br>postoperationunbind: Invoked after completing the unbind processing. |

postresponseadd: Invoked after sending the add response to the client.

postresponsebind: Invoked after sending the bind response to the client.

postresponsecompare: Invoked after sending the compare response to the client.

postresponsedelete: Invoked after sending the delete response to the client.

postresponseextended: Invoked after sending the extended response to the client.

postresponsemodify: Invoked after sending the modify response to the client.

postresponsemodifydn: Invoked after sending the modify DN response to the client.

postresponsesearch: Invoked after sending the search result done message to the client.

postsynchronizationadd: Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete: Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify: Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn: Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd: Invoked prior to performing the core add processing.

preoperationbind: Invoked prior to performing the core bind processing.

preoperationcompare: Invoked prior to performing the core compare processing.

preoperationdelete: Invoked prior to performing the core delete processing.

preoperationextended: Invoked prior to performing the core extended processing.

preoperationmodify: Invoked prior to performing the core modify processing.

preoperationmodifydn: Invoked prior to performing the core modify DN processing.

preoperationsearch: Invoked prior to performing the core search processing.

preparseabandon: Invoked prior to parsing an abandon request.

preparseadd: Invoked prior to parsing an add request.

preparsebind: Invoked prior to parsing a bind request.

preparsecompare: Invoked prior to parsing a compare request.

preparsedelete: Invoked prior to parsing a delete request.

| | |
|---|---|
| | preparseextended: Invoked prior to parsing an extended request.<br><br>preparsemodify: Invoked prior to parsing a modify request.<br><br>preparsemodifydn: Invoked prior to parsing a modify DN request.<br><br>preparsesearch: Invoked prior to parsing a search request.<br><br>preparseunbind: Invoked prior to parsing an unbind request.<br><br>searchresultentry: Invoked before sending a search result entry to the client.<br><br>searchresultreference: Invoked before sending a search result reference to the client.<br><br>shutdown: Invoked during a graceful directory server shutdown.<br><br>startup: Invoked during the directory server startup process.<br><br>subordinatedelete: Invoked in the course of deleting a subordinate entry of a delete operation.<br><br>subordinatemodifydn: Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Character Set Password Validator

The Character Set Password Validator determines whether a proposed password is acceptable by checking whether it contains a sufficient number of characters from one or more user-defined character sets and ranges.

For example, the validator can ensure that passwords must have at least one lowercase letter, one uppercase letter, one digit, and one symbol.

## Parent

The Character Set Password Validator object inherits from Password Validator.

## Character Set Password Validator Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| allow-unclassified-characters<br>character-set<br>character-set-ranges<br>enabled<br>min-character-sets | java-class |

## Basic Properties

### allow-unclassified-characters

| | |
|---|---|
| *Synopsis* | Indicates whether this password validator allows passwords to contain characters outside of any of the user-defined character sets and ranges. |
| *Description* | If this is "false", then only those characters in the user-defined character sets and ranges may be used in passwords. Any password containing a character not included in any character set or range will be rejected. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### character-set

| | |
|---|---|
| *Synopsis* | Specifies a character set containing characters that a password may contain and a value indicating the minimum number of characters required from that set. |
| *Description* | Each value must be an integer (indicating the minimum required characters from the set which may be zero, indicating that the character set is optional) followed by a colon and the characters to include in that set (for example, "3:abcdefghijklmnopqrstuvwxyz" indicates that a user password must contain at least three characters from the set of lowercase ASCII letters). Multiple character sets can be defined in separate values, although no character can appear in more than one character set. |
| *Default Value* | If no sets are specified, the validator only uses the defined character ranges. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

character-set-ranges

| | |
|---|---|
| *Synopsis* | Specifies a character range containing characters that a password may contain and a value indicating the minimum number of characters required from that range. |
| *Description* | Each value must be an integer (indicating the minimum required characters from the range which may be zero, indicating that the character range is optional) followed by a colon and one or more range specifications. A range specification is 3 characters: the first character allowed, a minus, and the last character allowed. For example, "3:A-Za-z0-9". The ranges in each value should not overlap, and the characters in each range specification should be ordered. |
| *Default Value* | If no ranges are specified, the validator only uses the defined character sets. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the password validator is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

min-character-sets

| | |
|---|---|
| *Synopsis* | Specifies the minimum number of character sets and ranges that a password must contain. |
| *Description* | This property should only be used in conjunction with optional character sets and ranges (those requiring zero characters). Its value must include any mandatory |

| | |
|---|---|
| | character sets and ranges (those requiring greater than zero characters). This is useful in situations where a password must contain characters from mandatory character sets and ranges, and characters from at least N optional character sets and ranges. For example, it is quite common to require that a password contains at least one non-alphanumeric character as well as characters from two alphanumeric character sets (lower-case, upper-case, digits). In this case, this property should be set to 3. |
| *Default Value* | The password must contain characters from each of the mandatory character sets and ranges and, if there are optional character sets and ranges, at least one character from one of the optional character sets and ranges. |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the password validator implementation. |
| *Default Value* | org.opends.server.extensions.CharacterSetPasswordValidator |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordValidator |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Clear Password Storage Scheme

The Clear Password Storage Scheme provides a mechanism for storing user passwords in clear text, without any form of obfuscation.

This scheme contains only an implementation for the user password syntax, with a storage scheme name of "CLEAR". The Clear Password Storage Scheme should only be used if there are client applications that specifically require this capability.

## Parent

The Clear Password Storage Scheme object inherits from Password Storage Scheme.

## Clear Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Clear Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.ClearPasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements: |

| | |
|---|---|
| | • org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Collective Attribute Subentries Virtual Attribute

The Collective Attribute Subentries Virtual Attribute generates a virtual attribute that specifies all collective attribute subentries that affect the entry.

## Parent

The Collective Attribute Subentries Virtual Attribute object inherits from Virtual Attribute.

## Collective Attribute Subentries Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>enabled<br>filter<br>group-dn<br>scope | conflict-behavior<br>java-class |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | collectiveAttributeSubentries |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |

| | |
|---|---|
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br><br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | virtual-overrides-real |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.<br><br>real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | org.opends.server.extensions.CollectiveAttributeSubentriesVirtualAttributeProvider |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Common Audit Access Log Publisher

*This is an abstract object type that cannot be instantiated.*

Common Audit Access Log Publishers publish access events to commons audit.

## Common Audit Access Log Publishers

The following Common Audit Access Log Publishers are available:

- CSV File Access Log Publisher
- External Access Log Publisher
- JSON File Based Access Log Publisher

These Common Audit Access Log Publishers inherit the properties described below.

## Parent

The Common Audit Access Log Publisher object inherits from Access Log Publisher.

## Common Audit Access Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>filtering-policy<br>java-class<br>log-control-oids | suppress-internal-operations<br>suppress-synchronization-operations |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

filtering-policy

| | |
|---|---|
| *Synopsis* | Specifies how filtering criteria should be applied to log records. |
| *Default Value* | no-filtering |
| *Allowed Values* | exclusive: Records must not match any of the filtering criteria in order to be logged.<br><br>inclusive: Records must match at least one of the filtering criteria in order to be logged.<br><br>no-filtering: No filtering will be performed, and all records will be logged. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the Access Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.AccessLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-control-oids

| | |
|---|---|
| *Synopsis* | Specifies whether control OIDs will be included in operation log records. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

suppress-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

suppress-synchronization-operations

| | |
|---|---|
| *Synopsis* | Indicates whether access messages that are generated by synchronization operations should be suppressed. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## Connection Handler

*This is an abstract object type that cannot be instantiated.*

Connection Handlers are responsible for handling all interaction with the clients, including accepting the connections, reading requests, and sending responses.

## Connection Handlers

The following Connection Handlers are available:

- HTTP Connection Handler
- JMX Connection Handler
- LDAP Connection Handler
- LDIF Connection Handler
- SNMP Connection Handler

These Connection Handlers inherit the properties described below.

## Connection Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| allowed-client<br>denied-client<br>enabled<br>java-class<br>restricted-client<br>restricted-client-connection-limit |

## Basic Properties

allowed-client

| | |
| --- | --- |
| *Synopsis* | A set of clients who will be allowed to establish connections to this Connection Handler. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed. |
| *Allowed Values* | An IP address mask. |

| | |
|---|---|
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

denied-client

| | |
|---|---|
| *Synopsis* | A set of clients who are not allowed to establish connections to this Connection Handler. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Connection Handler is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Connection Handler implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.ConnectionHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be limited to the maximum number of connections specified by the "restricted-client-connection-limit" property. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | No restrictions are imposed on the number of connections a client can open. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client-connection-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of connections a restricted client can open at the same time to this Connection Handler. |
| *Description* | Once Directory Server accepts the specified number of connections from a client specified in restricted-client, any additional connection will be rejected. The number of connections is maintained by IP address. Specifying a value for |

| | |
|---|---|
| | this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | 100 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

# Console Error Log Publisher

Console Error Log Publishers publish error messages to the console (STDOUT).

## Parent

The Console Error Log Publisher object inherits from Error Log Publisher.

## Console Error Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| default-severity<br>enabled<br>override-severity | java-class |

## Basic Properties

default-severity

| | |
|---|---|
| *Synopsis* | Specifies the default severity levels for the logger. |
| *Default Value* | error<br><br>warning |

| | |
|---|---|
| *Allowed Values* | all: Messages of all severity levels are logged.<br><br>debug: The error log severity that is used for messages that provide debugging information triggered during processing.<br><br>error: The error log severity that is used for messages that provide information about errors which may force the server to shut down or operate in a significantly degraded state.<br><br>info: The error log severity that is used for messages that provide information about significant events within the server that are not warnings or errors.<br><br>none: No messages of any severity are logged by default. This value is intended to be used in conjunction with the override-severity property to define an error logger that will publish no error message beside the errors of a given category.<br><br>notice: The error log severity that is used for the most important informational messages (i.e., information that should almost always be logged but is not associated with a warning or error condition).<br><br>warning: The error log severity that is used for messages that provide information about warnings triggered during processing. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

override-severity

| | |
|---|---|
| *Synopsis* | Specifies the override severity levels for the logger based on the category of the messages. |

| | |
|---|---|
| *Description* | Each override severity level should include the category and the severity levels to log for that category, for example, core=error,info,warning. Valid categories are: core, extensions, protocol, config, log, util, schema, plugin, jeb, backend, tools, task, access-control, admin, sync, version, setup, admin-tool, dsconfig, user-defined. Valid severities are: all, error, info, warning, notice, debug. |
| *Default Value* | All messages with the default severity levels are logged. |
| *Allowed Values* | A string in the form category=severity1,severity2... |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the Console Error Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.ConsoleErrorLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## Core Schema

Core Schema define the core schema elements to load.

Core schema provider configuration.

### Parent

The Core Schema object inherits from Schema Provider.

## Core Schema Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| disabled-matching-rule<br>disabled-syntax<br>enabled | allow-attribute-types-with-no-sup-or-syntax<br>allow-zero-length-values-directory-string<br>java-class<br>json-validation-policy<br>strict-format-boolean<br>strict-format-certificates<br>strict-format-country-string<br>strict-format-jpeg-photos<br>strict-format-telephone-numbers<br>strip-syntax-min-upper-bound-attribute-type-description |

## Basic Properties

### disabled-matching-rule

| | |
|---|---|
| *Synopsis* | The set of disabled matching rules. |
| *Description* | Matching rules must be specified using the syntax: OID, or use the default value 'NONE' to specify no value. |
| *Default Value* | NONE |
| *Allowed Values* | The OID of the disabled matching rule. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### disabled-syntax

| | |
|---|---|
| *Synopsis* | The set of disabled syntaxes. |
| *Description* | Syntaxes must be specified using the syntax: OID, or use the default value 'NONE' to specify no value. |
| *Default Value* | NONE |
| *Allowed Values* | The OID of the disabled syntax, or NONE |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Schema Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

allow-attribute-types-with-no-sup-or-syntax

| | |
|---|---|
| *Synopsis* | Indicates whether the schema should allow attribute type definitions that do not declare a superior attribute type or syntax |
| *Description* | When set to true, invalid attribute type definitions will use the default syntax. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

allow-zero-length-values-directory-string

| | |
|---|---|
| *Synopsis* | Indicates whether zero-length (that is, an empty string) values are allowed for directory string. |
| *Description* | This is technically not allowed by the revised LDAPv3 specification, but some environments may require it for backward compatibility with servers that do allow it. |

| | |
|---|---|
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Core Schema implementation. |
| *Default Value* | org.opends.server.schema.CoreSchemaProvider |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.schema.SchemaProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

json-validation-policy

| | |
|---|---|
| *Synopsis* | Specifies the policy that will be used when validating JSON syntax values. |
| *Default Value* | strict |
| *Allowed Values* | disabled: JSON syntax values will not be validated and, as a result any sequence of bytes will be acceptable.<br><br>lenient: JSON syntax values must comply with RFC 7159 except: 1) comments are allowed, 2) single quotes may be used instead of double quotes, and 3) unquoted control characters are allowed in strings.<br><br>strict: JSON syntax values must strictly conform to RFC 7159. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

### strict-format-boolean

| | |
|---|---|
| *Synopsis* | Indicates whether boolean values are required to strictly comply with the standard definition for this syntax. |
| *Description* | When set to true, only "TRUE" and "FALSE" will be acceptable, per RFC 4517. When set to false, the server will accept true/false, yes/no, 1/0, on/off. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

### strict-format-certificates

| | |
|---|---|
| *Synopsis* | Indicates whether X.509 Certificate values are required to strictly comply with the standard definition for this syntax. |
| *Description* | When set to false, certificates will not be validated and, as a result any sequence of bytes will be acceptable. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

### strict-format-country-string

| | |
|---|---|
| *Synopsis* | Indicates whether country code values are required to strictly comply with the standard definition for this syntax. |
| *Description* | When set to false, country codes will not be validated and, as a result any string containing 2 characters will be acceptable. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

strict-format-jpeg-photos

| | |
|---|---|
| *Synopsis* | Indicates whether to require JPEG values to strictly comply with the standard definition for this syntax. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

strict-format-telephone-numbers

| | |
|---|---|
| *Synopsis* | Indicates whether to require telephone number values to strictly comply with the standard definition for this syntax. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

strip-syntax-min-upper-bound-attribute-type-description

| | |
|---|---|
| *Synopsis* | Indicates whether the suggested minimum upper bound appended to an attribute's syntax OID in it's schema definition Attribute Type Description is stripped off. |
| *Description* | When retrieving the server's schema, some APIs (JNDI) fail in their syntax lookup methods, because they do not parse this value correctly. This configuration option |

| | |
|---|---|
| | allows the server to be configured to provide schema definitions these APIs can parse correctly. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# CRAM-MD5 SASL Mechanism Handler

The CRAM-MD5 SASL mechanism provides the ability for clients to perform password-based authentication in a manner that does not expose their password in the clear.

Rather than including the password in the bind request, the CRAM-MD5 mechanism uses a two-step process in which the client needs only to prove that it knows the password. The server sends randomly-generated data to the client that is to be used in the process, which makes it resistant to replay attacks. The one-way message digest algorithm ensures that the original clear-text password is not exposed. Note that the algorithm used by the CRAM-MD5 mechanism requires that both the client and the server have access to the clear-text password (or potentially a value that is derived from the clear-text password). In order to authenticate to the server using CRAM-MD5, the password for a user's account must be encoded using a reversible password storage scheme that allows the server to have access to the clear-text value.

## Parent

The CRAM-MD5 SASL Mechanism Handler object inherits from SASL Mechanism Handler.

## Dependencies

CRAM-MD5 SASL Mechanism Handlers depend on the following objects:

- Identity Mapper

## CRAM-MD5 SASL Mechanism Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>identity-mapper | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the SASL mechanism handler is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name(s) of the identity mapper(s) used with this SASL mechanism handler to match the authentication ID included in the SASL bind request to the corresponding user in the directory. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br>The referenced identity mapper(s) must be enabled when the CRAM-MD5 SASL Mechanism Handler is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation. |
| *Default Value* | org.opends.server.extensions.CRAMMD5SASLMechanismHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.SASLMechanismHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Common REST Metrics HTTP Endpoint

The Common REST Metrics HTTP Endpoint provides access to OpenDJ's monitoring information via the Common REST protocol.

## Parent

The Common REST Metrics HTTP Endpoint object inherits from HTTP Endpoint.

## Common REST Metrics HTTP Endpoint Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| authorization-mechanism<br>base-path<br>enabled<br>excluded-metric-pattern<br>included-metric-pattern | java-class |

## Basic Properties

authorization-mechanism

| | |
|---|---|
| *Synopsis* | The HTTP authorization mechanisms supported by this HTTP Endpoint. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing HTTP Authorization Mechanism . |

| | |
|---|---|
| | The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-path

| | |
|---|---|
| *Synopsis* | All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Endpoint is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

excluded-metric-pattern

| | |
|---|---|
| *Synopsis* | Zero or more regular expressions identifying metrics that should not be published. The metric name prefix must not be included in the filter. Exclusion patterns take precedence over inclusion patterns. |
| *Default Value* | None |

| | |
|---|---|
| *Allowed Values* | Any valid regular expression pattern which is supported by the java.util.regex.Pattern class (see https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 8). |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

included-metric-pattern

| | |
|---|---|
| *Synopsis* | Zero or more regular expressions identifying metrics that should be published. The metric name prefix must not be included in the filter. Exclusion patterns take precedence over inclusion patterns. |
| *Default Value* | None |
| *Allowed Values* | Any valid regular expression pattern which is supported by the java.util.regex.Pattern class (see https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 8). |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Common REST Metrics HTTP Endpoint implementation. |
| *Default Value* | org.opends.server.protocols.http.CrestMetricsEndpoint |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.HttpEndpoint |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |

| | |
|---|---|
| *Read-Only* | No |

# Crypt Password Storage Scheme

The Crypt Password Storage Scheme provides a mechanism for encoding user passwords like Unix crypt does. Like on most Unix systems, the password may be encrypted using different algorithms, either Unix crypt, md5, sha256 or sha512.

This scheme contains only an implementation for the user password syntax, with a storage scheme name of "CRYPT". Like on most Unixes, the "CRYPT" storage scheme has different algorithms, the default being Unix crypt. Warning: even though Unix crypt is a one-way digest, it is very weak by today's standards. Only the first 8 characters in a password are used, and it only uses the bottom 7 bits of each character. It only supports a 12-bit salt (meaning that there are only 4096 possible ways to encode a given password), so it is vulnerable to dictionary attacks. You should therefore use this algorithm only in cases where an external application expects to retrieve the password and verify it outside of the directory, instead of by performing an LDAP bind.

## Parent

The Crypt Password Storage Scheme object inherits from Password Storage Scheme.

## Crypt Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| crypt-password-storage-encryption-algorithm<br>enabled | java-class |

## Basic Properties

crypt-password-storage-encryption-algorithm

| | |
|---|---|
| *Synopsis* | Specifies the algorithm to use to encrypt new passwords. |
| *Description* | Select the crypt algorithm to use to encrypt new passwords. The value can either be "unix", which means the password is encrypted with the weak Unix crypt algorithm, or "md5" which means the password is encrypted with the BSD MD5 algorithm and has a $1$ prefix, or "sha256" which means the password is encrypted with the SHA256 algorithm and has a $5$ prefix, or "sha512" which means the password is encrypted with the SHA512 algorithm and has a $6$ prefix. |
| *Default Value* | unix |

| | |
|---|---|
| *Allowed Values* | md5: New passwords are encrypted with the BSD MD5 algorithm.<br>sha256: New passwords are encrypted with the Unix crypt SHA256 algorithm.<br>sha512: New passwords are encrypted with the Unix crypt SHA512 algorithm.<br>unix: New passwords are encrypted with the Unix crypt algorithm. Passwords are truncated at 8 characters and the top bit of each character is ignored. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Crypt Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.CryptPasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

# Crypto Manager

The Crypto Manager provides a common interface for performing compression, decompression, hashing, encryption and other kinds of cryptographic operations.

## Dependencies

Crypto Managers depend on the following objects:

- Key Manager Provider

## Crypto Manager Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| key-manager-provider<br>key-wrapping-transformation<br>master-key-alias | cipher-key-length<br>cipher-transformation<br>digest-algorithm<br>mac-algorithm<br>mac-key-length |

## Basic Properties

key-manager-provider

| | |
|---|---|
| *Synopsis* | The name of the key manager containing the master key-pair and any deprecated master key. |
| *Description* | The master key, which is identified using the "master-key-alias" property, will be used for encrypting secrets that are generated and distributed across the deployment. Master keys may be periodically rotated, but should never be removed from the referenced key manager because they may still be needed for decryption. The alias must correspond to a PrivateKeyEntry in the keystore and is typically an RSA key-pair. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Key Manager Provider .<br><br>The referenced key manager provider must be enabled. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-wrapping-transformation

| | |
|---|---|
| *Synopsis* | The preferred key wrapping transformation for the directory server. This value must be the same for all server instances in a replication topology. |
| *Default Value* | RSA/ECB/OAEPWITHSHA-256ANDMGF1PADDING |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property will take effect immediately but will only affect cryptographic operations performed after the change. |
| *Advanced* | No |
| *Read-Only* | No |

master-key-alias

| | |
|---|---|
| *Synopsis* | The alias of the master key-pair which should be used for encrypting secrets that are generated and distributed across the deployment. |
| *Description* | Master keys may be periodically rotated, but should never be removed from the referenced key manager because they may still be needed for decryption. The master key alias reference a PrivateKeyEntry in the keystore which is typically an RSA key-pair. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

### cipher-key-length

| | |
|---|---|
| *Synopsis* | Specifies the key length in bits for the preferred cipher. |
| *Default Value* | 128 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only affect cryptographic operations performed after the change. |
| *Advanced* | Yes |
| *Read-Only* | No |

### cipher-transformation

| | |
|---|---|
| *Synopsis* | Specifies the cipher for the directory server using the syntax algorithm/mode/padding. |
| *Description* | The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding. |
| *Default Value* | AES/CBC/PKCS5Padding |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only affect cryptographic operations performed after the change. |
| *Advanced* | Yes |
| *Read-Only* | No |

### digest-algorithm

| | |
|---|---|
| *Synopsis* | Specifies the preferred message digest algorithm for the directory server. |
| *Default Value* | SHA-256 |
| *Allowed Values* | A string. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and only affect cryptographic operations performed after the change. |
| *Advanced* | Yes |
| *Read-Only* | No |

mac-algorithm

| | |
|---|---|
| *Synopsis* | Specifies the preferred MAC algorithm for the directory server. |
| *Default Value* | HmacSHA256 |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only affect cryptographic operations performed after the change. |
| *Advanced* | Yes |
| *Read-Only* | No |

mac-key-length

| | |
|---|---|
| *Synopsis* | Specifies the key length in bits for the preferred MAC algorithm. |
| *Default Value* | 128 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only affect cryptographic operations performed after the change. |
| *Advanced* | Yes |
| *Read-Only* | No |

# CSV File Access Log Publisher

CSV File Access Log Publishers publish access messages to CSV files.

## Parent

The CSV File Access Log Publisher object inherits from Common Audit Access Log Publisher.

## Dependencies

CSV File Access Log Publishers depend on the following objects:

- Log Retention Policy
- Log Rotation Policy

## CSV File Access Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| csv-delimiter-char<br>enabled<br>filtering-policy<br>key-store-file<br>key-store-pin<br>log-control-oids<br>log-directory<br>log-field-blacklist<br>log-file-name-prefix<br>retention-policy<br>rotation-policy<br>tamper-evident | asynchronous<br>auto-flush<br>csv-eol-symbols<br>csv-quote-char<br>java-class<br>signature-time-interval<br>suppress-internal-operations<br>suppress-synchronization-operations |

## Basic Properties

csv-delimiter-char

| | |
|---|---|
| *Synopsis* | The delimiter character to use when writing in CSV format. |
| *Default Value* | , |
| *Allowed Values* | The delimiter character to use when writing in CSV format. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filtering-policy

| | |
|---|---|
| *Synopsis* | Specifies how filtering criteria should be applied to log records. |
| *Default Value* | no-filtering |
| *Allowed Values* | exclusive: Records must not match any of the filtering criteria in order to be logged.<br>inclusive: Records must match at least one of the filtering criteria in order to be logged.<br>no-filtering: No filtering will be performed, and all records will be logged. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-store-file

| | |
|---|---|
| *Synopsis* | Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. |
| *Description* | Changes to this property will take effect the next time that the key store is accessed. |
| *Default Value* | None |
| *Allowed Values* | A path to an existing file that is readable by the server. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

key-store-pin

| | |
|---|---|
| *Synopsis* | Specifies the clear-text PIN needed to access the CSV File Access Log Publisher . |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property will take effect the next time that the CSV File Access Log Publisher is accessed. |
| *Advanced* | No |
| *Read-Only* | No |

log-control-oids

| | |
|---|---|
| *Synopsis* | Specifies whether control OIDs will be included in operation log records. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-directory

| | |
|---|---|
| *Synopsis* | The directory to use for the log files generated by the CSV File Access Log Publisher. The path to the directory is relative to the server root. |
| *Default Value* | logs |
| *Allowed Values* | A path to an existing directory that is readable and writable by the server. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

log-field-blacklist

| | |
|---|---|
| *Synopsis* | List of fields that the server omits from access log messages. |
| *Description* | Valid values for this property are JSON paths for fields present in the log file. |
| *Default Value* | No message elements are blacklisted by default |
| *Allowed Values* | A JSON path to an existing object of the access event definition. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-file-name-prefix

| | |
|---|---|
| *Synopsis* | File name prefix (without extension) for CSV and JSON file based access log publishers. |
| *Default Value* | ldap-access |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

retention-policy

| | |
|---|---|
| *Synopsis* | The retention policy to use for the CSV File Access Log Publisher . |
| *Description* | When multiple policies are used, log files are cleaned when any of the policy's conditions are met. |
| *Default Value* | No retention policy is used and log files are never cleaned. |
| *Allowed Values* | The name of an existing Log Retention Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

rotation-policy

| | |
|---|---|
| *Synopsis* | The rotation policy to use for the CSV File Access Log Publisher . |
| *Description* | When multiple policies are used, rotation will occur if any policy's conditions are met. |
| *Default Value* | No rotation policy is used and log rotation will not occur. |
| *Allowed Values* | The name of an existing Log Rotation Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

tamper-evident

| | |
|---|---|
| *Synopsis* | Specifies whether the log should be signed in order to detect tampering. |
| *Description* | Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

asynchronous

| | |
|---|---|
| *Synopsis* | Indicates whether the CSV File Access Log Publisher will publish records asynchronously. |
| *Default Value* | true |

| | |
|---|---|
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

auto-flush

| | |
|---|---|
| *Synopsis* | Specifies whether to flush the writer after every log record. |
| *Description* | If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

csv-eol-symbols

| | |
|---|---|
| *Synopsis* | The string that marks the end of a line. |
| *Default Value* | Use the platform specific end of line character sequence. |
| *Allowed Values* | The string that marks the end of a line. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

csv-quote-char

| | |
|---|---|
| *Synopsis* | The character to append and prepend to a CSV field when writing in CSV format. |
| *Default Value* | " |

| | |
|---|---|
| *Allowed Values* | The quote character to use when writting in CSV format. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the CSV File Access Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.CsvFileAccessLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

signature-time-interval

| | |
|---|---|
| *Synopsis* | Specifies the interval at which to sign the log file when the tamper-evident option is enabled. |
| *Default Value* | 3s |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 1 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

suppress-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users. |

| | |
|---|---|
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

suppress-synchronization-operations

| | |
|---|---|
| *Synopsis* | Indicates whether access messages that are generated by synchronization operations should be suppressed. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# CSV File HTTP Access Log Publisher

CSV File HTTP Access Log Publishers publish HTTP access messages to CSV files.

## Parent

The CSV File HTTP Access Log Publisher object inherits from HTTP Access Log Publisher.

## Dependencies

CSV File HTTP Access Log Publishers depend on the following objects:

- Log Retention Policy
- Log Rotation Policy

# CSV File HTTP Access Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| csv-delimiter-char<br>enabled<br>key-store-file<br>key-store-pin<br>log-directory<br>log-field-blacklist<br>log-field-whitelist<br>log-file-name-prefix<br>retention-policy<br>rotation-policy<br>tamper-evident | asynchronous<br>auto-flush<br>csv-eol-symbols<br>csv-quote-char<br>java-class<br>signature-time-interval |

## Basic Properties

### csv-delimiter-char

| | |
|---|---|
| *Synopsis* | The delimiter character to use when writing in CSV format. |
| *Default Value* | , |
| *Allowed Values* | The delimiter character to use when writing in CSV format. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

key-store-file

| | |
|---|---|
| *Synopsis* | Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. |
| *Description* | Changes to this property will take effect the next time that the key store is accessed. |
| *Default Value* | None |
| *Allowed Values* | A path to an existing file that is readable by the server. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-store-pin

| | |
|---|---|
| *Synopsis* | Specifies the clear-text PIN needed to access the CSV File HTTP Access Log Publisher . |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property will take effect the next time that the CSV File HTTP Access Log Publisher is accessed. |
| *Advanced* | No |
| *Read-Only* | No |

log-directory

| | |
|---|---|
| *Synopsis* | The directory to use for the log files generated by the CSV File HTTP Access Log Publisher. The path to the directory is relative to the server root. |
| *Default Value* | logs |
| *Allowed Values* | A path to an existing directory that is readable and writable by the server. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

log-field-blacklist

| | |
|---|---|
| *Synopsis* | List of fields that the server omits from access log messages. |
| *Description* | Valid values for this property are JSON paths for fields present in the log file. |
| *Default Value* | No message elements are blacklisted by default |
| *Allowed Values* | A JSON path to an existing object of the access event definition. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-field-whitelist

| | |
|---|---|
| *Synopsis* | List of fields that the server includes in access log messages. |
| *Description* | Valid values for this property are JSON paths for fields present in the log file. |
| *Default Value* | Fields not containing sensitive information are whitelisted by default. |
| *Allowed Values* | A JSON path to an existing object of the access event definition. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-file-name-prefix

| | |
|---|---|
| *Synopsis* | File name prefix (without extension) for CSV and JSON file based access log publishers. |
| *Default Value* | http-access |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

retention-policy

| | |
|---|---|
| *Synopsis* | The retention policy to use for the CSV File HTTP Access Log Publisher . |
| *Description* | When multiple policies are used, log files are cleaned when any of the policy's conditions are met. |
| *Default Value* | No retention policy is used and log files are never cleaned. |
| *Allowed Values* | The name of an existing Log Retention Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

rotation-policy

| | |
|---|---|
| *Synopsis* | The rotation policy to use for the CSV File HTTP Access Log Publisher . |
| *Description* | When multiple policies are used, rotation will occur if any policy's conditions are met. |
| *Default Value* | No rotation policy is used and log rotation will not occur. |
| *Allowed Values* | The name of an existing Log Rotation Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

tamper-evident

| | |
|---|---|
| *Synopsis* | Specifies whether the log should be signed in order to detect tampering. |
| *Description* | Every log record will be signed, making it possible to verify that the log has not been tampered with. This feature has a significative impact on performance of the server. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

asynchronous

| | |
|---|---|
| *Synopsis* | Indicates whether the CSV File HTTP Access Log Publisher will publish records asynchronously. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

auto-flush

| | |
|---|---|
| *Synopsis* | Specifies whether to flush the writer after every log record. |
| *Description* | If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

csv-eol-symbols

| | |
|---|---|
| *Synopsis* | The string that marks the end of a line. |
| *Default Value* | Use the platform specific end of line character sequence. |
| *Allowed Values* | The string that marks the end of a line. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

csv-quote-char

| | |
|---|---|
| *Synopsis* | The character to append and prepend to a CSV field when writing in CSV format. |
| *Default Value* | " |
| *Allowed Values* | The quote character to use when writing in CSV format. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the CSV File HTTP Access Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

signature-time-interval

| | |
|---|---|
| *Synopsis* | Specifies the interval at which to sign the log file when secure option is enabled. |
| *Default Value* | 3s |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 1 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |

| | |
|---|---|
| *Read-Only* | No |

# Debug Log Publisher

*This is an abstract object type that cannot be instantiated.*

Debug Log Publishers are responsible for distributing debug log messages from the debug logger to a destination.

Debug log messages provide information that can be used for debugging or troubleshooting problems in the server, or for providing more detailed information about the processing that the server performs.

## Debug Log Publishers

The following Debug Log Publishers are available:

- File Based Debug Log Publisher

These Debug Log Publishers inherit the properties described below.

## Parent

The Debug Log Publisher object inherits from Log Publisher.

## Dependencies

The following objects belong to Debug Log Publishers:

- Debug Target

## Debug Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| default-debug-exceptions-only<br>default-include-throwable-cause<br>default-omit-method-entry-arguments<br>default-omit-method-return-value<br>default-throwable-stack-frames<br>enabled<br>java-class |

## Basic Properties

### default-debug-exceptions-only

| | |
|---|---|
| *Synopsis* | Indicates whether only logs with exception should be logged. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### default-include-throwable-cause

| | |
|---|---|
| *Synopsis* | Indicates whether to include the cause of exceptions in exception thrown and caught messages logged by default. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### default-omit-method-entry-arguments

| | |
|---|---|
| *Synopsis* | Indicates whether to include method arguments in debug messages logged by default. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

default-omit-method-return-value

| | |
|---|---|
| *Synopsis* | Indicates whether to include the return value in debug messages logged by default. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

default-throwable-stack-frames

| | |
|---|---|
| *Synopsis* | Indicates the number of stack frames to include in the stack trace for method entry and exception thrown messages. |
| *Default Value* | 2147483647 |
| *Allowed Values* | An integer.<br>Lower limit: 0.<br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the Debug Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.DebugLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Debug Target

Debug Targets define the types of messages logged by the debug logPublisher.

Debug targets allow for fine-grain control of which messages are logged based on the package, class, or method that generated the message. Each debug target configuration entry resides below the entry with RDN of "cn=Debug Target" immediately below the parent ds-cfg-debug-log-publisher entry.

## Dependencies

The following objects have Debug Targets:

- Debug Log Publisher

## Debug Target Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| debug-exceptions-only<br>debug-scope<br>enabled<br>include-throwable-cause |

| Basic Properties |
| --- |
| omit-method-entry-arguments<br>omit-method-return-value<br>throwable-stack-frames |

## Basic Properties

### debug-exceptions-only

| | |
| --- | --- |
| *Synopsis* | Indicates whether only logs with exception should be logged. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### debug-scope

| | |
| --- | --- |
| *Synopsis* | Specifies the fully-qualified OpenDJ Java package, class, or method affected by the settings in this target definition. Use the number character (#) to separate the class name and the method name (that is, org.opends.server.core.DirectoryServer#startUp). |
| *Default Value* | None |
| *Allowed Values* | The fully-qualified OpenDJ Java package, class, or method name. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

### enabled

| | |
| --- | --- |
| *Synopsis* | Indicates whether the Debug Target is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

include-throwable-cause

| | |
|---|---|
| *Synopsis* | Specifies the property to indicate whether to include the cause of exceptions in exception thrown and caught messages. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

omit-method-entry-arguments

| | |
|---|---|
| *Synopsis* | Specifies the property to indicate whether to include method arguments in debug messages. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

omit-method-return-value

| | |
|---|---|
| *Synopsis* | Specifies the property to indicate whether to include the return value in debug messages. |
| *Default Value* | false |
| *Allowed Values* | true |

| | |
|---|---|
| | false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

throwable-stack-frames

| | |
|---|---|
| *Synopsis* | Specifies the property to indicate the number of stack frames to include in the stack trace for method entry and exception thrown messages. |
| *Default Value* | 0 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Dictionary Password Validator

The Dictionary Password Validator determines whether a proposed password is acceptable based on whether the given password value appears in a provided dictionary file.

A large dictionary file is provided with the server, but the administrator can supply an alternate dictionary. In this case, then the dictionary must be a plain-text file with one word per line.

## Parent

The Dictionary Password Validator object inherits from Password Validator.

## Dictionary Password Validator Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| case-sensitive-validation | java-class |

| Basic Properties | Advanced Properties |
|---|---|
| check-substrings<br>dictionary-file<br>enabled<br>min-substring-length<br>test-reversed-password | |

## Basic Properties

### case-sensitive-validation

| | |
|---|---|
| *Synopsis* | Indicates whether this password validator is to treat password characters in a case-sensitive manner. |
| *Description* | If it is set to true, then the validator rejects a password only if it appears in the dictionary with exactly the same capitalization as provided by the user. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### check-substrings

| | |
|---|---|
| *Synopsis* | Indicates whether this password validator is to match portions of the password string against dictionary words. |
| *Description* | If "false" then only match the entire password against words otherwise ("true") check whether the password contains words. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### dictionary-file

| | |
|---|---|
| *Synopsis* | Specifies the path to the file containing a list of words that cannot be used as passwords. |
| *Description* | It should be formatted with one word per line. The value can be an absolute path or a path that is relative to the OpenDJ instance root. |
| *Default Value* | None |
| *Allowed Values* | The path to any text file contained on the system that is readable by the server. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the password validator is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

min-substring-length

| | |
|---|---|
| *Synopsis* | Indicates the minimal length of the substring within the password in case substring checking is enabled. |
| *Description* | If "check-substrings" option is set to true, then this parameter defines the length of the smallest word which should be used for substring matching. Use with caution because values below 3 might disqualify valid passwords. |
| *Default Value* | 5 |
| *Allowed Values* | An integer.<br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

test-reversed-password

| | |
|---|---|
| *Synopsis* | Indicates whether this password validator is to test the reversed value of the provided password as well as the order in which it was given. |
| *Description* | For example, if the user provides a new password of "password" and this configuration attribute is set to true, then the value "drowssap" is also tested against attribute values in the user's entry. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the password validator implementation. |
| *Default Value* | org.opends.server.extensions.DictionaryPasswordValidator |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordValidator |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## DIGEST-MD5 SASL Mechanism Handler

The DIGEST-MD5 SASL mechanism is used to perform all processing related to SASL DIGEST-MD5 authentication.

The DIGEST-MD5 SASL mechanism is very similar to the CRAM-MD5 mechanism in that it allows for password-based authentication without exposing the password in the clear (although it does require that both the client and the server have access to the clear-text password). Like the CRAM-MD5 mechanism, it uses data that is randomly generated by the server to make it resistant to replay attacks, but it also includes randomly-generated data from the client, which makes it also resistant to problems resulting from weak server-side random number generation.

## Parent

The DIGEST-MD5 SASL Mechanism Handler object inherits from SASL Mechanism Handler.

## Dependencies

DIGEST-MD5 SASL Mechanism Handlers depend on the following objects:

- Identity Mapper

## DIGEST-MD5 SASL Mechanism Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>identity-mapper<br>quality-of-protection<br>realm<br>server-fqdn | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the SASL mechanism handler is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name(s) of the identity mappers that are to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br><br>The referenced identity mapper(s) must be enabled when the DIGEST-MD5 SASL Mechanism Handler is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

quality-of-protection

| | |
|---|---|
| *Synopsis* | The name of a property that specifies the quality of protection the server will support. |
| *Default Value* | none |
| *Allowed Values* | confidentiality: Quality of protection equals authentication with integrity and confidentiality protection.<br><br>integrity: Quality of protection equals authentication with integrity protection.<br><br>none: QOP equals authentication only. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

realm

| | |
|---|---|
| *Synopsis* | Specifies the realms that is to be used by the server for DIGEST-MD5 authentication. |
| *Description* | If this value is not provided, then the server defaults to use the fully qualified hostname of the machine. |
| *Default Value* | If this value is not provided, then the server defaults to use the fully qualified hostname of the machine. |

| | |
|---|---|
| *Allowed Values* | Any realm string that does not contain a comma. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

server-fqdn

| | |
|---|---|
| *Synopsis* | Specifies the DNS-resolvable fully-qualified domain name for the server that is used when validating the digest-uri parameter during the authentication process. |
| *Description* | If this configuration attribute is present, then the server expects that clients use a digest-uri equal to "ldap/" followed by the value of this attribute. For example, if the attribute has a value of "directory.example.com", then the server expects clients to use a digest-uri of "ldap/directory.example.com". If no value is provided, then the server does not attempt to validate the digest-uri provided by the client and accepts any value. |
| *Default Value* | The server attempts to determine the fully-qualified domain name dynamically. |
| *Allowed Values* | The fully-qualified address that is expected for clients to use when connecting to the server and authenticating via DIGEST-MD5. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation. |
| *Default Value* | org.opends.server.extensions.DigestMD5SASLMechanismHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.SASLMechanismHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

# DSEE Compatible Access Control Handler

The DSEE Compatible Access Control Handler provides an implementation that uses syntax compatible with the Sun Java System Directory Server Enterprise Edition access control handlers.

## Parent

The DSEE Compatible Access Control Handler object inherits from Access Control Handler.

## DSEE Compatible Access Control Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>global-aci | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Access Control Handler is enabled. If set to FALSE, then any client (including unauthenticated or anonymous clients) is allowed to bind to the server and any connection with the "bypass-acl" privilege is allowed to perform any operation. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

global-aci

| | |
|---|---|
| *Synopsis* | Defines global access control rules. |
| *Description* | Global access control rules apply to all entries anywhere in the data managed by the OpenDJ directory server. The global access control rules may be overridden by more specific access control rules placed in the data. |
| *Default Value* | No global access control rules are defined, which means that no access is allowed for any data in the server unless specifically granted by access control rules in the data. |
| *Allowed Values* | An access control instruction (ACI). |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the DSEE Compatible Access Control Handler implementation. |
| *Default Value* | org.opends.server.authorization.dseecompat.AciHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.AccessControlHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Dynamic Group Implementation

The Dynamic Group Implementation provides a grouping mechanism in which the group membership is determined based on criteria defined in one or more LDAP URLs.

### Parent

The Dynamic Group Implementation object inherits from Group Implementation.

# Dynamic Group Implementation Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Group Implementation is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Dynamic Group Implementation implementation. |
| *Default Value* | org.opends.server.extensions.DynamicGroup |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.Group |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Entity Tag Virtual Attribute

The Entity Tag Virtual Attribute ensures that all entries contain an "entity tag" or "Etag" as defined in section 3.11 of RFC 2616.

The entity tag may be used by clients, in conjunction with the assertion control, for optimistic concurrency control, as a way to help prevent simultaneous updates of an entry from conflicting with each other.

## Parent

The Entity Tag Virtual Attribute object inherits from Virtual Attribute.

## Entity Tag Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>checksum-algorithm<br>enabled<br>excluded-attribute<br>filter<br>group-dn<br>scope | conflict-behavior<br>java-class |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | etag |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

checksum-algorithm

| | |
|---|---|
| *Synopsis* | The algorithm which should be used for calculating the entity tag checksum value. |
| *Default Value* | adler-32 |
| *Allowed Values* | adler-32: The Adler-32 checksum algorithm which is almost as reliable as a CRC-32 but can be computed much faster.<br><br>crc-32: The CRC-32 checksum algorithm. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### excluded-attribute

| | |
|---|---|
| *Synopsis* | The list of attributes which should be ignored when calculating the entity tag checksum value. |
| *Description* | Certain attributes like "ds-sync-hist" may vary between replicas due to different purging schedules and should not be included in the checksum. |
| *Default Value* | ds-sync-hist |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br><br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | real-overrides-virtual |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.<br><br>real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | org.opends.server.extensions.EntityTagVirtualAttributeProvider |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Entry Cache

*This is an abstract object type that cannot be instantiated.*

Entry Caches are responsible for caching entries which are likely to be accessed by client applications in order to improve OpenDJ directory server performance.

## Entry Caches

The following Entry Caches are available:

- FIFO Entry Cache
- Soft Reference Entry Cache

These Entry Caches inherit the properties described below.

## Entry Cache Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties |
| --- |
| cache-level<br>enabled<br>java-class |

## Basic Properties

### cache-level

| | |
| --- | --- |
| *Synopsis* | Specifies the cache level in the cache order if more than one instance of the cache is configured. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### enabled

| | |
| --- | --- |
| *Synopsis* | Indicates whether the Entry Cache is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### java-class

| | |
| --- | --- |
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Entry Cache implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements: |

| | |
|---|---|
| | • org.opends.server.api.EntryCache |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# entryDN Virtual Attribute

The entryDN Virtual Attribute generates the entryDN operational attribute in directory entries, which contains a normalized form of the entry's DN.

This attribute is defined in the draft-zeilenga-ldap-entrydn Internet Draft and contains the DN of the entry in which it is contained. This component provides the ability to use search filters containing the entry's DN.

## Parent

The entryDN Virtual Attribute object inherits from Virtual Attribute.

## entryDN Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>enabled<br>filter<br>group-dn<br>scope | conflict-behavior<br>java-class |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | entryDN |

| | |
|---|---|
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |

| | |
|---|---|
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br><br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | virtual-overrides-real |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.<br><br>real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | org.opends.server.extensions.EntryDNVirtualAttributeProvider |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

# entryUUID Plugin

The entryUUID Plugin generates values for the entryUUID operational attribute whenever an entry is added via protocol or imported from LDIF.

The entryUUID plug-in ensures that all entries added to the server, whether through an LDAP add operation or via an LDIF import, are assigned an entryUUID operational attribute if they do not already have one. The entryUUID attribute contains a universally unique identifier that can be used to identify an entry in a manner that does not change (even in the event of a modify DN operation). This plug-in generates a random UUID for entries created by an add operation, but the UUID is constructed from the DN of the entry during an LDIF import (which means that the same LDIF file can be imported on different systems but still get the same value for the entryUUID attribute). This behavior is based on the specification contained in RFC 4530. The implementation for the entry UUID plug-in is contained in the org.opends.server.plugins.EntryUUIDPlugin class. It must be configured with the preOperationAdd and ldifImport plug-in types, but it does not have any other custom configuration. This plug-in must be enabled in any directory that is intended to be used in a synchronization environment.

## Parent

The entryUUID Plugin object inherits from Plugin.

## entryUUID Plugin Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | invoke-for-internal-operations<br>java-class<br>plugin-type |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true |

| | |
|---|---|
| | false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

invoke-for-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in should be invoked for internal operations. |
| *Description* | Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the plug-in implementation. |
| *Default Value* | org.opends.server.plugins.EntryUUIDPlugin |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.plugin.DirectoryServerPlugin |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

plugin-type

| | |
|---|---|
| *Synopsis* | Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked. |
| *Default Value* | ldifimport<br><br>preoperationadd |
| *Allowed Values* | initialization: Invoked at the initialization of the directory server.<br><br>intermediateresponse: Invoked before sending an intermediate repsonse message to the client.<br><br>ldifimport: Invoked for each entry read during an LDIF import.<br><br>ldifimportbegin: Invoked at the beginning of an LDIF import session.<br><br>ldifimportend: Invoked at the end of an LDIF import session.<br><br>postconnect: Invoked whenever a new connection is established to the server.<br><br>postdisconnect: Invoked whenever an existing connection is terminated (by either the client or the server).<br><br>postoperationabandon: Invoked after completing the abandon processing.<br><br>postoperationadd: Invoked after completing the core add processing but before sending the response to the client.<br><br>postoperationbind: Invoked after completing the core bind processing but before sending the response to the client.<br><br>postoperationcompare: Invoked after completing the core compare processing but before sending the response to the client.<br><br>postoperationdelete: Invoked after completing the core delete processing but before sending the response to the client.<br><br>postoperationextended: Invoked after completing the core extended processing but before sending the response to the client.<br><br>postoperationmodify: Invoked after completing the core modify processing but before sending the response to the client.<br><br>postoperationmodifydn: Invoked after completing the core modify DN processing but before sending the response to the client.<br><br>postoperationsearch: Invoked after completing the core search processing but before sending the response to the client.<br><br>postoperationunbind: Invoked after completing the unbind processing.<br><br>postresponseadd: Invoked after sending the add response to the client.<br><br>postresponsebind: Invoked after sending the bind response to the client. |

postresponsecompare: Invoked after sending the compare response to the client.

postresponsedelete: Invoked after sending the delete response to the client.

postresponseextended: Invoked after sending the extended response to the client.

postresponsemodify: Invoked after sending the modify response to the client.

postresponsemodifydn: Invoked after sending the modify DN response to the client.

postresponsesearch: Invoked after sending the search result done message to the client.

postsynchronizationadd: Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete: Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify: Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn: Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd: Invoked prior to performing the core add processing.

preoperationbind: Invoked prior to performing the core bind processing.

preoperationcompare: Invoked prior to performing the core compare processing.

preoperationdelete: Invoked prior to performing the core delete processing.

preoperationextended: Invoked prior to performing the core extended processing.

preoperationmodify: Invoked prior to performing the core modify processing.

preoperationmodifydn: Invoked prior to performing the core modify DN processing.

preoperationsearch: Invoked prior to performing the core search processing.

preparseabandon: Invoked prior to parsing an abandon request.

preparseadd: Invoked prior to parsing an add request.

preparsebind: Invoked prior to parsing a bind request.

preparsecompare: Invoked prior to parsing a compare request.

preparsedelete: Invoked prior to parsing a delete request.

preparseextended: Invoked prior to parsing an extended request.

preparsemodify: Invoked prior to parsing a modify request.

| | |
|---|---|
| | preparsemodifydn: Invoked prior to parsing a modify DN request.<br>preparsesearch: Invoked prior to parsing a search request.<br>preparseunbind: Invoked prior to parsing an unbind request.<br>searchresultentry: Invoked before sending a search result entry to the client.<br>searchresultreference: Invoked before sending a search result reference to the client.<br>shutdown: Invoked during a graceful directory server shutdown.<br>startup: Invoked during the directory server startup process.<br>subordinatedelete: Invoked in the course of deleting a subordinate entry of a delete operation.<br>subordinatemodifydn: Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# entryUUID Virtual Attribute

The entryUUID Virtual Attribute ensures that all entries contained in private backends have values for the entryUUID operational attribute.

The entryUUID values are generated based on a normalized representation of the entry's DN, which does not cause a consistency problem because OpenDJ does not allow modify DN operations to be performed in private backends.

## Parent

The entryUUID Virtual Attribute object inherits from Virtual Attribute.

## entryUUID Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type | conflict-behavior |

| Basic Properties | Advanced Properties |
|---|---|
| base-dn<br>enabled<br>filter<br>group-dn<br>scope | java-class |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | entryUUID |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |

| | |
|---|---|
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | real-overrides-virtual |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.<br>real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | org.opends.server.extensions.EntryUUIDVirtualAttributeProvider |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Error Log Account Status Notification Handler

The Error Log Account Status Notification Handler is a notification handler that writes information to the server error log whenever an appropriate account status event occurs.

## Parent

The Error Log Account Status Notification Handler object inherits from Account Status Notification Handler.

## Error Log Account Status Notification Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| account-status-notification-type<br>enabled | java-class |

## Basic Properties

account-status-notification-type

| | |
|---|---|
| *Synopsis* | Indicates which types of event can trigger an account status notification. |
| *Default Value* | None |
| *Allowed Values* | account-disabled: Generate a notification whenever a user account has been disabled by an administrator. |

| | |
|---|---|
| | account-enabled: Generate a notification whenever a user account has been enabled by an administrator.<br><br>account-expired: Generate a notification whenever a user authentication has failed because the account has expired.<br><br>account-idle-locked: Generate a notification whenever a user account has been locked because it was idle for too long.<br><br>account-permanently-locked: Generate a notification whenever a user account has been permanently locked after too many failed attempts.<br><br>account-reset-locked: Generate a notification whenever a user account has been locked, because the password had been reset by an administrator but not changed by the user within the required interval.<br><br>account-temporarily-locked: Generate a notification whenever a user account has been temporarily locked after too many failed attempts.<br><br>account-unlocked: Generate a notification whenever a user account has been unlocked by an administrator.<br><br>password-changed: Generate a notification whenever a user changes his/her own password.<br><br>password-expired: Generate a notification whenever a user authentication has failed because the password has expired.<br><br>password-expiring: Generate a notification whenever a password expiration warning is encountered for a user password for the first time.<br><br>password-reset: Generate a notification whenever a user's password is reset by an administrator. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Error Log Account Status Notification Handler implementation. |
| *Default Value* | org.opends.server.extensions.ErrorLogAccountStatusNotificationHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.AccountStatusNotificationHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Error Log Publisher

*This is an abstract object type that cannot be instantiated.*

Error Log Publishers are responsible for distributing error log messages from the error logger to a destination.

Error log messages provide information about any warnings, errors, or significant events that are encountered during server processing.

### Error Log Publishers

The following Error Log Publishers are available:

- Console Error Log Publisher
- File Based Error Log Publisher

These Error Log Publishers inherit the properties described below.

## Parent

The Error Log Publisher object inherits from Log Publisher.

## Error Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| default-severity<br>enabled<br>java-class<br>override-severity |

## Basic Properties

default-severity

| | |
| --- | --- |
| *Synopsis* | Specifies the default severity levels for the logger. |
| *Default Value* | error<br><br>warning |
| *Allowed Values* | all: Messages of all severity levels are logged.<br><br>debug: The error log severity that is used for messages that provide debugging information triggered during processing.<br><br>error: The error log severity that is used for messages that provide information about errors which may force the server to shut down or operate in a significantly degraded state.<br><br>info: The error log severity that is used for messages that provide information about significant events within the server that are not warnings or errors.<br><br>none: No messages of any severity are logged by default. This value is intended to be used in conjunction with the override-severity property to define an error logger that will publish no error message beside the errors of a given category.<br><br>notice: The error log severity that is used for the most important informational messages (i.e., information that should almost always be logged but is not associated with a warning or error condition).<br><br>warning: The error log severity that is used for messages that provide information about warnings triggered during processing. |
| *Multi-valued* | Yes |
| *Required* | No |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the Error Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.ErrorLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

override-severity

| | |
|---|---|
| *Synopsis* | Specifies the override severity levels for the logger based on the category of the messages. |
| *Description* | Each override severity level should include the category and the severity levels to log for that category, for example, core=error,info,warning. Valid categories are: core, extensions, protocol, config, log, util, schema, plugin, jeb, backend, tools, task, access-control, admin, sync, version, setup, admin-tool, dsconfig, user-defined. Valid severities are: all, error, info, warning, notice, debug. |
| *Default Value* | All messages with the default severity levels are logged. |
| *Allowed Values* | A string in the form category=severity1,severity2... |

| | |
|---|---|
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Exact Match Identity Mapper

The Exact Match Identity Mapper maps an identifier string to user entries by searching for the entry containing a specified attribute whose value is the provided identifier. For example, the username provided by the client for DIGEST-MD5 authentication must match the value of the uid attribute

## Parent

The Exact Match Identity Mapper object inherits from Identity Mapper.

## Exact Match Identity Mapper Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>match-attribute<br>match-base-dn | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Identity Mapper is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

match-attribute

| | |
|---|---|
| *Synopsis* | Specifies the attribute whose value should exactly match the ID string provided to this identity mapper. |
| *Description* | At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry. The internal search performed includes a logical OR across all of these values. |
| *Default Value* | uid |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

match-base-dn

| | |
|---|---|
| *Synopsis* | Specifies the set of base DNs below which to search for users. |
| *Description* | The base DNs will be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all specified base DNs. |
| *Default Value* | The server searches below all public naming contexts local to the server. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Exact Match Identity Mapper implementation. |

| | |
|---|---|
| *Default Value* | org.opends.server.extensions.ExactMatchIdentityMapper |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.IdentityMapper |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Extended Operation Handler

*This is an abstract object type that cannot be instantiated.*

Extended Operation Handlers processes the different types of extended operations in the server.

## Extended Operation Handlers

The following Extended Operation Handlers are available:

- Cancel Extended Operation Handler
- Get Connection ID Extended Operation Handler
- Get Symmetric Key Extended Operation Handler
- Password Modify Extended Operation Handler
- Password Policy State Extended Operation Handler
- StartTLS Extended Operation Handler
- Who Am I Extended Operation Handler

These Extended Operation Handlers inherit the properties described below.

## Extended Operation Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| enabled |

| Basic Properties |
| --- |
| java-class |

## Basic Properties

enabled

| | |
| --- | --- |
| *Synopsis* | Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server). |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
| --- | --- |
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Extended Operation Handler implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.ExtendedOperationHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# External Access Log Publisher

External Access Log Publishers publish access messages to an external handler.

## Parent

The External Access Log Publisher object inherits from Common Audit Access Log Publisher.

# External Access Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| config-file<br>enabled<br>filtering-policy<br>log-control-oids<br>log-field-blacklist | java-class<br>suppress-internal-operations<br>suppress-synchronization-operations |

## Basic Properties

config-file

| | |
|---|---|
| *Synopsis* | The JSON configuration file that defines the External Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root. |
| *Default Value* | None |
| *Allowed Values* | A path to an existing file that is readable by the server. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filtering-policy

| | |
|---|---|
| *Synopsis* | Specifies how filtering criteria should be applied to log records. |
| *Default Value* | no-filtering |
| *Allowed Values* | exclusive: Records must not match any of the filtering criteria in order to be logged.<br><br>inclusive: Records must match at least one of the filtering criteria in order to be logged.<br><br>no-filtering: No filtering will be performed, and all records will be logged. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-control-oids

| | |
|---|---|
| *Synopsis* | Specifies whether control OIDs will be included in operation log records. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-field-blacklist

| | |
|---|---|
| *Synopsis* | List of fields that the server omits from access log messages. |
| *Description* | Valid values for this property are JSON paths for fields present in the log file. |
| *Default Value* | No message elements are blacklisted by default |
| *Allowed Values* | A JSON path to an existing object of the access event definition. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

### java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the External Access Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.ExternalAccessLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

### suppress-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

### suppress-synchronization-operations

| | |
|---|---|
| *Synopsis* | Indicates whether access messages that are generated by synchronization operations should be suppressed. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# External HTTP Access Log Publisher

External HTTP Access Log Publishers publish HTTP access messages to an external handler.

## Parent

The External HTTP Access Log Publisher object inherits from HTTP Access Log Publisher.

## External HTTP Access Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| config-file<br>enabled<br>log-field-blacklist<br>log-field-whitelist | java-class |

## Basic Properties

config-file

| | |
|---|---|
| *Synopsis* | The JSON configuration file that defines the External HTTP Access Log Publisher. The content of the JSON configuration file depends on the type of external audit event handler. The path to the file is relative to the server root. |
| *Default Value* | None |
| *Allowed Values* | A path to an existing file that is readable by the server. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-field-blacklist

| | |
|---|---|
| *Synopsis* | List of fields that the server omits from access log messages. |
| *Description* | Valid values for this property are JSON paths for fields present in the log file. |
| *Default Value* | No message elements are blacklisted by default |
| *Allowed Values* | A JSON path to an existing object of the access event definition. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-field-whitelist

| | |
|---|---|
| *Synopsis* | List of fields that the server includes in access log messages. |
| *Description* | Valid values for this property are JSON paths for fields present in the log file. |
| *Default Value* | Fields not containing sensitive information are whitelisted by default. |
| *Allowed Values* | A JSON path to an existing object of the access event definition. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the External HTTP Access Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# External SASL Mechanism Handler

The External SASL Mechanism Handler performs all processing related to SASL EXTERNAL authentication.

## Parent

The External SASL Mechanism Handler object inherits from SASL Mechanism Handler.

## Dependencies

External SASL Mechanism Handlers depend on the following objects:

- Certificate Mapper

## External SASL Mechanism Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| certificate-attribute<br>certificate-mapper<br>certificate-validation-policy<br>enabled | java-class |

## Basic Properties

certificate-attribute

| | |
|---|---|
| *Synopsis* | Specifies the name of the attribute to hold user certificates. |
| *Description* | This property must specify the name of a valid attribute type defined in the server schema. |
| *Default Value* | userCertificate |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

certificate-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name(s) of the certificate mapper(s) that should be used to match client certificates to user entries. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Certificate Mapper .<br><br>The referenced certificate mapper(s) must be enabled when the External SASL Mechanism Handler is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

certificate-validation-policy

| | |
|---|---|
| *Synopsis* | Indicates whether to attempt to validate the peer certificate against a certificate held in the user's entry. |
| *Default Value* | None |
| *Allowed Values* | always: Always require the peer certificate to be present in the user's entry.<br><br>ifpresent: If the user's entry contains one or more certificates, require that one of them match the peer certificate.<br><br>never: Do not look for the peer certificate to be present in the user's entry. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the SASL mechanism handler is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation. |
| *Default Value* | org.opends.server.extensions.ExternalSASLMechanismHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.SASLMechanismHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## FIFO Entry Cache

FIFO Entry Caches use a FIFO queue to keep track of the cached entries.

Entries that have been in the cache the longest are the most likely candidates for purging if space is needed. In contrast to other cache structures, the selection of entries to purge is not based on how frequently or recently the entries have been accessed. This requires significantly less locking (it will only be required when an entry is added or removed from the cache, rather than each time an entry

is accessed). Cache sizing is based on the percentage of free memory within the JVM, such that if enough memory is free, then adding an entry to the cache will not require purging, but if more than a specified percentage of the available memory within the JVM is already consumed, then one or more entries will need to be removed in order to make room for a new entry. It is also possible to configure a maximum number of entries for the cache. If this is specified, then the number of entries will not be allowed to exceed this value, but it may not be possible to hold this many entries if the available memory fills up first. Other configurable parameters for this cache include the maximum length of time to block while waiting to acquire a lock, and a set of filters that may be used to define criteria for determining which entries are stored in the cache. If a filter list is provided, then only entries matching at least one of the given filters will be stored in the cache.

## Parent

The FIFO Entry Cache object inherits from Entry Cache.

## FIFO Entry Cache Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| cache-level<br>enabled<br>exclude-filter<br>include-filter<br>max-entries<br>max-memory-percent | java-class<br>lock-timeout |

## Basic Properties

cache-level

| | |
|---|---|
| *Synopsis* | Specifies the cache level in the cache order if more than one instance of the cache is configured. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Entry Cache is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

exclude-filter

| | |
|---|---|
| *Synopsis* | The set of filters that define the entries that should be excluded from the cache. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

include-filter

| | |
|---|---|
| *Synopsis* | The set of filters that define the entries that should be included in the cache. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

max-entries

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of entries that we will allow in the cache. |
| *Default Value* | 2147483647 |
| *Allowed Values* | An integer. |

| | |
|---|---|
| | Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

max-memory-percent

| | |
|---|---|
| *Synopsis* | Specifies the maximum percentage of JVM memory used by the server before the entry caches stops caching and begins purging itself. |
| *Description* | Very low settings such as 10 or 20 (percent) can prevent this entry cache from having enough space to hold any of the entries to cache, making it appear that the server is ignoring or skipping the entry cache entirely. |
| *Default Value* | 90 |
| *Allowed Values* | An integer.<br>Lower limit: 1.<br>Upper limit: 100. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the FIFO Entry Cache implementation. |
| *Default Value* | org.opends.server.extensions.FIFOEntryCache |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.EntryCache |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

lock-timeout

| | |
|---|---|
| *Synopsis* | Specifies the length of time to wait while attempting to acquire a read or write lock. |
| *Default Value* | 2000.0ms |
| *Allowed Values* | Uses *Duration Syntax* .<br>Use "unlimited" or "-1" to indicate no limit.<br>Lower limit: 0 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# File Based Access Log Publisher

File Based Access Log Publishers publish access messages to the file system.

## Parent

The File Based Access Log Publisher object inherits from Access Log Publisher.

## Dependencies

File Based Access Log Publishers depend on the following objects:

- Log Retention Policy
- Log Rotation Policy

## File Based Access Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| append | asynchronous |

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>filtering-policy<br>log-control-oids<br>log-file<br>log-file-permissions<br>log-format<br>log-record-time-format<br>retention-policy<br>rotation-policy | auto-flush<br>buffer-size<br>java-class<br>queue-size<br>suppress-internal-operations<br>suppress-synchronization-operations<br>time-interval |

## Basic Properties

### append

| | |
|---|---|
| *Synopsis* | Specifies whether to append to existing log files. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### filtering-policy

| | |
|---|---|
| *Synopsis* | Specifies how filtering criteria should be applied to log records. |

| | |
|---|---|
| *Default Value* | no-filtering |
| *Allowed Values* | exclusive: Records must not match any of the filtering criteria in order to be logged.<br><br>inclusive: Records must match at least one of the filtering criteria in order to be logged.<br><br>no-filtering: No filtering will be performed, and all records will be logged. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-control-oids

| | |
|---|---|
| *Synopsis* | Specifies whether control OIDs will be included in operation log records. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-file

| | |
|---|---|
| *Synopsis* | The file name to use for the log files generated by the File Based Access Log Publisher. The path to the file is relative to the server root. |
| *Default Value* | None |
| *Allowed Values* | A path to an existing file that is readable by the server. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

log-file-permissions

| | |
|---|---|
| *Synopsis* | The UNIX permissions of the log files created by this File Based Access Log Publisher. |
| *Default Value* | 640 |
| *Allowed Values* | A valid UNIX mode string. The mode string must contain three digits between zero and seven. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-format

| | |
|---|---|
| *Synopsis* | Specifies how log records should be formatted and written to the access log. |
| *Default Value* | multi-line |
| *Allowed Values* | combined: Combine log records for operation requests and responses into a single record. This format should be used when log records are to be filtered based on response criteria (e.g. result code).<br><br>multi-line: Outputs separate log records for operation requests and responses. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-record-time-format

| | |
|---|---|
| *Synopsis* | Specifies the format string that is used to generate log record timestamps. |
| *Default Value* | dd/MMM/yyyy:HH:mm:ss Z |
| *Allowed Values* | Any valid format string that can be used with the java.text.SimpleDateFormat class. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

retention-policy

| | |
|---|---|
| *Synopsis* | The retention policy to use for the File Based Access Log Publisher . |

| | |
|---|---|
| *Description* | When multiple policies are used, log files are cleaned when any of the policy's conditions are met. |
| *Default Value* | No retention policy is used and log files are never cleaned. |
| *Allowed Values* | The name of an existing Log Retention Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

rotation-policy

| | |
|---|---|
| *Synopsis* | The rotation policy to use for the File Based Access Log Publisher . |
| *Description* | When multiple policies are used, rotation will occur if any policy's conditions are met. |
| *Default Value* | No rotation policy is used and log rotation will not occur. |
| *Allowed Values* | The name of an existing Log Rotation Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

asynchronous

| | |
|---|---|
| *Synopsis* | Indicates whether the File Based Access Log Publisher will publish records asynchronously. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |

| | |
|---|---|
| *Read-Only* | No |

auto-flush

| | |
|---|---|
| *Synopsis* | Specifies whether to flush the writer after every log record. |
| *Description* | If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

buffer-size

| | |
|---|---|
| *Synopsis* | Specifies the log file buffer size. |
| *Default Value* | 64kb |
| *Allowed Values* | Uses *Size Syntax* .<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the File Based Access Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.TextAccessLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

queue-size

| | |
|---|---|
| *Synopsis* | The maximum number of log records that can be stored in the asynchronous queue. |
| *Default Value* | 5000 |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

suppress-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

suppress-synchronization-operations

| | |
|---|---|
| *Synopsis* | Indicates whether access messages that are generated by synchronization operations should be suppressed. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

time-interval

| | |
|---|---|
| *Synopsis* | Specifies the interval at which to check whether the log files need to be rotated. |
| *Default Value* | 5s |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 1 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# File Based Audit Log Publisher

File Based Audit Log Publishers publish access messages to the file system.

## Parent

The File Based Audit Log Publisher object inherits from Access Log Publisher.

## Dependencies

File Based Audit Log Publishers depend on the following objects:

- Log Retention Policy
- Log Rotation Policy

## File Based Audit Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| append<br>enabled | asynchronous<br>auto-flush |

| Basic Properties | Advanced Properties |
|---|---|
| filtering-policy<br>log-file<br>log-file-permissions<br>retention-policy<br>rotation-policy | buffer-size<br>java-class<br>queue-size<br>suppress-internal-operations<br>suppress-synchronization-operations<br>time-interval |

## Basic Properties

### append

| | |
|---|---|
| *Synopsis* | Specifies whether to append to existing log files. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### filtering-policy

| | |
|---|---|
| *Synopsis* | Specifies how filtering criteria should be applied to log records. |
| *Default Value* | no-filtering |
| *Allowed Values* | exclusive: Records must not match any of the filtering criteria in order to be logged. |

| | |
|---|---|
| | inclusive: Records must match at least one of the filtering criteria in order to be logged.<br><br>no-filtering: No filtering will be performed, and all records will be logged. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-file

| | |
|---|---|
| *Synopsis* | The file name to use for the log files generated by the File Based Audit Log Publisher. The path to the file is relative to the server root. |
| *Default Value* | None |
| *Allowed Values* | A path to an existing file that is readable by the server. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

log-file-permissions

| | |
|---|---|
| *Synopsis* | The UNIX permissions of the log files created by this File Based Audit Log Publisher. |
| *Default Value* | 640 |
| *Allowed Values* | A valid UNIX mode string. The mode string must contain three digits between zero and seven. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

retention-policy

| | |
|---|---|
| *Synopsis* | The retention policy to use for the File Based Audit Log Publisher . |
| *Description* | When multiple policies are used, log files are cleaned when any of the policy's conditions are met. |
| *Default Value* | No retention policy is used and log files are never cleaned. |

| | |
|---|---|
| *Allowed Values* | The name of an existing Log Retention Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

rotation-policy

| | |
|---|---|
| *Synopsis* | The rotation policy to use for the File Based Audit Log Publisher . |
| *Description* | When multiple policies are used, rotation will occur if any policy's conditions are met. |
| *Default Value* | No rotation policy is used and log rotation will not occur. |
| *Allowed Values* | The name of an existing Log Rotation Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

asynchronous

| | |
|---|---|
| *Synopsis* | Indicates whether the File Based Audit Log Publisher will publish records asynchronously. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

auto-flush

| | |
|---|---|
| *Synopsis* | Specifies whether to flush the writer after every log record. |
| *Description* | If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

buffer-size

| | |
|---|---|
| *Synopsis* | Specifies the log file buffer size. |
| *Default Value* | 64kb |
| *Allowed Values* | Uses *Size Syntax* .<br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the File Based Audit Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.TextAuditLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

queue-size

| | |
|---|---|
| *Synopsis* | The maximum number of log records that can be stored in the asynchronous queue. |
| *Default Value* | 5000 |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

suppress-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

suppress-synchronization-operations

| | |
|---|---|
| *Synopsis* | Indicates whether access messages that are generated by synchronization operations should be suppressed. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

time-interval

| | |
|---|---|
| *Synopsis* | Specifies the interval at which to check whether the log files need to be rotated. |
| *Default Value* | 5s |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 1 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# File Based Debug Log Publisher

File Based Debug Log Publishers publish debug messages to the file system.

## Parent

The File Based Debug Log Publisher object inherits from Debug Log Publisher.

## Dependencies

File Based Debug Log Publishers depend on the following objects:

- Log Retention Policy
- Log Rotation Policy

## File Based Debug Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| append<br>default-debug-exceptions-only<br>default-include-throwable-cause<br>default-omit-method-entry-arguments<br>default-omit-method-return-value<br>default-throwable-stack-frames | asynchronous<br>auto-flush<br>buffer-size<br>java-class<br>queue-size<br>time-interval |

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>log-file<br>log-file-permissions<br>retention-policy<br>rotation-policy | |

## Basic Properties

### append

| | |
|---|---|
| *Synopsis* | Specifies whether to append to existing log files. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### default-debug-exceptions-only

| | |
|---|---|
| *Synopsis* | Indicates whether only logs with exception should be logged. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### default-include-throwable-cause

| | |
|---|---|
| *Synopsis* | Indicates whether to include the cause of exceptions in exception thrown and caught messages logged by default. |
| *Default Value* | true |
| *Allowed Values* | true |

| | |
|---|---|
| | false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

default-omit-method-entry-arguments

| | |
|---|---|
| *Synopsis* | Indicates whether to include method arguments in debug messages logged by default. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

default-omit-method-return-value

| | |
|---|---|
| *Synopsis* | Indicates whether to include the return value in debug messages logged by default. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

default-throwable-stack-frames

| | |
|---|---|
| *Synopsis* | Indicates the number of stack frames to include in the stack trace for method entry and exception thrown messages. |
| *Default Value* | 2147483647 |

| | |
|---|---|
| *Allowed Values* | An integer.<br>Lower limit: 0.<br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-file

| | |
|---|---|
| *Synopsis* | The file name to use for the log files generated by the File Based Debug Log Publisher . |
| *Description* | The path to the file is relative to the server root. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

log-file-permissions

| | |
|---|---|
| *Synopsis* | The UNIX permissions of the log files created by this File Based Debug Log Publisher . |

| | |
|---|---|
| *Default Value* | 640 |
| *Allowed Values* | A valid UNIX mode string. The mode string must contain three digits between zero and seven. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

retention-policy

| | |
|---|---|
| *Synopsis* | The retention policy to use for the File Based Debug Log Publisher . |
| *Description* | When multiple policies are used, log files are cleaned when any of the policy's conditions are met. |
| *Default Value* | No retention policy is used and log files are never cleaned. |
| *Allowed Values* | The name of an existing Log Retention Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

rotation-policy

| | |
|---|---|
| *Synopsis* | The rotation policy to use for the File Based Debug Log Publisher . |
| *Description* | When multiple policies are used, rotation will occur if any policy's conditions are met. |
| *Default Value* | No rotation policy is used and log rotation will not occur. |
| *Allowed Values* | The name of an existing Log Rotation Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

asynchronous

| | |
|---|---|
| *Synopsis* | Indicates whether the File Based Debug Log Publisher will publish records asynchronously. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

auto-flush

| | |
|---|---|
| *Synopsis* | Specifies whether to flush the writer after every log record. |
| *Description* | If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

buffer-size

| | |
|---|---|
| *Synopsis* | Specifies the log file buffer size. |
| *Default Value* | 64kb |
| *Allowed Values* | Uses *Size Syntax* .<br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |

| | |
|---|---|
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the File Based Debug Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.TextDebugLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

queue-size

| | |
|---|---|
| *Synopsis* | The maximum number of log records that can be stored in the asynchronous queue. |
| *Default Value* | 5000 |
| *Allowed Values* | An integer.<br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

time-interval

| | |
|---|---|
| *Synopsis* | Specifies the interval at which to check whether the log files need to be rotated. |
| *Default Value* | 5s |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 1 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

# File Based Error Log Publisher

File Based Error Log Publishers publish error messages to the file system.

## Parent

The File Based Error Log Publisher object inherits from Error Log Publisher.

## Dependencies

File Based Error Log Publishers depend on the following objects:

- Log Retention Policy
- Log Rotation Policy

## File Based Error Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| append<br>default-severity<br>enabled<br>log-file<br>log-file-permissions<br>override-severity<br>retention-policy<br>rotation-policy | asynchronous<br>auto-flush<br>buffer-size<br>java-class<br>queue-size<br>time-interval |

## Basic Properties

append

| | |
|---|---|
| *Synopsis* | Specifies whether to append to existing log files. |
| *Default Value* | true |
| *Allowed Values* | true |

| | |
|---|---|
| | false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

default-severity

| | |
|---|---|
| *Synopsis* | Specifies the default severity levels for the logger. |
| *Default Value* | error<br><br>warning |
| *Allowed Values* | all: Messages of all severity levels are logged.<br><br>debug: The error log severity that is used for messages that provide debugging information triggered during processing.<br><br>error: The error log severity that is used for messages that provide information about errors which may force the server to shut down or operate in a significantly degraded state.<br><br>info: The error log severity that is used for messages that provide information about significant events within the server that are not warnings or errors.<br><br>none: No messages of any severity are logged by default. This value is intended to be used in conjunction with the override-severity property to define an error logger that will publish no error message beside the errors of a given category.<br><br>notice: The error log severity that is used for the most important informational messages (i.e., information that should almost always be logged but is not associated with a warning or error condition).<br><br>warning: The error log severity that is used for messages that provide information about warnings triggered during processing. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |

| | |
|---|---|
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-file

| | |
|---|---|
| *Synopsis* | The file name to use for the log files generated by the File Based Error Log Publisher . |
| *Description* | The path to the file is relative to the server root. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

log-file-permissions

| | |
|---|---|
| *Synopsis* | The UNIX permissions of the log files created by this File Based Error Log Publisher . |
| *Default Value* | 640 |
| *Allowed Values* | A valid UNIX mode string. The mode string must contain three digits between zero and seven. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

override-severity

| | |
|---|---|
| *Synopsis* | Specifies the override severity levels for the logger based on the category of the messages. |

| | |
|---|---|
| *Description* | Each override severity level should include the category and the severity levels to log for that category, for example, core=error,info,warning. Valid categories are: core, extensions, protocol, config, log, util, schema, plugin, jeb, backend, tools, task, access-control, admin, sync, version, setup, admin-tool, dsconfig, user-defined. Valid severities are: all, error, info, warning, notice, debug. |
| *Default Value* | All messages with the default severity levels are logged. |
| *Allowed Values* | A string in the form category=severity1,severity2... |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

retention-policy

| | |
|---|---|
| *Synopsis* | The retention policy to use for the File Based Error Log Publisher . |
| *Description* | When multiple policies are used, log files will be cleaned when any of the policy's conditions are met. |
| *Default Value* | No retention policy is used and log files will never be cleaned. |
| *Allowed Values* | The name of an existing Log Retention Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

rotation-policy

| | |
|---|---|
| *Synopsis* | The rotation policy to use for the File Based Error Log Publisher . |
| *Description* | When multiple policies are used, rotation will occur if any policy's conditions are met. |
| *Default Value* | No rotation policy is used and log rotation will not occur. |
| *Allowed Values* | The name of an existing Log Rotation Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

asynchronous

| | |
|---|---|
| *Synopsis* | Indicates whether the File Based Error Log Publisher will publish records asynchronously. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

auto-flush

| | |
|---|---|
| *Synopsis* | Specifies whether to flush the writer after every log record. |
| *Description* | If the asynchronous writes option is used, the writer will be flushed after all the log records in the queue are written. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

buffer-size

| | |
|---|---|
| *Synopsis* | Specifies the log file buffer size. |
| *Default Value* | 64kb |
| *Allowed Values* | Uses *Size Syntax* .<br>Lower limit: 1. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the File Based Error Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.TextErrorLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

queue-size

| | |
|---|---|
| *Synopsis* | The maximum number of log records that can be stored in the asynchronous queue. |
| *Default Value* | 5000 |
| *Allowed Values* | An integer.<br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

time-interval

| | |
|---|---|
| *Synopsis* | Specifies the interval at which to check whether the log files need to be rotated. |
| *Default Value* | 5s |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 1 milliseconds. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# File Based HTTP Access Log Publisher

File Based HTTP Access Log Publishers publish HTTP access messages to the file system.

## Parent

The File Based HTTP Access Log Publisher object inherits from HTTP Access Log Publisher.

## Dependencies

File Based HTTP Access Log Publishers depend on the following objects:

- Log Retention Policy
- Log Rotation Policy

## File Based HTTP Access Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| append<br>enabled<br>log-file<br>log-file-permissions<br>log-format<br>log-record-time-format<br>retention-policy<br>rotation-policy | asynchronous<br>auto-flush<br>buffer-size<br>java-class<br>queue-size<br>time-interval |

## Basic Properties

append

| | |
|---|---|
| *Synopsis* | Specifies whether to append to existing log files. |

| | |
|---|---|
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-file

| | |
|---|---|
| *Synopsis* | The file name to use for the log files generated by the File Based HTTP Access Log Publisher. The path to the file is relative to the server root. |
| *Default Value* | None |
| *Allowed Values* | A path to an existing file that is readable by the server. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

log-file-permissions

| | |
|---|---|
| *Synopsis* | The UNIX permissions of the log files created by this File Based HTTP Access Log Publisher. |
| *Default Value* | 640 |

| | |
|---|---|
| *Allowed Values* | A valid UNIX mode string. The mode string must contain three digits between zero and seven. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-format

| | |
|---|---|
| *Synopsis* | Specifies how log records should be formatted and written to the HTTP access log. |
| *Default Value* | cs-host c-ip cs-username x-datetime cs-method cs-uri-stem cs-uri-query cs-version sc-status cs(User-Agent) x-connection-id x-etime x-transaction-id |
| *Allowed Values* | A space separated list of fields describing the extended log format to be used for logging HTTP accesses. Available values are listed on the W3C working draft http://www.w3.org/TR/WD-logfile.html and Microsoft website http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/676400bc-8969-4aa7-851a-9319490a9bbb.mspx?mfr=true OpenDJ supports the following standard fields: "c-ip", "c-port", "cs-host", "cs-method", "cs-uri", "cs-uri-stem", "cs-uri-query", "cs(User-Agent)", "cs-username", "cs-version", "s-computername", "s-ip", "s-port", "sc-status". OpenDJ supports the following application specific field extensions: "x-connection-id" displays the internal connection ID assigned to the HTTP client connection, "x-datetime" displays the completion date and time for the logged HTTP request and its ouput is controlled by the "ds-cfg-log-record-time-format" property, "x-etime" displays the total execution time for the logged HTTP request, "x-transaction-id" displays the transaction id associated to a request |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-record-time-format

| | |
|---|---|
| *Synopsis* | Specifies the format string that is used to generate log record timestamps. |
| *Default Value* | dd/MMM/yyyy:HH:mm:ss Z |
| *Allowed Values* | Any valid format string that can be used with the java.text.SimpleDateFormat class. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

retention-policy

| | |
|---|---|
| *Synopsis* | The retention policy to use for the File Based HTTP Access Log Publisher . |
| *Description* | When multiple policies are used, log files are cleaned when any of the policy's conditions are met. |
| *Default Value* | No retention policy is used and log files are never cleaned. |
| *Allowed Values* | The name of an existing Log Retention Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

rotation-policy

| | |
|---|---|
| *Synopsis* | The rotation policy to use for the File Based HTTP Access Log Publisher . |
| *Description* | When multiple policies are used, rotation will occur if any policy's conditions are met. |
| *Default Value* | No rotation policy is used and log rotation will not occur. |
| *Allowed Values* | The name of an existing Log Rotation Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

asynchronous

| | |
|---|---|
| *Synopsis* | Indicates whether the File Based HTTP Access Log Publisher will publish records asynchronously. |
| *Default Value* | true |
| *Allowed Values* | true |

| | |
|---|---|
| | false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

auto-flush

| | |
|---|---|
| *Synopsis* | Specifies whether to flush the writer after every log record. |
| *Description* | If the asynchronous writes option is used, the writer is flushed after all the log records in the queue are written. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

buffer-size

| | |
|---|---|
| *Synopsis* | Specifies the log file buffer size. |
| *Default Value* | 64kb |
| *Allowed Values* | Uses *Size Syntax* .<br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the File Based HTTP Access Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.TextHTTPAccessLogPublisher |

| | |
|---|---|
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

queue-size

| | |
|---|---|
| *Synopsis* | The maximum number of log records that can be stored in the asynchronous queue. |
| *Default Value* | 5000 |
| *Allowed Values* | An integer.<br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

time-interval

| | |
|---|---|
| *Synopsis* | Specifies the interval at which to check whether the log files need to be rotated. |
| *Default Value* | 5s |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 1 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# File Based Key Manager Provider

The File Based Key Manager Provider can be used to obtain the server certificate from a key store file on the local file system.

Multiple file formats may be supported, depending on the providers supported by the underlying Java runtime environment.

## Parent

The File Based Key Manager Provider object inherits from Key Manager Provider.

## File Based Key Manager Provider Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>key-store-file<br>key-store-pin<br>key-store-type | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Key Manager Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-store-file

| | |
|---|---|
| *Synopsis* | Specifies the path to the file that contains the private key information. This may be an absolute path, or a path that is relative to the OpenDJ instance root. |
| *Description* | Changes to this property will take effect the next time that the key manager is accessed. |
| *Default Value* | None |
| *Allowed Values* | A path to an existing file that is readable by the server. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-store-pin

| | |
|---|---|
| *Synopsis* | Specifies the clear-text PIN needed to access the File Based Key Manager Provider . |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property will take effect the next time that the File Based Key Manager Provider is accessed. |
| *Advanced* | No |
| *Read-Only* | No |

key-store-type

| | |
|---|---|
| *Synopsis* | Specifies the format for the data in the key store file. |
| *Description* | Valid values should always include 'JKS' and 'PKCS12', but different implementations may allow other values as well. If no value is provided, the JVM-default value is used. Changes to this configuration attribute will take effect the next time that the key manager is accessed. |
| *Default Value* | None |
| *Allowed Values* | Any key store format supported by the Java runtime environment. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the File Based Key Manager Provider implementation. |
| *Default Value* | org.opends.server.extensions.FileBasedKeyManagerProvider |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.KeyManagerProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# File Based Trust Manager Provider

The file-based trust manager provider determines whether to trust a presented certificate based on whether that certificate exists in a server trust store file.

The trust store file can be in either JKS (the default Java key store format) or PKCS#12 (a standard certificate format) form.

## Parent

The File Based Trust Manager Provider object inherits from Trust Manager Provider.

## File Based Trust Manager Provider Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>trust-store-file<br>trust-store-pin<br>trust-store-type | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicate whether the Trust Manager Provider is enabled for use. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

trust-store-file

| | |
|---|---|
| *Synopsis* | Specifies the path to the file containing the trust information. It can be an absolute path or a path that is relative to the OpenDJ instance root. |
| *Description* | Changes to this configuration attribute take effect the next time that the trust manager is accessed. |
| *Default Value* | None |
| *Allowed Values* | An absolute path or a path that is relative to the OpenDJ directory server instance root. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

trust-store-pin

| | |
|---|---|
| *Synopsis* | Specifies the clear-text PIN needed to access the File Based Trust Manager Provider . |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property will take effect the next time that the File Based Trust Manager Provider is accessed. |
| *Advanced* | No |
| *Read-Only* | No |

trust-store-type

| | |
|---|---|
| *Synopsis* | Specifies the format for the data in the trust store file. |
| *Description* | Valid values always include 'JKS' and 'PKCS12', but different implementations can allow other values as well. If no value is provided, then the JVM default value is used. Changes to this configuration attribute take effect the next time that the trust manager is accessed. |
| *Default Value* | None |
| *Allowed Values* | Any key store format supported by the Java runtime environment. The "JKS" and "PKCS12" formats are typically available in Java environments. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the File Based Trust Manager Provider implementation. |
| *Default Value* | org.opends.server.extensions.FileBasedTrustManagerProvider |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.TrustManagerProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## File Count Log Retention Policy

Retention policy based on the number of rotated log files on disk.

### Parent

The File Count Log Retention Policy object inherits from Log Retention Policy.

# File Count Log Retention Policy Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| number-of-files | java-class |

## Basic Properties

number-of-files

| | |
|---|---|
| *Synopsis* | Specifies the number of archived log files to retain before the oldest ones are cleaned. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the File Count Log Retention Policy implementation. |
| *Default Value* | org.opends.server.loggers.FileNumberRetentionPolicy |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.loggers.RetentionPolicy |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Fingerprint Certificate Mapper

The Fingerprint Certificate Mapper maps client certificates to user entries by looking for the MD5 or SHA1 fingerprint in a specified attribute of user entries.

## Parent

The Fingerprint Certificate Mapper object inherits from Certificate Mapper.

## Fingerprint Certificate Mapper Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>fingerprint-algorithm<br>fingerprint-attribute<br>issuer-attribute<br>user-base-dn | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Certificate Mapper is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

fingerprint-algorithm

| | |
|---|---|
| *Synopsis* | Specifies the name of the digest algorithm to compute the fingerprint of client certificates. |
| *Default Value* | None |
| *Allowed Values* | md5: Use the MD5 digest algorithm to compute certificate fingerprints.<br><br>sha1: Use the SHA-1 digest algorithm to compute certificate fingerprints. |

| | |
|---|---|
| | sha256: Use the SHA-256 digest algorithm to compute certificate fingerprints. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

fingerprint-attribute

| | |
|---|---|
| *Synopsis* | Specifies the attribute in which to look for the fingerprint. |
| *Description* | Values of the fingerprint attribute should exactly match the MD5 or SHA1 representation of the certificate fingerprint. |
| *Default Value* | None |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

issuer-attribute

| | |
|---|---|
| *Synopsis* | Specifies the name or OID of the attribute whose value should exactly match the certificate issuer DN. |
| *Description* | Certificate issuer verification should be enabled whenever multiple CAs are trusted in order to prevent impersonation. In particular, it is possible for different CAs to issue certificates having the same subject DN. |
| *Default Value* | The certificate issuer DN will not be verified. |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

user-base-dn

| | |
|---|---|
| *Synopsis* | Specifies the set of base DNs below which to search for users. |
| *Description* | The base DNs are used when performing searches to map the client certificates to a user entry. |
| *Default Value* | The server performs the search in all public naming contexts. |

| | |
|---|---|
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Fingerprint Certificate Mapper implementation. |
| *Default Value* | org.opends.server.extensions.FingerprintCertificateMapper |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.CertificateMapper |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Fixed Time Log Rotation Policy

Rotation policy based on a fixed time of day.

### Parent

The Fixed Time Log Rotation Policy object inherits from Log Rotation Policy.

### Fixed Time Log Rotation Policy Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| time-of-day | java-class |

### Basic Properties

time-of-day

| | |
|---|---|
| *Synopsis* | Specifies the time of day at which log rotation should occur. |
| *Default Value* | None |
| *Allowed Values* | 24 hour time of day in HHmm format. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Fixed Time Log Rotation Policy implementation. |
| *Default Value* | org.opends.server.loggers.FixedTimeRotationPolicy |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.RotationPolicy |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## Fractional LDIF Import Plugin

The Fractional LDIF Import Plugin is used internally by the replication plugin to support fractional replication.

It is used to check fractional configuration consistency with local domain one as well as to filter attributes when performing an online import from a remote backend to a local backend.

## Parent

The Fractional LDIF Import Plugin object inherits from Plugin.

## Fractional LDIF Import Plugin Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>java-class<br>plugin-type | invoke-for-internal-operations |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the plug-in implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.plugin.DirectoryServerPlugin |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-type

| | |
|---|---|
| *Synopsis* | Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked. |
| *Default Value* | None |
| *Allowed Values* | initialization: Invoked at the initialization of the directory server.<br><br>intermediateresponse: Invoked before sending an intermediate repsonse message to the client.<br><br>ldifimport: Invoked for each entry read during an LDIF import.<br><br>ldifimportbegin: Invoked at the beginning of an LDIF import session.<br><br>ldifimportend: Invoked at the end of an LDIF import session.<br><br>postconnect: Invoked whenever a new connection is established to the server.<br><br>postdisconnect: Invoked whenever an existing connection is terminated (by either the client or the server).<br><br>postoperationabandon: Invoked after completing the abandon processing.<br><br>postoperationadd: Invoked after completing the core add processing but before sending the response to the client.<br><br>postoperationbind: Invoked after completing the core bind processing but before sending the response to the client.<br><br>postoperationcompare: Invoked after completing the core compare processing but before sending the response to the client.<br><br>postoperationdelete: Invoked after completing the core delete processing but before sending the response to the client.<br><br>postoperationextended: Invoked after completing the core extended processing but before sending the response to the client.<br><br>postoperationmodify: Invoked after completing the core modify processing but before sending the response to the client.<br><br>postoperationmodifydn: Invoked after completing the core modify DN processing but before sending the response to the client.<br><br>postoperationsearch: Invoked after completing the core search processing but before sending the response to the client.<br><br>postoperationunbind: Invoked after completing the unbind processing.<br><br>postresponseadd: Invoked after sending the add response to the client.<br><br>postresponsebind: Invoked after sending the bind response to the client.<br><br>postresponsecompare: Invoked after sending the compare response to the client. |

postresponsedelete: Invoked after sending the delete response to the client.

postresponseextended: Invoked after sending the extended response to the client.

postresponsemodify: Invoked after sending the modify response to the client.

postresponsemodifydn: Invoked after sending the modify DN response to the client.

postresponsesearch: Invoked after sending the search result done message to the client.

postsynchronizationadd: Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete: Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify: Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn: Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd: Invoked prior to performing the core add processing.

preoperationbind: Invoked prior to performing the core bind processing.

preoperationcompare: Invoked prior to performing the core compare processing.

preoperationdelete: Invoked prior to performing the core delete processing.

preoperationextended: Invoked prior to performing the core extended processing.

preoperationmodify: Invoked prior to performing the core modify processing.

preoperationmodifydn: Invoked prior to performing the core modify DN processing.

preoperationsearch: Invoked prior to performing the core search processing.

preparseabandon: Invoked prior to parsing an abandon request.

preparseadd: Invoked prior to parsing an add request.

preparsebind: Invoked prior to parsing a bind request.

preparsecompare: Invoked prior to parsing a compare request.

preparsedelete: Invoked prior to parsing a delete request.

preparseextended: Invoked prior to parsing an extended request.

preparsemodify: Invoked prior to parsing a modify request.

preparsemodifydn: Invoked prior to parsing a modify DN request.

| | |
|---|---|
| | preparsesearch: Invoked prior to parsing a search request.<br><br>preparseunbind: Invoked prior to parsing an unbind request.<br><br>searchresultentry: Invoked before sending a search result entry to the client.<br><br>searchresultreference: Invoked before sending a search result reference to the client.<br><br>shutdown: Invoked during a graceful directory server shutdown.<br><br>startup: Invoked during the directory server startup process.<br><br>subordinatedelete: Invoked in the course of deleting a subordinate entry of a delete operation.<br><br>subordinatemodifydn: Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

invoke-for-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in should be invoked for internal operations. |
| *Description* | Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Free Disk Space Log Retention Policy

Retention policy based on the free disk space available.

This policy is only available on Java 6.

## Parent

The Free Disk Space Log Retention Policy object inherits from Log Retention Policy.

## Free Disk Space Log Retention Policy Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| free-disk-space | java-class |

## Basic Properties

free-disk-space

| | |
|---|---|
| *Synopsis* | Specifies the minimum amount of free disk space that should be available on the file system on which the archived log files are stored. |
| *Default Value* | None |
| *Allowed Values* | Uses *Size Syntax* .<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Free Disk Space Log Retention Policy implementation. |
| *Default Value* | org.opends.server.loggers.FreeDiskSpaceRetentionPolicy |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.RetentionPolicy |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Get Connection ID Extended Operation Handler

The Get Connection ID Extended Operation Handler provides a mechanism for clients to obtain the internal connection ID that the server uses to reference their client connection.

## Parent

The Get Connection ID Extended Operation Handler object inherits from Extended Operation Handler.

## Get Connection ID Extended Operation Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server). |
| *Default Value* | None |
| *Allowed Values* | true |

| | |
|---|---|
| | false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Get Connection ID Extended Operation Handler implementation. |
| *Default Value* | org.opends.server.extensions.GetConnectionIDExtendedOperation |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.ExtendedOperationHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Get Symmetric Key Extended Operation Handler

The Get Symmetric Key Extended Operation Handler is used by the OpenDJ cryptographic framework for creating and obtaining symmetric encryption keys.

### Parent

The Get Symmetric Key Extended Operation Handler object inherits from Extended Operation Handler.

### Get Symmetric Key Extended Operation Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server). |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Get Symmetric Key Extended Operation Handler implementation. |
| *Default Value* | org.opends.server.crypto.GetSymmetricKeyExtendedOperation |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.ExtendedOperationHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Global Configuration

The Global Configuration contains properties that affect the overall operation of the OpenDJ.

## Dependencies

Global Configurations depend on the following objects:

- Authentication Policy
- Identity Mapper

## Global Configuration Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| advertised-listen-address<br>allowed-client<br>bind-with-dn-requires-password<br>default-password-policy<br>denied-client<br>disabled-privilege<br>etime-resolution<br>group-id<br>idle-time-limit<br>je-backend-shared-cache-enabled<br>listen-address<br>lookthrough-limit<br>max-allowed-client-connections<br>max-psearches<br>proxied-authorization-identity-mapper<br>restricted-client<br>restricted-client-connection-limit<br>return-bind-error-messages<br>save-config-on-successful-startup<br>server-id<br>size-limit<br>subordinate-base-dn<br>time-limit<br>unauthenticated-requests-policy<br>writability-mode | add-missing-rdn-attributes<br>allow-attribute-name-exceptions<br>allowed-task<br>check-schema<br>cursor-entry-limit<br>invalid-attribute-syntax-behavior<br>max-internal-buffer-size<br>notify-abandoned-operations<br>single-structural-objectclass-behavior<br>trust-transaction-ids |

## Basic Properties

advertised-listen-address

| | |
|---|---|
| *Synopsis* | The advertised address(es) which clients should use for connecting to this Global Configuration. |
| *Description* | Multiple addresses may be provided as separate values for this attribute. The meta-address 0.0.0.0 is not permitted. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

allowed-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be allowed to establish connections to this Global Configuration. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

bind-with-dn-requires-password

| | |
|---|---|
| *Synopsis* | Indicates whether the directory server should reject any simple bind request that contains a DN but no password. |
| *Description* | Although such bind requests are technically allowed by the LDAPv3 specification (and should be treated as anonymous simple authentication), they may introduce security problems in applications that do not verify that the client actually provided a password. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

default-password-policy

| | |
|---|---|
| *Synopsis* | Specifies the name of the password policy that is in effect for users whose entries do not specify an alternate password policy (either via a real or virtual attribute). |
| *Description* | In addition, the default password policy will be used for providing default parameters for sub-entry based password policies when not provided or supported by the sub-entry itself. This property must reference a password policy and no other type of authentication policy. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Password Policy . |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

denied-client

| | |
|---|---|
| *Synopsis* | A set of clients who are not allowed to establish connections to this Global Configuration. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

disabled-privilege

| | |
|---|---|
| *Synopsis* | Specifies the name of a privilege that should not be evaluated by the server. |
| *Description* | If a privilege is disabled, then it is assumed that all clients (including unauthenticated clients) have that privilege. |
| *Default Value* | If no values are defined, then the server enforces all privileges. |
| *Allowed Values* | backend-backup: Allows the user to request that the server process backup or backup purge tasks.<br><br>backend-restore: Allows the user to request that the server process restore tasks.<br><br>bypass-acl: Allows the associated user to bypass access control checks performed by the server.<br><br>bypass-lockdown: Allows the associated user to bypass server lockdown mode.<br><br>cancel-request: Allows the user to cancel operations in progress on other client connections.<br><br>changelog-read: The privilege that provides the ability to perform read operations on the changelog<br><br>config-read: Allows the associated user to read the server configuration.<br><br>config-write: Allows the associated user to update the server configuration. The config-read privilege is also required.<br><br>data-sync: Allows the user to participate in data synchronization.<br><br>disconnect-client: Allows the user to terminate other client connections.<br><br>jmx-notify: Allows the associated user to subscribe to receive JMX notifications.<br><br>jmx-read: Allows the associated user to perform JMX read operations.<br><br>jmx-write: Allows the associated user to perform JMX write operations.<br><br>ldif-export: Allows the user to request that the server process LDIF export tasks.<br><br>ldif-import: Allows the user to request that the server process LDIF import tasks.<br><br>modify-acl: Allows the associated user to modify the server's access control configuration.<br><br>monitor-read: Allows the user to read the server monitoring information.<br><br>password-reset: Allows the user to reset user passwords.<br><br>privilege-change: Allows the user to make changes to the set of defined root privileges, as well as to grant and revoke privileges for users. |

| | |
|---|---|
| | proxied-auth: Allows the user to use the proxied authorization control, or to perform a bind that specifies an alternate authorization identity.<br><br>server-lockdown: Allows the user to place and bring the server of lockdown mode.<br><br>server-restart: Allows the user to request that the server perform an in-core restart.<br><br>server-shutdown: Allows the user to request that the server shut down.<br><br>subentry-write: Allows the associated user to perform LDAP subentry write operations.<br><br>unindexed-search: Allows the user to request that the server process a search that cannot be optimized using server indexes.<br><br>update-schema: Allows the user to make changes to the server schema. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

etime-resolution

| | |
|---|---|
| *Synopsis* | Specifies the resolution to use for operation elapsed processing time (etime) measurements. |
| *Default Value* | milliseconds |
| *Allowed Values* | milliseconds: Use millisecond resolution.<br><br>nanoseconds: Use nanosecond resolution. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-id

| | |
|---|---|
| *Synopsis* | Specifies the unique identifier of the group in which the directory server belongs. |
| *Description* | Directory servers are typically grouped according to their physical location, such as a rack or data center. Servers will prefer connecting to other servers within the same group. |
| *Default Value* | default |

| | |
|---|---|
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

idle-time-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum length of time that a client connection may remain established since its last completed operation. |
| *Description* | A value of "0 seconds" indicates that no idle time limit is enforced. |
| *Default Value* | 0 seconds |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 0 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

je-backend-shared-cache-enabled

| | |
|---|---|
| *Synopsis* | Indicates whether all the JE backends should share the same cache. |
| *Description* | When enabled, all the JE backends share the same cache. JE backends will make better use of memory: the cache will use around at most 75% of the JVM Old Gen size. Note that when this setting is enabled, it overrides all db-cache-percent and db-cache-size settings. Note also that cache misses in one backend could cause cached data for other backends to be evicted. When disabled, each JE backend will have its own cache sized according to their options db-cache-percent/db-cache-size. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | Restart the server for changes to take effect. |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

listen-address

| | |
|---|---|
| *Synopsis* | The network interface(s) on which this Global Configuration should listen for incoming client connections. |
| *Description* | Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the directory server will listen on all interfaces. |
| *Default Value* | 0.0.0.0 |
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

lookthrough-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of entries that the directory server should "look through" in the course of processing a search request. |
| *Description* | This includes any entry that the server must examine in the course of processing the request, regardless of whether it actually matches the search criteria. A value of 0 indicates that no lookthrough limit is enforced. Note that this is the default server-wide limit, but it may be overridden on a per-user basis using the ds-rlim-lookthrough-limit operational attribute. |
| *Default Value* | 5000 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

max-allowed-client-connections

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of client connections that may be established at any given time |
| *Description* | A value of 0 indicates that unlimited client connection is allowed. |

| | |
|---|---|
| *Default Value* | 0 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

max-psearches

| | |
|---|---|
| *Synopsis* | Defines the maximum number of concurrent persistent searches that can be performed on directory server |
| *Description* | The persistent search mechanism provides an active channel through which entries that change, and information about the changes that occur, can be communicated. Because each persistent search operation consumes resources, limiting the number of simultaneous persistent searches keeps the performance impact minimal. A value of -1 indicates that there is no limit on the persistent searches. |
| *Default Value* | -1 |
| *Allowed Values* | An integer.<br><br>Use "-1" or "unlimited" to indicate no limit.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

proxied-authorization-identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name of the identity mapper(s) to map authorization ID values (using the "u:" form) provided in the proxied authorization control to the corresponding user entry. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br><br>The referenced identity mapper(s) must be enabled. |
| *Multi-valued* | Yes |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be limited to the maximum number of connections specified by the "restricted-client-connection-limit" property. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | No restrictions are imposed on the number of connections a client can open. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client-connection-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of connections a restricted client can open at the same time to this Global Configuration. |
| *Description* | Once Directory Server accepts the specified number of connections from a client specified in restricted-client, any additional connection will be rejected. The number of connections is maintained by IP address. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | 100 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

return-bind-error-messages

| | |
|---|---|
| *Synopsis* | Indicates whether responses for failed bind operations should include a message string providing the reason for the authentication failure. |
| *Description* | Note that these messages may include information that could potentially be used by an attacker. If this option is disabled, then these messages appears only in the server's access log. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

save-config-on-successful-startup

| | |
|---|---|
| *Synopsis* | Indicates whether the directory server should save a copy of its configuration whenever the startup process completes successfully. |
| *Description* | This ensures that the server provides a "last known good" configuration, which can be used as a reference (or copied into the active config) if the server fails to start with the current "active" configuration. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

server-id

| | |
|---|---|
| *Synopsis* | Specifies a unique identifier for the directory server which will identify the server within a replication topology. |

| | |
|---|---|
| *Description* | Each directory server within the same replication topology must have a different server identifier. If no server identifier is specified then one must be provided in each replication server and replication domain configuration. |
| *Default Value* | Specified per replication server and domain. |
| *Allowed Values* | An alphanumeric string, may also contain underscore and hyphen characters |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | Restart the server for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

size-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of entries that can be returned to the client during a single search operation. |
| *Description* | A value of 0 indicates that no size limit is enforced. Note that this is the default server-wide limit, but it may be overridden on a per-user basis using the ds-rlim-size-limit operational attribute. |
| *Default Value* | 1000 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

subordinate-base-dn

| | |
|---|---|
| *Synopsis* | Specifies the set of base DNs used for singleLevel, wholeSubtree, and subordinateSubtree searches based at the root DSE. |
| *Default Value* | The set of all user-defined suffixes is used. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

time-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum length of time that should be spent processing a single search operation. |
| *Description* | A value of 0 seconds indicates that no time limit is enforced. Note that this is the default server-wide time limit, but it may be overridden on a per-user basis using the ds-rlim-time-limit operational attribute. |
| *Default Value* | 60 seconds |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 0 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

unauthenticated-requests-policy

| | |
|---|---|
| *Synopsis* | Controls how the directory server should handle requests received from a client that has not yet been authenticated, whose last authentication attempt was unsuccessful, or whose last authentication attempt used anonymous authentication. |
| *Default Value* | allow |
| *Allowed Values* | allow: Allows all unauthenticated requests, subject to privileges and ACIs.<br><br>allow-discovery: Disallows all unauthenticated requests except for Bind and StartTLS requests, and base object searches of the root DSE. Use this setting in order to support service discovery and keep-alive heartbeats which typically target the root DSE.<br><br>reject: Disallows all unauthenticated requests except for Bind and StartTLS requests. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

writability-mode

| | |
|---|---|
| *Synopsis* | Specifies the kinds of write operations the directory server can process. |
| *Default Value* | enabled |

| | |
|---|---|
| *Allowed Values* | disabled: The directory server rejects all write operations that are requested of it, regardless of their origin.<br><br>enabled: The directory server attempts to process all write operations that are requested of it, regardless of their origin.<br><br>internal-only: The directory server attempts to process write operations requested as internal operations or through synchronization, but rejects any such operations requested from external clients. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

add-missing-rdn-attributes

| | |
|---|---|
| *Synopsis* | Indicates whether the directory server should automatically add any attribute values contained in the entry's RDN into that entry when processing an add request. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

allow-attribute-name-exceptions

| | |
|---|---|
| *Synopsis* | Indicates whether the directory server should allow underscores in attribute names and allow attribute names to begin with numeric digits (both of which are violations of the LDAP standards). |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

allowed-task

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of a Java class that may be invoked in the server. |
| *Description* | Any attempt to invoke a task not included in the list of allowed tasks is rejected. |
| *Default Value* | If no values are defined, then the server does not allow any tasks to be invoked. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

check-schema

| | |
|---|---|
| *Synopsis* | Indicates whether schema enforcement is active. |
| *Description* | When schema enforcement is activated, the directory server ensures that all operations result in entries are valid according to the defined server schema. It is strongly recommended that this option be left enabled to prevent the inadvertent addition of invalid data into the server. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

cursor-entry-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of entry IDs that the directory server may retrieve by cursoring through an index during a search. |

| | |
|---|---|
| *Description* | A value of 0 indicates that no cursor entry limit is enforced. Note that this is the default server-wide limit, but it may be overridden on a per-user basis using the ds-rlim-cursor-entry-limit operational attribute. |
| *Default Value* | 100000 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

### invalid-attribute-syntax-behavior

| | |
|---|---|
| *Synopsis* | Specifies how the directory server should handle operations whenever an attribute value violates the associated attribute syntax. |
| *Default Value* | reject |
| *Allowed Values* | accept: The directory server silently accepts attribute values that are invalid according to their associated syntax. Matching operations targeting those values may not behave as expected.<br><br>reject: The directory server rejects attribute values that are invalid according to their associated syntax.<br><br>warn: The directory server accepts attribute values that are invalid according to their associated syntax, but also logs a warning message to the error log. Matching operations targeting those values may not behave as expected. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

### max-internal-buffer-size

| | |
|---|---|
| *Synopsis* | The threshold capacity beyond which internal cached buffers used for encoding and decoding entries and protocol messages will be trimmed after use. |
| *Description* | Individual buffers may grow very large when encoding and decoding large entries and protocol messages and should be reduced in size when they are no longer needed. This setting specifies the threshold at which a buffer is determined to have grown too big and should be trimmed down after use. |
| *Default Value* | 32 KB |
| *Allowed Values* | Uses *Size Syntax* . |

| | |
|---|---|
| | Lower limit: 512.<br><br>Upper limit: 1000000000. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

notify-abandoned-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the directory server should send a response to any operation that is interrupted via an abandon request. |
| *Description* | The LDAP specification states that abandoned operations should not receive any response, but this may cause problems with client applications that always expect to receive a response to each request. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

single-structural-objectclass-behavior

| | |
|---|---|
| *Synopsis* | Specifies how the directory server should handle operations an entry does not contain a structural object class or contains multiple structural classes. |
| *Default Value* | reject |
| *Allowed Values* | accept: The directory server silently accepts entries that do not contain exactly one structural object class. Certain schema features that depend on the entry's structural class may not behave as expected.<br><br>reject: The directory server rejects entries that do not contain exactly one structural object class.<br><br>warn: The directory server accepts entries that do not contain exactly one structural object class, but also logs a warning message to the error log. Certain schema features that depend on the entry's structural class may not behave as expected. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

trust-transaction-ids

| | |
|---|---|
| *Synopsis* | Indicates whether the directory server should trust the transaction ids that may be received from requests, either through a LDAP control or through a HTTP header. |
| *Description* | When enabled, the transaction IDs are created when the requests do not include one, then are logged; in addition, the server will add a sub-transaction ID control to all forwarded requests. When disabled, the incoming transaction IDs are discarded and new ones are created. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Global Access Control Policy

Provides coarse grained access control for all operations, regardless of whether they are destined for local or proxy backends. Global access control policies are applied in addition to ACIs and privileges.

For a read request (search, compare) to be accepted there must exist a policy granting the read permission to the targeted entry, as well as any attributes included in attribute assertions. Search result entries will also be filtered using the same criteria. Similarly, update requests (add, delete, modify, modify DN) are accepted if there exists a policy granting the write permission to the targeted entry(s), as well as any attributes included with the request. Finally, extended operations and controls are accepted as long as there exists an applicable policy allowing the extended operation or control, irrespective of the targeted entry. By default a policy will match all entries, all types of connection, and all users. The scope may be restricted by specifying any of the request-target-dn-*, user-dn-*, and connection-* properties.

## Dependencies

The following objects have Global Access Control Policies:

- Policy Based Access Control Handler

## Global Access Control Policy Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| allowed-attribute<br>allowed-attribute-exception<br>allowed-control<br>allowed-extended-operation<br>authentication-required<br>connection-client-address-equal-to<br>connection-client-address-not-equal-to<br>connection-minimum-ssf<br>connection-port-equal-to<br>connection-protocol-equal-to<br>permission<br>request-target-dn-equal-to<br>request-target-dn-equal-to-user-dn<br>request-target-dn-not-equal-to<br>user-dn-equal-to<br>user-dn-not-equal-to |

## Basic Properties

allowed-attribute

| | |
| --- | --- |
| *Synopsis* | Allows clients to read or write the specified attributes, along with their sub-types. |
| *Description* | Attributes that are subtypes of listed attributes are implicitly included. In addition, the list of attributes may include the wild-card '*', which represents all user attributes, or the wild-card '+', which represents all operational attributes, or the name of an object class prefixed with '@' to include all attributes defined by the object class. |
| *Default Value* | None |
| *Allowed Values* | The name of an attribute, an objectclass or a wild-card. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

allowed-attribute-exception

| | |
|---|---|
| *Synopsis* | Specifies zero or more attributes which, together with their sub-types, should not be included in the list of allowed attributes. |
| *Description* | This property is typically used when the list of attributes specified by the allowed-attribute property is too broad. It is especially useful when creating policies which grant access to all user attributes (*) except certain sensitive attributes, such as userPassword. |
| *Default Value* | None |
| *Allowed Values* | The name of an attribute, an objectclass or a wild-card. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

allowed-control

| | |
|---|---|
| *Synopsis* | Allows clients to use the specified LDAP controls. |
| *Default Value* | None |
| *Allowed Values* | The name or OID of a control, or a wild-card to allow all controls. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

allowed-extended-operation

| | |
|---|---|
| *Synopsis* | Allows clients to use the specified LDAP extended operations. |
| *Default Value* | None |
| *Allowed Values* | The name or OID of an extended operation, or a wild-card to allow all extensions. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

authentication-required

| | |
|---|---|
| *Synopsis* | Restricts the scope of the policy so that it only applies to authenticated users. |

| | |
|---|---|
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

connection-client-address-equal-to

| | |
|---|---|
| *Synopsis* | Restricts the scope of the policy so that it only applies to connections which match at least one of the specified client host names or address masks. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a sub-network with sub-network mask. |
| *Default Value* | None |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

connection-client-address-not-equal-to

| | |
|---|---|
| *Synopsis* | Restricts the scope of the policy so that it only applies to connections which match none of the specified client host names or address masks. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a sub-network with sub-network mask. |
| *Default Value* | None |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

connection-minimum-ssf

| | |
|---|---|
| *Synopsis* | Restricts the scope of the policy so that it only applies to connections having the specified minimum security strength factor. |
| *Description* | The security strength factor (ssf) pertains to the cipher key strength for connections using DIGEST-MD5, GSSAPI, SSL, or TLS. For example, to require that the connection must have a cipher strength of at least 256 bits, specify a value of 256. |
| *Default Value* | 0 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

connection-port-equal-to

| | |
|---|---|
| *Synopsis* | Restricts the scope of the policy so that it only applies to connections to any of the specified ports, for example 1389. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br><br>Lower limit: 1.<br><br>Upper limit: 65535. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

connection-protocol-equal-to

| | |
|---|---|
| *Synopsis* | Restricts the scope of the policy so that it only applies to connections which match any of the specified protocols. |
| *Default Value* | None |
| *Allowed Values* | The protocol name, such as LDAP, LDAPS, JMX, HTTP, or HTTPS. |
| *Multi-valued* | Yes |
| *Required* | No |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

permission

| | |
|---|---|
| *Synopsis* | Specifies the type of access allowed by this policy. |
| *Default Value* | No access. |
| *Allowed Values* | read: Read access<br><br>write: Write access |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

request-target-dn-equal-to

| | |
|---|---|
| *Synopsis* | Restricts the scope of the policy so that it only applies to requests which target entries matching at least one of the specified DN patterns. |
| *Description* | Valid DN filters are strings composed of zero or more wildcards and RDN components. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com). |
| *Default Value* | None |
| *Allowed Values* | A DN pattern. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

request-target-dn-equal-to-user-dn

| | |
|---|---|
| *Synopsis* | Restricts the scope of the policy so that it only applies to requests sent by authenticated users where the request's target DN is the same as the DN of the authorized user. |
| *Default Value* | false |

| | |
|---|---|
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

request-target-dn-not-equal-to

| | |
|---|---|
| *Synopsis* | Restricts the scope of the policy so that it only applies to requests which target entries matching none of the specified DN patterns. |
| *Description* | Valid DN filters are strings composed of zero or more wildcards and RDN components. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com). |
| *Default Value* | None |
| *Allowed Values* | A DN pattern. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

user-dn-equal-to

| | |
|---|---|
| *Synopsis* | Restricts the scope of the policy so that it only applies to authenticated users whose authorization DN matches at least one of the specified DN patterns. |
| *Description* | Valid DN filters are strings composed of zero or more wildcards and RDN components. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com). |
| *Default Value* | None |
| *Allowed Values* | A DN pattern. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

user-dn-not-equal-to

| | |
|---|---|
| *Synopsis* | Restricts the scope of the policy so that it only applies to authenticated users whose authorization DN matches none of the specified DN patterns. |
| *Description* | Valid DN filters are strings composed of zero or more wildcards and RDN components. A double wildcard ** replaces one or more RDN components (as in uid=dmiller,**,dc=example,dc=com). A simple wildcard * replaces either a whole RDN, or a whole type, or a value substring (as in uid=bj*,ou=people,dc=example,dc=com). |
| *Default Value* | None |
| *Allowed Values* | A DN pattern. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Governing Structure Rule Virtual Attribute

The Governing Structure Rule Virtual Attribute generates a virtual attribute that specifies the DIT structure rule with the schema definitions in effect for the entry. This attribute is defined in RFC 4512.

## Parent

The Governing Structure Rule Virtual Attribute object inherits from Virtual Attribute.

## Governing Structure Rule Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>enabled<br>filter<br>group-dn | conflict-behavior<br>java-class |

| Basic Properties | Advanced Properties |
|---|---|
| scope | |

## Basic Properties

### attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | governingStructureRule |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |

| | |
|---|---|
| *Allowed Values* | base-object: Search the base object only.<br><br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | virtual-overrides-real |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.<br><br>real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |

| | |
|---|---|
| *Default Value* | org.opends.server.extensions.GoverningSturctureRuleVirtualAttributeProvider |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Graphite Monitor Reporter Plugin

The Graphite Monitor Reporter Plugin contains information needed to push server monitoring metrics into a Graphite server.

The Graphite server host/port must be configured as well as the metric name prefix (e.g. "opendj.example.com"). Zero or more white or black list regexp based metric filters can be configured as well as the reporting interval.

## Parent

The Graphite Monitor Reporter Plugin object inherits from Plugin.

## Graphite Monitor Reporter Plugin Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>excluded-metric-pattern<br>graphite-server<br>included-metric-pattern<br>metric-name-prefix<br>reporting-interval | invoke-for-internal-operations<br>java-class<br>plugin-type |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in is enabled for use. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

excluded-metric-pattern

| | |
|---|---|
| *Synopsis* | Zero or more regular expressions identifying metrics that should not be published. The metric name prefix must not be included in the filter. Exclusion patterns take precedence over inclusion patterns. |
| *Default Value* | None |
| *Allowed Values* | Any valid regular expression pattern which is supported by the java.util.regex.Pattern class (see https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 8). |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

graphite-server

| | |
|---|---|
| *Synopsis* | The Graphite server address. |
| *Description* | When using an IPv6 address as the hostname, put brackets around the address as in "[IPv6Address]:port". |
| *Default Value* | None |
| *Allowed Values* | A host name or an IP address followed by a ":" and a port number.<br>Port number must be greater than 1 and less than 65535. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### included-metric-pattern

| | |
|---|---|
| *Synopsis* | Zero or more regular expressions identifying metrics that should be published. The metric name prefix must not be included in the filter. Exclusion patterns take precedence over inclusion patterns. |
| *Default Value* | None |
| *Allowed Values* | Any valid regular expression pattern which is supported by the java.util.regex.Pattern class (see https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 8). |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### metric-name-prefix

| | |
|---|---|
| *Synopsis* | The prefix that will be added to all metric names reported to Graphite. |
| *Description* | The prefix helps distinguish between metrics arriving from different instances of the same application, thereby allowing monitoring applications to monitor the entire service as well as drill-down to specific application instances. Consider including an identifier for the data center, the application type, and a unique identifier for the application instance in the prefix using a dot-separated structure. For example, 'ny.opendj.ds1' identifies the OpenDJ instance "ds1" in the New York data center. |
| *Default Value* | ds |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### reporting-interval

| | |
|---|---|
| *Synopsis* | The interval between successive publications of server metrics to Graphite. |
| *Description* | An interval in the range 10-60 seconds is recommended. Reducing the interval increases the accuracy of the metrics at the cost of network utilization. |
| *Default Value* | 10s |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 1 seconds. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

invoke-for-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in should be invoked for internal operations. |
| *Description* | Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the plug-in implementation. |
| *Default Value* | org.opends.server.plugins.GraphiteMonitorReporterPlugin |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.plugin.DirectoryServerPlugin |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

plugin-type

| | |
|---|---|
| *Synopsis* | Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked. |
| *Default Value* | startup<br><br>shutdown |
| *Allowed Values* | initialization: Invoked at the initialization of the directory server.<br><br>intermediateresponse: Invoked before sending an intermediate repsonse message to the client.<br><br>ldifimport: Invoked for each entry read during an LDIF import.<br><br>ldifimportbegin: Invoked at the beginning of an LDIF import session.<br><br>ldifimportend: Invoked at the end of an LDIF import session.<br><br>postconnect: Invoked whenever a new connection is established to the server.<br><br>postdisconnect: Invoked whenever an existing connection is terminated (by either the client or the server).<br><br>postoperationabandon: Invoked after completing the abandon processing.<br><br>postoperationadd: Invoked after completing the core add processing but before sending the response to the client.<br><br>postoperationbind: Invoked after completing the core bind processing but before sending the response to the client.<br><br>postoperationcompare: Invoked after completing the core compare processing but before sending the response to the client.<br><br>postoperationdelete: Invoked after completing the core delete processing but before sending the response to the client.<br><br>postoperationextended: Invoked after completing the core extended processing but before sending the response to the client.<br><br>postoperationmodify: Invoked after completing the core modify processing but before sending the response to the client.<br><br>postoperationmodifydn: Invoked after completing the core modify DN processing but before sending the response to the client.<br><br>postoperationsearch: Invoked after completing the core search processing but before sending the response to the client.<br><br>postoperationunbind: Invoked after completing the unbind processing.<br><br>postresponseadd: Invoked after sending the add response to the client.<br><br>postresponsebind: Invoked after sending the bind response to the client. |

postresponsecompare: Invoked after sending the compare response to the client.

postresponsedelete: Invoked after sending the delete response to the client.

postresponseextended: Invoked after sending the extended response to the client.

postresponsemodify: Invoked after sending the modify response to the client.

postresponsemodifydn: Invoked after sending the modify DN response to the client.

postresponsesearch: Invoked after sending the search result done message to the client.

postsynchronizationadd: Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete: Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify: Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn: Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd: Invoked prior to performing the core add processing.

preoperationbind: Invoked prior to performing the core bind processing.

preoperationcompare: Invoked prior to performing the core compare processing.

preoperationdelete: Invoked prior to performing the core delete processing.

preoperationextended: Invoked prior to performing the core extended processing.

preoperationmodify: Invoked prior to performing the core modify processing.

preoperationmodifydn: Invoked prior to performing the core modify DN processing.

preoperationsearch: Invoked prior to performing the core search processing.

preparseabandon: Invoked prior to parsing an abandon request.

preparseadd: Invoked prior to parsing an add request.

preparsebind: Invoked prior to parsing a bind request.

preparsecompare: Invoked prior to parsing a compare request.

preparsedelete: Invoked prior to parsing a delete request.

preparseextended: Invoked prior to parsing an extended request.

preparsemodify: Invoked prior to parsing a modify request.

| | |
|---|---|
| | preparsemodifydn: Invoked prior to parsing a modify DN request.<br>preparsesearch: Invoked prior to parsing a search request.<br>preparseunbind: Invoked prior to parsing an unbind request.<br>searchresultentry: Invoked before sending a search result entry to the client.<br>searchresultreference: Invoked before sending a search result reference to the client.<br>shutdown: Invoked during a graceful directory server shutdown.<br>startup: Invoked during the directory server startup process.<br>subordinatedelete: Invoked in the course of deleting a subordinate entry of a delete operation.<br>subordinatemodifydn: Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Group Implementation

*This is an abstract object type that cannot be instantiated.*

Group Implementations define named collections of users.

Different group implementations may have different ways of determining membership. For example, some groups may explicitly list the members, and/or they may dynamically determine membership.

## Group Implementations

The following Group Implementations are available:

- Dynamic Group Implementation
- Static Group Implementation
- Virtual Static Group Implementation

These Group Implementations inherit the properties described below.

# Group Implementation Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| enabled<br>java-class |

## Basic Properties

enabled

| | |
| --- | --- |
| *Synopsis* | Indicates whether the Group Implementation is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
| --- | --- |
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Group Implementation implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.Group |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# GSSAPI SASL Mechanism Handler

The GSSAPI SASL mechanism performs all processing related to SASL GSSAPI authentication using Kerberos V5.

The GSSAPI SASL mechanism provides the ability for clients to authenticate themselves to the server using existing authentication in a Kerberos environment. This mechanism provides the ability to achieve single sign-on for Kerberos-based clients.

## Parent

The GSSAPI SASL Mechanism Handler object inherits from SASL Mechanism Handler.

## Dependencies

GSSAPI SASL Mechanism Handlers depend on the following objects:

- Identity Mapper

## GSSAPI SASL Mechanism Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>identity-mapper<br>kdc-address<br>keytab<br>principal-name<br>quality-of-protection<br>realm<br>server-fqdn | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the SASL mechanism handler is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name(s) of the identity mapper(s) that are to be used with this SASL mechanism handler to match the Kerberos principal included in the SASL bind request to the corresponding user in the directory. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br><br>The referenced identity mapper(s) must be enabled when the GSSAPI SASL Mechanism Handler is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

kdc-address

| | |
|---|---|
| *Synopsis* | Specifies the address of the KDC that is to be used for Kerberos processing. |
| *Description* | If provided, this property must be a fully-qualified DNS-resolvable name. If this property is not provided, then the server attempts to determine it from the system-wide Kerberos configuration. |
| *Default Value* | The server attempts to determine the KDC address from the underlying system configuration. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

keytab

| | |
|---|---|
| *Synopsis* | Specifies the path to the keytab file that should be used for Kerberos processing. |

| | |
|---|---|
| *Description* | If provided, this is either an absolute path or one that is relative to the server instance root. |
| *Default Value* | The server attempts to use the system-wide default keytab. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

principal-name

| | |
|---|---|
| *Synopsis* | Specifies the principal name. |
| *Description* | It can either be a simple user name or a service name such as host/example.com. If this property is not provided, then the server attempts to build the principal name by appending the fully qualified domain name to the string "ldap/". |
| *Default Value* | The server attempts to determine the principal name from the underlying system configuration. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

quality-of-protection

| | |
|---|---|
| *Synopsis* | The name of a property that specifies the quality of protection the server will support. |
| *Default Value* | none |
| *Allowed Values* | confidentiality: Quality of protection equals authentication with integrity and confidentiality protection.<br><br>integrity: Quality of protection equals authentication with integrity protection.<br><br>none: QOP equals authentication only. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

realm

| | |
|---|---|
| *Synopsis* | Specifies the realm to be used for GSSAPI authentication. |
| *Default Value* | The server attempts to determine the realm from the underlying system configuration. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

server-fqdn

| | |
|---|---|
| *Synopsis* | Specifies the DNS-resolvable fully-qualified domain name for the system. |
| *Default Value* | The server attempts to determine the fully-qualified domain name dynamically . |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation. |
| *Default Value* | org.opends.server.extensions.GSSAPISASLMechanismHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.SASLMechanismHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

# Has Subordinates Virtual Attribute

The Has Subordinates Virtual Attribute generates a virtual attribute that indicates whether the entry has any subordinate entries.

## Parent

The Has Subordinates Virtual Attribute object inherits from Virtual Attribute.

## Has Subordinates Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>enabled<br>filter<br>group-dn<br>scope | conflict-behavior<br>java-class |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | hasSubordinates |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br><br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | virtual-overrides-real |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.<br><br>real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | org.opends.server.extensions.HasSubordinatesVirtualAttributeProvider |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Healthy HTTP endpoint

The Healthy HTTP endpoint provides a way to check whether the server is able to handle requests.

At any point in time, the server can become temporarily or permanently unable to handle requests. This endpoint returns 200 without content when the server is able to handle requests or 503 with a JSON containing the reasons why the server is not able to handle requests. The JSON response contains one or both of the following fields: "alive-errors": an array of serious errors. "healthy-errors":

an array of transient errors. When only field "healthy-errors" is returned, the server should eventually recover by itself without administrative actions. When "alive-errors" is returned, an administrative action is needed.

## Parent

The Healthy HTTP endpoint object inherits from HTTP Endpoint.

## Healthy HTTP endpoint Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| authorization-mechanism<br>base-path<br>enabled | java-class |

## Basic Properties

authorization-mechanism

| | |
|---|---|
| *Synopsis* | The HTTP authorization mechanisms supported by this HTTP Endpoint. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing HTTP Authorization Mechanism .<br><br>The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-path

| | |
|---|---|
| *Synopsis* | All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Endpoint is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Healthy HTTP endpoint implementation. |
| *Default Value* | org.opends.server.protocols.http.HealthyEndpoint |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.HttpEndpoint |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## HTTP Access Log Publisher

*This is an abstract object type that cannot be instantiated.*

HTTP Access Log Publishers are responsible for distributing HTTP access log messages from the HTTP access logger to a destination.

HTTP access log messages provide information about the types of HTTP requests processed by the server.

## HTTP Access Log Publishers

The following HTTP Access Log Publishers are available:

- CSV File HTTP Access Log Publisher
- External HTTP Access Log Publisher
- File Based HTTP Access Log Publisher
- JSON File Based HTTP Access Log Publisher

These HTTP Access Log Publishers inherit the properties described below.

## Parent

The HTTP Access Log Publisher object inherits from Log Publisher.

## HTTP Access Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| enabled<br>java-class |

## Basic Properties

enabled

| | |
| --- | --- |
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the HTTP Access Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.HTTPAccessLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# HTTP Anonymous Authorization Mechanism

The HTTP Anonymous Authorization Mechanism is used to define static authorization.

## Parent

The HTTP Anonymous Authorization Mechanism object inherits from HTTP Authorization Mechanism.

## HTTP Anonymous Authorization Mechanism Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>user-dn | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Authorization Mechanism is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

user-dn

| | |
|---|---|
| *Synopsis* | The authorization DN which will be used for performing anonymous operations. |
| *Default Value* | By default, operations will be performed using an anonymously bound connection. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the HTTP Anonymous Authorization Mechanism implementation. |
| *Default Value* | org.opends.server.protocols.http.authz.HttpAnonymousAuthorizationMechanism |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.protocols.http.authz.HttpAuthorizationMechanism |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# HTTP Authorization Mechanism

*This is an abstract object type that cannot be instantiated.*

The HTTP Authorization Mechanism is used to define HTTP authorization mechanism.

## HTTP Authorization Mechanisms

The following HTTP Authorization Mechanisms are available:

- HTTP Anonymous Authorization Mechanism
- HTTP Basic Authorization Mechanism
- HTTP OAuth2 Authorization Mechanism

These HTTP Authorization Mechanisms inherit the properties described below.

## Dependencies

The following objects depend on HTTP Authorization Mechanisms:

- HTTP Endpoint

## HTTP Authorization Mechanism Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Authorization Mechanism is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the HTTP Authorization Mechanism implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.protocols.http.authz.HttpAuthorizationMechanism |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## HTTP Basic Authorization Mechanism

The HTTP Basic Authorization Mechanism authenticates the end-user using credentials extracted from the HTTP Basic 'Authorization' header.

### Parent

The HTTP Basic Authorization Mechanism object inherits from HTTP Authorization Mechanism.

### Dependencies

HTTP Basic Authorization Mechanisms depend on the following objects:

- Identity Mapper

### HTTP Basic Authorization Mechanism Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| alt-authentication-enabled<br>alt-password-header<br>alt-username-header<br>enabled<br>identity-mapper | java-class |

## Basic Properties

### alt-authentication-enabled

| | |
|---|---|
| *Synopsis* | Specifies whether user credentials may be provided using alternative headers to the standard 'Authorize' header. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### alt-password-header

| | |
|---|---|
| *Synopsis* | Alternate HTTP headers to get the user's password from. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### alt-username-header

| | |
|---|---|
| *Synopsis* | Alternate HTTP headers to get the user's name from. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Authorization Mechanism is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name of the identity mapper(s) used to get the user's entry corresponding to the user-id provided in the HTTP authentication header. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br>The referenced identity mapper(s) must be enabled when the HTTP Basic Authorization Mechanism is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the HTTP Basic Authorization Mechanism implementation. |

| | |
|---|---|
| *Default Value* | org.opends.server.protocols.http.authz.HttpBasicAuthorizationMechanism |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.protocols.http.authz.HttpAuthorizationMechanism |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# HTTP Connection Handler

HTTP Connection Handlers provide HTTP services built on top of the underlying LDAP directory.

It routes HTTP requests to HTTP endpoints registered in the configuration.

## Parent

The HTTP Connection Handler object inherits from Connection Handler.

## Dependencies

HTTP Connection Handlers depend on the following objects:

- Key Manager Provider
- Trust Manager Provider

## HTTP Connection Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| advertised-listen-address<br>allowed-client<br>api-descriptor-enabled<br>denied-client<br>enabled<br>keep-stats<br>key-manager-provider<br>listen-address | accept-backlog<br>allow-tcp-reuse-address<br>buffer-size<br>java-class<br>max-blocked-write-time-limit<br>max-request-size<br>num-request-handlers<br>use-tcp-keep-alive |

| Basic Properties | Advanced Properties |
|---|---|
| listen-port<br>max-concurrent-ops-per-connection<br>restricted-client<br>restricted-client-connection-limit<br>ssl-cert-nickname<br>ssl-cipher-suite<br>ssl-client-auth-policy<br>ssl-protocol<br>trust-manager-provider<br>use-ssl | use-tcp-no-delay |

## Basic Properties

advertised-listen-address

| | |
|---|---|
| *Synopsis* | The advertised address(es) which clients should use for connecting to this HTTP Connection Handler. |
| *Description* | Multiple addresses may be provided as separate values for this attribute. The meta-address 0.0.0.0 is not permitted. |
| *Default Value* | None |
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

allowed-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be allowed to establish connections to this Connection Handler. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| | Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

api-descriptor-enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Connection Handler should publish Swagger and CREST API descriptors. |
| *Description* | When enabled, API descriptors facilitate development of new client client applications. The API descriptors are not protected and are not recommended for production systems." |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

denied-client

| | |
|---|---|
| *Synopsis* | A set of clients who are not allowed to establish connections to this Connection Handler. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Connection Handler is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

keep-stats

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Connection Handler should keep statistics. |
| *Description* | If enabled, the HTTP Connection Handler maintains statistics about the number and types of operations requested over HTTP and the amount of data sent and received. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the key manager that should be used with this HTTP Connection Handler . |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Key Manager Provider .<br>The referenced key manager provider must be enabled when the HTTP Connection Handler is enabled and configured to use SSL. |
| *Multi-valued* | No |
| *Required* | No |

| | |
|---|---|
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

listen-address

| | |
|---|---|
| *Synopsis* | The network interface(s) on which this HTTP Connection Handler should listen for incoming client connections. |
| *Description* | Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the directory server will listen on all interfaces. |
| *Default Value* | 0.0.0.0 |
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

listen-port

| | |
|---|---|
| *Synopsis* | Specifies the port number on which the HTTP Connection Handler will listen for connections from clients. |
| *Description* | Only a single port number may be provided. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br>Lower limit: 1.<br>Upper limit: 65535. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

max-concurrent-ops-per-connection

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of internal operations that each HTTP client connection can execute concurrently. |
| *Description* | This property allow to limit the impact that each HTTP request can have on the whole server by limiting the number of internal operations that each HTTP request can execute concurrently. A value of 0 means that no limit is enforced. |

| | |
|---|---|
| *Default Value* | Let the server decide. |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be limited to the maximum number of connections specified by the "restricted-client-connection-limit" property. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | No restrictions are imposed on the number of connections a client can open. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client-connection-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of connections a restricted client can open at the same time to this Connection Handler. |
| *Description* | Once Directory Server accepts the specified number of connections from a client specified in restricted-client, any additional connection will be rejected. The number of connections is maintained by IP address. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | 100 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cert-nickname

| | |
|---|---|
| *Synopsis* | Specifies the nicknames (also called the aliases) of the keys or key pairs that the HTTP Connection Handler should use when performing SSL communication. |
| *Description* | The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the HTTP Connection Handler is configured to use SSL. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cipher-suite

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL cipher suites that are allowed for use in SSL communication. |
| *Default Value* | Uses the default set of SSL cipher suites provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-client-auth-policy

| | |
|---|---|
| *Synopsis* | Specifies the policy that the HTTP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". |
| *Description* | This is only applicable if clients are allowed to use SSL. |
| *Default Value* | optional |
| *Allowed Values* | disabled: Clients must not provide their own certificates when performing SSL negotiation.<br><br>optional: Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate.<br><br>required: Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-protocol

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL protocols that are allowed for use in SSL communication. |
| *Default Value* | Uses the default set of SSL protocols provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

trust-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name(s) of the trust manager(s) that should be used with the HTTP Connection Handler. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Trust Manager Provider .<br><br>The referenced trust manager provider must be enabled when the HTTP Connection Handler is enabled, is configured to use SSL and its SSL client auth policy is set to required or optional. |
| *Multi-valued* | Yes |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

use-ssl

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Connection Handler should use SSL. |
| *Description* | If enabled, the HTTP Connection Handler will use SSL to encrypt communication with the clients. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

accept-backlog

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. |
| *Description* | This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established. |
| *Default Value* | 128 |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

allow-tcp-reuse-address

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Connection Handler should reuse socket descriptors. |
| *Description* | If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

buffer-size

| | |
|---|---|
| *Synopsis* | Specifies the size in bytes of the HTTP response message write buffer. |
| *Description* | This property specifies write buffer size allocated by the server for each client connection and used to buffer HTTP response messages data when writing. |
| *Default Value* | 4096 bytes |
| *Allowed Values* | Uses *Size Syntax* .<br>Lower limit: 1.<br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the HTTP Connection Handler implementation. |

| | |
|---|---|
| *Default Value* | org.opends.server.protocols.http.HTTPConnectionHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.ConnectionHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

max-blocked-write-time-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum length of time that attempts to write data to HTTP clients should be allowed to block. |
| *Description* | If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated. |
| *Default Value* | 2 minutes |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 0 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

max-request-size

| | |
|---|---|
| *Synopsis* | Specifies the size in bytes of the largest HTTP request message that will be allowed by the HTTP Connection Handler. |
| *Description* | This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory. |
| *Default Value* | 5 megabytes |
| *Allowed Values* | Uses *Size Syntax* .<br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |

| | |
|---|---|
| *Read-Only* | No |

num-request-handlers

| | |
|---|---|
| *Synopsis* | Specifies the number of request handlers that are used to read requests from clients. |
| *Description* | The HTTP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

use-tcp-keep-alive

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Connection Handler should use TCP keep-alive. |
| *Description* | If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

use-tcp-no-delay

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Connection Handler should use TCP no-delay. |

| | |
|---|---|
| *Description* | If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# HTTP Endpoint

*This is an abstract object type that cannot be instantiated.*

The HTTP Endpoint is used to define HTTP endpoint.

## HTTP Endpoints

The following HTTP Endpoints are available:

- Admin Endpoint
- Alive HTTP endpoint
- Common REST Metrics HTTP Endpoint
- Healthy HTTP endpoint
- Prometheus HTTP Endpoint
- Rest2LDAP Endpoint

These HTTP Endpoints inherit the properties described below.

## Dependencies

HTTP Endpoints depend on the following objects:

- HTTP Authorization Mechanism

## HTTP Endpoint Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| authorization-mechanism<br>base-path<br>enabled<br>java-class |

## Basic Properties

authorization-mechanism

| | |
| --- | --- |
| *Synopsis* | The HTTP authorization mechanisms supported by this HTTP Endpoint. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing HTTP Authorization Mechanism .<br><br>The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-path

| | |
| --- | --- |
| *Synopsis* | All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Endpoint is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the HTTP Endpoint implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.HttpEndpoint |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# HTTP OAuth2 Authorization Mechanism

*This is an abstract object type that cannot be instantiated.*

The HTTP OAuth2 Authorization Mechanism is used to define HTTP OAuth2 authorization mechanism.

## HTTP OAuth2 Authorization Mechanisms

The following HTTP OAuth2 Authorization Mechanisms are available:

- HTTP OAuth2 CTS Authorization Mechanism
- HTTP OAuth2 File Based Authorization Mechanism

- HTTP OAuth2 OpenAM Authorization Mechanism
- HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism

These HTTP OAuth2 Authorization Mechanisms inherit the properties described below.

## Parent

The HTTP OAuth2 Authorization Mechanism object inherits from HTTP Authorization Mechanism.

## Dependencies

HTTP OAuth2 Authorization Mechanisms depend on the following objects:

- Identity Mapper

## HTTP OAuth2 Authorization Mechanism Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| access-token-cache-enabled<br>access-token-cache-expiration<br>authzid-json-pointer<br>enabled<br>identity-mapper<br>required-scope | java-class |

## Basic Properties

access-token-cache-enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP OAuth2 Authorization Mechanism is enabled for use. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

access-token-cache-expiration

| | |
|---|---|
| *Synopsis* | Token cache expiration |
| *Default Value* | None |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 0 seconds.<br>Upper limit: 2147483647 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

authzid-json-pointer

| | |
|---|---|
| *Synopsis* | Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Authorization Mechanism is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name of the identity mapper(s) to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br><br>The referenced identity mapper(s) must be enabled when the HTTP OAuth2 Authorization Mechanism is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

required-scope

| | |
|---|---|
| *Synopsis* | Scopes required to grant access to the service. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the HTTP Authorization Mechanism implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.protocols.http.authz.HttpAuthorizationMechanism |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |

| | |
|---|---|
| *Read-Only* | No |

# HTTP OAuth2 CTS Authorization Mechanism

The HTTP OAuth2 CTS Authorization Mechanism is used to define OAuth2 authorization through a direct access to the CTS (Core Token Service).

## Parent

The HTTP OAuth2 CTS Authorization Mechanism object inherits from HTTP OAuth2 Authorization Mechanism.

## HTTP OAuth2 CTS Authorization Mechanism Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| access-token-cache-enabled<br>access-token-cache-expiration<br>authzid-json-pointer<br>base-dn<br>enabled<br>identity-mapper<br>required-scope | java-class |

## Basic Properties

access-token-cache-enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP OAuth2 Authorization Mechanism is enabled for use. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

access-token-cache-expiration

| | |
|---|---|
| *Synopsis* | Token cache expiration |
| *Default Value* | None |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 0 seconds.<br>Upper limit: 2147483647 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

authzid-json-pointer

| | |
|---|---|
| *Synopsis* | Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | The base DN of the Core Token Service where access token are stored. (example: ou=famrecords,ou=openam-session,ou=tokens,dc=example,dc=com) |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Authorization Mechanism is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name of the identity mapper(s) to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br>The referenced identity mapper(s) must be enabled when the HTTP OAuth2 Authorization Mechanism is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

required-scope

| | |
|---|---|
| *Synopsis* | Scopes required to grant access to the service. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the HTTP OAuth2 CTS Authorization Mechanism implementation. |
| *Default Value* | org.opends.server.protocols.http.authz.HttpOAuth2CtsAuthorizationMechanism |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.protocols.http.authz.HttpAuthorizationMechanism |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# HTTP OAuth2 File Based Authorization Mechanism

The HTTP OAuth2 File Based Authorization Mechanism is used to define OAuth2 authorization through a file based access-token resolution. For test purpose only, this mechanism is looking up for JSON access-token files under the specified path.

## Parent

The HTTP OAuth2 File Based Authorization Mechanism object inherits from HTTP OAuth2 Authorization Mechanism.

## HTTP OAuth2 File Based Authorization Mechanism Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| access-token-cache-enabled<br>access-token-cache-expiration<br>access-token-directory<br>authzid-json-pointer<br>enabled<br>identity-mapper<br>required-scope | java-class |

## Basic Properties

access-token-cache-enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP OAuth2 Authorization Mechanism is enabled for use. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

access-token-cache-expiration

| | |
|---|---|
| *Synopsis* | Token cache expiration |
| *Default Value* | None |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 0 seconds.<br>Upper limit: 2147483647 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

access-token-directory

| | |
|---|---|
| *Synopsis* | Directory containing token files. File names must be equal to the token strings. The file content must a JSON object with the following attributes: 'scope', 'expireTime' and all the field(s) needed to resolve the authzIdTemplate. |
| *Default Value* | oauth2-demo/ |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

authzid-json-pointer

| | |
|---|---|
| *Synopsis* | Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Authorization Mechanism is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name of the identity mapper(s) to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br><br>The referenced identity mapper(s) must be enabled when the HTTP OAuth2 Authorization Mechanism is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

required-scope

| | |
|---|---|
| *Synopsis* | Scopes required to grant access to the service. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the HTTP OAuth2 File Based Authorization Mechanism implementation. |
| *Default Value* | org.opends.server.protocols.http.authz.HttpOAuth2FileAuthorizationMechanism |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.protocols.http.authz.HttpAuthorizationMechanism |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## HTTP OAuth2 OpenAM Authorization Mechanism

The HTTP OAuth2 OpenAM Authorization Mechanism is used to define OAuth2 authorization using an OpenAM server as authorization server .

### Parent

The HTTP OAuth2 OpenAM Authorization Mechanism object inherits from HTTP OAuth2 Authorization Mechanism.

### Dependencies

HTTP OAuth2 OpenAM Authorization Mechanisms depend on the following objects:

- Key Manager Provider
- Trust Manager Provider

## HTTP OAuth2 OpenAM Authorization Mechanism Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| access-token-cache-enabled<br>access-token-cache-expiration<br>authzid-json-pointer<br>enabled<br>identity-mapper<br>key-manager-provider<br>required-scope<br>ssl-cert-nickname<br>ssl-cipher-suite<br>ssl-protocol<br>token-info-url<br>trust-manager-provider | java-class |

## Basic Properties

### access-token-cache-enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP OAuth2 Authorization Mechanism is enabled for use. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### access-token-cache-expiration

| | |
|---|---|
| *Synopsis* | Token cache expiration |
| *Default Value* | None |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 0 seconds. |

| | |
|---|---|
| | Upper limit: 2147483647 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

authzid-json-pointer

| | |
|---|---|
| *Synopsis* | Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Authorization Mechanism is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name of the identity mapper(s) to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br><br>The referenced identity mapper(s) must be enabled when the HTTP OAuth2 Authorization Mechanism is enabled. |

| | |
|---|---|
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the key manager that should be used with this HTTP OAuth2 OpenAM Authorization Mechanism . |
| *Default Value* | By default the system key manager(s) will be used. |
| *Allowed Values* | The name of an existing Key Manager Provider .<br><br>The referenced key manager provider must be enabled. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only for subsequent requests to the authorization server. |
| *Advanced* | No |
| *Read-Only* | No |

required-scope

| | |
|---|---|
| *Synopsis* | Scopes required to grant access to the service. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cert-nickname

| | |
|---|---|
| *Synopsis* | Specifies the nicknames (also called the aliases) of the keys or key pairs that the HTTP OAuth2 OpenAM Authorization Mechanism should use when performing SSL communication. |
| *Description* | The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an |

| | |
|---|---|
| | asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the HTTP OAuth2 OpenAM Authorization Mechanism is configured to use SSL. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cipher-suite

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL cipher suites that are allowed for use in SSL or TLS communication. |
| *Default Value* | Uses the default set of SSL cipher suites provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-protocol

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL protocols that are allowed for use in SSL or TLS communication. |
| *Default Value* | Uses the default set of SSL protocols provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

token-info-url

| | |
|---|---|
| *Synopsis* | Defines the OpenAM endpoint URL where the access-token resolution request should be sent. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

trust-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server. |
| *Default Value* | By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted. |
| *Allowed Values* | The name of an existing Trust Manager Provider .<br><br>The referenced trust manager provider must be enabled when SSL is enabled. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations. |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the HTTP OAuth2 OpenAM Authorization Mechanism implementation. |
| *Default Value* | org.opends.server.protocols.http.authz.HttpOAuth2OpenAmAuthorizationMechanism |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.protocols.http.authz.HttpAuthorizationMechanism |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism

The HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism is used to define OAuth2 authorization using an introspection (RFC7662) compliant authorization server.

## Parent

The HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism object inherits from HTTP OAuth2 Authorization Mechanism.

## Dependencies

HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanisms depend on the following objects:

- Key Manager Provider
- Trust Manager Provider

## HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| access-token-cache-enabled<br>access-token-cache-expiration<br>authzid-json-pointer<br>client-id<br>client-secret<br>enabled<br>identity-mapper<br>key-manager-provider<br>required-scope<br>ssl-cert-nickname | java-class |

| Basic Properties | Advanced Properties |
|---|---|
| ssl-cipher-suite<br>ssl-protocol<br>token-introspection-url<br>trust-manager-provider | |

## Basic Properties

### access-token-cache-enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP OAuth2 Authorization Mechanism is enabled for use. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### access-token-cache-expiration

| | |
|---|---|
| *Synopsis* | Token cache expiration |
| *Default Value* | None |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 0 seconds.<br>Upper limit: 2147483647 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### authzid-json-pointer

| | |
|---|---|
| *Synopsis* | Specifies the JSON pointer to the value to use as Authorization ID. The JSON pointer is applied to the resolved access token JSON document. |
| *Default Value* | None |
| *Allowed Values* | A string. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

client-id

| | |
|---|---|
| *Synopsis* | Client's ID to use during the HTTP basic authentication against the authorization server. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

client-secret

| | |
|---|---|
| *Synopsis* | Client's secret to use during the HTTP basic authentication against the authorization server. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Authorization Mechanism is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name of the identity mapper(s) to use in conjunction with the authzid-json-pointer to get the user corresponding to the acccess-token. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br><br>The referenced identity mapper(s) must be enabled when the HTTP OAuth2 Authorization Mechanism is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the key manager that should be used with this HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism . |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Key Manager Provider .<br><br>The referenced key manager provider must be enabled. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only for subsequent requests to the authorization server. |
| *Advanced* | No |
| *Read-Only* | No |

required-scope

| | |
|---|---|
| *Synopsis* | Scopes required to grant access to the service. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cert-nickname

| | |
|---|---|
| *Synopsis* | Specifies the nicknames (also called the aliases) of the keys or key pairs that the HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism should use when performing SSL communication. |
| *Description* | The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism is configured to use SSL. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cipher-suite

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL cipher suites that are allowed for use in SSL or TLS communication. |
| *Default Value* | Uses the default set of SSL cipher suites provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-protocol

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL protocols that are allowed for use in SSL or TLS communication. |
| *Default Value* | Uses the default set of SSL protocols provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

token-introspection-url

| | |
|---|---|
| *Synopsis* | Defines the token introspection endpoint URL where the access-token resolution request should be sent. (example: http://example.com/introspect) |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

trust-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the trust manager that should be used when negotiating SSL connections with the remote authorization server. |
| *Default Value* | By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted. |
| *Allowed Values* | The name of an existing Trust Manager Provider .<br><br>The referenced trust manager provider must be enabled when SSL is enabled. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations. |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism implementation. |
| *Default Value* | org.opends.server.protocols.http.authz.HttpOAuth2TokenIntrospectionAuthorizationMechani |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.protocols.http.authz.HttpAuthorizationMechanism |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## Identity Mapper

*This is an abstract object type that cannot be instantiated.*

Identity Mappers are responsible for establishing a mapping between an identifier string provided by a client, and the entry for the user that corresponds to that identifier. Identity Mappers are used to process several SASL mechanisms to map an authorization ID (e.g., a Kerberos principal when using GSSAPI) to a directory user. They are also used when processing requests with the proxied authorization control.

### Identity Mappers

The following Identity Mappers are available:

- Exact Match Identity Mapper
- Regular Expression Identity Mapper

These Identity Mappers inherit the properties described below.

### Dependencies

The following objects depend on Identity Mappers:

- CRAM-MD5 SASL Mechanism Handler
- DIGEST-MD5 SASL Mechanism Handler
- Global Configuration
- GSSAPI SASL Mechanism Handler
- HTTP Basic Authorization Mechanism
- HTTP OAuth2 Authorization Mechanism
- Password Modify Extended Operation Handler
- Plain SASL Mechanism Handler
- SCRAM-SHA-256 SASL Mechanism Handler
- SCRAM-SHA-512 SASL Mechanism Handler

## Identity Mapper Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| enabled<br>java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Identity Mapper is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Identity Mapper implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.IdentityMapper |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# Is Member Of Virtual Attribute

The Is Member Of Virtual Attribute generates the isMemberOf operational attribute, which contains the DNs of the groups in which the user is a member.

## Parent

The Is Member Of Virtual Attribute object inherits from Virtual Attribute.

## Is Member Of Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>enabled<br>filter<br>group-dn<br>scope | conflict-behavior<br>java-class |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |

| | |
|---|---|
| *Default Value* | isMemberOf |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |

| | |
|---|---|
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br><br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | virtual-overrides-real |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.<br><br>real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | org.opends.server.extensions.IsMemberOfVirtualAttributeProvider |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |

| | |
|---|---|
| *Read-Only* | No |

# JE Backend

A JE Backend stores application data in a Berkeley DB Java Edition database.

It is the traditional "directory server" backend and is similar to the backends provided by the Sun Java System Directory Server. The JE Backend stores the entries in an encoded form and also provides indexes that can be used to quickly locate target entries based on different kinds of criteria.

## Parent

The JE Backend object inherits from Pluggable Backend.

## JE Backend Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| backend-id<br>base-dn<br>cipher-key-length<br>cipher-transformation<br>compact-encoding<br>confidentiality-enabled<br>db-cache-percent<br>db-cache-size<br>db-directory<br>enabled<br>writability-mode | db-cache-mode<br>db-checkpointer-bytes-interval<br>db-checkpointer-wakeup-interval<br>db-cleaner-min-utilization<br>db-directory-permissions<br>db-durability<br>db-evictor-core-threads<br>db-evictor-keep-alive<br>db-evictor-max-threads<br>db-log-file-max<br>db-log-filecache-size<br>db-log-verifier-schedule<br>db-logging-file-handler-on<br>db-logging-level<br>db-num-cleaner-threads<br>db-num-lock-tables<br>db-run-cleaner<br>db-run-log-verifier<br>disk-full-threshold<br>disk-low-threshold<br>entries-compressed<br>import-offheap-memory-size<br>index-entry-limit<br>index-filter-analyzer-enabled<br>index-filter-analyzer-max-filters<br>java-class |

| Basic Properties | Advanced Properties |
|---|---|
| | je-property |

## Basic Properties

### backend-id

| | |
|---|---|
| *Synopsis* | Specifies a name to identify the associated backend. |
| *Description* | The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

### base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DN(s) for the data that the backend handles. |
| *Description* | A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN. |
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None<br><br>No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used. |
| *Advanced* | No |
| *Read-Only* | No |

### cipher-key-length

| | |
|---|---|
| *Synopsis* | Specifies the key length in bits for the preferred cipher. |

| | |
|---|---|
| *Default Value* | 128 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only affect cryptographic operations performed after the change. |
| *Advanced* | No |
| *Read-Only* | No |

cipher-transformation

| | |
|---|---|
| *Synopsis* | Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". |
| *Description* | The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding. |
| *Default Value* | AES/GCM/NoPadding |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only affect cryptographic operations performed after the change. |
| *Advanced* | No |
| *Read-Only* | No |

compact-encoding

| | |
|---|---|
| *Synopsis* | Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. |
| *Description* | Note that this property applies only to the entries themselves and does not impact the index data. It will also replace the attribute descriptions used in add and modify operations with normalized ones from the schema. |
| *Default Value* | true |
| *Allowed Values* | true |

| | |
|---|---|
| | false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data. |
| *Advanced* | No |
| *Read-Only* | No |

confidentiality-enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the backend should make entries in database files readable only by Directory Server. |
| *Description* | Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

db-cache-percent

| | |
|---|---|
| *Synopsis* | Specifies the percentage of JVM memory to allocate to the database cache. |
| *Description* | Specifies the percentage of memory available to the JVM that should be used for caching database contents. Note that this is only used if the value of the db-cache-size property is set to "0 MB". Otherwise, the value of that property is used instead to control the cache size configuration. Note also that this option is ignored if the global option je-backend-shared-cache-enabled is true. |
| *Default Value* | 50 |
| *Allowed Values* | An integer.<br><br>Lower limit: 1.<br><br>Upper limit: 90. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

db-cache-size

| | |
|---|---|
| *Synopsis* | The amount of JVM memory to allocate to the database cache. |
| *Description* | Specifies the amount of memory that should be used for caching database contents. A value of "0 MB" indicates that the db-cache-percent property should be used instead to specify the cache size. Note also that this option is ignored if the global option je-backend-shared-cache-enabled is true. |
| *Default Value* | 0 MB |
| *Allowed Values* | Uses *Size Syntax* . |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

db-directory

| | |
|---|---|
| *Synopsis* | Specifies the path to the filesystem directory that is used to hold the Berkeley DB Java Edition database files containing the data for this backend. |
| *Description* | The path may be either an absolute path or a path relative to the directory containing the base of the OpenDJ directory server installation. The path may be any valid directory path in which the server has appropriate permissions to read and write files and has sufficient space to hold the database contents. |
| *Default Value* | db |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the backend is enabled in the server. |
| *Description* | If a backend is not enabled, then its contents are not accessible when processing operations. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

writability-mode

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the backend should use when processing write operations. |
| *Default Value* | enabled |
| *Allowed Values* | disabled: Causes all write attempts to fail.<br>enabled: Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).<br>internal-only: Causes external write attempts to fail but allows writes by replication and internal operations. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

db-cache-mode

| | |
|---|---|
| *Synopsis* | The strategy that will be used for caching database content in memory. |
| *Description* | Specifies whether the database heap cache should keep only internal nodes or both internal and leaf nodes. |
| *Default Value* | cache-ln |
| *Allowed Values* | adaptive: Regularly check the database and cache metrics and set the best cache mode accordingly. |

| | |
|---|---|
| | cache-ln: Keep both internal and leaf nodes in the database heap cache. This can improve performance when the database is relatively small and when the database fits entirely into the database cache. This mode requires the cache to be rebuilt after each restart.<br><br>evict-ln: Keep only internal nodes in the database heap cache. Leaf nodes will only be cached by the file system. This mode improves performance most when the database is too big to fit entirely into the database cache, or when the cache size would require an overly large JVM heap. This mode has the advantage of keeping the cache hot between restarts. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

db-checkpointer-bytes-interval

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of bytes that may be written to the database before it is forced to perform a checkpoint. |
| *Description* | This can be used to bound the recovery time that may be required if the database environment is opened without having been properly closed. If this property is set to a non-zero value, the checkpointer wakeup interval is not used. To use time-based checkpointing, set this property to zero. |
| *Default Value* | 500mb |
| *Allowed Values* | Uses *Size Syntax* .<br><br>Upper limit: 9223372036854775807. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

db-checkpointer-wakeup-interval

| | |
|---|---|
| *Synopsis* | Specifies the maximum length of time that may pass between checkpoints. |
| *Description* | Note that this is only used if the value of the checkpointer bytes interval is zero. |
| *Default Value* | 30s |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 1 seconds.<br><br>Upper limit: 4500 seconds. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

db-cleaner-min-utilization

| | |
|---|---|
| *Synopsis* | Specifies the occupancy percentage for "live" data in this backend's database. |
| *Description* | When the amount of "live" data in the database drops below this value, cleaners will act to increase the occupancy percentage by compacting the database. |
| *Default Value* | 50 |
| *Allowed Values* | An integer.<br>Lower limit: 0.<br>Upper limit: 90. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

db-directory-permissions

| | |
|---|---|
| *Synopsis* | Specifies the permissions that should be applied to the directory containing the server database files. |
| *Description* | They should be expressed as three-digit octal values, which is the traditional representation for UNIX file permissions. The three digits represent the permissions that are available for the directory's owner, group members, and other users (in that order), and each digit is the octal representation of the read, write, and execute bits. Note that this only impacts permissions on the database directory and not on the files written into that directory. On UNIX systems, the user's umask controls permissions given to the database files. |
| *Default Value* | 700 |
| *Allowed Values* | Any octal value between 700 and 777 (the owner must always have read, write, and execute permissions on the directory). |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

### db-durability

| | |
|---|---|
| *Synopsis* | Configures the durability level that will be used when committing a transaction. |
| *Description* | High levels of durability offer a greater guarantee that the transaction is persisted to disk, but trade that off for lower performance. |
| *Default Value* | medium |
| *Allowed Values* | high: Write and synchronously flush the log on transaction commit. Transactions exhibit full durability and will not be lost if the application or operating system fails.<br><br>low: Do not write or synchronously flush the log on transaction commit. Database integrity will be maintained, but if the application or system fails, it is possible some number of the most recently committed transactions may be undone (lost) during recovery.<br><br>medium: Write but do not synchronously flush the log on transaction commit. Database integrity will be maintained, but if the operating system fails, it is possible some number of the most recently committed transactions may be undone (lost) during recovery. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

### db-evictor-core-threads

| | |
|---|---|
| *Synopsis* | Specifies the core number of threads in the eviction thread pool. |
| *Description* | Specifies the core number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool. |
| *Default Value* | 1 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0.<br><br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

### db-evictor-keep-alive

| | |
|---|---|
| *Synopsis* | The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. |
| *Description* | The duration that excess threads in the eviction thread pool will stay idle. After this period, idle threads will terminate. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool. |
| *Default Value* | 600s |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 1 seconds.<br>Upper limit: 86400 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

### db-evictor-max-threads

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of threads in the eviction thread pool. |
| *Description* | Specifies the maximum number of threads in the eviction thread pool. These threads help keep memory usage within cache bounds, offloading work from application threads. db-evictor-core-threads, db-evictor-max-threads and db-evictor-keep-alive are used to configure the core, max and keepalive attributes for the eviction thread pool. |
| *Default Value* | 10 |
| *Allowed Values* | An integer.<br>Lower limit: 1.<br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

### db-log-file-max

| | |
|---|---|
| *Synopsis* | Specifies the maximum size of each individual database log file. |
| *Default Value* | 1gb |

| | |
|---|---|
| *Allowed Values* | Uses *Size Syntax* .<br>Lower limit: 1000000.<br>Upper limit: 2147483648. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

db-log-filecache-size

| | |
|---|---|
| *Synopsis* | Specifies the size of the file handle cache. |
| *Description* | The file handle cache is used to keep as much opened log files as possible. When the cache is smaller than the number of logs, the database needs to close some handles and open log files it needs, resulting in less optimal performances. Ideally, the size of the cache should be higher than the number of files contained in the database. Make sure the OS number of open files per process is also tuned appropriately. |
| *Default Value* | 200 |
| *Allowed Values* | An integer.<br>Lower limit: 3.<br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

db-log-verifier-schedule

| | |
|---|---|
| *Synopsis* | Specifies when the background log verifier should run if enabled. By default, verification is performed every day at midnight, local time. |
| *Description* | The schedule is specified using a Crontab style format string as defined in https://en.wikipedia.org/wiki/Cron#Configuration_file. Note that times and dates are specified in local time, not UTC time. If the verifier is already running at the scheduled time, the scheduled run is skipped. |
| *Default Value* | 0 0 * * * |
| *Allowed Values* | A crontab format string (minute hour day month dayofweek). |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

db-logging-file-handler-on

| | |
|---|---|
| *Synopsis* | Indicates whether the database should maintain a je.info file in the same directory as the database log directory. |
| *Description* | This file contains information about the internal processing performed by the underlying database. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

db-logging-level

| | |
|---|---|
| *Synopsis* | Specifies the log level that should be used by the database when it is writing information into the je.info file. |
| *Description* | The database trace logging level is (in increasing order of verbosity) chosen from: OFF, SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST, ALL. |
| *Default Value* | CONFIG |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

db-num-cleaner-threads

| | |
|---|---|
| *Synopsis* | Specifies the number of threads that the backend should maintain to keep the database log files at or near the desired utilization. |
| *Description* | In environments with high write throughput, multiple cleaner threads may be required to maintain the desired utilization. |

| | |
|---|---|
| *Default Value* | Let the server decide. |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

db-num-lock-tables

| | |
|---|---|
| *Synopsis* | Specifies the number of lock tables that are used by the underlying database. |
| *Description* | This can be particularly important to help improve scalability by avoiding contention on systems with large numbers of CPUs. The value of this configuration property should be set to a prime number that is less than or equal to the number of worker threads configured for use in the server. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | An integer.<br><br>Lower limit: 1.<br><br>Upper limit: 32767. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

db-run-cleaner

| | |
|---|---|
| *Synopsis* | Indicates whether the cleaner threads should be enabled to compact the database. |
| *Description* | The cleaner threads are used to periodically compact the database when it reaches a percentage of occupancy lower than the amount specified by the db-cleaner-min-utilization property. They identify database files with a low percentage of live data, and relocate their remaining live data to the end of the log. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

db-run-log-verifier

| | |
|---|---|
| *Synopsis* | Indicates whether the background verifier should verify checksums in the database log. |
| *Description* | If enabled, the entire log is periodically read sequentially and verified. The schedule can be controlled using the db-log-verifier-schedule property. If the verification process detects backend database corruption then the server logs an error message and the backend is taken offline. The corrupted backend should be restored from backup before it can be used again. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

disk-full-threshold

| | |
|---|---|
| *Synopsis* | Full disk threshold to limit database updates |
| *Description* | When the available free space on the disk used by this database instance falls below the value specified, no updates are permitted and the server returns an UNWILLING_TO_PERFORM error. Updates are allowed again as soon as free space rises above the threshold. |
| *Default Value* | 5% of the filesystem size, plus 1 GB |
| *Allowed Values* | Uses *Size Syntax* . |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

disk-low-threshold

| | |
|---|---|
| *Synopsis* | Low disk threshold to limit database updates |

| | |
|---|---|
| *Description* | Specifies the "low" free space on the disk. When the available free space on the disk used by this database instance falls below the value specified, protocol updates on this database are permitted only by a user with the BYPASS_LOCKDOWN privilege. |
| *Default Value* | 5% of the filesystem size, plus 5 GB |
| *Allowed Values* | Uses *Size Syntax* . |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

entries-compressed

| | |
|---|---|
| *Synopsis* | Indicates whether the backend should attempt to compress entries before storing them in the database. |
| *Description* | Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data. |
| *Advanced* | Yes |
| *Read-Only* | No |

import-offheap-memory-size

| | |
|---|---|
| *Synopsis* | Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index). |
| *Default Value* | Use only heap memory. |
| *Allowed Values* | Uses *Size Syntax* . |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

index-entry-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. |
| *Description* | This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis. A value of 0 means there is no limit. Changing the index entry limit significantly can result in serious performance degradation. Please read the documentation before changing this setting. |
| *Default Value* | 4000 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0.<br><br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit. |
| *Advanced* | Yes |
| *Read-Only* | No |

index-filter-analyzer-enabled

| | |
|---|---|
| *Synopsis* | Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. |
| *Description* | Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

index-filter-analyzer-max-filters

| | |
|---|---|
| *Synopsis* | The maximum number of search filter statistics to keep. |
| *Description* | When the maximum number of search filter is reached, the least used one will be deleted. |
| *Default Value* | 25 |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the backend implementation. |
| *Default Value* | org.opends.server.backends.jeb.JEBackend |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.Backend |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

je-property

| | |
|---|---|
| *Synopsis* | Specifies the database and environment properties for the Berkeley DB Java Edition database serving the data for this backend. |
| *Description* | Any Berkeley DB Java Edition property can be specified using the following form: property-name=property-value. Refer to OpenDJ documentation for further information on related properties, their implications, and range values. The definitive identification of all the property parameters is available in the example.properties file of Berkeley DB Java Edition distribution. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# JMX Alert Handler

The JMX Alert Handler is used to generate JMX notifications to alert administrators of significant events that occur within the server.

## Parent

The JMX Alert Handler object inherits from Alert Handler.

## JMX Alert Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| disabled-alert-type<br>enabled<br>enabled-alert-type | java-class |

## Basic Properties

disabled-alert-type

| | |
|---|---|
| *Synopsis* | Specifies the names of the alert types that are disabled for this alert handler. |
| *Description* | If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed. |
| *Default Value* | If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Alert Handler is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled-alert-type

| | |
|---|---|
| *Synopsis* | Specifies the names of the alert types that are enabled for this alert handler. |
| *Description* | If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed. |
| *Default Value* | All alerts with types not included in the set of disabled alert types are allowed. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the JMX Alert Handler implementation. |

| | |
|---|---|
| *Default Value* | org.opends.server.extensions.JMXAlertHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.AlertHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# JMX Connection Handler

The JMX Connection Handler is used to interact with clients using the Java Management Extensions (JMX) protocol.

## Parent

The JMX Connection Handler object inherits from Connection Handler.

## Dependencies

JMX Connection Handlers depend on the following objects:

- Key Manager Provider

## JMX Connection Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| allowed-client<br>denied-client<br>enabled<br>key-manager-provider<br>listen-address<br>listen-port<br>restricted-client<br>restricted-client-connection-limit<br>rmi-port<br>ssl-cert-nickname<br>use-ssl | java-class |

## Basic Properties

### allowed-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be allowed to establish connections to this Connection Handler. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

### denied-client

| | |
|---|---|
| *Synopsis* | A set of clients who are not allowed to establish connections to this Connection Handler. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Connection Handler is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the key manager that should be used with this JMX Connection Handler . |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Key Manager Provider .<br><br>The referenced key manager provider must be enabled when the JMX Connection Handler is enabled and configured to use SSL. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections. |
| *Advanced* | No |
| *Read-Only* | No |

listen-address

| | |
|---|---|
| *Synopsis* | Specifies the address on which this JMX Connection Handler should listen for connections from JMX clients. |
| *Description* | If no value is provided, then the JMX Connection Handler listens on all interfaces. |
| *Default Value* | 0.0.0.0 |
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | Restart the server for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

listen-port

| | |
|---|---|
| *Synopsis* | Specifies the port number on which the JMX Connection Handler will listen for connections from clients. |
| *Description* | Only a single port number may be provided. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br>Lower limit: 1.<br>Upper limit: 65535. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be limited to the maximum number of connections specified by the "restricted-client-connection-limit" property. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | No restrictions are imposed on the number of connections a client can open. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client-connection-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of connections a restricted client can open at the same time to this Connection Handler. |
| *Description* | Once Directory Server accepts the specified number of connections from a client specified in restricted-client, any additional connection will be rejected. The number of connections is maintained by IP address. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | 100 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

rmi-port

| | |
|---|---|
| *Synopsis* | Specifies the port number on which the JMX RMI service will listen for connections from clients. A value of 0 indicates the service to choose a port of its own. |
| *Description* | If the value provided is different than 0, the value will be used as the RMI port. Otherwise, the RMI service will choose a port of its own. |
| *Default Value* | 0 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0.<br><br>Upper limit: 65535. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cert-nickname

| | |
|---|---|
| *Synopsis* | Specifies the nicknames (also called the aliases) of the keys or key pairs that the JMX Connection Handler should use when performing SSL communication. |

| | |
|---|---|
| *Description* | The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the JMX Connection Handler is configured to use SSL. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

use-ssl

| | |
|---|---|
| *Synopsis* | Indicates whether the JMX Connection Handler should use SSL. |
| *Description* | If enabled, the JMX Connection Handler will use SSL to encrypt communication with the clients. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the JMX Connection Handler implementation. |
| *Default Value* | org.opends.server.protocols.jmx.JmxConnectionHandler |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.ConnectionHandler |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# JSON Equality Matching Rule

JSON Equality Matching Rules determine whether two JSON values are equivalent using a custom set of rules.

It is possible to select which JSON fields should be used for matching as well as whether those fields, if they are strings, should be normalized first by trimming white space and/or ignoring case differences.

## Parent

The JSON Equality Matching Rule object inherits from Schema Provider.

## JSON Equality Matching Rule Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| case-sensitive-strings<br>enabled<br>ignore-white-space<br>json-keys<br>matching-rule-name<br>matching-rule-oid | java-class |

## Basic Properties

case-sensitive-strings

| | |
|---|---|
| *Synopsis* | Indicates whether JSON string comparisons should be case-sensitive. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>When this property is changed, indexes using this matching rule must be rebuilt. |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Schema Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

ignore-white-space

| | |
|---|---|
| *Synopsis* | Indicates whether JSON string comparisons should ignore white space. |
| *Description* | When enabled, all leading and trailing white space will be removed and intermediate white space will be reduced to a single character. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>When this property is changed, indexes using this matching rule must be rebuilt. |
| *Advanced* | No |
| *Read-Only* | No |

json-keys

| | |
|---|---|
| *Synopsis* | Specifies which JSON fields should be compared in order to determine whether two JSON objects are equivalent. |

| | |
|---|---|
| *Description* | This parameter is a list of space-delimited JSON pointers. |
| *Default Value* | None |
| *Allowed Values* | A non-empty list of space-delimited JSON pointers. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None<br>When this property is changed, indexes using this matching rule must be rebuilt. |
| *Advanced* | No |
| *Read-Only* | No |

matching-rule-name

| | |
|---|---|
| *Synopsis* | The name of the custom JSON matching rule. |
| *Default Value* | The matching rule will not have a name. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

matching-rule-oid

| | |
|---|---|
| *Synopsis* | The numeric OID of the custom JSON matching rule. |
| *Default Value* | None |
| *Allowed Values* | The OID of the matching rule. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the JSON Equality Matching Rule implementation. |
| *Default Value* | org.opends.server.schema.JsonEqualityMatchingRuleProvider |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.schema.SchemaProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# JSON File Based Access Log Publisher

JSON File Based Access Log Publishers publish access messages to JSON files.

## Parent

The JSON File Based Access Log Publisher object inherits from Common Audit Access Log Publisher.

## Dependencies

JSON File Based Access Log Publishers depend on the following objects:

- Log Retention Policy
- Log Rotation Policy

## JSON File Based Access Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>filtering-policy<br>log-control-oids<br>log-directory<br>log-field-blacklist<br>log-file-name-prefix<br>retention-policy<br>rotation-policy | java-class<br>suppress-internal-operations<br>suppress-synchronization-operations |

## Basic Properties

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### filtering-policy

| | |
|---|---|
| *Synopsis* | Specifies how filtering criteria should be applied to log records. |
| *Default Value* | no-filtering |
| *Allowed Values* | exclusive: Records must not match any of the filtering criteria in order to be logged.<br>inclusive: Records must match at least one of the filtering criteria in order to be logged.<br>no-filtering: No filtering will be performed, and all records will be logged. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### log-control-oids

| | |
|---|---|
| *Synopsis* | Specifies whether control OIDs will be included in operation log records. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

log-directory

| | |
|---|---|
| *Synopsis* | The directory to use for the log files generated by the JSON File Based Access Log Publisher. The path to the directory is relative to the server root. |
| *Default Value* | logs |
| *Allowed Values* | A path to an existing directory that is readable and writable by the server. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

log-field-blacklist

| | |
|---|---|
| *Synopsis* | List of fields that the server omits from access log messages. |
| *Description* | Valid values for this property are JSON paths for fields present in the log file. |
| *Default Value* | No message elements are blacklisted by default |
| *Allowed Values* | A JSON path to an existing object of the access event definition. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-file-name-prefix

| | |
|---|---|
| *Synopsis* | File name prefix (without extension) for CSV and JSON file based access log publishers. |
| *Default Value* | ldap-access |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

retention-policy

| | |
|---|---|
| *Synopsis* | The retention policy to use for the JSON File Based Access Log Publisher. |
| *Description* | When multiple policies are used, log files are cleaned when any of the policy's conditions are met. |
| *Default Value* | No retention policy is used and log files are never cleaned. |
| *Allowed Values* | The name of an existing Log Retention Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

rotation-policy

| | |
|---|---|
| *Synopsis* | The rotation policy to use for the JSON File Based Access Log Publisher. |
| *Description* | When multiple policies are used, rotation will occur if any policy's conditions are met. |
| *Default Value* | No rotation policy is used and log rotation will not occur. |
| *Allowed Values* | The name of an existing Log Rotation Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the JSON File Based Access Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.JsonFileAccessLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

suppress-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether internal operations (for example, operations that are initiated by plugins) should be logged along with the operations that are requested by users. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

suppress-synchronization-operations

| | |
|---|---|
| *Synopsis* | Indicates whether access messages that are generated by synchronization operations should be suppressed. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# JSON File Based HTTP Access Log Publisher

JSON File Based HTTP Access Log Publishers Publish access messages to Json files.

## Parent

The JSON File Based HTTP Access Log Publisher object inherits from HTTP Access Log Publisher.

## Dependencies

JSON File Based HTTP Access Log Publishers depend on the following objects:

- Log Retention Policy
- Log Rotation Policy

## JSON File Based HTTP Access Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>log-directory<br>log-field-blacklist<br>log-field-whitelist<br>log-file-name-prefix<br>retention-policy<br>rotation-policy | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-directory

| | |
|---|---|
| *Synopsis* | The directory to use for the log files generated by the JSON File Based HTTP Access Log Publisher. The path to the directory is relative to the server root. |
| *Default Value* | logs |
| *Allowed Values* | A path to an existing directory that is readable and writable by the server. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

log-field-blacklist

| | |
|---|---|
| *Synopsis* | List of fields that the server omits from access log messages. |
| *Description* | Valid values for this property are JSON paths for fields present in the log file. |
| *Default Value* | No message elements are blacklisted by default |
| *Allowed Values* | A JSON path to an existing object of the access event definition. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-field-whitelist

| | |
|---|---|
| *Synopsis* | List of fields that the server includes in access log messages. |
| *Description* | Valid values for this property are JSON paths for fields present in the log file. |
| *Default Value* | Fields not containing sensitive information are whitelisted by default. |
| *Allowed Values* | A JSON path to an existing object of the access event definition. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-file-name-prefix

| | |
|---|---|
| *Synopsis* | File name prefix (without extension) for CSV and JSON file based access log publishers. |
| *Default Value* | http-access |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

retention-policy

| | |
|---|---|
| *Synopsis* | The retention policy to use for the JSON File Based HTTP Access Log Publisher. |
| *Description* | When multiple policies are used, log files are cleaned when any of the policy's conditions are met. |
| *Default Value* | No retention policy is used and log files are never cleaned. |
| *Allowed Values* | The name of an existing Log Retention Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

rotation-policy

| | |
|---|---|
| *Synopsis* | The rotation policy to use for the JSON File Based HTTP Access Log Publisher. |
| *Description* | When multiple policies are used, rotation will occur if any policy's conditions are met. |
| *Default Value* | No rotation policy is used and log rotation will not occur. |
| *Allowed Values* | The name of an existing Log Rotation Policy . |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the JSON File Based HTTP Access Log Publisher implementation. |
| *Default Value* | org.opends.server.loggers.CommonAuditHTTPAccessLogPublisher |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.LogPublisher |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# JSON Ordering Matching Rule

JSON Ordering Matching Rules determine the relative order of two JSON values using a custom set of rules.

It is possible to select which JSON fields should be used for matching as well as whether those fields, if they are strings, should be normalized first by trimming white space and/or ignoring case differences.

## Parent

The JSON Ordering Matching Rule object inherits from Schema Provider.

## JSON Ordering Matching Rule Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| case-sensitive-strings<br>enabled<br>ignore-white-space<br>json-keys<br>matching-rule-name<br>matching-rule-oid | java-class |

## Basic Properties

case-sensitive-strings

| | |
|---|---|
| *Synopsis* | Indicates whether JSON string comparisons should be case-sensitive. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None<br><br>When this property is changed, indexes using this matching rule must be rebuilt. |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Schema Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

ignore-white-space

| | |
|---|---|
| *Synopsis* | Indicates whether JSON string comparisons should ignore white space. |
| *Description* | When enabled, all leading and trailing white space will be removed and intermediate white space will be reduced to a single character. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>When this property is changed, indexes using this matching rule must be rebuilt. |
| *Advanced* | No |
| *Read-Only* | No |

json-keys

| | |
|---|---|
| *Synopsis* | Specifies which JSON fields should be compared in order to determine the relative order of two JSON objects |
| *Description* | This parameter is a list of space-delimited JSON pointers. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | A non-empty list of space-delimited JSON pointers. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None<br>When this property is changed, indexes using this matching rule must be rebuilt. |
| *Advanced* | No |
| *Read-Only* | No |

matching-rule-name

| | |
|---|---|
| *Synopsis* | The name of the custom JSON matching rule. |
| *Default Value* | The matching rule will not have a name. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

matching-rule-oid

| | |
|---|---|
| *Synopsis* | The numeric OID of the custom JSON matching rule. |
| *Default Value* | None |
| *Allowed Values* | The OID of the matching rule. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the JSON Ordering Matching Rule implementation. |

| | |
|---|---|
| *Default Value* | org.opends.server.schema.JsonOrderingMatchingRuleProvider |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.schema.SchemaProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# JSON Query Equality Matching Rule

The JSON Query Equality Matching Rule Provider provides the ability to configure customized JSON query equality matching rules.

The core schema provides a default 'jsonQueryMatch' equality matching rule for JSON values which match JSON strings according to the LDAP 'caseIgnoreMatch' semantics (i.e trim white space and ignore case differences), as well as the indexing of all JSON fields. This schema provider allows users to create custom JSON matching rules which may use different string matching semantics and, more importantly, may only index a restricted set of JSON fields, thereby consuming less backend resources.

## Parent

The JSON Query Equality Matching Rule object inherits from Schema Provider.

## JSON Query Equality Matching Rule Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| case-sensitive-strings<br>enabled<br>ignore-white-space<br>indexed-field<br>matching-rule-name<br>matching-rule-oid | java-class |

## Basic Properties

case-sensitive-strings

| | |
|---|---|
| *Synopsis* | Indicates whether JSON string comparisons should be case-sensitive. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Schema Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

ignore-white-space

| | |
|---|---|
| *Synopsis* | Indicates whether JSON string comparisons should ignore white-space. |
| *Description* | When enabled all leading and trailing white space will be removed and intermediate white space will be reduced to a single character. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

indexed-field

| | |
|---|---|
| *Synopsis* | Specifies which JSON fields should be indexed. |
| *Description* | A field will be indexed if it matches any of the configured field patterns. |
| *Default Value* | All JSON fields will be indexed. |
| *Allowed Values* | A JSON pointer which may include wild-cards. A single '*' wild-card matches at most a single path element, whereas a double '**' matches zero or more path elements. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

matching-rule-name

| | |
|---|---|
| *Synopsis* | The name of the custom JSON matching rule. |
| *Default Value* | The matching rule will not have a name. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

matching-rule-oid

| | |
|---|---|
| *Synopsis* | The numeric OID of the custom JSON matching rule. |
| *Default Value* | None |
| *Allowed Values* | The OID of the matching rule. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the JSON Query Equality Matching Rule implementation. |
| *Default Value* | org.opends.server.schema.JsonQueryEqualityMatchingRuleProvider |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.schema.SchemaProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Key Manager Provider

*This is an abstract object type that cannot be instantiated.*

Key Manager Providers are responsible for managing the key material that is used to authenticate an SSL connection to its peer.

Key Manager Providers essentially provide access to the certificate that is used by the server when performing SSL or StartTLS negotiation.

## Key Manager Providers

The following Key Manager Providers are available:

- File Based Key Manager Provider
- LDAP Key Manager Provider
- PKCS#11 Key Manager Provider

These Key Manager Providers inherit the properties described below.

## Dependencies

The following objects depend on Key Manager Providers:

- Administration Connector
- Crypto Manager
- HTTP Connection Handler

- HTTP OAuth2 OpenAM Authorization Mechanism
- HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism
- JMX Connection Handler
- LDAP Connection Handler
- Proxy Backend
- Replication Service Discovery Mechanism
- Replication Synchronization Provider
- Static Service Discovery Mechanism

## Key Manager Provider Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| enabled<br>java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Key Manager Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the Key Manager Provider implementation. |
| *Default Value* | None |

| | |
|---|---|
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.KeyManagerProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# Last Mod Plugin

The Last Mod Plugin is used to ensure that the creatorsName and createTimestamp attributes are included in an entry whenever it is added to the server and also to ensure that the modifiersName and modifyTimestamp attributes are updated whenever an entry is modified or renamed.

This behavior is described in RFC 4512. The implementation for the LastMod plugin is contained in the org.opends.server.plugins.LastModPlugin class. It must be configured with the preOperationAdd, preOperationModify, and preOperationModifyDN plugin types, but it does not have any other custom configuration.

## Parent

The Last Mod Plugin object inherits from Plugin.

## Last Mod Plugin Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | invoke-for-internal-operations<br>java-class<br>plugin-type |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true |

| | |
|---|---|
| | false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

invoke-for-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in should be invoked for internal operations. |
| *Description* | Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the plug-in implementation. |
| *Default Value* | org.opends.server.plugins.LastModPlugin |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.plugin.DirectoryServerPlugin |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

plugin-type

| | |
|---|---|
| *Synopsis* | Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked. |
| *Default Value* | preoperationadd<br><br>preoperationmodify<br><br>preoperationmodifydn |
| *Allowed Values* | initialization: Invoked at the initialization of the directory server.<br><br>intermediateresponse: Invoked before sending an intermediate repsonse message to the client.<br><br>ldifimport: Invoked for each entry read during an LDIF import.<br><br>ldifimportbegin: Invoked at the beginning of an LDIF import session.<br><br>ldifimportend: Invoked at the end of an LDIF import session.<br><br>postconnect: Invoked whenever a new connection is established to the server.<br><br>postdisconnect: Invoked whenever an existing connection is terminated (by either the client or the server).<br><br>postoperationabandon: Invoked after completing the abandon processing.<br><br>postoperationadd: Invoked after completing the core add processing but before sending the response to the client.<br><br>postoperationbind: Invoked after completing the core bind processing but before sending the response to the client.<br><br>postoperationcompare: Invoked after completing the core compare processing but before sending the response to the client.<br><br>postoperationdelete: Invoked after completing the core delete processing but before sending the response to the client.<br><br>postoperationextended: Invoked after completing the core extended processing but before sending the response to the client.<br><br>postoperationmodify: Invoked after completing the core modify processing but before sending the response to the client.<br><br>postoperationmodifydn: Invoked after completing the core modify DN processing but before sending the response to the client.<br><br>postoperationsearch: Invoked after completing the core search processing but before sending the response to the client.<br><br>postoperationunbind: Invoked after completing the unbind processing.<br><br>postresponseadd: Invoked after sending the add response to the client. |

postresponsebind: Invoked after sending the bind response to the client.

postresponsecompare: Invoked after sending the compare response to the client.

postresponsedelete: Invoked after sending the delete response to the client.

postresponseextended: Invoked after sending the extended response to the client.

postresponsemodify: Invoked after sending the modify response to the client.

postresponsemodifydn: Invoked after sending the modify DN response to the client.

postresponsesearch: Invoked after sending the search result done message to the client.

postsynchronizationadd: Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete: Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify: Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn: Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd: Invoked prior to performing the core add processing.

preoperationbind: Invoked prior to performing the core bind processing.

preoperationcompare: Invoked prior to performing the core compare processing.

preoperationdelete: Invoked prior to performing the core delete processing.

preoperationextended: Invoked prior to performing the core extended processing.

preoperationmodify: Invoked prior to performing the core modify processing.

preoperationmodifydn: Invoked prior to performing the core modify DN processing.

preoperationsearch: Invoked prior to performing the core search processing.

preparseabandon: Invoked prior to parsing an abandon request.

preparseadd: Invoked prior to parsing an add request.

preparsebind: Invoked prior to parsing a bind request.

preparsecompare: Invoked prior to parsing a compare request.

preparsedelete: Invoked prior to parsing a delete request.

preparseextended: Invoked prior to parsing an extended request.

| | |
|---|---|
| | preparsemodify: Invoked prior to parsing a modify request.<br><br>preparsemodifydn: Invoked prior to parsing a modify DN request.<br><br>preparsesearch: Invoked prior to parsing a search request.<br><br>preparseunbind: Invoked prior to parsing an unbind request.<br><br>searchresultentry: Invoked before sending a search result entry to the client.<br><br>searchresultreference: Invoked before sending a search result reference to the client.<br><br>shutdown: Invoked during a graceful directory server shutdown.<br><br>startup: Invoked during the directory server startup process.<br><br>subordinatedelete: Invoked in the course of deleting a subordinate entry of a delete operation.<br><br>subordinatemodifydn: Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# LDAP Attribute Description List Plugin

The LDAP Attribute Description List Plugin provides the ability for clients to include an attribute list in a search request that names object classes instead of (or in addition to) attributes.

For example, if a client wishes to retrieve all of the attributes in the inetOrgPerson object class, then that client can include "@inetOrgPerson" in the attribute list rather than naming all of those attributes individually. This behavior is based on the specification contained in RFC 4529. The implementation for the LDAP attribute description list plugin is contained in the org.opends.server.plugins.LDAPADListPlugin class. It must be configured with the preParseSearch plugin type, but does not have any other custom configuration.

## Parent

The LDAP Attribute Description List Plugin object inherits from Plugin.

# LDAP Attribute Description List Plugin Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | invoke-for-internal-operations<br>java-class<br>plugin-type |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

invoke-for-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in should be invoked for internal operations. |
| *Description* | Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the plug-in implementation. |
| *Default Value* | org.opends.server.plugins.LDAPADListPlugin |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.plugin.DirectoryServerPlugin |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

plugin-type

| | |
|---|---|
| *Synopsis* | Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked. |
| *Default Value* | preparsesearch |
| *Allowed Values* | initialization: Invoked at the initialization of the directory server.<br>intermediateresponse: Invoked before sending an intermediate repsonse message to the client.<br>ldifimport: Invoked for each entry read during an LDIF import.<br>ldifimportbegin: Invoked at the beginning of an LDIF import session.<br>ldifimportend: Invoked at the end of an LDIF import session.<br>postconnect: Invoked whenever a new connection is established to the server.<br>postdisconnect: Invoked whenever an existing connection is terminated (by either the client or the server).<br>postoperationabandon: Invoked after completing the abandon processing.<br>postoperationadd: Invoked after completing the core add processing but before sending the response to the client.<br>postoperationbind: Invoked after completing the core bind processing but before sending the response to the client.<br>postoperationcompare: Invoked after completing the core compare processing but before sending the response to the client. |

postoperationdelete: Invoked after completing the core delete processing but before sending the response to the client.

postoperationextended: Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify: Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn: Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch: Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind: Invoked after completing the unbind processing.

postresponseadd: Invoked after sending the add response to the client.

postresponsebind: Invoked after sending the bind response to the client.

postresponsecompare: Invoked after sending the compare response to the client.

postresponsedelete: Invoked after sending the delete response to the client.

postresponseextended: Invoked after sending the extended response to the client.

postresponsemodify: Invoked after sending the modify response to the client.

postresponsemodifydn: Invoked after sending the modify DN response to the client.

postresponsesearch: Invoked after sending the search result done message to the client.

postsynchronizationadd: Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete: Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify: Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn: Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd: Invoked prior to performing the core add processing.

preoperationbind: Invoked prior to performing the core bind processing.

preoperationcompare: Invoked prior to performing the core compare processing.

preoperationdelete: Invoked prior to performing the core delete processing.

preoperationextended: Invoked prior to performing the core extended processing.

| | |
|---|---|
| | preoperationmodify: Invoked prior to performing the core modify processing.<br>preoperationmodifydn: Invoked prior to performing the core modify DN processing.<br>preoperationsearch: Invoked prior to performing the core search processing.<br>preparseabandon: Invoked prior to parsing an abandon request.<br>preparseadd: Invoked prior to parsing an add request.<br>preparsebind: Invoked prior to parsing a bind request.<br>preparsecompare: Invoked prior to parsing a compare request.<br>preparsedelete: Invoked prior to parsing a delete request.<br>preparseextended: Invoked prior to parsing an extended request.<br>preparsemodify: Invoked prior to parsing a modify request.<br>preparsemodifydn: Invoked prior to parsing a modify DN request.<br>preparsesearch: Invoked prior to parsing a search request.<br>preparseunbind: Invoked prior to parsing an unbind request.<br>searchresultentry: Invoked before sending a search result entry to the client.<br>searchresultreference: Invoked before sending a search result reference to the client.<br>shutdown: Invoked during a graceful directory server shutdown.<br>startup: Invoked during the directory server startup process.<br>subordinatedelete: Invoked in the course of deleting a subordinate entry of a delete operation.<br>subordinatemodifydn: Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# LDAP Connection Handler

The LDAP Connection Handler is used to interact with clients using LDAP.

It provides full support for LDAPv3 and limited support for LDAPv2.

## Parent

The LDAP Connection Handler object inherits from Connection Handler.

## Dependencies

LDAP Connection Handlers depend on the following objects:

- Key Manager Provider
- Trust Manager Provider

## LDAP Connection Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| advertised-listen-address<br>allow-ldap-v2<br>allow-start-tls<br>allowed-client<br>denied-client<br>enabled<br>keep-stats<br>key-manager-provider<br>listen-address<br>listen-port<br>restricted-client<br>restricted-client-connection-limit<br>ssl-cert-nickname<br>ssl-cipher-suite<br>ssl-client-auth-policy<br>ssl-protocol<br>trust-manager-provider<br>use-ssl | accept-backlog<br>allow-tcp-reuse-address<br>buffer-size<br>java-class<br>max-blocked-write-time-limit<br>max-request-size<br>num-request-handlers<br>send-rejection-notice<br>use-tcp-keep-alive<br>use-tcp-no-delay |

## Basic Properties

advertised-listen-address

| | |
|---|---|
| *Synopsis* | The advertised address(es) which clients should use for connecting to this LDAP Connection Handler. |

| | |
|---|---|
| *Description* | Multiple addresses may be provided as separate values for this attribute. The meta-address 0.0.0.0 is not permitted. |
| *Default Value* | None |
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

allow-ldap-v2

| | |
|---|---|
| *Synopsis* | Indicates whether connections from LDAPv2 clients are allowed. |
| *Description* | If LDAPv2 clients are allowed, then only a minimal degree of special support are provided for them to ensure that LDAPv3-specific protocol elements (for example, Configuration Guide 25 controls, extended response messages, intermediate response messages, referrals) are not sent to an LDAPv2 client. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

allow-start-tls

| | |
|---|---|
| *Synopsis* | Indicates whether clients are allowed to use StartTLS. |
| *Description* | If enabled, the LDAP Connection Handler allows clients to use the StartTLS extended operation to initiate secure communication over an otherwise insecure channel. Note that this is only allowed if the LDAP Connection Handler is not configured to use SSL, and if the server is configured with a valid key manager provider and a valid trust manager provider. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

allowed-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be allowed to establish connections to this Connection Handler. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

denied-client

| | |
|---|---|
| *Synopsis* | A set of clients who are not allowed to establish connections to this Connection Handler. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Connection Handler is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

keep-stats

| | |
|---|---|
| *Synopsis* | Indicates whether the LDAP Connection Handler should keep statistics. |
| *Description* | If enabled, the LDAP Connection Handler maintains statistics about the number and types of operations requested over LDAP and the amount of data sent and received. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the key manager that should be used with this LDAP Connection Handler . |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Key Manager Provider .<br>The referenced key manager provider must be enabled when the LDAP Connection Handler is enabled and configured to use SSL or StartTLS. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections. |
| *Advanced* | No |
| *Read-Only* | No |

listen-address

| | |
|---|---|
| *Synopsis* | The network interface(s) on which this LDAP Connection Handler should listen for incoming client connections. |
| *Description* | Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the directory server will listen on all interfaces. |
| *Default Value* | 0.0.0.0 |
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

listen-port

| | |
|---|---|
| *Synopsis* | Specifies the port number on which the LDAP Connection Handler will listen for connections from clients. |
| *Description* | Only a single port number may be provided. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br><br>Lower limit: 1.<br><br>Upper limit: 65535. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be limited to the maximum number of connections specified by the "restricted-client-connection-limit" property. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | No restrictions are imposed on the number of connections a client can open. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client-connection-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of connections a restricted client can open at the same time to this Connection Handler. |
| *Description* | Once Directory Server accepts the specified number of connections from a client specified in restricted-client, any additional connection will be rejected. The number of connections is maintained by IP address. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | 100 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cert-nickname

| | |
|---|---|
| *Synopsis* | Specifies the nicknames (also called the aliases) of the keys or key pairs that the LDAP Connection Handler should use when performing SSL communication. |

| | |
|---|---|
| *Description* | The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the LDAP Connection Handler is configured to use SSL. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cipher-suite

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL cipher suites that are allowed for use in SSL or StartTLS communication. |
| *Default Value* | Uses the default set of SSL cipher suites provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but will only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-client-auth-policy

| | |
|---|---|
| *Synopsis* | Specifies the policy that the LDAP Connection Handler should use regarding client SSL certificates. Clients can use the SASL EXTERNAL mechanism only if the policy is set to "optional" or "required". |
| *Description* | This is only applicable if clients are allowed to use SSL. |
| *Default Value* | optional |
| *Allowed Values* | disabled: Clients must not provide their own certificates when performing SSL negotiation.<br><br>optional: Clients are requested to provide their own certificates when performing SSL negotiation. The connection is nevertheless accepted if the client does not provide a certificate. |

| | |
|---|---|
| | required: Clients are required to provide their own certificates when performing SSL negotiation and are refused access if they do not provide a certificate. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-protocol

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL protocols that are allowed for use in SSL or StartTLS communication. |
| *Default Value* | Uses the default set of SSL protocols provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

trust-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name(s) of the trust manager(s) that should be used with the LDAP Connection Handler . |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Trust Manager Provider .<br><br>The referenced trust manager provider must be enabled when the LDAP Connection Handler is enabled, configured to use SSL or StartTLS and its SSL client auth policy is set to required or optional. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections. |
| *Advanced* | No |
| *Read-Only* | No |

use-ssl

| | |
|---|---|
| *Synopsis* | Indicates whether the LDAP Connection Handler should use SSL. |
| *Description* | If enabled, the LDAP Connection Handler will use SSL to encrypt communication with the clients. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

accept-backlog

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of pending connection attempts that are allowed to queue up in the accept backlog before the server starts rejecting new connection attempts. |
| *Description* | This is primarily an issue for cases in which a large number of connections are established to the server in a very short period of time (for example, a benchmark utility that creates a large number of client threads that each have their own connection to the server) and the connection handler is unable to keep up with the rate at which the new connections are established. |
| *Default Value* | 128 |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

allow-tcp-reuse-address

| | |
|---|---|
| *Synopsis* | Indicates whether the LDAP Connection Handler should reuse socket descriptors. |

| | |
|---|---|
| *Description* | If enabled, the SO_REUSEADDR socket option is used on the server listen socket to potentially allow the reuse of socket descriptors for clients in a TIME_WAIT state. This may help the server avoid temporarily running out of socket descriptors in cases in which a very large number of short-lived connections have been established from the same client system. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

buffer-size

| | |
|---|---|
| *Synopsis* | Specifies the size in bytes of the LDAP response message write buffer. |
| *Description* | This property specifies write buffer size allocated by the server for each client connection and used to buffer LDAP response messages data when writing. |
| *Default Value* | 4096 bytes |
| *Allowed Values* | Uses *Size Syntax* .<br>Lower limit: 1.<br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the LDAP Connection Handler implementation. |
| *Default Value* | org.opends.server.protocols.ldap.LDAPConnectionHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.ConnectionHandler |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

max-blocked-write-time-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum length of time that attempts to write data to LDAP clients should be allowed to block. |
| *Description* | If an attempt to write data to a client takes longer than this length of time, then the client connection is terminated. |
| *Default Value* | 2 minutes |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 0 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

max-request-size

| | |
|---|---|
| *Synopsis* | Specifies the size in bytes of the largest LDAP request message that will be allowed by this LDAP Connection handler. |
| *Description* | This property is analogous to the maxBERSize configuration attribute of the Sun Java System Directory Server. This can help prevent denial-of-service attacks by clients that indicate they send extremely large requests to the server causing it to attempt to allocate large amounts of memory. |
| *Default Value* | 5 megabytes |
| *Allowed Values* | Uses *Size Syntax* .<br><br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

num-request-handlers

| | |
|---|---|
| *Synopsis* | Specifies the number of request handlers that are used to read requests from clients. |

| | |
|---|---|
| *Description* | The LDAP Connection Handler uses one thread to accept new connections from clients, but uses one or more additional threads to read requests from existing client connections. This ensures that new requests are read efficiently and that the connection handler itself does not become a bottleneck when the server is under heavy load from many clients at the same time. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

send-rejection-notice

| | |
|---|---|
| *Synopsis* | Indicates whether the LDAP Connection Handler should send a notice of disconnection extended response message to the client if a new connection is rejected for some reason. |
| *Description* | The extended response message may provide an explanation indicating the reason that the connection was rejected. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

use-tcp-keep-alive

| | |
|---|---|
| *Synopsis* | Indicates whether the LDAP Connection Handler should use TCP keep-alive. |
| *Description* | If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware. |
| *Default Value* | true |
| *Allowed Values* | true |

| | |
|---|---|
| | false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

use-tcp-no-delay

| | |
|---|---|
| *Synopsis* | Indicates whether the LDAP Connection Handler should use TCP no-delay. |
| *Description* | If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# LDAP Key Manager Provider

The LDAP key manager provider uses an LDAP key store managed by the server to obtain server certificates.

## Parent

The LDAP Key Manager Provider object inherits from Key Manager Provider.

## LDAP Key Manager Provider Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| base-dn<br>enabled<br>key-store-pin | java-class |

## Basic Properties

### base-dn

| | |
|---|---|
| *Synopsis* | The base DN beneath which LDAP key store entries are located. |
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Key Manager Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### key-store-pin

| | |
|---|---|
| *Synopsis* | Specifies the clear-text PIN needed to access the LDAP Key Manager Provider . |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |

| | |
|---|---|
| *Admin Action Required* | None<br><br>Changes to this property will take effect the next time that the LDAP Key Manager Provider is accessed. |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the LDAP Key Manager Provider implementation. |
| *Default Value* | org.opends.server.extensions.LDAPKeyManagerProvider |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.KeyManagerProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## LDAP Pass Through Authentication Policy

An authentication policy for users whose credentials are managed by a remote LDAP directory service.

Authentication attempts will be redirected to the remote LDAP directory service based on a combination of the criteria specified in this policy and the content of the user's entry in this directory server.

### Parent

The LDAP Pass Through Authentication Policy object inherits from Authentication Policy.

### Dependencies

LDAP Pass Through Authentication Policies depend on the following objects:

- Password Storage Scheme
- Trust Manager Provider

## LDAP Pass Through Authentication Policy Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| cached-password-storage-scheme<br>cached-password-ttl<br>connection-timeout<br>mapped-attribute<br>mapped-search-base-dn<br>mapped-search-bind-dn<br>mapped-search-bind-password<br>mapped-search-filter-template<br>mapping-policy<br>primary-remote-ldap-server<br>secondary-remote-ldap-server<br>source-address<br>trust-manager-provider<br>use-password-caching<br>use-ssl | java-class<br>ssl-cipher-suite<br>ssl-protocol<br>use-tcp-keep-alive<br>use-tcp-no-delay |

## Basic Properties

cached-password-storage-scheme

| | |
|---|---|
| *Synopsis* | Specifies the name of a password storage scheme which should be used for encoding cached passwords. |
| *Description* | Changing the password storage scheme will cause all existing cached passwords to be discarded. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Password Storage Scheme .<br><br>The referenced password storage schemes must be enabled. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

cached-password-ttl

| | |
|---|---|
| *Synopsis* | Specifies the maximum length of time that a locally cached password may be used for authentication before it is refreshed from the remote LDAP service. |
| *Description* | This property represents a cache timeout. Increasing the timeout period decreases the frequency that bind operations are delegated to the remote LDAP service, but increases the risk of users authenticating using stale passwords. Note that authentication attempts which fail because the provided password does not match the locally cached password will always be retried against the remote LDAP service. |
| *Default Value* | 8 hours |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 0 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

connection-timeout

| | |
|---|---|
| *Synopsis* | Specifies the timeout used when connecting to remote LDAP directory servers, performing SSL negotiation, and for individual search and bind requests. |
| *Description* | If the timeout expires then the current operation will be aborted and retried against another LDAP server if one is available. |
| *Default Value* | 3 seconds |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 0 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

mapped-attribute

| | |
|---|---|
| *Synopsis* | Specifies one or more attributes in the user's entry whose value(s) will determine the bind DN used when authenticating to the remote LDAP directory service. This property is mandatory when using the "mapped-bind" or "mapped-search" mapping policies. |

| | |
|---|---|
| *Description* | At least one value must be provided. All values must refer to the name or OID of an attribute type defined in the directory server schema. At least one of the named attributes must exist in a user's local entry in order for authentication to proceed. When multiple attributes or values are found in the user's entry then the behavior is determined by the mapping policy. |
| *Default Value* | None |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

mapped-search-base-dn

| | |
|---|---|
| *Synopsis* | Specifies the set of base DNs below which to search for users in the remote LDAP directory service. This property is mandatory when using the "mapped-search" mapping policy. |
| *Description* | If multiple values are given, searches are performed below all specified base DNs. |
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

mapped-search-bind-dn

| | |
|---|---|
| *Synopsis* | Specifies the bind DN which should be used to perform user searches in the remote LDAP directory service. |
| *Default Value* | Searches will be performed anonymously. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

mapped-search-bind-password

| | |
|---|---|
| *Synopsis* | Specifies the bind password which should be used to perform user searches in the remote LDAP directory service. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

mapped-search-filter-template

| | |
|---|---|
| *Synopsis* | If defined, overrides the filter used when searching for the user, substituting %s with the value of the local entry's "mapped-attribute". |
| *Description* | The filter-template may include ZERO or ONE %s substitutions. If multiple mapped-attributes are configured, multiple renditions of this template will be aggregated into one larger filter using an OR (\|) operator. An example use-case for this property would be to use a different attribute type on the mapped search. For example, mapped-attribute could be set to "uid" and filter-template to "(samAccountName=%s)". You can also use the filter to restrict search results. For example: "{@code (&(uid=%s)(objectclass=student))}" |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

mapping-policy

| | |
|---|---|
| *Synopsis* | Specifies the mapping algorithm for obtaining the bind DN from the user's entry. |
| *Default Value* | unmapped |
| *Allowed Values* | mapped-bind: Bind to the remote LDAP directory service using a DN obtained from an attribute in the user's entry. This policy will check each attribute named in the "mapped-attribute" property. If more than one attribute or value is present then the first one will be used.<br><br>mapped-search: Bind to the remote LDAP directory service using the DN of an entry obtained using a search against the remote LDAP directory service. The search filter will comprise of an equality matching filter whose attribute type is the "mapped-attribute" property, and whose assertion value is the attribute value obtained from the user's entry. If more than one attribute or value is present then |

| | |
|---|---|
| | the filter will be composed of multiple equality filters combined using a logical OR (union).<br><br>unmapped: Bind to the remote LDAP directory service using the DN of the user's entry in this directory server. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

primary-remote-ldap-server

| | |
|---|---|
| *Synopsis* | Specifies the primary list of remote LDAP servers which should be used for pass through authentication. |
| *Description* | If more than one LDAP server is specified then operations may be distributed across them. If all of the primary LDAP servers are unavailable then operations will fail-over to the set of secondary LDAP servers, if defined. When using an IPv6 address as the hostname, put brackets around the address as in "[IPv6Address]:port". |
| *Default Value* | None |
| *Allowed Values* | A host name or an IP address followed by a ":" and a port number.<br><br>Port number must be greater than 1 and less than 65535. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

secondary-remote-ldap-server

| | |
|---|---|
| *Synopsis* | Specifies the secondary list of remote LDAP servers which should be used for pass through authentication in the event that the primary LDAP servers are unavailable. |
| *Description* | If more than one LDAP server is specified then operations may be distributed across them. Operations will be rerouted to the primary LDAP servers as soon as they are determined to be available. When using an IPv6 address as the hostname, put brackets around the address as in "[IPv6Address]:port". |
| *Default Value* | No secondary LDAP servers. |
| *Allowed Values* | A host name or an IP address followed by a ":" and a port number.<br><br>Port number must be greater than 1 and less than 65535. |

| | |
|---|---|
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

source-address

| | |
|---|---|
| *Synopsis* | If specified, the server will bind to the address before connecting to the remote server. |
| *Description* | The address must be one assigned to an existing network interface. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

trust-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the trust manager that should be used when negotiating SSL connections with remote LDAP directory servers. |
| *Default Value* | By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted. |
| *Allowed Values* | The name of an existing Trust Manager Provider .<br><br>The referenced trust manager provider must be enabled when SSL is enabled. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations. |
| *Advanced* | No |
| *Read-Only* | No |

use-password-caching

| | |
|---|---|
| *Synopsis* | Indicates whether passwords should be cached locally within the user's entry. |
| *Default Value* | false |

| | |
|---|---|
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

use-ssl

| | |
|---|---|
| *Synopsis* | Indicates whether the LDAP Pass Through Authentication Policy should use SSL. |
| *Description* | If enabled, the LDAP Pass Through Authentication Policy will use SSL to encrypt communication with the clients. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class which provides the LDAP Pass Through Authentication Policy implementation. |
| *Default Value* | org.opends.server.extensions.LDAPPassThroughAuthenticationPolicyFactory |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.AuthenticationPolicyFactory |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |

| | |
|---|---|
| *Read-Only* | No |

ssl-cipher-suite

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL cipher suites that are allowed for use in SSL based LDAP connections. |
| *Default Value* | Uses the default set of SSL cipher suites provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but will only impact new SSL LDAP connections created after the change. |
| *Advanced* | Yes |
| *Read-Only* | No |

ssl-protocol

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL protocols which are allowed for use in SSL based LDAP connections. |
| *Default Value* | Uses the default set of SSL protocols provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but will only impact new SSL LDAP connections created after the change. |
| *Advanced* | Yes |
| *Read-Only* | No |

use-tcp-keep-alive

| | |
|---|---|
| *Synopsis* | Indicates whether LDAP connections should use TCP keep-alive. |
| *Description* | If enabled, the SO_KEEPALIVE socket option is used to indicate that TCP keepalive messages should periodically be sent to the client to verify that the associated connection is still valid. This may also help prevent cases in which intermediate network hardware could silently drop an otherwise idle client connection, provided that the keepalive interval configured in the underlying operating system is smaller than the timeout enforced by the network hardware. |
| *Default Value* | true |
| *Allowed Values* | true |

| | |
|---|---|
| | false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

use-tcp-no-delay

| | |
|---|---|
| *Synopsis* | Indicates whether LDAP connections should use TCP no-delay. |
| *Description* | If enabled, the TCP_NODELAY socket option is used to ensure that response messages to the client are sent immediately rather than potentially waiting to determine whether additional response messages can be sent in the same packet. In most cases, using the TCP_NODELAY socket option provides better performance and lower response times, but disabling it may help for some cases in which the server sends a large number of entries to a client in response to a search request. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# LDAP Trust Manager Provider

The LDAP trust manager provider determines whether to trust a presented certificate based on whether that certificate exists in an LDAP key store managed by the server.

## Parent

The LDAP Trust Manager Provider object inherits from Trust Manager Provider.

## LDAP Trust Manager Provider Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| base-dn<br>enabled<br>trust-store-pin | java-class |

## Basic Properties

### base-dn

| | |
|---|---|
| *Synopsis* | The base DN beneath which LDAP key store entries are located. |
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### enabled

| | |
|---|---|
| *Synopsis* | Indicate whether the Trust Manager Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### trust-store-pin

| | |
|---|---|
| *Synopsis* | Specifies the clear-text PIN needed to access the LDAP Trust Manager Provider . |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |

| | |
|---|---|
| *Admin Action Required* | None<br><br>Changes to this property will take effect the next time that the LDAP Trust Manager Provider is accessed. |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the LDAP Trust Manager Provider implementation. |
| *Default Value* | org.opends.server.extensions.LDAPTrustManagerProvider |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.TrustManagerProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## LDIF Backend

The LDIF Backend provides a mechanism for interacting with data stored in an LDIF file.

All basic LDAP operations are supported in the LDIF backend although it has minimal support for custom controls.

### Parent

The LDIF Backend object inherits from Local Backend.

### LDIF Backend Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| backend-id<br>base-dn<br>enabled<br>is-private-backend<br>ldif-file<br>writability-mode | java-class |

## Basic Properties

### backend-id

| | |
|---|---|
| *Synopsis* | Specifies a name to identify the associated backend. |
| *Description* | The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

### base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DN(s) for the data that the backend handles. |
| *Description* | A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN. |
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None<br><br>No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used. |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the backend is enabled in the server. |
| *Description* | If a backend is not enabled, then its contents are not accessible when processing operations. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

is-private-backend

| | |
|---|---|
| *Synopsis* | Indicates whether the backend should be considered a private backend, which indicates that it is used for storing operational data rather than user-defined information. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

ldif-file

| | |
|---|---|
| *Synopsis* | Specifies the path to the LDIF file containing the data for this backend. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

writability-mode

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the backend should use when processing write operations. |
| *Default Value* | enabled |
| *Allowed Values* | disabled: Causes all write attempts to fail.<br><br>enabled: Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).<br><br>internal-only: Causes external write attempts to fail but allows writes by replication and internal operations. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the backend implementation. |
| *Default Value* | org.opends.server.backends.LDIFBackend |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.Backend |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# LDIF Connection Handler

The LDIF Connection Handler is used to process changes in the server using internal operations, where the changes to process are read from an LDIF file.

The connection handler periodically looks for the existence of a new file, processes the changes contained in that file as internal operations, and writes the result to an output file with comments indicating the result of the processing. NOTE: By default LDIF Connection Handler operations are not logged because they are internal operations. If you want to log these operations, allow internal logging in the access log publisher.

## Parent

The LDIF Connection Handler object inherits from Connection Handler.

## LDIF Connection Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| allowed-client<br>denied-client<br>enabled<br>ldif-directory<br>poll-interval<br>restricted-client<br>restricted-client-connection-limit | java-class |

## Basic Properties

allowed-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be allowed to establish connections to this Connection Handler. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

denied-client

| | |
|---|---|
| *Synopsis* | A set of clients who are not allowed to establish connections to this Connection Handler. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Connection Handler is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

ldif-directory

| | |
|---|---|
| *Synopsis* | Specifies the path to the directory in which the LDIF files should be placed. |
| *Default Value* | config/auto-process-ldif |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

poll-interval

| | |
|---|---|
| *Synopsis* | Specifies how frequently the LDIF connection handler should check the LDIF directory to determine whether a new LDIF file has been added. |
| *Default Value* | 5 seconds |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 1 milliseconds. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be limited to the maximum number of connections specified by the "restricted-client-connection-limit" property. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | No restrictions are imposed on the number of connections a client can open. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| | Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client-connection-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of connections a restricted client can open at the same time to this Connection Handler. |
| *Description* | Once Directory Server accepts the specified number of connections from a client specified in restricted-client, any additional connection will be rejected. The number of connections is maintained by IP address. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | 100 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the LDIF Connection Handler implementation. |
| *Default Value* | org.opends.server.protocols.LDIFConnectionHandler |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.ConnectionHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

# Length Based Password Validator

The Length Based Password Validator is used to determine whether a proposed password is acceptable based on whether the number of characters it contains falls within an acceptable range of values.

Both upper and lower bounds may be defined.

## Parent

The Length Based Password Validator object inherits from Password Validator.

## Length Based Password Validator Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>max-password-length<br>min-password-length | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the password validator is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

max-password-length

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of characters that can be included in a proposed password. |
| *Description* | A value of zero indicates that there will be no upper bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length. |
| *Default Value* | 0 |
| *Allowed Values* | An integer.<br>Lower limit: 0.<br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

min-password-length

| | |
|---|---|
| *Synopsis* | Specifies the minimum number of characters that must be included in a proposed password. |
| *Description* | A value of zero indicates that there will be no lower bound enforced. If both minimum and maximum lengths are defined, then the minimum length must be less than or equal to the maximum length. |
| *Default Value* | 6 |
| *Allowed Values* | An integer.<br>Lower limit: 0.<br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the password validator implementation. |
| *Default Value* | org.opends.server.extensions.LengthBasedPasswordValidator |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordValidator |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Local Backend

*This is an abstract object type that cannot be instantiated.*

Local Backends are responsible for providing access to the underlying data presented by the server.

The data may be stored locally in an embedded database, remotely in an external system, or generated on the fly (for example, calculated from other information that is available).

## Local Backends

The following Local Backends are available:

- LDIF Backend
- Memory Backend
- Monitor Backend
- Null Backend
- Pluggable Backend
- Schema Backend
- Task Backend

These Local Backends inherit the properties described below.

## Parent

The Local Backend object inherits from Backend.

# Local Backend Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| backend-id<br>enabled<br>java-class<br>writability-mode |

## Basic Properties

### backend-id

| | |
| --- | --- |
| *Synopsis* | Specifies a name to identify the associated backend. |
| *Description* | The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

### enabled

| | |
| --- | --- |
| *Synopsis* | Indicates whether the backend is enabled in the server. |
| *Description* | If a backend is not enabled, then its contents are not accessible when processing operations. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the backend implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.Backend |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

writability-mode

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the backend should use when processing write operations. |
| *Default Value* | None |
| *Allowed Values* | disabled: Causes all write attempts to fail.<br>enabled: Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).<br>internal-only: Causes external write attempts to fail but allows writes by replication and internal operations. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Log Publisher

*This is an abstract object type that cannot be instantiated.*

Log Publishers are responsible for distributing log messages from different loggers to a destination.

## Log Publishers

The following Log Publishers are available:

- Access Log Publisher
- Debug Log Publisher
- Error Log Publisher
- HTTP Access Log Publisher

These Log Publishers inherit the properties described below.

## Log Publisher Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| enabled<br>java-class |

## Basic Properties

enabled

| | |
| --- | --- |
| *Synopsis* | Indicates whether the Log Publisher is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
| --- | --- |
| *Synopsis* | The fully-qualified name of the Java class that provides the Log Publisher implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.loggers.LogPublisher |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Log Retention Policy

*This is an abstract object type that cannot be instantiated.*

Log Retention Policies are used to specify when log files should be cleaned.

## Log Retention Policies

The following Log Retention Policies are available:

- File Count Log Retention Policy
- Free Disk Space Log Retention Policy
- Size Limit Log Retention Policy

These Log Retention Policies inherit the properties described below.

## Dependencies

The following objects depend on Log Retention Policies:

- CSV File Access Log Publisher
- CSV File HTTP Access Log Publisher
- File Based Access Log Publisher
- File Based Audit Log Publisher
- File Based Debug Log Publisher
- File Based Error Log Publisher
- File Based HTTP Access Log Publisher
- JSON File Based Access Log Publisher
- JSON File Based HTTP Access Log Publisher

## Log Retention Policy Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| java-class |

## Basic Properties

java-class

| | |
| --- | --- |
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Log Retention Policy implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.RetentionPolicy |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Log Rotation Policy

*This is an abstract object type that cannot be instantiated.*

Log Rotation Policies are used to specify when log files should be rotated.

## Log Rotation Policies

The following Log Rotation Policies are available:

- Fixed Time Log Rotation Policy
- Size Limit Log Rotation Policy
- Time Limit Log Rotation Policy

These Log Rotation Policies inherit the properties described below.

## Dependencies

The following objects depend on Log Rotation Policies:

- CSV File Access Log Publisher
- CSV File HTTP Access Log Publisher
- File Based Access Log Publisher
- File Based Audit Log Publisher
- File Based Debug Log Publisher
- File Based Error Log Publisher
- File Based HTTP Access Log Publisher
- JSON File Based Access Log Publisher
- JSON File Based HTTP Access Log Publisher

## Log Rotation Policy Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| java-class |

## Basic Properties

java-class

| | |
| --- | --- |
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Log Rotation Policy implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.loggers.RotationPolicy |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

# Mail Server

Mail Servers are used to define how to connect and authenticate to an external mail server.

Mail servers (SMTP MTAs) may require that messages are submitted on particular network ports, over TLS, and using certain authentication credentials.

## Dependencies

Mail Servers depend on the following objects:

- Trust Manager Provider

## Mail Server Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| auth-password<br>auth-username<br>enabled<br>smtp-server<br>trust-manager-provider<br>use-ssl<br>use-start-tls | smtp-property |

## Basic Properties

auth-password

| | |
|---|---|
| *Synopsis* | Specifies the password for authenticating to the SMTP server. You must also set the auth-name. |
| *Default Value* | Do not authenticate to the remote SMTP server. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

auth-username

| | |
|---|---|
| *Synopsis* | Specifies the username for authenticating to the SMTP server. |
| *Default Value* | Do not authenticate to the remote SMTP server. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Mail Server is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

smtp-server

| | |
|---|---|
| *Synopsis* | Specifies the address (and optional port number) for a mail server that can be used to send email messages via SMTP. |
| *Description* | It may be an IP address or resolvable hostname, optionally followed by a colon and a port number. |
| *Default Value* | None |
| *Allowed Values* | A hostname, optionally followed by a ":" followed by a port number. If not specified, port 587 is used. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

trust-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the trust manager that should be used when negotiating SSL connections with remote mail servers. |
| *Default Value* | By default, no trust manager is specified indicating that only certificates signed by the authorities associated with this JVM will be accepted. |
| *Allowed Values* | The name of an existing Trust Manager Provider .<br><br>The referenced trust manager provider must be enabled when SSL or StartTLS is enabled. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only impact subsequent SSL connection negotiations. |
| *Advanced* | No |
| *Read-Only* | No |

use-ssl

| | |
|---|---|
| *Synopsis* | Indicates whether the Mail Server should use SSL. |
| *Description* | If enabled, the Mail Server will use SSL to encrypt communication with the clients. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

use-start-tls

| | |
|---|---|
| *Synopsis* | Indicates whether to use StartTLS. |
| *Description* | If enabled, the Mail Server will use the StartTLS command after connecting to initiate secure communication over an otherwise insecure channel. Note that this is only allowed if the Mail Server is not configured to use SSL. |
| *Default Value* | true |

| | |
|---|---|
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

smtp-property

| | |
|---|---|
| *Synopsis* | Specifies additional options to pass when submitting messages. |
| *Description* | Any supported property can be specified here. Refer to the documentation at https://javaee.github.io/javamail/docs/api/javax/mail/package-summary.html#properties for further information on related properties, their implications, and range values. Note these extra properties will be added after the normal properties are set for this Mail Server. |
| *Default Value* | No additional properties. |
| *Allowed Values* | A property name followed by an "=" and then the property value. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## MD5 Password Storage Scheme

The MD5 Password Storage Scheme provides a mechanism for encoding user passwords using an unsalted form of the MD5 message digest algorithm. Because the implementation does not use any kind of salting mechanism, a given password always has the same encoded form.

This scheme contains only an implementation for the user password syntax, with a storage scheme name of "MD5". Although the MD5 digest algorithm is relatively secure, recent cryptanalysis work has identified mechanisms for generating MD5 collisions. This does not impact the security of this algorithm as it is used in OpenDJ, but it is recommended that the MD5 password storage scheme only be used if client applications require it for compatibility purposes, and that a stronger digest like SSHA or SSHA256 be used for environments in which MD5 support is not required.

## Parent

The MD5 Password Storage Scheme object inherits from Password Storage Scheme.

## MD5 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the MD5 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.MD5PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Member Virtual Attribute

The Member Virtual Attribute generates a member or uniqueMember attribute whose values are the DNs of the members of a specified virtual static group.

This component is used to implement virtual static group functionality, in which it is possible to create an entry that looks like a static group but obtains all of its membership from a dynamic group (or some other type of group, including another static group). This implementation is most efficient when attempting to determine whether a given user is a member of a group (for example, with a filter like "(uniqueMember=uid=john.doe,ou=People,dc=example,dc=com)") when the search does not actually return the membership attribute. Although it works to generate the entire set of values for the member or uniqueMember attribute, this can be an expensive operation for a large group.

## Parent

The Member Virtual Attribute object inherits from Virtual Attribute.

## Member Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| allow-retrieving-membership<br>attribute-type<br>base-dn<br>conflict-behavior<br>enabled<br>filter<br>group-dn<br>scope | java-class |

## Basic Properties

allow-retrieving-membership

| | |
|---|---|
| *Synopsis* | Indicates whether to handle requests that request all values for the virtual attribute. |

| | |
|---|---|
| *Description* | This operation can be very expensive in some cases and is not consistent with the primary function of virtual static groups, which is to make it possible to use static group idioms to determine whether a given user is a member. If this attribute is set to false, attempts to retrieve the entire set of values receive an empty set, and only attempts to determine whether the attribute has a specific value or set of values (which is the primary anticipated use for virtual static groups) are handled properly. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | None |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | virtual-overrides-real |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.<br><br>real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |

| | |
|---|---|
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br><br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | org.opends.server.extensions.MemberVirtualAttributeProvider |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Memory Backend

The Memory Backend provides a directory server backend implementation that stores entries in memory, for development and testing.

There is no persistence of any kind, and the backend contents are cleared whenever the backend is brought online or offline and when the server is restarted.

### Parent

The Memory Backend object inherits from Local Backend.

### Memory Backend Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| backend-id | java-class |

| Basic Properties | Advanced Properties |
|---|---|
| base-dn<br>enabled<br>writability-mode | |

## Basic Properties

backend-id

| | |
|---|---|
| *Synopsis* | Specifies a name to identify the associated backend. |
| *Description* | The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DN(s) for the data that the backend handles. |
| *Description* | A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN. |
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None<br><br>No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used. |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the backend is enabled in the server. |
| *Description* | If a backend is not enabled, then its contents are not accessible when processing operations. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

writability-mode

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the backend should use when processing write operations. |
| *Default Value* | enabled |
| *Allowed Values* | disabled: Causes all write attempts to fail.<br><br>enabled: Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).<br><br>internal-only: Causes external write attempts to fail but allows writes by replication and internal operations. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the backend implementation. |
| *Default Value* | org.opends.server.backends.MemoryBackend |

| | |
|---|---|
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.Backend |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Monitor Backend

The Monitor Backend allows clients to access the information made available by directory server monitor providers.

## Parent

The Monitor Backend object inherits from Local Backend.

## Monitor Backend Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| backend-id<br>enabled<br>writability-mode | java-class |

## Basic Properties

backend-id

| | |
|---|---|
| *Synopsis* | Specifies a name to identify the associated backend. |
| *Description* | The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the backend is enabled in the server. |
| *Description* | If a backend is not enabled, then its contents are not accessible when processing operations. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

writability-mode

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the backend should use when processing write operations. |
| *Default Value* | disabled |
| *Allowed Values* | disabled: Causes all write attempts to fail.<br>enabled: Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).<br>internal-only: Causes external write attempts to fail but allows writes by replication and internal operations. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the backend implementation. |
| *Default Value* | org.opends.server.backends.MonitorBackend |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.Backend |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Null Backend

The Null Backend provides a directory server backend that implements a /dev/null like behavior for development and testing.

The Null Backend behaves as follows: all search operations return success but no data; all write operations do nothing; bind operations fail with invalid credentials; compare operations are only possible on objectClass and return true for top, nullBackendObject, and extensibleObject. In addition controls are supported although this implementation does not provide any specific emulation for controls. Generally known request controls are accepted and default response controls returned where applicable. Searches within a Null Backend are always considered indexed. Null Backends are for development and testing only.

## Parent

The Null Backend object inherits from Local Backend.

## Null Backend Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| backend-id<br>base-dn<br>enabled<br>writability-mode | java-class |

## Basic Properties

### backend-id

| | |
|---|---|
| *Synopsis* | Specifies a name to identify the associated backend. |
| *Description* | The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

### base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DN(s) for the data that the backend handles. |
| *Description* | A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN. |
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None<br><br>No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used. |
| *Advanced* | No |
| *Read-Only* | No |

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the backend is enabled in the server. |
| *Description* | If a backend is not enabled, then its contents are not accessible when processing operations. |
| *Default Value* | None |

| | |
|---|---|
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

writability-mode

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the backend should use when processing write operations. |
| *Default Value* | enabled |
| *Allowed Values* | disabled: Causes all write attempts to fail.<br><br>enabled: Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).<br><br>internal-only: Causes external write attempts to fail but allows writes by replication and internal operations. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the backend implementation. |
| *Default Value* | org.opends.server.backends.NullBackend |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.Backend |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Num Subordinates Virtual Attribute

The Num Subordinates Virtual Attribute generates a virtual attribute that specifies the number of immediate child entries that exist below the entry.

## Parent

The Num Subordinates Virtual Attribute object inherits from Virtual Attribute.

## Num Subordinates Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>enabled<br>filter<br>group-dn<br>scope | conflict-behavior<br>java-class |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | numSubordinates |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |
| *Multi-valued* | Yes |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br><br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | virtual-overrides-real |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.<br><br>real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | org.opends.server.extensions.NumSubordinatesVirtualAttributeProvider |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Password Expiration Time Virtual Attribute

The Password Expiration Time Virtual Attribute generates a virtual attribute which shows the password expiration date.

## Parent

The Password Expiration Time Virtual Attribute object inherits from Virtual Attribute.

## Password Expiration Time Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>enabled<br>filter<br>group-dn<br>scope | conflict-behavior<br>java-class |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | ds-pwp-password-expiration-time |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |

| | |
|---|---|
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br><br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | virtual-overrides-real |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used. |

| | |
|---|---|
| | real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | org.opends.server.extensions.PasswordExpirationTimeVirtualAttributeProvider |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Password Generator

*This is an abstract object type that cannot be instantiated.*

Password Generators are used by the password modify extended operation to construct a new password for the user.

The server allows any number of password validators to be defined. This can impose any kinds of restrictions on the characteristics of valid passwords. Therefore, it is not feasible for the server to attempt to generate a password on its own that will meet all the requirements of all the validators. The password generator makes it possible to provide custom logic for creating a new password.

## Password Generators

The following Password Generators are available:

- Random Password Generator

These Password Generators inherit the properties described below.

## Dependencies

The following objects depend on Password Generators:

- Password Policy

## Password Generator Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| enabled<br>java-class |

## Basic Properties

enabled

| | |
| --- | --- |
| *Synopsis* | Indicates whether the Password Generator is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
| --- | --- |
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Password Generator implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordGenerator |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Password Modify Extended Operation Handler

The Password Modify Extended Operation Handler allows end users to change their own passwords, or administrators to reset user passwords.

The password modify extended operation is defined in RFC 3062. It includes the ability for users to provide their current password for further confirmation of their identity when changing the password, and it also includes the ability to generate a new password if the user does not provide one.

## Parent

The Password Modify Extended Operation Handler object inherits from Extended Operation Handler.

## Dependencies

Password Modify Extended Operation Handlers depend on the following objects:

- Identity Mapper

## Password Modify Extended Operation Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>identity-mapper | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server). |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name(s) of the identity mapper(s) that should be used in conjunction with the password modify extended operation. |
| *Description* | This property is used to identify a user based on an authorization ID in the 'u:' form. Changes to this property take effect immediately. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br>The referenced identity mapper(s) must be enabled when the Password Modify Extended Operation Handler is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Password Modify Extended Operation Handler implementation. |
| *Default Value* | org.opends.server.extensions.PasswordModifyExtendedOperation |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.ExtendedOperationHandler |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Password Policy

Password Policies define a number of password management rules, as well as requirements for authentication processing.

## Parent

The Password Policy object inherits from Authentication Policy.

## Dependencies

Password Policies depend on the following objects:

- Account Status Notification Handler
- Password Generator
- Password Storage Scheme
- Password Validator

## Password Policy Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| account-status-notification-handler<br>allow-expired-password-changes<br>allow-user-password-changes<br>default-password-storage-scheme<br>deprecated-password-storage-scheme<br>expire-passwords-without-warning<br>force-change-on-add<br>force-change-on-reset<br>grace-login-count<br>idle-lockout-interval<br>last-login-time-attribute<br>last-login-time-format | allow-multiple-password-values<br>allow-pre-encoded-passwords<br>java-class<br>skip-validation-for-administrators<br>state-update-failure-policy |

| Basic Properties | Advanced Properties |
|---|---|
| lockout-duration<br>lockout-failure-count<br>lockout-failure-expiration-interval<br>max-password-age<br>max-password-reset-age<br>min-password-age<br>password-attribute<br>password-change-requires-current-password<br>password-expiration-warning-interval<br>password-generator<br>password-history-count<br>password-history-duration<br>password-validator<br>previous-last-login-time-format<br>require-change-by-time<br>require-secure-authentication<br>require-secure-password-changes | |

## Basic Properties

account-status-notification-handler

| | |
|---|---|
| *Synopsis* | Specifies the names of the account status notification handlers that are used with the associated password storage scheme. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Account Status Notification Handler .<br><br>The referenced account status notification handlers must be enabled. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

allow-expired-password-changes

| | |
|---|---|
| *Synopsis* | Indicates whether a user whose password is expired is still allowed to change that password using the password modify extended operation. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

allow-user-password-changes

| | |
|---|---|
| *Synopsis* | Indicates whether users can change their own passwords. |
| *Description* | This check is made in addition to access control evaluation. Both must allow the password change for it to occur. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

default-password-storage-scheme

| | |
|---|---|
| *Synopsis* | Specifies the names of the password storage schemes that are used to encode clear-text passwords for this password policy. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Password Storage Scheme .<br>The referenced password storage schemes must be enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

deprecated-password-storage-scheme

| | |
|---|---|
| *Synopsis* | Specifies the names of the password storage schemes that are considered deprecated for this password policy. |
| *Description* | If a user with this password policy authenticates to the server and his/her password is encoded with a deprecated scheme, those values are removed and replaced with values encoded using the default password storage scheme(s). |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | The name of an existing Password Storage Scheme .<br><br>The referenced password storage schemes must be enabled. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

expire-passwords-without-warning

| | |
|---|---|
| *Synopsis* | Indicates whether the directory server allows a user's password to expire even if that user has never seen an expiration warning notification. |
| *Description* | If this property is true, accounts always expire when the expiration time arrives. If this property is false or disabled, the user always receives at least one warning notification, and the password expiration is set to the warning time plus the warning interval. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

force-change-on-add

| | |
|---|---|
| *Synopsis* | Indicates whether users are forced to change their passwords upon first authenticating to the directory server after their account has been created. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

force-change-on-reset

| | |
|---|---|
| *Synopsis* | Indicates whether users are forced to change their passwords if they are reset by an administrator. |
| *Description* | For this purpose, anyone with permission to change a given user's password other than that user is considered an administrator. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

grace-login-count

| | |
|---|---|
| *Synopsis* | Specifies the number of grace logins that a user is allowed after the account has expired to allow that user to choose a new password. |
| *Description* | A value of 0 indicates that no grace logins are allowed. |
| *Default Value* | 0 |
| *Allowed Values* | An integer.<br>Lower limit: 0.<br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

idle-lockout-interval

| | |
|---|---|
| *Synopsis* | Specifies the maximum length of time that an account may remain idle (that is, the associated user does not authenticate to the server) before that user is locked out. |
| *Description* | The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, weeks, or years. A value of 0 seconds indicates that idle accounts are not automatically locked out. This feature is available only if the last login time is maintained. |
| *Default Value* | 0 seconds |

| | |
|---|---|
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 0 seconds.<br>Upper limit: 2147483647 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

last-login-time-attribute

| | |
|---|---|
| *Synopsis* | Specifies the name or OID of the attribute type that is used to hold the last login time for users with the associated password policy. |
| *Description* | This attribute type must be defined in the directory server schema and must either be defined as an operational attribute or must be allowed by the set of objectClasses for all users with the associated password policy. |
| *Default Value* | None |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

last-login-time-format

| | |
|---|---|
| *Synopsis* | Specifies the format string that is used to generate the last login time value for users with the associated password policy. |
| *Description* | This format string conforms to the syntax described in the API documentation for the java.text.SimpleDateFormat class. |
| *Default Value* | None |
| *Allowed Values* | Any valid format string that can be used with the java.text.SimpleDateFormat class. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

lockout-duration

| | |
|---|---|
| *Synopsis* | Specifies the length of time that an account is locked after too many authentication failures. |
| *Description* | The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, weeks, or years. A value of 0 seconds indicates that the account must remain locked until an administrator resets the password. |
| *Default Value* | 0 seconds |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 0 seconds.<br>Upper limit: 2147483647 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

lockout-failure-count

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of authentication failures that a user is allowed before the account is locked out. |
| *Description* | A value of 0 indicates that accounts are never locked out due to failed attempts. |
| *Default Value* | 0 |
| *Allowed Values* | An integer.<br>Lower limit: 0.<br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

lockout-failure-expiration-interval

| | |
|---|---|
| *Synopsis* | Specifies the length of time before an authentication failure is no longer counted against a user for the purposes of account lockout. |
| *Description* | The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, weeks, or years. A value of 0 seconds indicates that the |

| | |
|---|---|
| | authentication failures must never expire. The failure count is always cleared upon a successful authentication. |
| *Default Value* | 0 seconds |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 0 seconds.<br>Upper limit: 2147483647 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

max-password-age

| | |
|---|---|
| *Synopsis* | Specifies the maximum length of time that a user can continue using the same password before it must be changed (that is, the password expiration interval). |
| *Description* | The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, weeks, or years. A value of 0 seconds disables password expiration. |
| *Default Value* | 0 seconds |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 0 seconds.<br>Upper limit: 2147483647 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

max-password-reset-age

| | |
|---|---|
| *Synopsis* | Specifies the maximum length of time that users have to change passwords after they have been reset by an administrator before they become locked. |
| *Description* | The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, weeks, or years. A value of 0 seconds disables this feature. |
| *Default Value* | 0 seconds |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 0 seconds. |

| | |
|---|---|
| | Upper limit: 2147483647 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

min-password-age

| | |
|---|---|
| *Synopsis* | Specifies the minimum length of time after a password change before the user is allowed to change the password again. |
| *Description* | The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, weeks, or years. This setting can be used to prevent users from changing their passwords repeatedly over a short period of time to flush an old password from the history so that it can be re-used. |
| *Default Value* | 0 seconds |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 0 seconds.<br>Upper limit: 2147483647 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

password-attribute

| | |
|---|---|
| *Synopsis* | Specifies the attribute type used to hold user passwords. |
| *Description* | This attribute type must be defined in the server schema, and it must have either the user password or auth password syntax. |
| *Default Value* | None |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

password-change-requires-current-password

| | |
|---|---|
| *Synopsis* | Indicates whether user password changes must include the user's current password before the change is allowed. This can be done with either the password modify extended operation, or a modify operation using delete and add. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

password-expiration-warning-interval

| | |
|---|---|
| *Synopsis* | Specifies the maximum length of time before a user's password actually expires that the server begins to include warning notifications in bind responses for that user. |
| *Description* | The value of this attribute is an integer followed by a unit of seconds, minutes, hours, days, weeks, or years. A value of 0 seconds disables the warning interval. |
| *Default Value* | 5 days |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 0 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

password-generator

| | |
|---|---|
| *Synopsis* | Specifies the name of the password generator that is used with the associated password policy. |
| *Description* | This is used in conjunction with the password modify extended operation to generate a new password for a user when none was provided in the request. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Password Generator .<br><br>The referenced password generator must be enabled. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

password-history-count

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of former passwords to maintain in the password history. |
| *Description* | When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero indicates that either no password history is to be maintained (if the password history duration has a value of zero seconds), or that there is no maximum number of passwords to maintain in the history (if the password history duration has a value greater than zero seconds). |
| *Default Value* | 0 |
| *Allowed Values* | An integer.<br>Lower limit: 0.<br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

password-history-duration

| | |
|---|---|
| *Synopsis* | Specifies the maximum length of time that passwords remain in the password history. |
| *Description* | When choosing a new password, the proposed password is checked to ensure that it does not match the current password, nor any other password in the history list. A value of zero seconds indicates that either no password history is to be maintained (if the password history count has a value of zero), or that there is no maximum duration for passwords in the history (if the password history count has a value greater than zero). |
| *Default Value* | 0 seconds |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 0 seconds.<br>Upper limit: 2147483647 seconds. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

password-validator

| | |
|---|---|
| *Synopsis* | Specifies the names of the password validators that are used with the associated password storage scheme. |
| *Description* | The password validators are invoked when a user attempts to provide a new password, to determine whether the new password is acceptable. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Password Validator .<br><br>The referenced password validators must be enabled. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

previous-last-login-time-format

| | |
|---|---|
| *Synopsis* | Specifies the format string(s) that might have been used with the last login time at any point in the past for users associated with the password policy. |
| *Description* | These values are used to make it possible to parse previous values, but are not used to set new values. The format strings conform to the syntax described in the API documentation for the java.text.SimpleDateFormat class. |
| *Default Value* | None |
| *Allowed Values* | Any valid format string that can be used with the java.text.SimpleDateFormat class. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

require-change-by-time

| | |
|---|---|
| *Synopsis* | Specifies the time by which all users with the associated password policy must change their passwords. |

| | |
|---|---|
| *Description* | The value is expressed in a generalized time format. If this time is equal to the current time or is in the past, then all users are required to change their passwords immediately. The behavior of the server in this mode is identical to the behavior observed when users are forced to change their passwords after an administrative reset. |
| *Default Value* | None |
| *Allowed Values* | A valid timestamp in generalized time form (for example, a value of "20070409185811Z" indicates a value of April 9, 2007 at 6:58:11 pm GMT). |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

require-secure-authentication

| | |
|---|---|
| *Synopsis* | Indicates whether users with the associated password policy are required to authenticate in a secure manner. |
| *Description* | This might mean either using a secure communication channel between the client and the server, or using a SASL mechanism that does not expose the credentials. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

require-secure-password-changes

| | |
|---|---|
| *Synopsis* | Indicates whether users with the associated password policy are required to change their password in a secure manner that does not expose the credentials. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

allow-multiple-password-values

| | |
|---|---|
| *Synopsis* | Indicates whether user entries can have multiple distinct values for the password attribute. |
| *Description* | This is potentially dangerous because many mechanisms used to change the password do not work well with such a configuration. If multiple password values are allowed, then any of them can be used to authenticate, and they are all subject to the same policy constraints. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

allow-pre-encoded-passwords

| | |
|---|---|
| *Synopsis* | Indicates whether users can change their passwords by providing a pre-encoded value. |
| *Description* | This can cause a security risk because the clear-text version of the password is not known and therefore validation checks cannot be applied to it. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class which provides the Password Policy implementation. |
| *Default Value* | org.opends.server.core.PasswordPolicyFactory |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.AuthenticationPolicyFactory |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

skip-validation-for-administrators

| | |
|---|---|
| *Synopsis* | Indicates whether passwords set by administrators are allowed to bypass the password validation process that is required for user password changes. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

state-update-failure-policy

| | |
|---|---|
| *Synopsis* | Specifies how the server deals with the inability to update password policy state information during an authentication attempt. |
| *Description* | In particular, this property can be used to control whether an otherwise successful bind operation fails if a failure occurs while attempting to update password policy state information (for example, to clear a record of previous authentication failures or to update the last login time). It can also be used to control whether to reject a bind request if it is known ahead of time that it will not be possible to update the authentication failure times in the event of an unsuccessful bind attempt (for example, if the backend writability mode is disabled). |
| *Default Value* | reactive |
| *Allowed Values* | ignore: If a bind attempt would otherwise be successful, then do not reject it if a problem occurs while attempting to update the password policy state information for the user. |

| | |
|---|---|
| | proactive: Proactively reject any bind attempt if it is known ahead of time that it would not be possible to update the user's password policy state information.<br><br>reactive: Even if a bind attempt would otherwise be successful, reject it if a problem occurs while attempting to update the password policy state information for the user. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Password Policy Import Plugin

The Password Policy Import Plugin ensures that clear-text passwords contained in LDIF entries are properly encoded before they are stored in the appropriate directory server backend.

## Parent

The Password Policy Import Plugin object inherits from Plugin.

## Dependencies

Password Policy Import Plugins depend on the following objects:

- Password Storage Scheme

## Password Policy Import Plugin Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| default-auth-password-storage-scheme<br>default-user-password-storage-scheme<br>enabled | invoke-for-internal-operations<br>java-class<br>plugin-type |

## Basic Properties

default-auth-password-storage-scheme

| | |
|---|---|
| *Synopsis* | Specifies the names of password storage schemes that to be used for encoding passwords contained in attributes with the auth password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy should be used to govern them. |
| *Default Value* | If the default password policy uses an attribute with the auth password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes auth password values using the "SHA1" scheme. |
| *Allowed Values* | The name of an existing Password Storage Scheme .<br><br>The referenced password storage schemes must be enabled when the Password Policy Import plug-in is enabled. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

default-user-password-storage-scheme

| | |
|---|---|
| *Synopsis* | Specifies the names of the password storage schemes to be used for encoding passwords contained in attributes with the user password syntax for entries that do not include the ds-pwp-password-policy-dn attribute specifying which password policy is to be used to govern them. |
| *Default Value* | If the default password policy uses the attribute with the user password syntax, then the server uses the default password storage schemes for that password policy. Otherwise, it encodes user password values using the "SSHA" scheme. |
| *Allowed Values* | The name of an existing Password Storage Scheme .<br><br>The referenced password storage schemes must be enabled when the Password Policy Import Plugin is enabled. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

invoke-for-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in should be invoked for internal operations. |
| *Description* | Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the plug-in implementation. |
| *Default Value* | org.opends.server.plugins.PasswordPolicyImportPlugin |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.plugin.DirectoryServerPlugin |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

plugin-type

| | |
|---|---|
| *Synopsis* | Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked. |
| *Default Value* | ldifimport |
| *Allowed Values* | initialization: Invoked at the initialization of the directory server.<br><br>intermediateresponse: Invoked before sending an intermediate repsonse message to the client.<br><br>ldifimport: Invoked for each entry read during an LDIF import.<br><br>ldifimportbegin: Invoked at the beginning of an LDIF import session.<br><br>ldifimportend: Invoked at the end of an LDIF import session.<br><br>postconnect: Invoked whenever a new connection is established to the server.<br><br>postdisconnect: Invoked whenever an existing connection is terminated (by either the client or the server).<br><br>postoperationabandon: Invoked after completing the abandon processing.<br><br>postoperationadd: Invoked after completing the core add processing but before sending the response to the client.<br><br>postoperationbind: Invoked after completing the core bind processing but before sending the response to the client.<br><br>postoperationcompare: Invoked after completing the core compare processing but before sending the response to the client.<br><br>postoperationdelete: Invoked after completing the core delete processing but before sending the response to the client.<br><br>postoperationextended: Invoked after completing the core extended processing but before sending the response to the client.<br><br>postoperationmodify: Invoked after completing the core modify processing but before sending the response to the client.<br><br>postoperationmodifydn: Invoked after completing the core modify DN processing but before sending the response to the client.<br><br>postoperationsearch: Invoked after completing the core search processing but before sending the response to the client.<br><br>postoperationunbind: Invoked after completing the unbind processing.<br><br>postresponseadd: Invoked after sending the add response to the client.<br><br>postresponsebind: Invoked after sending the bind response to the client.<br><br>postresponsecompare: Invoked after sending the compare response to the client. |

postresponsedelete: Invoked after sending the delete response to the client.

postresponseextended: Invoked after sending the extended response to the client.

postresponsemodify: Invoked after sending the modify response to the client.

postresponsemodifydn: Invoked after sending the modify DN response to the client.

postresponsesearch: Invoked after sending the search result done message to the client.

postsynchronizationadd: Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete: Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify: Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn: Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd: Invoked prior to performing the core add processing.

preoperationbind: Invoked prior to performing the core bind processing.

preoperationcompare: Invoked prior to performing the core compare processing.

preoperationdelete: Invoked prior to performing the core delete processing.

preoperationextended: Invoked prior to performing the core extended processing.

preoperationmodify: Invoked prior to performing the core modify processing.

preoperationmodifydn: Invoked prior to performing the core modify DN processing.

preoperationsearch: Invoked prior to performing the core search processing.

preparseabandon: Invoked prior to parsing an abandon request.

preparseadd: Invoked prior to parsing an add request.

preparsebind: Invoked prior to parsing a bind request.

preparsecompare: Invoked prior to parsing a compare request.

preparsedelete: Invoked prior to parsing a delete request.

preparseextended: Invoked prior to parsing an extended request.

preparsemodify: Invoked prior to parsing a modify request.

preparsemodifydn: Invoked prior to parsing a modify DN request.

| | |
|---|---|
| | preparsesearch: Invoked prior to parsing a search request.<br><br>preparseunbind: Invoked prior to parsing an unbind request.<br><br>searchresultentry: Invoked before sending a search result entry to the client.<br><br>searchresultreference: Invoked before sending a search result reference to the client.<br><br>shutdown: Invoked during a graceful directory server shutdown.<br><br>startup: Invoked during the directory server startup process.<br><br>subordinatedelete: Invoked in the course of deleting a subordinate entry of a delete operation.<br><br>subordinatemodifydn: Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Password Policy State Extended Operation Handler

The Password Policy State Extended Operation Handler provides the ability for administrators to request and optionally alter password policy state information for a specified user.

## Parent

The Password Policy State Extended Operation Handler object inherits from Extended Operation Handler.

## Password Policy State Extended Operation Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server). |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Password Policy State Extended Operation Handler implementation. |
| *Default Value* | org.opends.server.extensions.PasswordPolicyStateExtendedOperation |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.ExtendedOperationHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Password Policy Subentry Virtual Attribute

The Password Policy Subentry Virtual Attribute generates a virtual attribute that points to the Password Policy subentry in effect for the entry.

## Parent

The Password Policy Subentry Virtual Attribute object inherits from Virtual Attribute.

## Password Policy Subentry Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>enabled<br>filter<br>group-dn<br>scope | conflict-behavior<br>java-class |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | pwdPolicySubentry |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |

| | |
|---|---|
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br><br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | virtual-overrides-real |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used. |

| | |
|---|---|
| | real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | org.opends.server.extensions.PasswordPolicySubentryVirtualAttributeProvider |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Password Storage Scheme

*This is an abstract object type that cannot be instantiated.*

Password Storage Schemes encode new passwords provided by users so that they are stored in an encoded manner. This makes it difficult or impossible for someone to determine the clear-text passwords from the encoded values.

Password Storage Schemes also determine whether a clear-text password provided by a client matches the encoded value stored in the server.

## Password Storage Schemes

The following Password Storage Schemes are available:

- AES Password Storage Scheme

- Base64 Password Storage Scheme
- Bcrypt Password Storage Scheme
- Blowfish Password Storage Scheme
- Clear Password Storage Scheme
- Crypt Password Storage Scheme
- MD5 Password Storage Scheme
- PBKDF2 Password Storage Scheme
- PKCS#5 V2.0 Scheme 2 Password Storage Scheme
- RC4 Password Storage Scheme
- Salted MD5 Password Storage Scheme
- Salted SHA-1 Password Storage Scheme
- Salted SHA-256 Password Storage Scheme
- Salted SHA-384 Password Storage Scheme
- Salted SHA-512 Password Storage Scheme
- SCRAM-SHA-256 Password Storage Scheme
- SCRAM-SHA-512 Password Storage Scheme
- SHA-1 Password Storage Scheme
- Triple-DES Password Storage Scheme

These Password Storage Schemes inherit the properties described below.

## Dependencies

The following objects depend on Password Storage Schemes:

- LDAP Pass Through Authentication Policy
- Password Policy
- Password Policy Import Plugin

## Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| enabled<br>java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Password Storage Scheme implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Password Validator

*This is an abstract object type that cannot be instantiated.*

Password Validators are responsible for determining whether a proposed password is acceptable for use and could include checks like ensuring it meets minimum length requirements, that it has an appropriate range of characters, or that it is not in the history.

The password policy for a user specifies the set of password validators that should be used whenever that user provides a new password. In order to activate a password validator, the corresponding configuration entry must be enabled, and the DN of that entry should be included in the password-validator attribute of the password policy in which you want that validator active. All password validator configuration entries must contain the password-validator structural objectclass.

## Password Validators

The following Password Validators are available:

- Attribute Value Password Validator
- Character Set Password Validator
- Dictionary Password Validator
- Length Based Password Validator
- Repeated Characters Password Validator
- Similarity Based Password Validator
- Unique Characters Password Validator

These Password Validators inherit the properties described below.

## Dependencies

The following objects depend on Password Validators:

- Password Policy

## Password Validator Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| enabled<br>java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the password validator is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the password validator implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordValidator |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# PBKDF2-HMAC-SHA256 Password Storage Scheme

The PBKDF2-HMAC-SHA256 Password Storage Scheme provides a mechanism for encoding user passwords using the PBKDF2-HMAC-SHA256 message digest algorithm.

This scheme contains an implementation for the user password syntax, with a storage scheme name of "PBKDF2-HMAC-SHA256".

## Parent

The PBKDF2-HMAC-SHA256 Password Storage Scheme object inherits from PBKDF2 Password Storage Scheme.

# PBKDF2-HMAC-SHA256 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>pbkdf2-iterations<br>rehash-policy | java-class |

## Basic Properties

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### pbkdf2-iterations

| | |
|---|---|
| *Synopsis* | The number of algorithm iterations to make. NIST recommends at least 1000. |
| *Description* | By default, changes to this setting impact only newly created and updated passwords. However, if the rehash-policy is set to always or only-increase, it causes the server to recalculate each user's password hash on their next authentication, and write the new hash to the user's entry on disk. Changing the number of iterations therefore leads to a short-term spike in CPU and disk use as the server updates each user's password when they next authenticate. Longer term, increasing this settings results in more secure passwords at the expense of longer response times and lower throughput. |
| *Default Value* | 10000 |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

rehash-policy

| | |
|---|---|
| *Synopsis* | Indicates whether the server should rehash passwords after the cost has been changed. |
| *Description* | Passwords will be rehashed when a user successfully authenticates. Note that rehashing will increase the write load on the server. |
| *Default Value* | never |
| *Allowed Values* | always: Rehash passwords when the cost is increased or decreased.<br><br>never: Never rehash passwords.<br><br>only-increase: Only rehash passwords when the cost has been increased (do not downgrade the security of the hashed password). |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the PBKDF2-HMAC-SHA256 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.PBKDF2HmacSHA256PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# PBKDF2-HMAC-SHA512 Password Storage Scheme

The PBKDF2-HMAC-SHA512 Password Storage Scheme provides a mechanism for encoding user passwords using the PBKDF2-HMAC-SHA512 message digest algorithm.

This scheme contains an implementation for the user password syntax, with a storage scheme name of "PBKDF2-HMAC-SHA512".

## Parent

The PBKDF2-HMAC-SHA512 Password Storage Scheme object inherits from PBKDF2 Password Storage Scheme.

## PBKDF2-HMAC-SHA512 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>pbkdf2-iterations<br>rehash-policy | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

pbkdf2-iterations

| | |
|---|---|
| *Synopsis* | The number of algorithm iterations to make. NIST recommends at least 1000. |
| *Description* | By default, changes to this setting impact only newly created and updated passwords. However, if the rehash-policy is set to always or only-increase, |

| | |
|---|---|
| | it causes the server to recalculate each user's password hash on their next authentication, and write the new hash to the user's entry on disk. Changing the number of iterations therefore leads to a short-term spike in CPU and disk use as the server updates each user's password when they next authenticate. Longer term, increasing this settings results in more secure passwords at the expense of longer response times and lower throughput. |
| *Default Value* | 10000 |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

rehash-policy

| | |
|---|---|
| *Synopsis* | Indicates whether the server should rehash passwords after the cost has been changed. |
| *Description* | Passwords will be rehashed when a user successfully authenticates. Note that rehashing will increase the write load on the server. |
| *Default Value* | never |
| *Allowed Values* | always: Rehash passwords when the cost is increased or decreased.<br><br>never: Never rehash passwords.<br><br>only-increase: Only rehash passwords when the cost has been increased (do not downgrade the security of the hashed password). |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the PBKDF2-HMAC-SHA512 Password Storage Scheme implementation. |

| | |
|---|---|
| *Default Value* | org.opends.server.extensions.PBKDF2HmacSHA512PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# PBKDF2 Password Storage Scheme

*This is an abstract object type that cannot be instantiated.*

The PBKDF2 Password Storage Scheme provides a mechanism for encoding user passwords using the PBKDF2 message digest algorithm. PBKDF2 is the shortname for PBKDF2-HMAC-SHA1.

This scheme contains an implementation for the user password syntax, with a storage scheme name of "PBKDF2".

## PBKDF2 Password Storage Schemes

The following PBKDF2 Password Storage Schemes are available:

- PBKDF2-HMAC-SHA256 Password Storage Scheme
- PBKDF2-HMAC-SHA512 Password Storage Scheme

These PBKDF2 Password Storage Schemes inherit the properties described below.

## Parent

The PBKDF2 Password Storage Scheme object inherits from Password Storage Scheme.

## PBKDF2 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

| Basic Properties | Advanced Properties |
|---|---|
| pbkdf2-iterations<br>rehash-policy | |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

pbkdf2-iterations

| | |
|---|---|
| *Synopsis* | The number of algorithm iterations to make. NIST recommends at least 1000. |
| *Description* | By default, changes to this setting impact only newly created and updated passwords. However, if the rehash-policy is set to always or only-increase, it causes the server to recalculate each user's password hash on their next authentication, and write the new hash to the user's entry on disk. Changing the number of iterations therefore leads to a short-term spike in CPU and disk use as the server updates each user's password when they next authenticate. Longer term, increasing this settings results in more secure passwords at the expense of longer response times and lower throughput. |
| *Default Value* | 10000 |
| *Allowed Values* | An integer.<br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

rehash-policy

| | |
|---|---|
| *Synopsis* | Indicates whether the server should rehash passwords after the cost has been changed. |
| *Description* | Passwords will be rehashed when a user successfully authenticates. Note that rehashing will increase the write load on the server. |
| *Default Value* | never |
| *Allowed Values* | always: Rehash passwords when the cost is increased or decreased.<br><br>never: Never rehash passwords.<br><br>only-increase: Only rehash passwords when the cost has been increased (do not downgrade the security of the hashed password). |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the PBKDF2 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.PBKDF2PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## PKCS#11 Key Manager Provider

The PKCS#11 Key Manager Provider enables the server to access the private key information through the PKCS11 interface.

This standard interface is used by cryptographic accelerators and hardware security modules.

## Parent

The PKCS#11 Key Manager Provider object inherits from Key Manager Provider.

## PKCS#11 Key Manager Provider Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>key-store-pin<br>key-store-type | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Key Manager Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-store-pin

| | |
|---|---|
| *Synopsis* | Specifies the clear-text PIN needed to access the PKCS#11 Key Manager Provider . |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property will take effect the next time that the PKCS#11 Key Manager Provider is accessed. |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

key-store-type

| | |
|---|---|
| *Synopsis* | Specifies the type of PKCS#11 key manager, when the specific name must be explicit. |
| *Description* | . If no type is specified, the default value of "PKCS11" will be used. |
| *Default Value* | PKCS11 |
| *Allowed Values* | Any PKCS#11 key store format supported by this Java runtime environment. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | Restart the server for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the PKCS#11 Key Manager Provider implementation. |
| *Default Value* | org.opends.server.extensions.PKCS11KeyManagerProvider |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.KeyManagerProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## PKCS#11 Trust Manager Provider

The PKCS#11 Trust Manager Provider enables the server to manage trust information through the PKCS11 interface

This standard interface is used by cryptographic accelerators and hardware security modules.

## Parent

The PKCS#11 Trust Manager Provider object inherits from Trust Manager Provider.

## PKCS#11 Trust Manager Provider Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>trust-store-pin<br>trust-store-type | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicate whether the Trust Manager Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

trust-store-pin

| | |
|---|---|
| *Synopsis* | Specifies the clear-text PIN needed to access the PKCS#11 Trust Manager Provider . |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property will take effect the next time that the PKCS#11 Trust Manager Provider is accessed. |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

trust-store-type

| | |
|---|---|
| *Synopsis* | Specifies the type of PKCS#11 trust manager, when the specific name must be explicit. |
| *Description* | . If no type is specified, the default value of "PKCS11" will be used. |
| *Default Value* | PKCS11 |
| *Allowed Values* | Any PKCS#11 key store format supported by this Java runtime environment. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | Restart the server for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the PKCS#11 Trust Manager Provider implementation. |
| *Default Value* | org.opends.server.extensions.Pkcs11TrustManagerProvider |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.TrustManagerProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## PKCS#5 V2.0 Scheme 2 Password Storage Scheme

The PKCS#5 V2.0 Scheme 2 Password Storage Scheme provides a mechanism for encoding user passwords using the Atlassian PBKDF2-based message digest algorithm.

This scheme contains an implementation for the user password syntax, with a storage scheme name of "PKCS5S2".

## Parent

The PKCS#5 V2.0 Scheme 2 Password Storage Scheme object inherits from Password Storage Scheme.

## PKCS#5 V2.0 Scheme 2 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the PKCS#5 V2.0 Scheme 2 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.PKCS5S2PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordStorageScheme |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Plain SASL Mechanism Handler

The Plain SASL Mechanism Handler performs all processing related to SASL PLAIN authentication.

The PLAIN SASL mechanism provides the ability for clients to authenticate using a username and password. This authentication is very similar to standard LDAP simple authentication, with the exception that it can authenticate based on an authentication ID (for example, a username) rather than requiring a full DN, and it can also include an authorization ID in addition to the authentication ID. Note that the SASL PLAIN mechanism does not make any attempt to protect the password.

## Parent

The Plain SASL Mechanism Handler object inherits from SASL Mechanism Handler.

## Dependencies

Plain SASL Mechanism Handlers depend on the following objects:

- Identity Mapper

## Plain SASL Mechanism Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>identity-mapper | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the SASL mechanism handler is enabled for use. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name(s) of the identity mapper(s) that is to be used with this SASL mechanism handler to match the authentication or authorization ID included in the SASL bind request to the corresponding user in the directory. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br><br>The referenced identity mapper(s) must be enabled when the Plain SASL Mechanism Handler is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation. |
| *Default Value* | org.opends.server.extensions.PlainSASLMechanismHandler |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.SASLMechanismHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

# Pluggable Backend

*This is an abstract object type that cannot be instantiated.*

A Pluggable Backend stores application data in a pluggable database.

## Pluggable Backends

The following Pluggable Backends are available:

- JE Backend

These Pluggable Backends inherit the properties described below.

## Parent

The Pluggable Backend object inherits from Local Backend.

## Dependencies

The following objects belong to Pluggable Backends:

- Backend Index
- Backend VLV Index

## Pluggable Backend Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| backend-id<br>base-dn<br>cipher-key-length<br>cipher-transformation<br>compact-encoding<br>confidentiality-enabled<br>enabled<br>java-class | entries-compressed<br>import-offheap-memory-size<br>index-entry-limit<br>index-filter-analyzer-enabled<br>index-filter-analyzer-max-filters |

| Basic Properties | Advanced Properties |
|---|---|
| writability-mode | |

## Basic Properties

### backend-id

| | |
|---|---|
| *Synopsis* | Specifies a name to identify the associated backend. |
| *Description* | The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

### base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DN(s) for the data that the backend handles. |
| *Description* | A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN. |
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None<br><br>No administrative action is required by default although some action may be required on a per-backend basis before the new base DN may be used. |
| *Advanced* | No |
| *Read-Only* | No |

### cipher-key-length

| | |
|---|---|
| *Synopsis* | Specifies the key length in bits for the preferred cipher. |

| | |
|---|---|
| *Default Value* | 128 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only affect cryptographic operations performed after the change. |
| *Advanced* | No |
| *Read-Only* | No |

cipher-transformation

| | |
|---|---|
| *Synopsis* | Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". |
| *Description* | The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding. |
| *Default Value* | AES/GCM/NoPadding |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only affect cryptographic operations performed after the change. |
| *Advanced* | No |
| *Read-Only* | No |

compact-encoding

| | |
|---|---|
| *Synopsis* | Indicates whether the backend should use a compact form when encoding entries by compressing the attribute descriptions and object class sets. |
| *Description* | Note that this property applies only to the entries themselves and does not impact the index data. It will also replace the attribute descriptions used in add and modify operations with normalized ones from the schema. |
| *Default Value* | true |
| *Allowed Values* | true |

| | |
|---|---|
| | false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data. |
| *Advanced* | No |
| *Read-Only* | No |

confidentiality-enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the backend should make entries in database files readable only by Directory Server. |
| *Description* | Confidentiality is achieved by enrypting entries before writing them to the underlying storage. Entry encryption will protect data on disk from unauthorised parties reading the files; for complete protection, also set confidentiality for sensitive attributes indexes. The property cannot be set to false if some of the indexes have confidentiality set to true. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the backend is enabled in the server. |
| *Description* | If a backend is not enabled, then its contents are not accessible when processing operations. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the backend implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.Backend |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

writability-mode

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the backend should use when processing write operations. |
| *Default Value* | enabled |
| *Allowed Values* | disabled: Causes all write attempts to fail.<br>enabled: Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).<br>internal-only: Causes external write attempts to fail but allows writes by replication and internal operations. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

entries-compressed

| | |
|---|---|
| *Synopsis* | Indicates whether the backend should attempt to compress entries before storing them in the database. |
| *Description* | Note that this property applies only to the entries themselves and does not impact the index data. Further, the effectiveness of the compression is based on the type of data contained in the entry. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this setting take effect only for writes that occur after the change is made. It is not retroactively applied to existing data. |
| *Advanced* | Yes |
| *Read-Only* | No |

import-offheap-memory-size

| | |
|---|---|
| *Synopsis* | Specifies the amount of off-heap memory dedicated to the online operation (import-ldif, rebuild-index). |
| *Default Value* | Use only heap memory. |
| *Allowed Values* | Uses *Size Syntax* . |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

index-entry-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of entries that is allowed to match a given index key before that particular index key is no longer maintained. |
| *Description* | This property is analogous to the ALL IDs threshold in the Sun Java System Directory Server. Note that this is the default limit for the backend, and it may be overridden on a per-attribute basis. A value of 0 means there is no limit. Changing the index entry limit significantly can result in serious performance degradation. Please read the documentation before changing this setting. |
| *Default Value* | 4000 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |

| | |
|---|---|
| | Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>If any index keys have already reached this limit, indexes need to be rebuilt before they are allowed to use the new limit. |
| *Advanced* | Yes |
| *Read-Only* | No |

index-filter-analyzer-enabled

| | |
|---|---|
| *Synopsis* | Indicates whether to gather statistical information about the search filters processed by the directory server while evaluating the usage of indexes. |
| *Description* | Analyzing indexes requires gathering search filter usage patterns from user requests, especially for values as specified in the filters and subsequently looking the status of those values into the index files. When a search requests is processed, internal or user generated, a first phase uses indexes to find potential entries to be returned. Depending on the search filter, if the index of one of the specified attributes matches too many entries (exceeds the index entry limit), the search becomes non-indexed. In any case, all entries thus gathered (or the entire DIT) are matched against the filter for actually returning the search result. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

index-filter-analyzer-max-filters

| | |
|---|---|
| *Synopsis* | The maximum number of search filter statistics to keep. |
| *Description* | When the maximum number of search filter is reached, the least used one will be deleted. |
| *Default Value* | 25 |
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Plugin

*This is an abstract object type that cannot be instantiated.*

Plugins provide a mechanism for executing custom code at specified points in operation processing and in the course of other events like connection establishment and termination, server startup and shutdown, and LDIF import and export.

## Plugins

The following Plugins are available:

- Attribute Cleanup Plugin
- Change Number Control Plugin
- entryUUID Plugin
- Fractional LDIF Import Plugin
- Graphite Monitor Reporter Plugin
- Last Mod Plugin
- LDAP Attribute Description List Plugin
- Password Policy Import Plugin
- Referential Integrity Plugin
- Samba Password Plugin
- Seven Bit Clean Plugin
- Unique Attribute Plugin

These Plugins inherit the properties described below.

## Dependencies

The following objects have Plugins:

- Plugin Root

## Plugin Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>java-class<br>plugin-type | invoke-for-internal-operations |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the plug-in implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.plugin.DirectoryServerPlugin |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-type

| | |
|---|---|
| *Synopsis* | Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked. |
| *Default Value* | None |
| *Allowed Values* | initialization: Invoked at the initialization of the directory server.<br><br>intermediateresponse: Invoked before sending an intermediate repsonse message to the client.<br><br>ldifimport: Invoked for each entry read during an LDIF import.<br><br>ldifimportbegin: Invoked at the beginning of an LDIF import session.<br><br>ldifimportend: Invoked at the end of an LDIF import session.<br><br>postconnect: Invoked whenever a new connection is established to the server.<br><br>postdisconnect: Invoked whenever an existing connection is terminated (by either the client or the server).<br><br>postoperationabandon: Invoked after completing the abandon processing.<br><br>postoperationadd: Invoked after completing the core add processing but before sending the response to the client.<br><br>postoperationbind: Invoked after completing the core bind processing but before sending the response to the client.<br><br>postoperationcompare: Invoked after completing the core compare processing but before sending the response to the client.<br><br>postoperationdelete: Invoked after completing the core delete processing but before sending the response to the client.<br><br>postoperationextended: Invoked after completing the core extended processing but before sending the response to the client.<br><br>postoperationmodify: Invoked after completing the core modify processing but before sending the response to the client.<br><br>postoperationmodifydn: Invoked after completing the core modify DN processing but before sending the response to the client.<br><br>postoperationsearch: Invoked after completing the core search processing but before sending the response to the client.<br><br>postoperationunbind: Invoked after completing the unbind processing.<br><br>postresponseadd: Invoked after sending the add response to the client.<br><br>postresponsebind: Invoked after sending the bind response to the client.<br><br>postresponsecompare: Invoked after sending the compare response to the client. |

postresponsedelete: Invoked after sending the delete response to the client.

postresponseextended: Invoked after sending the extended response to the client.

postresponsemodify: Invoked after sending the modify response to the client.

postresponsemodifydn: Invoked after sending the modify DN response to the client.

postresponsesearch: Invoked after sending the search result done message to the client.

postsynchronizationadd: Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete: Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify: Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn: Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd: Invoked prior to performing the core add processing.

preoperationbind: Invoked prior to performing the core bind processing.

preoperationcompare: Invoked prior to performing the core compare processing.

preoperationdelete: Invoked prior to performing the core delete processing.

preoperationextended: Invoked prior to performing the core extended processing.

preoperationmodify: Invoked prior to performing the core modify processing.

preoperationmodifydn: Invoked prior to performing the core modify DN processing.

preoperationsearch: Invoked prior to performing the core search processing.

preparseabandon: Invoked prior to parsing an abandon request.

preparseadd: Invoked prior to parsing an add request.

preparsebind: Invoked prior to parsing a bind request.

preparsecompare: Invoked prior to parsing a compare request.

preparsedelete: Invoked prior to parsing a delete request.

preparseextended: Invoked prior to parsing an extended request.

preparsemodify: Invoked prior to parsing a modify request.

preparsemodifydn: Invoked prior to parsing a modify DN request.

| | |
|---|---|
| | preparsesearch: Invoked prior to parsing a search request.<br><br>preparseunbind: Invoked prior to parsing an unbind request.<br><br>searchresultentry: Invoked before sending a search result entry to the client.<br><br>searchresultreference: Invoked before sending a search result reference to the client.<br><br>shutdown: Invoked during a graceful directory server shutdown.<br><br>startup: Invoked during the directory server startup process.<br><br>subordinatedelete: Invoked in the course of deleting a subordinate entry of a delete operation.<br><br>subordinatemodifydn: Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

invoke-for-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in should be invoked for internal operations. |
| *Description* | Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Plugin Root

The Plugin Root defines the parent entry for all plug-ins defined in the server.

It can also include configuration attributes that define the order in which those plug-ins are to be loaded and invoked.

## Dependencies

The following objects belong to Plugin Roots:

- Plugin

## Plugin Root Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| plugin-order-intermediate-response<br>plugin-order-ldif-import<br>plugin-order-ldif-import-begin<br>plugin-order-ldif-import-end<br>plugin-order-post-connect<br>plugin-order-post-disconnect<br>plugin-order-post-operation-abandon<br>plugin-order-post-operation-add<br>plugin-order-post-operation-bind<br>plugin-order-post-operation-compare<br>plugin-order-post-operation-delete<br>plugin-order-post-operation-extended<br>plugin-order-post-operation-modify<br>plugin-order-post-operation-modify-dn<br>plugin-order-post-operation-search<br>plugin-order-post-operation-unbind<br>plugin-order-post-response-add<br>plugin-order-post-response-bind<br>plugin-order-post-response-compare<br>plugin-order-post-response-delete<br>plugin-order-post-response-extended<br>plugin-order-post-response-modify<br>plugin-order-post-response-modify-dn<br>plugin-order-post-response-search<br>plugin-order-post-synchronization-add<br>plugin-order-post-synchronization-delete<br>plugin-order-post-synchronization-modify<br>plugin-order-post-synchronization-modify-dn |

| Basic Properties |
| --- |
| plugin-order-pre-operation-add |
| plugin-order-pre-operation-bind |
| plugin-order-pre-operation-compare |
| plugin-order-pre-operation-delete |
| plugin-order-pre-operation-extended |
| plugin-order-pre-operation-modify |
| plugin-order-pre-operation-modify-dn |
| plugin-order-pre-operation-search |
| plugin-order-pre-parse-abandon |
| plugin-order-pre-parse-add |
| plugin-order-pre-parse-bind |
| plugin-order-pre-parse-compare |
| plugin-order-pre-parse-delete |
| plugin-order-pre-parse-extended |
| plugin-order-pre-parse-modify |
| plugin-order-pre-parse-modify-dn |
| plugin-order-pre-parse-search |
| plugin-order-pre-parse-unbind |
| plugin-order-search-result-entry |
| plugin-order-search-result-reference |
| plugin-order-shutdown |
| plugin-order-startup |
| plugin-order-subordinate-delete |
| plugin-order-subordinate-modify-dn |

## Basic Properties

plugin-order-intermediate-response

| | |
| --- | --- |
| *Synopsis* | Specifies the order in which intermediate response plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which intermediate response plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-ldif-import

| | |
|---|---|
| *Synopsis* | Specifies the order in which LDIF import plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which LDIF import plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-ldif-import-begin

| | |
|---|---|
| *Synopsis* | Specifies the order in which LDIF import begin plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which LDIF import begin plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-ldif-import-end

| | |
|---|---|
| *Synopsis* | Specifies the order in which LDIF import end plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which LDIF import end plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-connect

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-connect plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-connect plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-disconnect

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-disconnect plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-disconnect plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-operation-abandon

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-operation abandon plug-ins are to be loaded and invoked. |

| | |
|---|---|
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-operation abandon plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-operation-add

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-operation add plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-operation add plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-operation-bind

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-operation bind plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-operation bind plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-operation-compare

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-operation compare plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-operation compare plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-operation-delete

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-operation delete plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-operation delete plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-operation-extended

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-operation extended operation plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-operation extended operation plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-operation-modify

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-operation modify plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-operation modify plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-operation-modify-dn

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-operation modify DN plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-operation modify DN plug-ins are loaded and invoked is undefined. |

| | |
|---|---|
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-operation-search

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-operation search plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-operation search plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-operation-unbind

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-operation unbind plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-operation unbind plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-response-add

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-response add plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-response add plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-response-bind

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-response bind plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-response bind plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-response-compare

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-response compare plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |

| | |
|---|---|
| *Default Value* | The order in which post-response compare plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-response-delete

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-response delete plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-response delete plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-response-extended

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-response extended operation plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-response extended operation plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-response-modify

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-response modify plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-response modify plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-response-modify-dn

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-response modify DN plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-response modify DN plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-response-search

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-response search plug-ins are to be loaded and invoked. |

| | |
|---|---|
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-response search plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-synchronization-add

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-synchronization add plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-synchronization add plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-synchronization-delete

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-synchronization delete plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-synchronization delete plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-synchronization-modify

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-synchronization modify plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-synchronization modify plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-post-synchronization-modify-dn

| | |
|---|---|
| *Synopsis* | Specifies the order in which post-synchronization modify DN plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which post-synchronization modify DN plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-operation-add

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-operation add plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-operation add plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-operation-bind

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-operation bind plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-operation bind plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-operation-compare

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-operation compare plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-operation compare plug-ins are loaded and invoked is undefined. |

| | |
|---|---|
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-operation-delete

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-operation delete plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-operation delete plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-operation-extended

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-operation extended operation plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-operation extended operation plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-operation-modify

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-operation modify plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-operation modify plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-operation-modify-dn

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-operation modify DN plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-operation modify DN plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-operation-search

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-operation search plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |

| | |
|---|---|
| *Default Value* | The order in which pre-operation searc plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-parse-abandon

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-parse abandon plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-parse abandon plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-parse-add

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-parse add plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-parse add plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### plugin-order-pre-parse-bind

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-parse bind plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-parse bind plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### plugin-order-pre-parse-compare

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-parse compare plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-parse compare plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### plugin-order-pre-parse-delete

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-parse delete plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-parse delete plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-parse-extended

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-parse extended operation plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-parse extended operation plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-parse-modify

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-parse modify plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-parse modify plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-parse-modify-dn

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-parse modify DN plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-parse modify DN plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-parse-search

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-parse search plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-parse search plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-pre-parse-unbind

| | |
|---|---|
| *Synopsis* | Specifies the order in which pre-parse unbind plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which pre-parse unbind plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-search-result-entry

| | |
|---|---|
| *Synopsis* | Specifies the order in which search result entry plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which search result entry plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-search-result-reference

| | |
|---|---|
| *Synopsis* | Specifies the order in which search result reference plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which search result reference plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-shutdown

| | |
|---|---|
| *Synopsis* | Specifies the order in which shutdown plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which shutdown plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-startup

| | |
|---|---|
| *Synopsis* | Specifies the order in which startup plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which startup plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-subordinate-delete

| | |
|---|---|
| *Synopsis* | Specifies the order in which subordinate delete plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which subordinate delete plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

plugin-order-subordinate-modify-dn

| | |
|---|---|
| *Synopsis* | Specifies the order in which subordinate modify DN plug-ins are to be loaded and invoked. |
| *Description* | The value is a comma-delimited list of plug-in names (where the plug-in name is the RDN value from the plug-in configuration entry DN). The list can include at most one asterisk to indicate the position of any unspecified plug-in (and the relative order of those unspecified plug-ins is undefined). |
| *Default Value* | The order in which subordinate modify DN plug-ins are loaded and invoked is undefined. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Policy Based Access Control Handler

A policy based access control handler implements a coarse grained access control model suitable for use in proxies.

Access control rules are defined using individual access control policy entries. A user's access is defined as the union of all access control rules that apply to that user. In other words, an individual access control rule can only grant additional access and can not remove rights granted by another rule. This approach results in an access control policy which is easier to understand and audit, since all rules can be understood in isolation.

## Parent

The Policy Based Access Control Handler object inherits from Access Control Handler.

## Dependencies

The following objects belong to Policy Based Access Control Handlers:

- Global Access Control Policy

## Policy Based Access Control Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Access Control Handler is enabled. If set to FALSE, then any client (including unauthenticated or anonymous clients) is allowed to bind to the server and any connection with the "bypass-acl" privilege is allowed to perform any operation. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Policy Based Access Control Handler implementation. |
| *Default Value* | org.opends.server.authorization.policy.PolicyBasedAccessControlHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.AccessControlHandler |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Prometheus HTTP Endpoint

The Prometheus HTTP Endpoint exposes OpenDJ's monitoring metrics using Prometheus text format.

## Parent

The Prometheus HTTP Endpoint object inherits from HTTP Endpoint.

## Prometheus HTTP Endpoint Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| authorization-mechanism<br>base-path<br>enabled<br>excluded-metric-pattern<br>included-metric-pattern | java-class |

## Basic Properties

authorization-mechanism

| | |
|---|---|
| *Synopsis* | The HTTP authorization mechanisms supported by this HTTP Endpoint. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing HTTP Authorization Mechanism .<br><br>The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-path

| | |
|---|---|
| *Synopsis* | All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Endpoint is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

excluded-metric-pattern

| | |
|---|---|
| *Synopsis* | Zero or more regular expressions identifying metrics that should not be published. The metric name prefix must not be included in the filter. Exclusion patterns take precedence over inclusion patterns. |
| *Default Value* | None |
| *Allowed Values* | Any valid regular expression pattern which is supported by the java.util.regex.Pattern class (see https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 8). |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

included-metric-pattern

| | |
|---|---|
| *Synopsis* | Zero or more regular expressions identifying metrics that should be published. The metric name prefix must not be included in the filter. Exclusion patterns take precedence over inclusion patterns. |
| *Default Value* | None |
| *Allowed Values* | Any valid regular expression pattern which is supported by the java.util.regex.Pattern class (see https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 8). |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Prometheus HTTP Endpoint implementation. |
| *Default Value* | org.opends.server.protocols.http.PrometheusEndpoint |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.HttpEndpoint |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## Proxy Backend

A Proxy Backend forwards LDAP requests to other servers.

A Proxy Backend uses the proxied authorization control to forward LDAP requests on behalf of the proxy users. As a consequence, the remote servers must support the proxied authorization control and the proxy user must have appropriate privileges and permissions allowing them to use the control.

## Parent

The Proxy Backend object inherits from Backend.

## Dependencies

Proxy Backends depend on the following objects:

- Key Manager Provider
- Service Discovery Mechanism

## Proxy Backend Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| backend-id<br>base-dn<br>bind-connection-pool-idle-timeout<br>bind-connection-pool-max-size<br>bind-connection-pool-min-size<br>connection-timeout<br>discovery-interval<br>enabled<br>heartbeat-interval<br>heartbeat-search-request-base-dn<br>key-manager-provider<br>load-balancing-algorithm<br>partition-base-dn<br>proxy-user-dn<br>proxy-user-password<br>request-connection-pool-size<br>route-all<br>shard<br>ssl-cert-nickname<br>use-sasl-external | hash-function<br>java-class |

## Basic Properties

backend-id

| | |
|---|---|
| *Synopsis* | Specifies a name to identify the associated backend. |
| *Description* | The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DN(s) for the data that the backend handles. |
| *Description* | A single backend may be responsible for one or more base DNs. Note that no two backends may have the same base DN although one backend may have a base DN that is below a base DN provided by another backend (similar to the use of sub-suffixes in the Sun Java System Directory Server). If any of the base DNs is subordinate to a base DN for another backend, then all base DNs for that backend must be subordinate to that same base DN. When the "route-all" property is set to "true" then the "base-dn" property is ignored. |
| *Default Value* | Unless route-all is enabled, a proxy with empty base DNs does not handle any requests. This helps incrementally building a proxy's configuration. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>No administrative action is required. |
| *Advanced* | No |
| *Read-Only* | No |

bind-connection-pool-idle-timeout

| | |
|---|---|
| *Synopsis* | The time out period after which unused non-core bind connections will be closed and removed from the bind connection pool. |
| *Default Value* | 10s |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 1 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

bind-connection-pool-max-size

| | |
|---|---|
| *Synopsis* | Maximum size of the connection pool that will be used for sending bind requests |
| *Description* | Only one bind request at a time can be pending on a connection and bind requests may take a significant amount of time to process depending on the remote server's password policies. Therefore, the maximum pool size should be reasonably high in order to be able to process bind requests concurrently. |
| *Default Value* | 1024 |
| *Allowed Values* | An integer.<br>Use "-1" or "unlimited" to indicate no limit.<br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

bind-connection-pool-min-size

| | |
|---|---|
| *Synopsis* | Minimum size of the connection pool that will be used for sending bind requests |
| *Default Value* | 4 |
| *Allowed Values* | An integer.<br>Use "-1" or "unlimited" to indicate no limit.<br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

connection-timeout

| | |
|---|---|
| *Synopsis* | Specifies the timeout used when connecting to servers, performing SSL negotiation, and for individual search and bind requests. |
| *Description* | If the timeout expires then the current operation will be aborted and retried against another LDAP server if one is available. |
| *Default Value* | 3s |

| | |
|---|---|
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 10 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

discovery-interval

| | |
|---|---|
| *Synopsis* | Interval between two server configuration discovery executions. |
| *Description* | Specifies how frequently to read the configuration of the servers in order to discover any configuration change. |
| *Default Value* | 60s |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 1 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the backend is enabled in the server. |
| *Description* | If a backend is not enabled, then its contents are not accessible when processing operations. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

heartbeat-interval

| | |
|---|---|
| *Synopsis* | Specifies the heartbeat interval that the Proxy Backend will use when communicating with the remote servers. |
| *Description* | The Proxy Backend sends a heartbeat request to the servers every heartbeat interval. The heartbeat serves 3 purposes: keepalive, heartbeat and recovery. The hearbeat requests are small requests sent to prevent the connection from appearing idle and being forcefully closed (keepalive). The heartbeat responses inform the Proxy Backend the server is available (heartbeat). If a heartbeat answer is not received within the interval, the Proxy Backend closes the unresponsive connection and connects to another server. After an unresponsive connection is closed, the server is contacted each heartbeat interval to determine whether it is available again (recovery). |
| *Default Value* | 10s |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 10 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

heartbeat-search-request-base-dn

| | |
|---|---|
| *Synopsis* | Specifies the name of the entry that will be targeted by heartbeat requests. |
| *Description* | By default heartbeat requests will attempt to read the remote server's root DSE, which is sufficient to determine whether the remote server is available, but it will not detect whether a particular backend is available. Set the heartbeat request base DN to the base entry of the backend containing application data in order to detect whether a remote server is available and handling requests against the backend. |
| *Default Value* | |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the key manager that should be used with this Proxy Backend. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | The name of an existing Key Manager Provider .<br><br>The referenced key manager provider must be enabled when the Proxy Backend is enabled and configured to use SASL/External certificate authentication. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections. |
| *Advanced* | No |
| *Read-Only* | No |

load-balancing-algorithm

| | |
|---|---|
| *Synopsis* | How to load balance between servers within a shard |
| *Default Value* | affinity |
| *Allowed Values* | affinity: Always route requests with the same target DN to the same server<br><br>least-requests: Use the server with the least requests being currently serviced |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

partition-base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DN(s) which will be used for "affinity" load-balancing algorithm and data distribution |
| *Description* | This settings only applies for "affinity" load-balancing and data distribution. When applied to "affinity" load-balancing within a single shard, this setting provides consistency for add/delete operations targeting entries within the same sub-tree. Entries immediately subordinate to the partition base DNs will be considered to be the root of a sub-tree whose entries belong to the same shard. For example, a partition base DN of "ou=people,dc=example,dc=com" would mean that "uid=bjensen,ou=people,dc=example,dc=com" and "deviceid=12345,uid=bjensen,ou=people,dc=example,dc=com" both belong to the same shard, and all operations targeting them would be routed to the same remote server. When applied to data distribution across multiple shards, this setting consistently routes operations targeting an entry below the partition DN to the same shard. Requests targeting the partition DN or above are routed to any shard. Search requests are routed |

| | |
|---|---|
| | to all shards unless their scope is under the partition DN. For example, if the partition base DN is set to "ou=people,dc=example,dc=com", a search with base DN "uid=bjensen,ou=people,dc=example,dc=com" or "deviceid=12345,uid=bjensen,ou=people,dc=example,dc=com" is always routed to the same shard. A search with base DN "ou=people,dc=example,dc=com" is routed to all shards. |
| *Default Value* | No consistency for add/delete operations. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

proxy-user-dn

| | |
|---|---|
| *Synopsis* | The bind DN that is used to forward LDAP requests to remote servers. |
| *Description* | The proxy connects to the remote server using this bind DN and uses the proxied authorization control to forward requests on behalf of the proxy users. This bind DN must exist on all the remote servers. |
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

proxy-user-password

| | |
|---|---|
| *Synopsis* | Clear-text password associated with the proxy bind DN. |
| *Description* | The proxy password must be the same on all the remote servers. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property will take effect the next time that the Proxy Backend is accessed. |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

request-connection-pool-size

| | |
|---|---|
| *Synopsis* | The size of the connection pool which will be used for sending all requests other than bind requests. |
| *Description* | Unlike bind requests, other types of request may be processed concurrently on the same connection, so this connection pool should be configured with a smaller number of connections, such as 10. |
| *Default Value* | 10 |
| *Allowed Values* | An integer.<br><br>Use "-1" or "unlimited" to indicate no limit.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

route-all

| | |
|---|---|
| *Synopsis* | Route requests to all discovered public naming contexts. |
| *Description* | When the "route-all" property is set to "true" then the "base-dn" property is ignored. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

shard

| | |
|---|---|
| *Synopsis* | Specifies one or more shards which will be used for distributing data and requests. |

| | |
|---|---|
| *Description* | When multiple shards are configured, this setting consistently routes write requests for the same target entry below the partition DN to the same shard. Requests targeting an entry under the partition DN are always routed to a single shard. Requests targeting the partition DN or above are routed to any shard. Search requests are routed to all shards unless their scope is under the partition DN. For example, a search with base DN "uid=bjensen,ou=people,dc=example,dc=com" or "deviceid=12345,uid=bjensen,ou=people,dc=example,dc=com" is always routed to the same shard. A search with base DN "ou=people,dc=example,dc=com" is routed to all shards. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Service Discovery Mechanism . |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cert-nickname

| | |
|---|---|
| *Synopsis* | Specifies the nicknames (also called the aliases) of the keys or key pairs that the Proxy Backend should use when performing SSL communication. |
| *Description* | The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Proxy Backend is configured to use SSL. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

use-sasl-external

| | |
|---|---|
| *Synopsis* | Indicates whether the Proxy Backend should use certificate based authentication when communicating with backend servers. |
| *Description* | If enabled, the Proxy Backend will use mutual TLS when connecting to backend servers. Once the TLS handshake has completed, a SASL/External LDAP bind |

| | |
|---|---|
| | request will be sent in order to associate the TLS client certificate with an LDAP account on the remote backend server. A key manager provider containing the client certificate must be configured in order to use this feature. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

hash-function

| | |
|---|---|
| *Synopsis* | Specifies the hash function which will be used for data distribution. |
| *Description* | This setting only applies to data distribution. Once this server is deployed, this setting must not be modified. Doing so could result in data loss. The hash function is used by the router to map incoming requests to a target server based on the request's target DN. The role of the hash function is to ensure that the flow of incoming requests is evenly distributed on the set of servers. |
| *Default Value* | murmur3 |
| *Allowed Values* | md5: Use the MD5 hash algorithm. This hash function does not distribute data evenly and should not be used in new deployments.<br><br>murmur3: Use the Murmur3 hash algorithm. This hash function distributes data more evenly than MD5 and should be used in new deployments. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the backend implementation. |
| *Default Value* | org.opends.server.backends.ProxyBackend |

| | |
|---|---|
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.Backend |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Random Password Generator

The Random Password Generator creates random passwords based on fixed-length strings built from one or more character sets.

## Parent

The Random Password Generator object inherits from Password Generator.

## Random Password Generator Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>password-character-set<br>password-format | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Generator is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

password-character-set

| | |
|---|---|
| *Synopsis* | Specifies one or more named character sets. |
| *Description* | This is a multi-valued property, with each value defining a different character set. The format of the character set is the name of the set followed by a colon and the characters that are in that set. For example, the value "alpha:abcdefghijklmnopqrstuvwxyz" defines a character set named "alpha" containing all of the lower-case ASCII alphabetic characters. |
| *Default Value* | None |
| *Allowed Values* | A character set name (consisting of ASCII letters) followed by a colon and the set of characters that are included in that character set. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

password-format

| | |
|---|---|
| *Synopsis* | Specifies the format to use for the generated password. |
| *Description* | The value is a comma-delimited list of elements in which each of those elements is comprised of the name of a character set defined in the password-character-set property, a colon, and the number of characters to include from that set. For example, a value of "alpha:3,numeric:2,alpha:3" generates an 8-character password in which the first three characters are from the "alpha" set, the next two are from the "numeric" set, and the final three are from the "alpha" set. |
| *Default Value* | None |
| *Allowed Values* | A comma-delimited list whose elements comprise a valid character set name, a colon, and a positive integer indicating the number of characters from that set to be included. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Random Password Generator implementation. |
| *Default Value* | org.opends.server.extensions.RandomPasswordGenerator |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordGenerator |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# RC4 Password Storage Scheme

The RC4 Password Storage Scheme provides a mechanism for encoding user passwords using the RC4 reversible encryption mechanism.

This scheme contains only an implementation for the user password syntax, with a storage scheme name of "RC4".

## Parent

The RC4 Password Storage Scheme object inherits from Password Storage Scheme.

## RC4 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |

| | |
|---|---|
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the RC4 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.RC4PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## Referential Integrity Plugin

The Referential Integrity Plugin maintains referential integrity for DN valued attributes.

The values of these attributes can reference entries that have been deleted by a delete operation or renamed by a modify DN operation. The referential integrity plug-in either removes stale references to deleted entries or updates references to renamed entries. The plug-in allows the scope of this referential check to be limited to a set of base DNs if desired. The plug-in also can be configured to perform the referential checking in the background mode specified intervals.

### Parent

The Referential Integrity Plugin object inherits from Plugin.

# Referential Integrity Plugin Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>check-references<br>check-references-filter-criteria<br>check-references-scope-criteria<br>enabled<br>log-file<br>update-interval | invoke-for-internal-operations<br>java-class<br>plugin-type |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute types for which referential integrity is to be maintained. |
| *Description* | At least one attribute type must be specified, and the syntax of any attributes must be either a distinguished name (1.3.6.1.4.1.1466.115.121.1.12) or name and optional UID (1.3.6.1.4.1.1466.115.121.1.34). |
| *Default Value* | None |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DN that limits the scope within which referential integrity is maintained. |
| *Default Value* | Referential integrity is maintained in all public naming contexts. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

check-references

| | |
|---|---|
| *Synopsis* | Specifies whether reference attributes must refer to existing entries. |
| *Description* | When this property is set to true, this plugin will ensure that any new references added as part of an add or modify operation point to existing entries, and that the referenced entries match the filter criteria for the referencing attribute, if specified. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

check-references-filter-criteria

| | |
|---|---|
| *Synopsis* | Specifies additional filter criteria which will be enforced when checking references. |
| *Description* | If a reference attribute has filter criteria defined then this plugin will ensure that any new references added as part of an add or modify operation refer to an existing entry which matches the specified filter. |
| *Default Value* | None |
| *Allowed Values* | An attribute-filter mapping. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

check-references-scope-criteria

| | |
|---|---|
| *Synopsis* | Specifies whether referenced entries must reside within the same naming context as the entry containing the reference. |
| *Description* | The reference scope will only be enforced when reference checking is enabled. |
| *Default Value* | global |
| *Allowed Values* | global: References may refer to existing entries located anywhere in the Directory. |

| | |
|---|---|
| | naming-context: References must refer to existing entries located within the same naming context. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

log-file

| | |
|---|---|
| *Synopsis* | Specifies the log file location where the update records are written when the plug-in is in background-mode processing. |
| *Description* | The default location is the logs directory of the server instance, using the file name "referint". |
| *Default Value* | logs/referint |
| *Allowed Values* | A path to an existing file that is readable by the server. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

update-interval

| | |
|---|---|
| *Synopsis* | Specifies the interval in seconds when referential integrity updates are made. |
| *Description* | If this value is 0, then the updates are made synchronously in the foreground. |

| | |
|---|---|
| *Default Value* | 0 seconds |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 0 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

invoke-for-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in should be invoked for internal operations. |
| *Description* | Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the plug-in implementation. |
| *Default Value* | org.opends.server.plugins.ReferentialIntegrityPlugin |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.plugin.DirectoryServerPlugin |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

plugin-type

| | |
|---|---|
| *Synopsis* | Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked. |
| *Default Value* | postoperationdelete<br><br>postoperationmodifydn<br><br>subordinatemodifydn<br><br>subordinatedelete<br><br>preoperationadd<br><br>preoperationmodify |
| *Allowed Values* | initialization: Invoked at the initialization of the directory server.<br><br>intermediateresponse: Invoked before sending an intermediate repsonse message to the client.<br><br>ldifimport: Invoked for each entry read during an LDIF import.<br><br>ldifimportbegin: Invoked at the beginning of an LDIF import session.<br><br>ldifimportend: Invoked at the end of an LDIF import session.<br><br>postconnect: Invoked whenever a new connection is established to the server.<br><br>postdisconnect: Invoked whenever an existing connection is terminated (by either the client or the server).<br><br>postoperationabandon: Invoked after completing the abandon processing.<br><br>postoperationadd: Invoked after completing the core add processing but before sending the response to the client.<br><br>postoperationbind: Invoked after completing the core bind processing but before sending the response to the client.<br><br>postoperationcompare: Invoked after completing the core compare processing but before sending the response to the client.<br><br>postoperationdelete: Invoked after completing the core delete processing but before sending the response to the client.<br><br>postoperationextended: Invoked after completing the core extended processing but before sending the response to the client.<br><br>postoperationmodify: Invoked after completing the core modify processing but before sending the response to the client. |

postoperationmodifydn: Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch: Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind: Invoked after completing the unbind processing.

postresponseadd: Invoked after sending the add response to the client.

postresponsebind: Invoked after sending the bind response to the client.

postresponsecompare: Invoked after sending the compare response to the client.

postresponsedelete: Invoked after sending the delete response to the client.

postresponseextended: Invoked after sending the extended response to the client.

postresponsemodify: Invoked after sending the modify response to the client.

postresponsemodifydn: Invoked after sending the modify DN response to the client.

postresponsesearch: Invoked after sending the search result done message to the client.

postsynchronizationadd: Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete: Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify: Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn: Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd: Invoked prior to performing the core add processing.

preoperationbind: Invoked prior to performing the core bind processing.

preoperationcompare: Invoked prior to performing the core compare processing.

preoperationdelete: Invoked prior to performing the core delete processing.

preoperationextended: Invoked prior to performing the core extended processing.

preoperationmodify: Invoked prior to performing the core modify processing.

preoperationmodifydn: Invoked prior to performing the core modify DN processing.

preoperationsearch: Invoked prior to performing the core search processing.

preparseabandon: Invoked prior to parsing an abandon request.

| | |
|---|---|
| | preparseadd: Invoked prior to parsing an add request.<br>preparsebind: Invoked prior to parsing a bind request.<br>preparsecompare: Invoked prior to parsing a compare request.<br>preparsedelete: Invoked prior to parsing a delete request.<br>preparseextended: Invoked prior to parsing an extended request.<br>preparsemodify: Invoked prior to parsing a modify request.<br>preparsemodifydn: Invoked prior to parsing a modify DN request.<br>preparsesearch: Invoked prior to parsing a search request.<br>preparseunbind: Invoked prior to parsing an unbind request.<br>searchresultentry: Invoked before sending a search result entry to the client.<br>searchresultreference: Invoked before sending a search result reference to the client.<br>shutdown: Invoked during a graceful directory server shutdown.<br>startup: Invoked during the directory server startup process.<br>subordinatedelete: Invoked in the course of deleting a subordinate entry of a delete operation.<br>subordinatemodifydn: Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Regular Expression Identity Mapper

The Regular Expression Identity Mapper provides a way to use a regular expression to translate the provided identifier when searching for the appropriate user entry.

This may be used, for example, if the provided identifier is expected to be an e-mail address or Kerberos principal, but only the username portion (the part before the "@" symbol) should be used in the mapping process. Note that a replacement will be made only if all or part of the provided ID string matches the given match pattern. If no part of the ID string matches the provided pattern, the given ID string is used without any alteration.

## Parent

The Regular Expression Identity Mapper object inherits from Identity Mapper.

## Regular Expression Identity Mapper Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>match-attribute<br>match-base-dn<br>match-pattern<br>replace-pattern | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Identity Mapper is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

match-attribute

| | |
|---|---|
| *Synopsis* | Specifies the name or OID of the attribute whose value should match the provided identifier string after it has been processed by the associated regular expression. |
| *Description* | All values must refer to the name or OID of an attribute type defined in the directory server schema. If multiple attributes or OIDs are provided, at least one of those attributes must contain the provided ID string value in exactly one entry. |
| *Default Value* | uid |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

match-base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DN(s) that should be used when performing searches to map the provided ID string to a user entry. If multiple values are given, searches are performed below all the specified base DNs. |
| *Default Value* | The server searches below all public naming contexts local to the server. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

match-pattern

| | |
|---|---|
| *Synopsis* | Specifies the regular expression pattern that is used to identify portions of the ID string that will be replaced. |
| *Description* | Any portion of the ID string that matches this pattern is replaced in accordance with the provided replace pattern (or is removed if no replace pattern is specified). If multiple substrings within the given ID string match this pattern, all occurrences are replaced. If no part of the given ID string matches this pattern, the ID string is not altered. Exactly one match pattern value must be provided, and it must be a valid regular expression as described in the API documentation for the java.util.regex.Pattern class, including support for capturing groups. |
| *Default Value* | None |
| *Allowed Values* | Any valid regular expression pattern which is supported by the java.util.regex.Pattern class (see https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html for documentation about this class for Java SE 8). |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

replace-pattern

| | |
|---|---|
| *Synopsis* | Specifies the replacement pattern that should be used for substrings in the ID string that match the provided regular expression pattern. |
| *Description* | If no replacement pattern is provided, then any matching portions of the ID string will be removed (i.e., replaced with an empty string). The replacement pattern |

| | |
|---|---|
| | may include a string from a capturing group by using a dollar sign ($) followed by an integer value that indicates which capturing group should be used. |
| *Default Value* | The replace pattern will be the empty string. |
| *Allowed Values* | Any valid replacement string that is allowed by the java.util.regex.Matcher class. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Regular Expression Identity Mapper implementation. |
| *Default Value* | org.opends.server.extensions.RegularExpressionIdentityMapper |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.IdentityMapper |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Repeated Characters Password Validator

The Repeated Characters Password Validator is used to determine whether a proposed password is acceptable based on the number of times any character appears consecutively in a password value.

It ensures that user passwords do not contain strings of the same character repeated several times, like "aaaaaa" or "aaabbb".

### Parent

The Repeated Characters Password Validator object inherits from Password Validator.

# Repeated Characters Password Validator Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| case-sensitive-validation<br>enabled<br>max-consecutive-length | java-class |

## Basic Properties

case-sensitive-validation

| | |
|---|---|
| *Synopsis* | Indicates whether this password validator should treat password characters in a case-sensitive manner. |
| *Description* | If the value of this property is false, the validator ignores any differences in capitalization when looking for consecutive characters in the password. If the value is true, the validator considers a character to be repeating only if all consecutive occurrences use the same capitalization. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the password validator is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

max-consecutive-length

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of times that any character can appear consecutively in a password value. |
| *Description* | A value of zero indicates that no maximum limit is enforced. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the password validator implementation. |
| *Default Value* | org.opends.server.extensions.RepeatedCharactersPasswordValidator |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordValidator |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Replication Domain

A Replication Domain comprises of several Directory Servers sharing the same synchronized set of data.

## Dependencies

The following objects have Replication Domains:

- Replication Synchronization Provider

## Replication Domain Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| base-dn<br>ecl-include<br>ecl-include-for-deletes<br>enabled<br>fractional-exclude<br>fractional-include |

## Basic Properties

base-dn

| | |
| --- | --- |
| *Synopsis* | Specifies the base DN of the replicated data. |
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

ecl-include

| | |
| --- | --- |
| *Synopsis* | Specifies a list of attributes which should be published with every change log entry, regardless of whether the attribute itself has changed. |
| *Description* | The list of attributes may include wild cards such as "*" and "+" as well as object class references prefixed with an at sign, for example "@person". The included attributes will be published using the "includedAttributes" operational attribute as a single LDIF value rather like the "changes" attribute. For modify and modifyDN operations the included attributes will be taken from the entry before any changes were applied. |
| *Default Value* | None |
| *Allowed Values* | A string. |

| | |
|---|---|
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

ecl-include-for-deletes

| | |
|---|---|
| *Synopsis* | Specifies a list of attributes which should be published with every delete operation change log entry, in addition to those specified by the "ecl-include" property. |
| *Description* | This property provides a means for applications to archive entries after they have been deleted. See the description of the "ecl-include" property for further information about how the included attributes are published. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Replication Domain is enabled in the server. |
| *Description* | If a Replication Domain is not enabled, then its contents will not be replicated. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

fractional-exclude

| | |
|---|---|
| *Synopsis* | Allows to exclude some attributes to replicate to this server. |
| *Description* | If fractional-exclude configuration attribute is used, attributes specified in this attribute will be ignored (not added/modified/deleted) when an operation |

| | |
|---|---|
| | performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-include attribute. |
| *Default Value* | None |
| *Allowed Values* | The name of one or more attribute types in the named object class to be excluded. The object class may be "*" indicating that the attribute type(s) should be excluded regardless of the type of entry they belong to. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

fractional-include

| | |
|---|---|
| *Synopsis* | Allows to include some attributes to replicate to this server. |
| *Description* | If fractional-include configuration attribute is used, only attributes specified in this attribute will be added/modified/deleted when an operation performed from another directory server is being replayed in the local server. Note that the usage of this configuration attribute is mutually exclusive with the usage of the fractional-exclude attribute. |
| *Default Value* | None |
| *Allowed Values* | The name of one or more attribute types in the named object class to be included. The object class may be "*" indicating that the attribute type(s) should be included regardless of the type of entry they belong to. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Replication Server

Replication Servers publish updates to Directory Servers within a Replication Domain.

## Dependencies

The following objects have Replication Servers:

- Replication Synchronization Provider

# Replication Server Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| advertised-listen-address<br>changelog-enabled<br>changelog-enabled-excluded-domains<br>cipher-key-length<br>cipher-transformation<br>confidentiality-enabled<br>degraded-status-threshold<br>listen-address<br>replication-db-directory<br>replication-port<br>weight | disk-full-threshold<br>disk-low-threshold |

## Basic Properties

### advertised-listen-address

| | |
|---|---|
| *Synopsis* | The advertised address(es) which clients should use for connecting to this Replication Server. |
| *Description* | Multiple addresses may be provided as separate values for this attribute. The meta-address 0.0.0.0 is not permitted. |
| *Default Value* | None |
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### changelog-enabled

| | |
|---|---|
| *Synopsis* | Specifies whether the "cn=changelog" backend will be available to client applications. |
| *Default Value* | enabled |
| *Allowed Values* | disabled: The "cn=changelog" backend will not be available to client applications.<br><br>enabled: The "cn=changelog" backend will be available to client applications. It will support searches using changelog cookies and "change numbers" as per the internet draft, http://tools.ietf.org/html/draft-good-ldap-changelog-04. Change |

| | |
|---|---|
| | numbers are globally consistent across all servers. This mode requires additional CPU, disk accesses and storage, so it should not be used unless change number based browsing is required.<br><br>enabled-cookie-mode-only: The "cn=changelog" backend will be available to client applications. However, it will only support searches using changelog cookies. Changes are published immediately, and in an order which may vary from one server to another. This mode does not require additional server resources. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

changelog-enabled-excluded-domains

| | |
|---|---|
| *Synopsis* | Specifies the base DNs of domains to exclude from the change number indexer when changelog is enabled. |
| *Default Value* | When changelog is enabled, searches using "change numbers" is available for all domains (in other words, change number indexer includes all domains). |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

cipher-key-length

| | |
|---|---|
| *Synopsis* | Specifies the key length in bits for the preferred cipher. |
| *Default Value* | 128 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only affect cryptographic operations performed after the change. |
| *Advanced* | No |
| *Read-Only* | No |

### cipher-transformation

| | |
|---|---|
| *Synopsis* | Specifies the cipher for the directory server. The syntax is "algorithm/mode/padding". |
| *Description* | The full transformation is required: specifying only an algorithm and allowing the cipher provider to supply the default mode and padding is not supported, because there is no guarantee these default values are the same among different implementations. Some cipher algorithms, including RC4 and ARCFOUR, do not have a mode or padding, and hence must be specified using NONE for the mode field and NoPadding for the padding field. For example, RC4/NONE/NoPadding. |
| *Default Value* | AES/GCM/NoPadding |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only affect cryptographic operations performed after the change. |
| *Advanced* | No |
| *Read-Only* | No |

### confidentiality-enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the replication change-log should make records readable only by Directory Server. Throughput and disk space are affected by the more expensive operations taking place. |
| *Description* | Confidentiality is achieved by encrypting records on all domains managed by this replication server. Encrypting the records prevents unauthorized parties from accessing contents of LDAP operations. For complete protection, consider enabling secure communications between servers. Change number indexing is not affected by the setting. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only affect operations performed after the change. |
| *Advanced* | No |
| *Read-Only* | No |

### degraded-status-threshold

| | |
|---|---|
| *Synopsis* | The number of pending changes as threshold value for putting a directory server in degraded status. |
| *Description* | This value represents a number of pending changes a replication server has in queue for sending to a directory server. Once this value is crossed, the matching directory server goes in degraded status. When number of pending changes goes back under this value, the directory server is put back in normal status. 0 means status analyzer is disabled and directory servers are never put in degraded status. |
| *Default Value* | 5000 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### listen-address

| | |
|---|---|
| *Synopsis* | The network interface(s) on which this Replication Server should listen for incoming client connections. |
| *Description* | Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the directory server will listen on all interfaces. |
| *Default Value* | 0.0.0.0 |
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### replication-db-directory

| | |
|---|---|
| *Synopsis* | The path where the Replication Server stores all persistent information. |
| *Default Value* | changelogDb |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

replication-port

| | |
|---|---|
| *Synopsis* | The port on which this Replication Server waits for connections from other Replication Servers or Directory Servers. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br>Lower limit: 1.<br>Upper limit: 65535. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

weight

| | |
|---|---|
| *Synopsis* | The weight of the replication server. |
| *Description* | The weight affected to the replication server. Each replication server of the topology has a weight. When combined together, the weights of the replication servers of a same group can be translated to a percentage that determines the quantity of directory servers of the topology that should be connected to a replication server. For instance imagine a topology with 3 replication servers (with the same group id) with the following weights: RS1=1, RS2=1, RS3=2. This means that RS1 should have 25% of the directory servers connected in the topology, RS2 25%, and RS3 50%. This may be useful if the replication servers of the topology have a different power and one wants to spread the load between the replication servers according to their power. |
| *Default Value* | 1 |
| *Allowed Values* | An integer.<br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

disk-full-threshold

| | |
|---|---|
| *Synopsis* | The free disk space threshold at which point a warning alert notification will be triggered and the replication server will disconnect from the rest of the replication topology. |
| *Description* | When the available free space on the disk used by the replication changelog falls below the value specified, this replication server will stop. Connected Directory Servers will fail over to another RS. The replication server will restart again as soon as free space rises above the low threshold. |
| *Default Value* | 5% of the filesystem size, plus 1 GB |
| *Allowed Values* | Uses *Size Syntax* . |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

disk-low-threshold

| | |
|---|---|
| *Synopsis* | The free disk space threshold at which point a warning alert notification will be triggered. |
| *Description* | When the available free space on the disk used by the replication changelog falls below the value specified, a warning is sent and logged. Normal operation will continue but administrators are advised to take action to free some disk space. |
| *Default Value* | 5% of the filesystem size, plus 5 GB |
| *Allowed Values* | Uses *Size Syntax* . |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Replication Service Discovery Mechanism

A Replication Service Discovery Mechanism returns the set of directory servers participating in a replication topology.

The Replication Service Discovery Mechanism specifies the replication servers whose configuration is periodically read to discover available replicas.

## Parent

The Replication Service Discovery Mechanism object inherits from Service Discovery Mechanism.

## Dependencies

Replication Service Discovery Mechanisms depend on the following objects:

- Key Manager Provider
- Trust Manager Provider

## Replication Service Discovery Mechanism Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| bind-dn<br>bind-password<br>bootstrap-replication-server<br>discovery-interval<br>key-manager-provider<br>primary-group-id<br>ssl-cert-nickname<br>ssl-cipher-suite<br>ssl-protocol<br>trust-manager-provider<br>use-sasl-external<br>use-ssl<br>use-start-tls | java-class |

## Basic Properties

bind-dn

| | |
|---|---|
| *Synopsis* | The bind DN for periodically reading replication server configurations |
| *Description* | The bind DN must be present on all replication servers and directory servers, it must be able to read the server configuration. |
| *Default Value* | None |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

bind-password

| | |
|---|---|
| *Synopsis* | The clear-text bind password for periodically reading replication server configurations. |
| *Description* | The bind password must be the same on all replication and directory servers. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

bootstrap-replication-server

| | |
|---|---|
| *Synopsis* | The addresses of one or more replication servers within the topology which this server should connect to in order to discover the rest of the topology. |
| *Description* | Addresses must be specified using the administration port of the remote replication servers using the syntax "hostname:admin-port". When using an IPv6 address as the hostname, put brackets around the address as in "[IPv6Address]:admin-port". |
| *Default Value* | None |
| *Allowed Values* | A host name or an IP address followed by a ":" and a port number.<br><br>Port number must be greater than 1 and less than 65535. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

discovery-interval

| | |
|---|---|
| *Synopsis* | Interval between two replication server configuration discovery queries. |
| *Description* | Specifies how frequently to query a replication server configuration in order to discover information about available directory server replicas. |

| | |
|---|---|
| *Default Value* | 60s |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 1 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the key manager that should be used with this Replication Service Discovery Mechanism. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Key Manager Provider .<br><br>The referenced key manager provider must be enabled when the Replication Service Discovery Mechanism is enabled and configured to use SASL/External certificate authentication. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections. |
| *Advanced* | No |
| *Read-Only* | No |

primary-group-id

| | |
|---|---|
| *Synopsis* | Replication domain group ID of preferred directory server replicas. |
| *Description* | Directory server replicas with this replication domain group ID will be preferred over other directory server replicas. Secondary server replicas will only be used when all primary server replicas become unavailable. |
| *Default Value* | All the server replicas will be treated the same. |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

ssl-cert-nickname

| | |
|---|---|
| *Synopsis* | Specifies the nicknames (also called the aliases) of the keys or key pairs that the Replication Service Discovery Mechanism should use when performing SSL communication. |
| *Description* | The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Replication Service Discovery Mechanism is configured to use SSL. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cipher-suite

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL cipher suites that are allowed for use in SSL or TLS communication. |
| *Default Value* | Uses the default set of SSL cipher suites provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-protocol

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL protocols that are allowed for use in SSL or TLS communication. |
| *Default Value* | Uses the default set of SSL protocols provided by the server's JVM. |
| *Allowed Values* | A string. |

| | |
|---|---|
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

trust-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the trust manager that should be used with the Replication Service Discovery Mechanism. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Trust Manager Provider .<br><br>The referenced trust manager provider must be enabled when this Replication Service Discovery Mechanism is configured to use SSL or StartTLS. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections. |
| *Advanced* | No |
| *Read-Only* | No |

use-sasl-external

| | |
|---|---|
| *Synopsis* | Indicates whether the Replication Service Discovery Mechanism should use certificate based authentication when communicating with backend servers. |
| *Description* | If enabled, the Replication Service Discovery Mechanism will use mutual TLS when connecting to backend servers. Once the TLS handshake has completed, a SASL/External LDAP bind request will be sent in order to associate the TLS client certificate with an LDAP account on the remote backend server. A key manager provider containing the client certificate must be configured in order to use this feature. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

use-ssl

| | |
|---|---|
| *Synopsis* | Indicates whether the Replication Service Discovery Mechanism should use SSL. |
| *Description* | If enabled, the Replication Service Discovery Mechanism will use SSL to encrypt communication with the clients. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

use-start-tls

| | |
|---|---|
| *Synopsis* | Indicates whether the Replication Service Discovery Mechanism should use Start TLS. |
| *Description* | If enabled, the Replication Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Replication Service Discovery Mechanism implementation. |

| | |
|---|---|
| *Default Value* | org.opends.server.discovery.ReplicationServiceDiscoveryMechanism |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.discovery.ServiceDiscoveryMechanism |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Replication Synchronization Provider

The Replication Synchronization Provider provides multi-master replication of data across multiple directory server instances.

## Parent

The Replication Synchronization Provider object inherits from Synchronization Provider.

## Dependencies

Replication Synchronization Providers depend on the following objects:

- Key Manager Provider
- Trust Manager Provider

The following objects belong to Replication Synchronization Providers:

- Replication Domain
- Replication Server

## Replication Synchronization Provider Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| bootstrap-replication-server<br>enabled<br>health-checks-enabled | changetime-heartbeat-interval<br>connection-timeout<br>java-class |

| Basic Properties | Advanced Properties |
|---|---|
| heartbeat-interval<br>initialization-window-size<br>isolation-policy<br>key-manager-provider<br>log-changenumber<br>max-replication-delay-health-check<br>referrals-url<br>replication-purge-delay<br>source-address<br>ssl-cert-nickname<br>ssl-cipher-suite<br>ssl-encryption<br>ssl-protocol<br>trust-manager-provider | num-update-replay-threads<br>solve-conflicts |

## Basic Properties

### bootstrap-replication-server

| | |
|---|---|
| *Synopsis* | The addresses of one or more replication servers within the topology which this server should connect to in order to discover the rest of the topology. |
| *Description* | Addresses must be specified using the replication port of the remote replication servers using the syntax "hostname:repl-port". When using an IPv6 address as the hostname, put brackets around the address as in "[IPv6Address]:repl-port". |
| *Default Value* | Adding a replication server or a replication domain requires this to be filled. |
| *Allowed Values* | A host name or an IP address followed by a ":" and a port number.<br><br>Port number must be greater than 1 and less than 65535. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Synchronization Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

health-checks-enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Replication Synchronization Providers health-checker is enabled. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

heartbeat-interval

| | |
|---|---|
| *Synopsis* | Specifies the heartbeat interval that the directory server will use when communicating with Replication Servers. |
| *Description* | The directory server expects a regular heartbeat coming from the Replication Server within the specified interval. If a heartbeat is not received within the interval, the Directory Server closes its connection and connects to another Replication Server. |
| *Default Value* | 30s |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 100 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

initialization-window-size

| | |
|---|---|
| *Synopsis* | Specifies the window size that this directory server may use when communicating with remote Directory Servers for initialization. |
| *Default Value* | 100 |
| *Allowed Values* | An integer. |

| | |
|---|---|
| | Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

isolation-policy

| | |
|---|---|
| *Synopsis* | Specifies the behavior of the directory server when writing to replicated data while none of the configured Replication Servers are available. |
| *Default Value* | reject-all-updates |
| *Allowed Values* | accept-all-updates: The server accepts updates even when it cannot send them to any Replication Server. When a Replication Server again becomes available, the server attempts to resend the updates. This does not guarantee that updates will be successfully resent. This mode can cause high replication latency.<br><br>reject-all-updates: Indicates that all updates attempted on this Replication Synchronization Provider are rejected when no Replication Server is available. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

key-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the key manager that should be used with this Replication Synchronization Provider. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Key Manager Provider .<br><br>The referenced key manager provider must be enabled. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections. |
| *Advanced* | No |
| *Read-Only* | No |

log-changenumber

| | |
|---|---|
| *Synopsis* | Indicates if this server logs the ChangeNumber in access log. |
| *Description* | This boolean indicates if the domain should log the ChangeNumber of replicated operations in the access log. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

max-replication-delay-health-check

| | |
|---|---|
| *Synopsis* | The maximum replication delay for considering the Replication Synchronization Provider healthy. |
| *Default Value* | 5s |
| *Allowed Values* | Uses *Duration Syntax* .<br>Lower limit: 1 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

referrals-url

| | |
|---|---|
| *Synopsis* | The URLs other LDAP servers should use to refer to the local server. |
| *Description* | URLs used by peer servers in the topology to refer to the local server through LDAP referrals. If this attribute is not defined, every URLs available to access this server will be used. If defined, only URLs specified here will be used. |
| *Default Value* | None |
| *Allowed Values* | A LDAP URL compliant with RFC 2255. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### replication-purge-delay

| | |
|---|---|
| *Synopsis* | Minimum lifetime of changelog data and old replication meta-data in directory entries. Changelog data and replication meta-data older than this setting is eligible to be removed. |
| *Description* | After the purge delay has passed, the server removes old changelog data over time when it applies new updates. Replication meta-data is stored in changed directory entries. The server removes old replication meta-data either when the entry is next modified, or by a dedicated purge task, whichever happens first. The server temporarily stops removing old data when it has been unable to process updates for an extended period of time. For example, the server stops removing data when the server is offline, and when it cannot access other servers due to a network partition. Once old data is removed, the server can no longer use it for replication. Changelog and replication meta-data older than the purge delay must therefore be considered stale. Backups must be newer than the purge delay, including the time it takes to restore a backup. |
| *Default Value* | 3 days |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 0 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### source-address

| | |
|---|---|
| *Synopsis* | If specified, the server will bind to the address before connecting to the remote server. |
| *Description* | The address must be one assigned to an existing network interface. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### ssl-cert-nickname

| | |
|---|---|
| *Synopsis* | Specifies the nicknames (also called the aliases) of the keys or key pairs that the Replication Synchronization Provider should use when performing SSL communication. |

| | |
|---|---|
| *Description* | The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Replication Synchronization Provider is configured to use SSL. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | Restart the server for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cipher-suite

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL cipher suites that are allowed for use in SSL or TLS communication. |
| *Default Value* | Uses the default set of SSL cipher suites provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-encryption

| | |
|---|---|
| *Synopsis* | Specifies whether SSL/TLS is used to provide encrypted communication between two OpenDJ server components. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| | Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-protocol

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL protocols that are allowed for use in SSL or TLS communication. |
| *Default Value* | Uses the default set of SSL protocols provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

trust-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the trust manager that should be used with the Replication Synchronization Provider . |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Trust Manager Provider .<br><br>The referenced trust manager provider must be enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections. |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

changetime-heartbeat-interval

| | |
|---|---|
| *Synopsis* | Specifies the heartbeat interval that the directory server will use when sending its local change time to the Replication Server. |
| *Description* | The directory server sends a regular heartbeat to the Replication within the specified interval. The heartbeat indicates the change time of the directory server to the Replication Server. |
| *Default Value* | 1000ms |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 0 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

connection-timeout

| | |
|---|---|
| *Synopsis* | Specifies the timeout used when connecting to peers and when performing SSL negotiation. |
| *Default Value* | 5 seconds |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 0 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Replication Synchronization Provider implementation. |
| *Default Value* | org.opends.server.replication.plugin.MultimasterReplication |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.SynchronizationProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |

| | |
|---|---|
| *Read-Only* | No |

num-update-replay-threads

| | |
|---|---|
| *Synopsis* | Specifies the number of update replay threads. |
| *Description* | This value is the number of threads created for replaying every updates received for all the replication domains. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | An integer.<br>Lower limit: 1.<br>Upper limit: 65535. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

solve-conflicts

| | |
|---|---|
| *Synopsis* | Indicates if this server solves conflict. |
| *Description* | This boolean indicates if this domain keeps the historical meta-data necessary to solve conflicts. When set to false the server will not maintain historical meta-data and will therefore not be able to solve conflict. This should therefore be done only if the replication is used in a single master type of deployment. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Rest2LDAP Endpoint

The Rest2LDAP Endpoint provides RESTful access to LDAP application data using a set of customizable data transformations.

## Parent

The Rest2LDAP Endpoint object inherits from HTTP Endpoint.

## Rest2LDAP Endpoint Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| authorization-mechanism<br>base-path<br>config-directory<br>enabled | java-class<br>return-null-for-missing-properties |

## Basic Properties

authorization-mechanism

| | |
|---|---|
| *Synopsis* | The HTTP authorization mechanisms supported by this HTTP Endpoint. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing HTTP Authorization Mechanism .<br><br>The referenced authorization mechanism must be enabled when the HTTP Endpoint is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-path

| | |
|---|---|
| *Synopsis* | All HTTP requests matching the base path or subordinate to it will be routed to the HTTP endpoint unless a more specific HTTP endpoint is found. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | Yes |

config-directory

| | |
|---|---|
| *Synopsis* | The directory containing the Rest2Ldap configuration file(s) for this specific endpoint. |
| *Description* | The directory must be readable by the server and may contain multiple configuration files, one for each supported version of the REST endpoint. If a relative path is used then it will be resolved against the server's instance directory. |
| *Default Value* | None |
| *Allowed Values* | A directory that is readable by the server. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the HTTP Endpoint is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Rest2LDAP Endpoint implementation. |
| *Default Value* | org.opends.server.protocols.http.rest2ldap.Rest2LdapEndpoint |
| *Allowed Values* | A Java class that extends or implements: |

| | |
|---|---|
| | • org.opends.server.api.HttpEndpoint |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

return-null-for-missing-properties

| | |
|---|---|
| *Synopsis* | Indicates whether missing (unmapped) JSON properties should be included in JSON resources. |
| *Description* | By default JSON properties that do not have a corresponding LDAP attribute are unmapped and not included in JSON resources returned by the REST endpoint. Set this option to true if unmapped JSON properties should be included with a value of null. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Root DSE Backend

The Root DSE Backend contains the directory server root DSE.

This is a special meta-backend that dynamically generates the root DSE entry for base-level searches and simply redirects to other backends for operations in other scopes.

## Root DSE Backend Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| show-all-attributes<br>show-subordinate-naming-contexts |

## Basic Properties

show-all-attributes

| | |
|---|---|
| *Synopsis* | Indicates whether all attributes in the root DSE are to be treated like user attributes (and therefore returned to clients by default) regardless of the directory server schema configuration. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

show-subordinate-naming-contexts

| | |
|---|---|
| *Synopsis* | Indicates whether subordinate naming contexts should be visible in the namingContexts attribute of the RootDSE. By default only top level naming contexts are visible |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Salted MD5 Password Storage Scheme

The Salted MD5 Password Storage Scheme provides a mechanism for encoding user passwords using a salted form of the MD5 message digest algorithm.

This scheme contains an implementation for the user password syntax, with a storage scheme name of "SMD5", and an implementation of the auth password syntax, with a storage scheme name of "MD5". Although the MD5 digest algorithm is relatively secure, recent cryptanalysis work has identified mechanisms for generating MD5 collisions. This does not impact the security of this

algorithm as it is used in OpenDJ, but it is recommended that the MD5 password storage scheme only be used if client applications require it for compatibility purposes, and that a stronger digest like SSHA or SSHA256 be used for environments in which MD5 support is not required.

## Parent

The Salted MD5 Password Storage Scheme object inherits from Password Storage Scheme.

## Salted MD5 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Salted MD5 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.SaltedMD5PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements: |

| | |
|---|---|
| | • org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Salted SHA-1 Password Storage Scheme

The Salted SHA-1 Password Storage Scheme provides a mechanism for encoding user passwords using a salted form of the SHA-1 message digest algorithm.

This scheme contains an implementation for the user password syntax, with a storage scheme name of "SSHA", and an implementation of the auth password syntax, with a storage scheme name of "SHA1".

## Parent

The Salted SHA-1 Password Storage Scheme object inherits from Password Storage Scheme.

## Salted SHA-1 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Salted SHA-1 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.SaltedSHA1PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## Salted SHA-256 Password Storage Scheme

The Salted SHA-256 Password Storage Scheme provides a mechanism for encoding user passwords using a salted form of the 256-bit SHA-2 message digest algorithm.

This scheme contains an implementation for the user password syntax, with a storage scheme name of "SSHA256", and an implementation of the auth password syntax, with a storage scheme name of "SHA256".

### Parent

The Salted SHA-256 Password Storage Scheme object inherits from Password Storage Scheme.

### Salted SHA-256 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Salted SHA-256 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.SaltedSHA256PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Salted SHA-384 Password Storage Scheme

The Salted SHA-384 Password Storage Scheme provides a mechanism for encoding user passwords using a salted form of the 384-bit SHA-2 message digest algorithm.

This scheme contains an implementation for the user password syntax, with a storage scheme name of "SSHA384", and an implementation of the auth password syntax, with a storage scheme name of "SHA384".

## Parent

The Salted SHA-384 Password Storage Scheme object inherits from Password Storage Scheme.

## Salted SHA-384 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Salted SHA-384 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.SaltedSHA384PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Salted SHA-512 Password Storage Scheme

The Salted SHA-512 Password Storage Scheme provides a mechanism for encoding user passwords using a salted form of the 512-bit SHA-2 message digest algorithm.

This scheme contains an implementation for the user password syntax, with a storage scheme name of "SSHA512", and an implementation of the auth password syntax, with a storage scheme name of "SHA512".

## Parent

The Salted SHA-512 Password Storage Scheme object inherits from Password Storage Scheme.

## Salted SHA-512 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Salted SHA-512 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.SaltedSHA512PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## Samba Password Plugin

Samba Password Synchronization Plugin.

This plugin captures clear-text password changes for a user and generates LanMan or NTLM hashes for the respective Samba attributes (sambaLMPassword and sambaNTPassword).

### Parent

The Samba Password Plugin object inherits from Plugin.

### Samba Password Plugin Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>java-class<br>pwd-sync-policy<br>samba-administrator-dn | invoke-for-internal-operations<br>plugin-type |

## Basic Properties

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the plug-in implementation. |
| *Default Value* | org.opends.server.plugins.SambaPasswordPlugin |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.plugin.DirectoryServerPlugin |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### pwd-sync-policy

| | |
|---|---|
| *Synopsis* | Specifies which Samba passwords should be kept synchronized. |
| *Default Value* | sync-nt-password |
| *Allowed Values* | sync-lm-password: Synchronize the LanMan password attribute "sambaLMPassword"<br><br>sync-nt-password: Synchronize the NT password attribute "sambaNTPassword" |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

samba-administrator-dn

| | |
|---|---|
| *Synopsis* | Specifies the distinguished name of the user which Samba uses to perform Password Modify extended operations against this directory server in order to synchronize the userPassword attribute after the LanMan or NT passwords have been updated. |
| *Description* | The user must have the 'password-reset' privilege and should not be a root user. This user name can be used in order to identify Samba connections and avoid double re-synchronization of the same password. If this property is left undefined, then no password updates will be skipped. |
| *Default Value* | Synchronize all updates to user passwords |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

invoke-for-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in should be invoked for internal operations. |
| *Description* | Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

plugin-type

| | |
|---|---|
| *Synopsis* | Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked. |
| *Default Value* | preoperationmodify<br><br>postoperationextended |
| *Allowed Values* | initialization: Invoked at the initialization of the directory server.<br><br>intermediateresponse: Invoked before sending an intermediate repsonse message to the client.<br><br>ldifimport: Invoked for each entry read during an LDIF import.<br><br>ldifimportbegin: Invoked at the beginning of an LDIF import session.<br><br>ldifimportend: Invoked at the end of an LDIF import session.<br><br>postconnect: Invoked whenever a new connection is established to the server.<br><br>postdisconnect: Invoked whenever an existing connection is terminated (by either the client or the server).<br><br>postoperationabandon: Invoked after completing the abandon processing.<br><br>postoperationadd: Invoked after completing the core add processing but before sending the response to the client.<br><br>postoperationbind: Invoked after completing the core bind processing but before sending the response to the client.<br><br>postoperationcompare: Invoked after completing the core compare processing but before sending the response to the client.<br><br>postoperationdelete: Invoked after completing the core delete processing but before sending the response to the client.<br><br>postoperationextended: Invoked after completing the core extended processing but before sending the response to the client.<br><br>postoperationmodify: Invoked after completing the core modify processing but before sending the response to the client.<br><br>postoperationmodifydn: Invoked after completing the core modify DN processing but before sending the response to the client.<br><br>postoperationsearch: Invoked after completing the core search processing but before sending the response to the client.<br><br>postoperationunbind: Invoked after completing the unbind processing.<br><br>postresponseadd: Invoked after sending the add response to the client.<br><br>postresponsebind: Invoked after sending the bind response to the client. |

postresponsecompare: Invoked after sending the compare response to the client.

postresponsedelete: Invoked after sending the delete response to the client.

postresponseextended: Invoked after sending the extended response to the client.

postresponsemodify: Invoked after sending the modify response to the client.

postresponsemodifydn: Invoked after sending the modify DN response to the client.

postresponsesearch: Invoked after sending the search result done message to the client.

postsynchronizationadd: Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete: Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify: Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn: Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd: Invoked prior to performing the core add processing.

preoperationbind: Invoked prior to performing the core bind processing.

preoperationcompare: Invoked prior to performing the core compare processing.

preoperationdelete: Invoked prior to performing the core delete processing.

preoperationextended: Invoked prior to performing the core extended processing.

preoperationmodify: Invoked prior to performing the core modify processing.

preoperationmodifydn: Invoked prior to performing the core modify DN processing.

preoperationsearch: Invoked prior to performing the core search processing.

preparseabandon: Invoked prior to parsing an abandon request.

preparseadd: Invoked prior to parsing an add request.

preparsebind: Invoked prior to parsing a bind request.

preparsecompare: Invoked prior to parsing a compare request.

preparsedelete: Invoked prior to parsing a delete request.

preparseextended: Invoked prior to parsing an extended request.

preparsemodify: Invoked prior to parsing a modify request.

| | |
|---|---|
| | preparsemodifydn: Invoked prior to parsing a modify DN request.<br><br>preparsesearch: Invoked prior to parsing a search request.<br><br>preparseunbind: Invoked prior to parsing an unbind request.<br><br>searchresultentry: Invoked before sending a search result entry to the client.<br><br>searchresultreference: Invoked before sending a search result reference to the client.<br><br>shutdown: Invoked during a graceful directory server shutdown.<br><br>startup: Invoked during the directory server startup process.<br><br>subordinatedelete: Invoked in the course of deleting a subordinate entry of a delete operation.<br><br>subordinatemodifydn: Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# SASL Mechanism Handler

*This is an abstract object type that cannot be instantiated.*

The SASL mechanism handler configuration entry is the parent for all SASL mechanism handlers defined in the OpenDJ directory server.

SASL mechanism handlers are responsible for authenticating users during the course of processing a SASL (Simple Authentication and Security Layer, as defined in RFC 4422) bind.

## SASL Mechanism Handlers

The following SASL Mechanism Handlers are available:

- Anonymous SASL Mechanism Handler
- CRAM-MD5 SASL Mechanism Handler
- DIGEST-MD5 SASL Mechanism Handler
- External SASL Mechanism Handler

- GSSAPI SASL Mechanism Handler
- Plain SASL Mechanism Handler
- SCRAM-SHA-256 SASL Mechanism Handler
- SCRAM-SHA-512 SASL Mechanism Handler

These SASL Mechanism Handlers inherit the properties described below.

## SASL Mechanism Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| enabled<br>java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the SASL mechanism handler is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.SASLMechanismHandler |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# Schema Backend

The Schema Backend provides access to the directory server schema information, including the attribute types, object classes, attribute syntaxes, matching rules, matching rule uses, DIT content rules, and DIT structure rules that it contains.

The server allows "modify" operations in this backend to alter the server schema definitions. The configuration entry for this backend is based on the ds-cfg-schema-backend structural object class. Note that any attribute types included in this entry that are not included in this object class (or the parent ds-cfg-backend class) appears directly in the schema entry.

## Parent

The Schema Backend object inherits from Local Backend.

## Schema Backend Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| backend-id<br>enabled<br>show-all-attributes<br>writability-mode | java-class<br>schema-entry-dn |

## Basic Properties

backend-id

| | |
|---|---|
| *Synopsis* | Specifies a name to identify the associated backend. |
| *Description* | The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the backend is enabled in the server. |
| *Description* | If a backend is not enabled, then its contents are not accessible when processing operations. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

show-all-attributes

| | |
|---|---|
| *Synopsis* | Indicates whether to treat all attributes in the schema entry as if they were user attributes regardless of their configuration. |
| *Description* | This may provide compatibility with some applications that expect schema attributes like attributeTypes and objectClasses to be included by default even if they are not requested. Note that the ldapSyntaxes attribute is always treated as operational in order to avoid problems with attempts to modify the schema over protocol. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

writability-mode

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the backend should use when processing write operations. |

| | |
|---|---|
| *Default Value* | enabled |
| *Allowed Values* | disabled: Causes all write attempts to fail.<br><br>enabled: Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).<br><br>internal-only: Causes external write attempts to fail but allows writes by replication and internal operations. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the backend implementation. |
| *Default Value* | org.opends.server.backends.SchemaBackend |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.Backend |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

schema-entry-dn

| | |
|---|---|
| *Synopsis* | Defines the base DNs of the subtrees in which the schema information is published in addition to the value included in the base-dn property. |
| *Description* | The value provided in the base-dn property is the only one that appears in the subschemaSubentry operational attribute of the server's root DSE (which is necessary because that is a single-valued attribute) and as a virtual attribute in other entries. The schema-entry-dn attribute may be used to make the schema information available in other locations to accommodate certain client applications that have been hard-coded to expect the schema to reside in a specific location. |

| | |
|---|---|
| *Default Value* | cn=schema |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Schema Provider

*This is an abstract object type that cannot be instantiated.*

Schema Providers define the schema elements to load.

Schema provider configuration.

## Schema Providers

The following Schema Providers are available:

- Core Schema
- JSON Equality Matching Rule
- JSON Ordering Matching Rule
- JSON Query Equality Matching Rule

These Schema Providers inherit the properties described below.

## Schema Provider Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| enabled<br>java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Schema Provider is enabled for use. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Schema Provider implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.schema.SchemaProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# SCRAM-SHA-256 Password Storage Scheme

The SCRAM-SHA-256 Password Storage Scheme provides a mechanism for encoding user passwords for use with the SASL SCRAM authentication mechanism defined in RFC 5802.

This scheme contains an implementation for the user password syntax, and uses the scheme name SCRAM-SHA-256. Password values are encoded using the format described in RFC 5803.

## Parent

The SCRAM-SHA-256 Password Storage Scheme object inherits from Password Storage Scheme.

## SCRAM-SHA-256 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>scram-iterations | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scram-iterations

| | |
|---|---|
| *Synopsis* | The number of iterations to use when deriving the salted password. |
| *Default Value* | 10000 |
| *Allowed Values* | An integer.<br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SCRAM-SHA-256 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.ScramSha256PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements: |

| | |
|---|---|
| | • org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# SCRAM-SHA-256 SASL Mechanism Handler

The SCRAM-SHA-256 SASL mechanism performs all processing related to SASL SCRAM-SHA-256 authentication.

The SCRAM-SHA-256 SASL mechanism is defined in RFCs 5802 and 7677 and replaces the deprecated CRAM-MD5 and DIGEST-MD5 mechanisms. It is a cost-based password authentication approach, similar to PBKDF2, with the important difference that the computational effort is delegated to the client applications. This mechanism can only be used in conjunction with the SCRAM-SHA-256 password storage scheme.

## Parent

The SCRAM-SHA-256 SASL Mechanism Handler object inherits from SASL Mechanism Handler.

## Dependencies

SCRAM-SHA-256 SASL Mechanism Handlers depend on the following objects:

- Identity Mapper

## SCRAM-SHA-256 SASL Mechanism Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>identity-mapper | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the SASL mechanism handler is enabled for use. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name(s) of the identity mappers that are to be used with this SASL mechanism handler for matching the authentication or authorization ID included in SASL bind requests with users in the directory. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br><br>The referenced identity mapper(s) must be enabled when the SCRAM-SHA-256 SASL Mechanism Handler is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation. |
| *Default Value* | org.opends.server.extensions.ScramSha256SASLMechanismHandler |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.SASLMechanismHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |

| | |
|---|---|
| *Read-Only* | No |

# SCRAM-SHA-512 Password Storage Scheme

The SCRAM-SHA-512 Password Storage Scheme provides a mechanism for encoding user passwords for use with the SASL SCRAM authentication mechanism defined in RFC 5802.

This scheme contains an implementation for the user password syntax, and uses the scheme name SCRAM-SHA-512. Password values are encoded using the format described in RFC 5803.

## Parent

The SCRAM-SHA-512 Password Storage Scheme object inherits from Password Storage Scheme.

## SCRAM-SHA-512 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>scram-iterations | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scram-iterations

| | |
|---|---|
| *Synopsis* | The number of iterations to use when deriving the salted password. |
| *Default Value* | 10000 |

| | |
|---|---|
| *Allowed Values* | An integer.<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SCRAM-SHA-512 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.ScramSha512PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## SCRAM-SHA-512 SASL Mechanism Handler

The SCRAM-SHA-512 SASL mechanism performs all processing related to SASL SCRAM-SHA-512 authentication.

The SCRAM-SHA-512 SASL mechanism is defined in RFCs 5802 and 7677 and replaces the deprecated CRAM-MD5 and DIGEST-MD5 mechanisms. It is a cost-based password authentication approach, similar to PBKDF2, with the important difference that the computational effort is delegated to the client applications. This mechanism can only be used in conjunction with the SCRAM-SHA-512 password storage scheme.

### Parent

The SCRAM-SHA-512 SASL Mechanism Handler object inherits from SASL Mechanism Handler.

## Dependencies

SCRAM-SHA-512 SASL Mechanism Handlers depend on the following objects:

- Identity Mapper

## SCRAM-SHA-512 SASL Mechanism Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>identity-mapper | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the SASL mechanism handler is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

identity-mapper

| | |
|---|---|
| *Synopsis* | Specifies the name(s) of the identity mappers that are to be used with this SASL mechanism handler for matching the authentication or authorization ID included in SASL bind requests with users in the directory. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Identity Mapper .<br><br>The referenced identity mapper(s) must be enabled when the SCRAM-SHA-512 SASL Mechanism Handler is enabled. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SASL mechanism handler implementation. |
| *Default Value* | org.opends.server.extensions.ScramSha512SASLMechanismHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.SASLMechanismHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Service Discovery Mechanism

*This is an abstract object type that cannot be instantiated.*

A Service Discovery Mechanism identifies a set of LDAP servers for load balancing

### Service Discovery Mechanisms

The following Service Discovery Mechanisms are available:

- Replication Service Discovery Mechanism
- Static Service Discovery Mechanism

These Service Discovery Mechanisms inherit the properties described below.

### Dependencies

The following objects depend on Service Discovery Mechanisms:

- Proxy Backend

## Service Discovery Mechanism Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| java-class |

## Basic Properties

java-class

| | |
| --- | --- |
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Service Discovery Mechanism implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.discovery.ServiceDiscoveryMechanism |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

# Seven Bit Clean Plugin

The Seven Bit Clean Plugin ensures that values for a specified set of attributes are 7-bit clean.

That is, for those attributes, the values are not allowed to contain any bytes having the high-order bit set, which is used to indicate the presence of non-ASCII characters. Some applications do not properly handle attribute values that contain non-ASCII characters, and this plug-in can help ensure that attributes used by those applications do not contain characters that can cause problems in those applications.

## Parent

The Seven Bit Clean Plugin object inherits from Plugin.

## Seven Bit Clean Plugin Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>enabled | invoke-for-internal-operations<br>java-class<br>plugin-type |

## Basic Properties

### attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the name or OID of an attribute type for which values should be checked to ensure that they are 7-bit clean. |
| *Default Value* | uid<br>mail<br>userPassword |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DN below which the checking is performed. |
| *Description* | Any attempt to update a value for one of the configured attributes below this base DN must be 7-bit clean for the operation to be allowed. |
| *Default Value* | All entries below all public naming contexts will be checked. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true |

| | |
|---|---|
| | false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

invoke-for-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in should be invoked for internal operations. |
| *Description* | Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked. |
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the plug-in implementation. |
| *Default Value* | org.opends.server.plugins.SevenBitCleanPlugin |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.plugin.DirectoryServerPlugin |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

plugin-type

| | |
|---|---|
| *Synopsis* | Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked. |
| *Default Value* | ldifimport<br><br>preparseadd<br><br>preparsemodify<br><br>preparsemodifydn |
| *Allowed Values* | initialization: Invoked at the initialization of the directory server.<br><br>intermediateresponse: Invoked before sending an intermediate repsonse message to the client.<br><br>ldifimport: Invoked for each entry read during an LDIF import.<br><br>ldifimportbegin: Invoked at the beginning of an LDIF import session.<br><br>ldifimportend: Invoked at the end of an LDIF import session.<br><br>postconnect: Invoked whenever a new connection is established to the server.<br><br>postdisconnect: Invoked whenever an existing connection is terminated (by either the client or the server).<br><br>postoperationabandon: Invoked after completing the abandon processing.<br><br>postoperationadd: Invoked after completing the core add processing but before sending the response to the client.<br><br>postoperationbind: Invoked after completing the core bind processing but before sending the response to the client.<br><br>postoperationcompare: Invoked after completing the core compare processing but before sending the response to the client.<br><br>postoperationdelete: Invoked after completing the core delete processing but before sending the response to the client.<br><br>postoperationextended: Invoked after completing the core extended processing but before sending the response to the client.<br><br>postoperationmodify: Invoked after completing the core modify processing but before sending the response to the client.<br><br>postoperationmodifydn: Invoked after completing the core modify DN processing but before sending the response to the client.<br><br>postoperationsearch: Invoked after completing the core search processing but before sending the response to the client.<br><br>postoperationunbind: Invoked after completing the unbind processing. |

postresponseadd: Invoked after sending the add response to the client.

postresponsebind: Invoked after sending the bind response to the client.

postresponsecompare: Invoked after sending the compare response to the client.

postresponsedelete: Invoked after sending the delete response to the client.

postresponseextended: Invoked after sending the extended response to the client.

postresponsemodify: Invoked after sending the modify response to the client.

postresponsemodifydn: Invoked after sending the modify DN response to the client.

postresponsesearch: Invoked after sending the search result done message to the client.

postsynchronizationadd: Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete: Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify: Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn: Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd: Invoked prior to performing the core add processing.

preoperationbind: Invoked prior to performing the core bind processing.

preoperationcompare: Invoked prior to performing the core compare processing.

preoperationdelete: Invoked prior to performing the core delete processing.

preoperationextended: Invoked prior to performing the core extended processing.

preoperationmodify: Invoked prior to performing the core modify processing.

preoperationmodifydn: Invoked prior to performing the core modify DN processing.

preoperationsearch: Invoked prior to performing the core search processing.

preparseabandon: Invoked prior to parsing an abandon request.

preparseadd: Invoked prior to parsing an add request.

preparsebind: Invoked prior to parsing a bind request.

preparsecompare: Invoked prior to parsing a compare request.

preparsedelete: Invoked prior to parsing a delete request.

| | |
|---|---|
| | preparseextended: Invoked prior to parsing an extended request.<br>preparsemodify: Invoked prior to parsing a modify request.<br>preparsemodifydn: Invoked prior to parsing a modify DN request.<br>preparsesearch: Invoked prior to parsing a search request.<br>preparseunbind: Invoked prior to parsing an unbind request.<br>searchresultentry: Invoked before sending a search result entry to the client.<br>searchresultreference: Invoked before sending a search result reference to the client.<br>shutdown: Invoked during a graceful directory server shutdown.<br>startup: Invoked during the directory server startup process.<br>subordinatedelete: Invoked in the course of deleting a subordinate entry of a delete operation.<br>subordinatemodifydn: Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# SHA-1 Password Storage Scheme

The SHA-1 Password Storage Scheme provides a mechanism for encoding user passwords using an unsalted form of the SHA-1 message digest algorithm. Because the implementation does not use any kind of salting mechanism, a given password always has the same encoded form.

This scheme contains only an implementation for the user password syntax, with a storage scheme name of "SHA".

## Parent

The SHA-1 Password Storage Scheme object inherits from Password Storage Scheme.

## SHA-1 Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SHA-1 Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.SHA1PasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Similarity Based Password Validator

The Similarity Based Password Validator determines whether a proposed password is acceptable by measuring how similar it is to the user's current password.

In particular, it uses the Levenshtein Distance algorithm to determine the minimum number of changes (where a change may be inserting, deleting, or replacing a character) to transform one string into the other. It can be used to prevent users from making only minor changes to their current password when setting a new password. Note that for this password validator to be effective, it is necessary to have access to the user's current password. Therefore, if this password validator is to be enabled, the password-change-requires-current-password attribute in the password policy configuration must also be set to true.

## Parent

The Similarity Based Password Validator object inherits from Password Validator.

## Similarity Based Password Validator Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>min-password-difference | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the password validator is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

min-password-difference

| | |
|---|---|
| *Synopsis* | Specifies the minimum difference of new and old password. |
| *Description* | A value of zero indicates that no difference between passwords is acceptable. |
| *Default Value* | None |
| *Allowed Values* | An integer. |

| | |
|---|---|
| | Lower limit: 0.<br><br>Upper limit: 2147483647. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the password validator implementation. |
| *Default Value* | org.opends.server.extensions.SimilarityBasedPasswordValidator |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordValidator |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Size Limit Log Retention Policy

Retention policy based on the amount of space taken by all the log files on disk.

### Parent

The Size Limit Log Retention Policy object inherits from Log Retention Policy.

### Size Limit Log Retention Policy Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| disk-space-used | java-class |

## Basic Properties

disk-space-used

| | |
|---|---|
| *Synopsis* | Specifies the maximum total disk space used by the log files. |
| *Default Value* | None |
| *Allowed Values* | Uses *Size Syntax* .<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Size Limit Log Retention Policy implementation. |
| *Default Value* | org.opends.server.loggers.SizeBasedRetentionPolicy |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.loggers.RetentionPolicy |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Size Limit Log Rotation Policy

Rotation policy based on the size of the log file.

## Parent

The Size Limit Log Rotation Policy object inherits from Log Rotation Policy.

## Size Limit Log Rotation Policy Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| file-size-limit | java-class |

## Basic Properties

file-size-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum size that a log file can reach before it is rotated. |
| *Default Value* | None |
| *Allowed Values* | Uses *Size Syntax* .<br><br>Lower limit: 1. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Size Limit Log Rotation Policy implementation. |
| *Default Value* | org.opends.server.loggers.SizeBasedRotationPolicy |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.loggers.RotationPolicy |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# SMTP Account Status Notification Handler

The SMTP Account Status Notification Handler is a notification handler that sends email messages to end users and/or administrators whenever an account status notification is generated.

## Parent

The SMTP Account Status Notification Handler object inherits from Account Status Notification Handler.

## SMTP Account Status Notification Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| email-address-attribute-type<br>enabled<br>message-subject<br>message-template-file<br>recipient-address<br>sender-address | java-class<br>send-email-as-html<br>send-message-without-end-user-address |

## Basic Properties

email-address-attribute-type

| | |
|---|---|
| *Synopsis* | Specifies which attribute in the user's entries may be used to obtain the email address when notifying the end user. |
| *Description* | You can specify more than one email address as separate values. In this case, the OpenDJ server sends a notification to all email addresses identified. |
| *Default Value* | If no email address attribute types are specified, then no attempt is made to send email notification messages to end users. Only those users specified in the set of additional recipient addresses are sent the notification messages. |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | Yes |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Account Status Notification Handler is enabled. Only enabled handlers are invoked whenever a related event occurs in the server. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

message-subject

| | |
|---|---|
| *Synopsis* | Specifies the subject that should be used for email messages generated by this account status notification handler. |
| *Description* | The values for this property should begin with the name of an account status notification type followed by a colon and the subject that should be used for the associated notification message. If an email message is generated for an account status notification type for which no subject is defined, then that message is given a generic subject. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

message-template-file

| | |
|---|---|
| *Synopsis* | Specifies the path to the file containing the message template to generate the email notification messages. |

| | |
|---|---|
| *Description* | The values for this property should begin with the name of an account status notification type followed by a colon and the path to the template file that should be used for that notification type. If an account status notification has a notification type that is not associated with a message template file, then no email message is generated for that notification. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

recipient-address

| | |
|---|---|
| *Synopsis* | Specifies an email address to which notification messages are sent, either instead of or in addition to the end user for whom the notification has been generated. |
| *Description* | This may be used to ensure that server administrators also receive a copy of any notification messages that are generated. |
| *Default Value* | If no additional recipient addresses are specified, then only the end users that are the subjects of the account status notifications receive the notification messages. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

sender-address

| | |
|---|---|
| *Synopsis* | Specifies the email address from which the message is sent. Note that this does not necessarily have to be a legitimate email address. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SMTP Account Status Notification Handler implementation. |
| *Default Value* | org.opends.server.extensions.SMTPAccountStatusNotificationHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.AccountStatusNotificationHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

send-email-as-html

| | |
|---|---|
| *Synopsis* | Indicates whether an email notification message should be sent as HTML. |
| *Description* | If this value is true, email notification messages are marked as text/html. Otherwise outgoing email messages are assumed to be plaintext and marked as text/plain. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

send-message-without-end-user-address

| | |
|---|---|
| *Synopsis* | Indicates whether an email notification message should be generated and sent to the set of notification recipients even if the user entry does not contain any values for any of the email address attributes (that is, in cases when it is not be possible to notify the end user). |
| *Description* | This is only applicable if both one or more email address attribute types and one or more additional recipient addresses are specified. |

| | |
|---|---|
| *Default Value* | true |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# SMTP Alert Handler

The SMTP Alert Handler may be used to send e-mail messages to notify administrators of significant events that occur within the server.

## Parent

The SMTP Alert Handler object inherits from Alert Handler.

## SMTP Alert Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| disabled-alert-type<br>enabled<br>enabled-alert-type<br>message-body<br>message-subject<br>recipient-address<br>sender-address | java-class |

## Basic Properties

disabled-alert-type

| | |
|---|---|
| *Synopsis* | Specifies the names of the alert types that are disabled for this alert handler. |
| *Description* | If there are any values for this attribute, then no alerts with any of the specified types are allowed. If there are no values for this attribute, then only alerts with |

| | |
|---|---|
| | a type included in the set of enabled alert types are allowed, or if there are no values for the enabled alert types option, then all alert types are allowed. |
| *Default Value* | If there is a set of enabled alert types, then only alerts with one of those types are allowed. Otherwise, all alerts are allowed. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Alert Handler is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled-alert-type

| | |
|---|---|
| *Synopsis* | Specifies the names of the alert types that are enabled for this alert handler. |
| *Description* | If there are any values for this attribute, then only alerts with one of the specified types are allowed (unless they are also included in the disabled alert types). If there are no values for this attribute, then any alert with a type not included in the list of disabled alert types is allowed. |
| *Default Value* | All alerts with types not included in the set of disabled alert types are allowed. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

message-body

| | |
|---|---|
| *Synopsis* | Specifies the body that should be used for email messages generated by this alert handler. |
| *Description* | The token "%%alert-type%%" is dynamically replaced with the alert type string. The token "%%alert-id%%" is dynamically replaced with the alert ID value. The token "%%alert-message%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

message-subject

| | |
|---|---|
| *Synopsis* | Specifies the subject that should be used for email messages generated by this alert handler. |
| *Description* | The token "%%alert-type%%" is dynamically replaced with the alert type string. The token "%%alert-id%%" is dynamically replaced with the alert ID value. The token "%%alert-message%%" is dynamically replaced with the alert message. The token "\n" is replaced with an end-of-line marker. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

recipient-address

| | |
|---|---|
| *Synopsis* | Specifies an email address to which the messages should be sent. |
| *Description* | Multiple values may be provided if there should be more than one recipient. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

sender-address

| | |
|---|---|
| *Synopsis* | Specifies the email address to use as the sender for messages generated by this alert handler. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SMTP Alert Handler implementation. |
| *Default Value* | org.opends.server.extensions.SMTPAlertHandler |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.AlertHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## SNMP Connection Handler

The SNMP Connection Handler can be used to process SNMP requests to retrieve monitoring information described by the MIB 2605. Supported protocol are SNMP V1, V2c and V3.

The SNMP connection handler will process SNMP requests sent by SNMP Managers to retrieve information described the MIB 2605. To enable the SNMP Connection Handler, the ds-cfg-opendmk-jarfile parameter has to be set to the OpenDMK jar files location.

## Parent

The SNMP Connection Handler object inherits from Connection Handler.

## SNMP Connection Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| allowed-client<br>allowed-manager<br>allowed-user<br>community<br>denied-client<br>enabled<br>listen-address<br>listen-port<br>registered-mbean<br>restricted-client<br>restricted-client-connection-limit<br>security-agent-file<br>security-level<br>trap-port<br>traps-community<br>traps-destination | java-class |

## Basic Properties

allowed-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be allowed to establish connections to this Connection Handler. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | All clients with addresses that do not match an address on the deny list are allowed. If there is no deny list, then all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

allowed-manager

| | |
|---|---|
| *Synopsis* | Specifies the hosts of the managers to be granted the access rights. This property is required for SNMP v1 and v2 security configuration. An asterisk (*) opens access to all managers. |
| *Default Value* | * |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

allowed-user

| | |
|---|---|
| *Synopsis* | Specifies the users to be granted the access rights. This property is required for SNMP v3 security configuration. An asterisk (*) opens access to all users. |
| *Default Value* | * |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

community

| | |
|---|---|
| *Synopsis* | Specifies the v1,v2 community or the v3 context name allowed to access the MIB 2605 monitoring information or the USM MIB. The mapping between "community" and "context name" is set. |
| *Default Value* | OpenDJ |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

denied-client

| | |
|---|---|
| *Synopsis* | A set of clients who are not allowed to establish connections to this Connection Handler. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. If both allowed and denied client masks are defined and a client connection matches one or more masks in both lists, then the connection is denied. If only a denied list is specified, then any client not matching a mask in that list is allowed. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | If an allow list is specified, then only clients with addresses on the allow list are allowed. Otherwise, all clients are allowed. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Connection Handler is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

listen-address

| | |
|---|---|
| *Synopsis* | Specifies the address or set of addresses on which this SNMP Connection Handler should listen for connections from SNMP clients. |

| | |
|---|---|
| *Description* | Multiple addresses may be provided as separate values for this attribute. If no values are provided, then the SNMP Connection Handler listens on all interfaces. |
| *Default Value* | 0.0.0.0 |
| *Allowed Values* | A hostname or an IP address. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | Restart the server for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | Yes |

listen-port

| | |
|---|---|
| *Synopsis* | Specifies the port number on which the SNMP Connection Handler will listen for connections from clients. |
| *Description* | Only a single port number may be provided. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br>Lower limit: 1.<br>Upper limit: 65535. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

registered-mbean

| | |
|---|---|
| *Synopsis* | Indicates whether the SNMP objects have to be registered in the directory server MBeanServer or not allowing to access SNMP Objects with RMI connector if enabled. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

restricted-client

| | |
|---|---|
| *Synopsis* | A set of clients who will be limited to the maximum number of connections specified by the "restricted-client-connection-limit" property. |
| *Description* | Valid values include a host name, a fully qualified domain name, a domain name, an IP address, or a subnetwork with subnetwork mask. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | No restrictions are imposed on the number of connections a client can open. |
| *Allowed Values* | An IP address mask. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

restricted-client-connection-limit

| | |
|---|---|
| *Synopsis* | Specifies the maximum number of connections a restricted client can open at the same time to this Connection Handler. |
| *Description* | Once Directory Server accepts the specified number of connections from a client specified in restricted-client, any additional connection will be rejected. The number of connections is maintained by IP address. Specifying a value for this property in a connection handler will override any value set in the global configuration. |
| *Default Value* | 100 |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately and do not interfere with established connections. |
| *Advanced* | No |
| *Read-Only* | No |

security-agent-file

| | |
|---|---|
| *Synopsis* | Specifies the USM security configuration to receive authenticated only SNMP requests. |
| *Default Value* | config/snmp/security/opendj-snmp.security |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

security-level

| | |
|---|---|
| *Synopsis* | Specifies the type of security level : NoAuthNoPriv : No security mechanisms activated, AuthNoPriv : Authentication activated with no privacy, AuthPriv : Authentication with privacy activated. This property is required for SNMP V3 security configuration. |
| *Default Value* | authnopriv |
| *Allowed Values* | authnopriv: Authentication activated with no privacy.<br><br>authpriv: Authentication with privacy activated.<br><br>noauthnopriv: No security mechanisms activated. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

trap-port

| | |
|---|---|
| *Synopsis* | Specifies the port to use to send SNMP Traps. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

traps-community

| | |
|---|---|
| *Synopsis* | Specifies the community string that must be included in the traps sent to define managers (trap-destinations). This property is used in the context of SNMP v1, v2 and v3. |
| *Default Value* | OpenDJ |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

traps-destination

| | |
|---|---|
| *Synopsis* | Specifies the hosts to which V1 traps will be sent. V1 Traps are sent to every host listed. |
| *Description* | If this list is empty, V1 traps are sent to "localhost". Each host in the list must be identifed by its name or complete IP Addess. |
| *Default Value* | If the list is empty, V1 traps are sent to "localhost". |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the SNMP Connection Handler implementation. |
| *Default Value* | org.opends.server.snmp.SNMPConnectionHandler |

| | |
|---|---|
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.ConnectionHandler |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Soft Reference Entry Cache

The Soft Reference Entry Cache is a directory server entry cache implementation that uses soft references to manage objects to allow them to be freed if the JVM is running low on memory.

## Parent

The Soft Reference Entry Cache object inherits from Entry Cache.

## Soft Reference Entry Cache Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| cache-level<br>enabled<br>exclude-filter<br>include-filter | java-class<br>lock-timeout |

## Basic Properties

cache-level

| | |
|---|---|
| *Synopsis* | Specifies the cache level in the cache order if more than one instance of the cache is configured. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br>Lower limit: 1. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Entry Cache is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

exclude-filter

| | |
|---|---|
| *Synopsis* | The set of filters that define the entries that should be excluded from the cache. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

include-filter

| | |
|---|---|
| *Synopsis* | The set of filters that define the entries that should be included in the cache. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |

| | |
|---|---|
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Soft Reference Entry Cache implementation. |
| *Default Value* | org.opends.server.extensions.SoftReferenceEntryCache |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.EntryCache |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

lock-timeout

| | |
|---|---|
| *Synopsis* | Specifies the length of time in milliseconds to wait while attempting to acquire a read or write lock. |
| *Default Value* | 3000ms |
| *Allowed Values* | Uses *Duration Syntax* .<br>Use "unlimited" or "-1" to indicate no limit.<br>Lower limit: 0 milliseconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

## StartTLS Extended Operation Handler

The StartTLS Extended Operation Handler provides the ability clients to use the StartTLS extended operation to initiate a secure communication channel over an otherwise clear-text LDAP connection.

## Parent

The StartTLS Extended Operation Handler object inherits from Extended Operation Handler.

## StartTLS Extended Operation Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server). |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the StartTLS Extended Operation Handler implementation. |
| *Default Value* | org.opends.server.extensions.StartTLSExtendedOperation |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.ExtendedOperationHandler |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Static Group Implementation

The Static Group Implementation provides a grouping mechanism in which the group membership is based on an explicit list of the DNs of the users that are members of the group.

Note that it is possible to nest static groups by including the DN of a nested group in the member list for the parent group.

## Parent

The Static Group Implementation object inherits from Group Implementation.

## Static Group Implementation Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Group Implementation is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Static Group Implementation implementation. |
| *Default Value* | org.opends.server.extensions.StaticGroup |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.Group |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Static Service Discovery Mechanism

A Static Service Discovery Mechanism returns a fixed list of LDAP directory servers.

A change in configuration to any of the specified directory servers must be manually applied on all Static Service Discovery Mechanisms that reference it.

### Parent

The Static Service Discovery Mechanism object inherits from Service Discovery Mechanism.

### Dependencies

Static Service Discovery Mechanisms depend on the following objects:

- Key Manager Provider
- Trust Manager Provider

### Static Service Discovery Mechanism Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| discovery-interval<br>key-manager-provider<br>primary-server<br>secondary-server<br>ssl-cert-nickname<br>ssl-cipher-suite<br>ssl-protocol<br>trust-manager-provider<br>use-sasl-external<br>use-ssl<br>use-start-tls | java-class |

## Basic Properties

### discovery-interval

| | |
|---|---|
| *Synopsis* | Interval between two server configuration discovery executions. |
| *Description* | Specifies how frequently to read the configuration of the servers in order to discover their new information. |
| *Default Value* | 60s |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 1 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### key-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the key manager that should be used with this Static Service Discovery Mechanism. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Key Manager Provider .<br><br>The referenced key manager provider must be enabled when the Static Service Discovery Mechanism is enabled and configured to use SASL/External certificate authentication. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |

| | |
|---|---|
| | Changes to this property take effect immediately, but only for subsequent attempts to access the key manager provider for associated client connections. |
| *Advanced* | No |
| *Read-Only* | No |

primary-server

| | |
|---|---|
| *Synopsis* | Specifies a list of servers that will be used in preference to secondary servers when available. |
| *Description* | When using an IPv6 address as the hostname, put brackets around the address as in "[IPv6Address]:port". |
| *Default Value* | None |
| *Allowed Values* | A host name or an IP address followed by a ":" and a port number.<br><br>Port number must be greater than 1 and less than 65535. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

secondary-server

| | |
|---|---|
| *Synopsis* | Specifies a list of servers that will be used in place of primary servers when all primary servers are unavailable. |
| *Description* | When using an IPv6 address as the hostname, put brackets around the address as in "[IPv6Address]:port". |
| *Default Value* | None |
| *Allowed Values* | A host name or an IP address followed by a ":" and a port number.<br><br>Port number must be greater than 1 and less than 65535. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cert-nickname

| | |
|---|---|
| *Synopsis* | Specifies the nicknames (also called the aliases) of the keys or key pairs that the Static Service Discovery Mechanism should use when performing SSL communication. |

| | |
|---|---|
| *Description* | The property can be used multiple times (referencing different nicknames) when server certificates with different public key algorithms are used in parallel (for example, RSA, DSA, and ECC-based algorithms). When a nickname refers to an asymmetric (public/private) key pair, the nickname for the public key certificate and associated private key entry must match exactly. A single nickname is used to retrieve both the public key and the private key. This is only applicable when the Static Service Discovery Mechanism is configured to use SSL. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-cipher-suite

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL cipher suites that are allowed for use in SSL or TLS communication. |
| *Default Value* | Uses the default set of SSL cipher suites provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change. |
| *Advanced* | No |
| *Read-Only* | No |

ssl-protocol

| | |
|---|---|
| *Synopsis* | Specifies the names of the SSL protocols that are allowed for use in SSL or TLS communication. |
| *Default Value* | Uses the default set of SSL protocols provided by the server's JVM. |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately but only impact new SSL/TLS-based sessions created after the change. |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

trust-manager-provider

| | |
|---|---|
| *Synopsis* | Specifies the name of the trust manager that should be used with the Static Service Discovery Mechanism. |
| *Default Value* | None |
| *Allowed Values* | The name of an existing Trust Manager Provider .<br><br>The referenced trust manager provider must be enabled when this Static Service Discovery Mechanism is configured to use SSL or StartTLS. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None<br><br>Changes to this property take effect immediately, but only for subsequent attempts to access the trust manager provider for associated client connections. |
| *Advanced* | No |
| *Read-Only* | No |

use-sasl-external

| | |
|---|---|
| *Synopsis* | Indicates whether the Static Service Discovery Mechanism should use certificate based authentication when communicating with backend servers. |
| *Description* | If enabled, the Static Service Discovery Mechanism will use mutual TLS when connecting to backend servers. Once the TLS handshake has completed, a SASL/ External LDAP bind request will be sent in order to associate the TLS client certificate with an LDAP account on the remote backend server. A key manager provider containing the client certificate must be configured in order to use this feature. |
| *Default Value* | false |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

use-ssl

| | |
|---|---|
| *Synopsis* | Indicates whether the Static Service Discovery Mechanism should use SSL. |
| *Description* | If enabled, the Static Service Discovery Mechanism will use SSL to encrypt communication with the clients. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

use-start-tls

| | |
|---|---|
| *Synopsis* | Indicates whether the Static Service Discovery Mechanism should use Start TLS. |
| *Description* | If enabled, the Static Service Discovery Mechanism will use Start TLS to encrypt communication with remote servers. |
| *Default Value* | false |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Static Service Discovery Mechanism implementation. |
| *Default Value* | org.opends.server.discovery.StaticServiceDiscoveryMechanism |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.discovery.ServiceDiscoveryMechanism |

| | |
|---|---|
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Structural Object Class Virtual Attribute

The Structural Object Class Virtual Attribute generates a virtual attribute that specifies the structural object class with the schema definitions in effect for the entry. This attribute is defined in RFC 4512.

## Parent

The Structural Object Class Virtual Attribute object inherits from Virtual Attribute.

## Structural Object Class Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>enabled<br>filter<br>group-dn<br>scope | conflict-behavior<br>java-class |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | structuralObjectClass |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |

| | |
|---|---|
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br><br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | virtual-overrides-real |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.<br><br>real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | org.opends.server.extensions.StructuralObjectClassVirtualAttributeProvider |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Subject Attribute To User Attribute Certificate Mapper

The Subject Attribute To User Attribute Certificate Mapper maps client certificates to user entries by mapping the values of attributes contained in the certificate subject to attributes contained in user entries.

## Parent

The Subject Attribute To User Attribute Certificate Mapper object inherits from Certificate Mapper.

## Subject Attribute To User Attribute Certificate Mapper Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>issuer-attribute<br>subject-attribute-mapping<br>user-base-dn | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Certificate Mapper is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

issuer-attribute

| | |
|---|---|
| *Synopsis* | Specifies the name or OID of the attribute whose value should exactly match the certificate issuer DN. |
| *Description* | Certificate issuer verification should be enabled whenever multiple CAs are trusted in order to prevent impersonation. In particular, it is possible for different CAs to issue certificates having the same subject DN. |
| *Default Value* | The certificate issuer DN will not be verified. |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | No |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

subject-attribute-mapping

| | |
|---|---|
| *Synopsis* | Specifies a mapping between certificate attributes and user attributes. |
| *Description* | Each value should be in the form "certattr:userattr" where certattr is the name of the attribute in the certificate subject and userattr is the name of the corresponding attribute in user entries. There may be multiple mappings defined, and when performing the mapping values for all attributes present in the certificate subject that have mappings defined must be present in the corresponding user entries. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

user-base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry. |
| *Default Value* | The server will perform the search in all public naming contexts. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Subject Attribute To User Attribute Certificate Mapper implementation. |

| | |
|---|---|
| *Default Value* | org.opends.server.extensions.SubjectAttributeToUserAttributeCertificateMapper |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.CertificateMapper |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Subject DN To User Attribute Certificate Mapper

The Subject DN To User Attribute Certificate Mapper maps client certificates to user entries by looking for the certificate subject DN in a specified attribute of user entries.

## Parent

The Subject DN To User Attribute Certificate Mapper object inherits from Certificate Mapper.

## Subject DN To User Attribute Certificate Mapper Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>issuer-attribute<br>subject-attribute<br>user-base-dn | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Certificate Mapper is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

issuer-attribute

| | |
|---|---|
| *Synopsis* | Specifies the name or OID of the attribute whose value should exactly match the certificate issuer DN. |
| *Description* | Certificate issuer verification should be enabled whenever multiple CAs are trusted in order to prevent impersonation. In particular, it is possible for different CAs to issue certificates having the same subject DN. |
| *Default Value* | The certificate issuer DN will not be verified. |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

subject-attribute

| | |
|---|---|
| *Synopsis* | Specifies the name or OID of the attribute whose value should exactly match the certificate subject DN. |
| *Default Value* | None |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

user-base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs that should be used when performing searches to map the client certificate to a user entry. |
| *Default Value* | The server will perform the search in all public naming contexts. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Subject DN To User Attribute Certificate Mapper implementation. |
| *Default Value* | org.opends.server.extensions.SubjectDNToUserAttributeCertificateMapper |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.CertificateMapper |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Subject Equals DN Certificate Mapper

The Subject Equals DN Certificate Mapper maps client certificates to user entries based on the assumption that the certificate subject is the same as the DN of the target user entry.

### Parent

The Subject Equals DN Certificate Mapper object inherits from Certificate Mapper.

### Subject Equals DN Certificate Mapper Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled<br>issuer-attribute | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Certificate Mapper is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

issuer-attribute

| | |
|---|---|
| *Synopsis* | Specifies the name or OID of the attribute whose value should exactly match the certificate issuer DN. |
| *Description* | Certificate issuer verification should be enabled whenever multiple CAs are trusted in order to prevent impersonation. In particular, it is possible for different CAs to issue certificates having the same subject DN. |
| *Default Value* | The certificate issuer DN will not be verified. |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Subject Equals DN Certificate Mapper implementation. |
| *Default Value* | org.opends.server.extensions.SubjectEqualsDNCertificateMapper |
| *Allowed Values* | A Java class that extends or implements: |

| | |
|---|---|
| | • org.opends.server.api.CertificateMapper |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Subschema Subentry Virtual Attribute

The Subschema Subentry Virtual Attribute generates a virtual attribute that specifies the location of the subschemaSubentry with the schema definitions in effect for the entry. This attribute is defined in RFC 4512.

## Parent

The Subschema Subentry Virtual Attribute object inherits from Virtual Attribute.

## Subschema Subentry Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>enabled<br>filter<br>group-dn<br>scope | conflict-behavior<br>java-class |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | subschemaSubentry |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |

| | |
|---|---|
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br><br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | virtual-overrides-real |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.<br><br>real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | org.opends.server.extensions.SubschemaSubentryVirtualAttributeProvider |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Synchronization Provider

*This is an abstract object type that cannot be instantiated.*

Synchronization Providers are responsible for handling synchronization of the directory server data with other OpenDJ instances or other data repositories.

The OpenDJ directory server takes a centralized approach to replication, rather than the point-to-point approach taken by Sun Java System Directory Server. In OpenDJ, one or more replication servers are created in the environment. The replication servers typically do not store user data but keep a log of all changes made within the topology. Each directory server instance in the topology is pointed at the replication servers. This plan simplifies the deployment and management of the environment. Although you can run the replication server on the same system (or even in the same instance) as the directory server, the two servers can be separated onto different systems. This approach can provide better performance or functionality in large environments.

## Synchronization Providers

The following Synchronization Providers are available:

- Replication Synchronization Provider

These Synchronization Providers inherit the properties described below.

## Synchronization Provider Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| enabled<br>java-class |

## Basic Properties

enabled

| | |
| --- | --- |
| *Synopsis* | Indicates whether the Synchronization Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Synchronization Provider implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.SynchronizationProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Task Backend

The Task Backend provides a mechanism for scheduling tasks in the OpenDJ directory server. Tasks are intended to provide access to certain types of administrative functions in the server that may not be convenient to perform remotely.

OpenDJ supports tasks to backup and restore backends, to import and export LDIF files, and to stop and restart the server. The details of a task are in an entry that is below the root of the Task Backend. The Task Backend is responsible for decoding that task entry and ensuring that it is processed as requested. Tasks may be invoked immediately, but they may also be scheduled for execution at some future time. The task backend can also process recurring tasks to ensure that maintenance operations (for example, backups) are performed automatically on a regular basis.

## Parent

The Task Backend object inherits from Local Backend.

## Task Backend Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| backend-id<br>enabled<br>notification-sender-address<br>task-backing-file<br>task-retention-time | java-class |

| Basic Properties | Advanced Properties |
|---|---|
| writability-mode | |

## Basic Properties

### backend-id

| | |
|---|---|
| *Synopsis* | Specifies a name to identify the associated backend. |
| *Description* | The name must be unique among all backends in the server. The backend ID may not be altered after the backend is created in the server. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | Yes |

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the backend is enabled in the server. |
| *Description* | If a backend is not enabled, then its contents are not accessible when processing operations. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### notification-sender-address

| | |
|---|---|
| *Synopsis* | Specifies the email address to use as the sender (that is, the "From:" address) address for notification mail messages generated when a task completes execution. |
| *Default Value* | The default sender address used is "opendj-task-notification@" followed by the canonical address of the system on which the server is running. |

| | |
|---|---|
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

task-backing-file

| | |
|---|---|
| *Synopsis* | Specifies the path to the backing file for storing information about the tasks configured in the server. |
| *Description* | It may be either an absolute path or a relative path to the base of the OpenDJ directory server instance. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

task-retention-time

| | |
|---|---|
| *Synopsis* | Specifies the length of time that task entries should be retained after processing on the associated task has been completed. |
| *Default Value* | 24 hours |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 0 seconds. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

writability-mode

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the backend should use when processing write operations. |

| | |
|---|---|
| *Default Value* | enabled |
| *Allowed Values* | disabled: Causes all write attempts to fail.<br><br>enabled: Allows write operations to be performed in that backend (if the requested operation is valid, the user has permission to perform the operation, the backend supports that type of write operation, and the global writability-mode property is also enabled).<br><br>internal-only: Causes external write attempts to fail but allows writes by replication and internal operations. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the backend implementation. |
| *Default Value* | org.opends.server.backends.task.TaskBackend |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.Backend |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Time Limit Log Rotation Policy

Rotation policy based on the time since last rotation.

### Parent

The Time Limit Log Rotation Policy object inherits from Log Rotation Policy.

# Time Limit Log Rotation Policy Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| rotation-interval | java-class |

## Basic Properties

rotation-interval

| | |
|---|---|
| *Synopsis* | Specifies the time interval between rotations. |
| *Default Value* | None |
| *Allowed Values* | Uses *Duration Syntax* .<br><br>Lower limit: 1 milliseconds. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Time Limit Log Rotation Policy implementation. |
| *Default Value* | org.opends.server.loggers.TimeLimitRotationPolicy |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.loggers.RotationPolicy |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |

| | |
|---|---|
| *Read-Only* | No |

# Traditional Work Queue

The Traditional Work Queue is a type of work queue that uses a number of worker threads that watch a queue and pick up an operation to process whenever one becomes available.

The traditional work queue is a FIFO queue serviced by a fixed number of worker threads. This fixed number of threads can be changed on the fly, with the change taking effect as soon as it is made. You can limit the size of the work queue to a specified number of operations. When this many operations are in the queue, waiting to be picked up by threads, any new requests are rejected with an error message.

## Parent

The Traditional Work Queue object inherits from Work Queue.

## Traditional Work Queue Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| num-worker-threads | java-class |

## Basic Properties

num-worker-threads

| | |
|---|---|
| *Synopsis* | Specifies the number of worker threads to be used for processing operations placed in the queue. |
| *Description* | If the value is increased, the additional worker threads are created immediately. If the value is reduced, the appropriate number of threads are destroyed as operations complete processing. |
| *Default Value* | Let the server decide. |
| *Allowed Values* | An integer.<br><br>Lower limit: 1.<br><br>Upper limit: 2147483647. |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Traditional Work Queue implementation. |
| *Default Value* | org.opends.server.extensions.TraditionalWorkQueue |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.WorkQueue |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | Restart the server for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

## Triple-DES Password Storage Scheme

The Triple-DES Password Storage Scheme provides a mechanism for encoding user passwords using the triple-DES (DES/EDE) reversible encryption mechanism.

This scheme contains only an implementation for the user password syntax, with a storage scheme name of "3DES".

### Parent

The Triple-DES Password Storage Scheme object inherits from Password Storage Scheme.

### Triple-DES Password Storage Scheme Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Password Storage Scheme is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Triple-DES Password Storage Scheme implementation. |
| *Default Value* | org.opends.server.extensions.TripleDESPasswordStorageScheme |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.PasswordStorageScheme |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

# Trust Manager Provider

*This is an abstract object type that cannot be instantiated.*

Trust Manager Providers determine whether to trust presented certificates.

## Trust Manager Providers

The following Trust Manager Providers are available:

- cn=admin data Trust Manager Provider
- Blind Trust Manager Provider
- File Based Trust Manager Provider
- LDAP Trust Manager Provider
- PKCS#11 Trust Manager Provider

These Trust Manager Providers inherit the properties described below.

## Dependencies

The following objects depend on Trust Manager Providers:

- Administration Connector
- HTTP Connection Handler
- HTTP OAuth2 OpenAM Authorization Mechanism
- HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism
- LDAP Connection Handler
- LDAP Pass Through Authentication Policy
- Mail Server
- Replication Service Discovery Mechanism
- Replication Synchronization Provider
- Static Service Discovery Mechanism

## Trust Manager Provider Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
| --- |
| enabled<br>java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicate whether the Trust Manager Provider is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | The fully-qualified name of the Java class that provides the Trust Manager Provider implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.TrustManagerProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Unique Attribute Plugin

The Unique Attribute Plugin enforces constraints on the value of an attribute within a portion of the directory.

The values for each attribute must be unique within each base DN specified in the plugin's base-dn property or within all of the server's public naming contexts if no base DNs were specified.

## Parent

The Unique Attribute Plugin object inherits from Plugin.

# Unique Attribute Plugin Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| base-dn<br>enabled<br>type | invoke-for-internal-operations<br>java-class<br>plugin-type |

## Basic Properties

### base-dn

| | |
|---|---|
| *Synopsis* | Specifies a base DN within which the attribute must be unique. |
| *Default Value* | The plug-in uses the server's public naming contexts in the searches. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

### type

| | |
|---|---|
| *Synopsis* | Specifies the attribute types to check for value uniqueness. Each attribute value must be unique for all specified attribute types. For example, if both uid and cn |

| | |
|---|---|
| | types are specified, then each uid and cn value must be unique for all uid and cn attributes under the specified base DN(s). |
| *Default Value* | None |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

invoke-for-internal-operations

| | |
|---|---|
| *Synopsis* | Indicates whether the plug-in should be invoked for internal operations. |
| *Description* | Any plug-in that can be invoked for internal operations must ensure that it does not create any new internal operatons that can cause the same plug-in to be re-invoked. |
| *Default Value* | true |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | Yes |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the plug-in implementation. |
| *Default Value* | org.opends.server.plugins.UniqueAttributePlugin |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.plugin.DirectoryServerPlugin |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | Yes |
| *Read-Only* | No |

plugin-type

| | |
|---|---|
| *Synopsis* | Specifies the set of plug-in types for the plug-in, which specifies the times at which the plug-in is invoked. |
| *Default Value* | preoperationadd<br>preoperationmodify<br>preoperationmodifydn<br>postoperationadd<br>postoperationmodify<br>postoperationmodifydn<br>postsynchronizationadd<br>postsynchronizationmodify<br>postsynchronizationmodifydn |
| *Allowed Values* | initialization: Invoked at the initialization of the directory server.<br>intermediateresponse: Invoked before sending an intermediate repsonse message to the client.<br>ldifimport: Invoked for each entry read during an LDIF import.<br>ldifimportbegin: Invoked at the beginning of an LDIF import session.<br>ldifimportend: Invoked at the end of an LDIF import session.<br>postconnect: Invoked whenever a new connection is established to the server.<br>postdisconnect: Invoked whenever an existing connection is terminated (by either the client or the server).<br>postoperationabandon: Invoked after completing the abandon processing.<br>postoperationadd: Invoked after completing the core add processing but before sending the response to the client.<br>postoperationbind: Invoked after completing the core bind processing but before sending the response to the client.<br>postoperationcompare: Invoked after completing the core compare processing but before sending the response to the client.<br>postoperationdelete: Invoked after completing the core delete processing but before sending the response to the client. |

postoperationextended: Invoked after completing the core extended processing but before sending the response to the client.

postoperationmodify: Invoked after completing the core modify processing but before sending the response to the client.

postoperationmodifydn: Invoked after completing the core modify DN processing but before sending the response to the client.

postoperationsearch: Invoked after completing the core search processing but before sending the response to the client.

postoperationunbind: Invoked after completing the unbind processing.

postresponseadd: Invoked after sending the add response to the client.

postresponsebind: Invoked after sending the bind response to the client.

postresponsecompare: Invoked after sending the compare response to the client.

postresponsedelete: Invoked after sending the delete response to the client.

postresponseextended: Invoked after sending the extended response to the client.

postresponsemodify: Invoked after sending the modify response to the client.

postresponsemodifydn: Invoked after sending the modify DN response to the client.

postresponsesearch: Invoked after sending the search result done message to the client.

postsynchronizationadd: Invoked after completing post-synchronization processing for an add operation.

postsynchronizationdelete: Invoked after completing post-synchronization processing for a delete operation.

postsynchronizationmodify: Invoked after completing post-synchronization processing for a modify operation.

postsynchronizationmodifydn: Invoked after completing post-synchronization processing for a modify DN operation.

preoperationadd: Invoked prior to performing the core add processing.

preoperationbind: Invoked prior to performing the core bind processing.

preoperationcompare: Invoked prior to performing the core compare processing.

preoperationdelete: Invoked prior to performing the core delete processing.

preoperationextended: Invoked prior to performing the core extended processing.

preoperationmodify: Invoked prior to performing the core modify processing.

| | |
|---|---|
| | preoperationmodifydn: Invoked prior to performing the core modify DN processing.<br><br>preoperationsearch: Invoked prior to performing the core search processing.<br><br>preparseabandon: Invoked prior to parsing an abandon request.<br><br>preparseadd: Invoked prior to parsing an add request.<br><br>preparsebind: Invoked prior to parsing a bind request.<br><br>preparsecompare: Invoked prior to parsing a compare request.<br><br>preparsedelete: Invoked prior to parsing a delete request.<br><br>preparseextended: Invoked prior to parsing an extended request.<br><br>preparsemodify: Invoked prior to parsing a modify request.<br><br>preparsemodifydn: Invoked prior to parsing a modify DN request.<br><br>preparsesearch: Invoked prior to parsing a search request.<br><br>preparseunbind: Invoked prior to parsing an unbind request.<br><br>searchresultentry: Invoked before sending a search result entry to the client.<br><br>searchresultreference: Invoked before sending a search result reference to the client.<br><br>shutdown: Invoked during a graceful directory server shutdown.<br><br>startup: Invoked during the directory server startup process.<br><br>subordinatedelete: Invoked in the course of deleting a subordinate entry of a delete operation.<br><br>subordinatemodifydn: Invoked in the course of moving or renaming an entry subordinate to the target of a modify DN operation. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Unique Characters Password Validator

The Unique Characters Password Validator is used to determine whether a proposed password is acceptable based on the number of unique characters that it contains.

This validator can be used to prevent simple passwords that contain only a few characters like "aabbcc" or "abcabc".

## Parent

The Unique Characters Password Validator object inherits from Password Validator.

## Unique Characters Password Validator Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| case-sensitive-validation<br>enabled<br>min-unique-characters | java-class |

## Basic Properties

case-sensitive-validation

| | |
|---|---|
| *Synopsis* | Indicates whether this password validator should treat password characters in a case-sensitive manner. |
| *Description* | A value of true indicates that the validator does not consider a capital letter to be the same as its lower-case counterpart. A value of false indicates that the validator ignores differences in capitalization when looking at the number of unique characters in the password. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the password validator is enabled for use. |
| *Default Value* | None |

| | |
|---|---|
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

min-unique-characters

| | |
|---|---|
| *Synopsis* | Specifies the minimum number of unique characters that a password will be allowed to contain. |
| *Description* | A value of zero indicates that no minimum value is enforced. |
| *Default Value* | None |
| *Allowed Values* | An integer.<br><br>Lower limit: 0. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the password validator implementation. |
| *Default Value* | org.opends.server.extensions.UniqueCharactersPasswordValidator |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.PasswordValidator |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |

| | |
|---|---|
| *Read-Only* | No |

# User Defined Virtual Attribute

The User Defined Virtual Attribute creates virtual attributes with user-defined values in entries that match the criteria defined in the plug-in's configuration.

The functionality of these attributes is similar to Class of Service (CoS) in the Sun Java System Directory Server.

## Parent

The User Defined Virtual Attribute object inherits from Virtual Attribute.

## User Defined Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| attribute-type<br>base-dn<br>conflict-behavior<br>enabled<br>filter<br>group-dn<br>scope<br>value | java-class |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | None |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |

| | |
|---|---|
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | real-overrides-virtual |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.<br><br>real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |

| | |
|---|---|
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

value

| | |
|---|---|
| *Synopsis* | Specifies the values to be included in the virtual attribute. |
| *Default Value* | None |
| *Allowed Values* | A string. |
| *Multi-valued* | Yes |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | org.opends.server.extensions.UserDefinedVirtualAttributeProvider |

| | |
|---|---|
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Virtual Attribute

*This is an abstract object type that cannot be instantiated.*

Virtual Attributes are responsible for dynamically generating attribute values that appear in entries but are not persistently stored in the backend.

Virtual attributes are associated with a virtual attribute provider, which contains the logic for generating the value.

## Virtual Attributes

The following Virtual Attributes are available:

- Collective Attribute Subentries Virtual Attribute
- Entity Tag Virtual Attribute
- entryDN Virtual Attribute
- entryUUID Virtual Attribute
- Governing Structure Rule Virtual Attribute
- Has Subordinates Virtual Attribute
- Is Member Of Virtual Attribute
- Member Virtual Attribute
- Num Subordinates Virtual Attribute
- Password Expiration Time Virtual Attribute
- Password Policy Subentry Virtual Attribute

- Structural Object Class Virtual Attribute
- Subschema Subentry Virtual Attribute
- User Defined Virtual Attribute

These Virtual Attributes inherit the properties described below.

## Virtual Attribute Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| attribute-type<br>base-dn<br>conflict-behavior<br>enabled<br>filter<br>group-dn<br>java-class<br>scope |

## Basic Properties

attribute-type

| | |
|---|---|
| *Synopsis* | Specifies the attribute type for the attribute whose values are to be dynamically assigned by the virtual attribute. |
| *Default Value* | None |
| *Allowed Values* | The name of an attribute type defined in the LDAP schema. |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

base-dn

| | |
|---|---|
| *Synopsis* | Specifies the base DNs for the branches containing entries that are eligible to use this virtual attribute. |
| *Description* | If no values are given, then the server generates virtual attributes anywhere in the server. |

| | |
|---|---|
| *Default Value* | The location of the entry in the server is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

conflict-behavior

| | |
|---|---|
| *Synopsis* | Specifies the behavior that the server is to exhibit for entries that already contain one or more real values for the associated attribute. |
| *Default Value* | real-overrides-virtual |
| *Allowed Values* | merge-real-and-virtual: Indicates that the virtual attribute provider is to preserve any real values contained in the entry and merge them with the set of generated virtual values so that both the real and virtual values are used.<br><br>real-overrides-virtual: Indicates that any real values contained in the entry are preserved and used, and virtual values are not generated.<br><br>virtual-overrides-real: Indicates that the virtual attribute provider suppresses any real values contained in the entry and generates virtual values and uses them. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Virtual Attribute is enabled for use. |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

filter

| | |
|---|---|
| *Synopsis* | Specifies the search filters to be applied against entries to determine if the virtual attribute is to be generated for those entries. |
| *Description* | If no values are given, then any entry is eligible to have the value generated. If one or more filters are specified, then only entries that match at least one of those filters are allowed to have the virtual attribute. |
| *Default Value* | (objectClass=*) |
| *Allowed Values* | Any valid search filter string. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

group-dn

| | |
|---|---|
| *Synopsis* | Specifies the DNs of the groups whose members can be eligible to use this virtual attribute. |
| *Description* | If no values are given, then group membership is not taken into account when generating the virtual attribute. If one or more group DNs are specified, then only members of those groups are allowed to have the virtual attribute. |
| *Default Value* | Group membership is not taken into account when determining whether an entry is eligible to use this virtual attribute. |
| *Allowed Values* | A valid DN. |
| *Multi-valued* | Yes |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the virtual attribute provider class that generates the attribute values. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.VirtualAttributeProvider |
| *Multi-valued* | No |
| *Required* | Yes |

| | |
|---|---|
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

scope

| | |
|---|---|
| *Synopsis* | Specifies the LDAP scope associated with base DNs for entries that are eligible to use this virtual attribute. |
| *Default Value* | whole-subtree |
| *Allowed Values* | base-object: Search the base object only.<br><br>single-level: Search the immediate children of the base object but do not include any of their descendants or the base object itself.<br><br>subordinate-subtree: Search the entire subtree below the base object but do not include the base object itself.<br><br>whole-subtree: Search the base object and the entire subtree below the base object. |
| *Multi-valued* | No |
| *Required* | No |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

# Virtual Static Group Implementation

The Virtual Static Group Implementation provides a grouping mechanism in which the membership for the virtual static group is based on the membership for another group defined within the server.

The primary benefit of virtual static groups is that they make it possible to present other types of groups (for example, dynamic groups) as if they were static groups for the benefit of applications that do not support alternate grouping mechanisms.

## Parent

The Virtual Static Group Implementation object inherits from Group Implementation.

## Virtual Static Group Implementation Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Group Implementation is enabled. |
| *Default Value* | None |
| *Allowed Values* | true<br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Virtual Static Group Implementation implementation. |
| *Default Value* | org.opends.server.extensions.VirtualStaticGroup |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.Group |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Who Am I Extended Operation Handler

The Who Am I Extended Operation Handler provides the ability for clients to request their authorization identity using the "Who Am I?" extended operation as defined in RFC 4532.

## Parent

The Who Am I Extended Operation Handler object inherits from Extended Operation Handler.

## Who Am I Extended Operation Handler Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| Basic Properties | Advanced Properties |
|---|---|
| enabled | java-class |

## Basic Properties

enabled

| | |
|---|---|
| *Synopsis* | Indicates whether the Extended Operation Handler is enabled (that is, whether the types of extended operations are allowed in the server). |
| *Default Value* | None |
| *Allowed Values* | true<br><br>false |
| *Multi-valued* | No |
| *Required* | Yes |
| *Admin Action Required* | None |
| *Advanced* | No |
| *Read-Only* | No |

## Advanced Properties

Use the `--advanced` option to access advanced properties.

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Who Am I Extended Operation Handler implementation. |
| *Default Value* | org.opends.server.extensions.WhoAmIExtendedOperation |
| *Allowed Values* | A Java class that extends or implements:<br><br>• org.opends.server.api.ExtendedOperationHandler |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | The object must be disabled and re-enabled for changes to take effect. |
| *Advanced* | Yes |
| *Read-Only* | No |

# Work Queue

*This is an abstract object type that cannot be instantiated.*

The Work Queue provides the configuration for the server work queue and is responsible for ensuring that requests received from clients are processed in a timely manner.

Only a single work queue can be defined in the server. Whenever a connection handler receives a client request, it should place the request in the work queue to be processed appropriately.

## Work Queues

The following Work Queues are available:

- Traditional Work Queue

These Work Queues inherit the properties described below.

## Work Queue Properties

You can use configuration expressions to set property values at startup time. For details, see "*Property Value Substitution*".

| **Basic Properties** |
|---|
| java-class |

## Basic Properties

java-class

| | |
|---|---|
| *Synopsis* | Specifies the fully-qualified name of the Java class that provides the Work Queue implementation. |
| *Default Value* | None |
| *Allowed Values* | A Java class that extends or implements:<br>• org.opends.server.api.WorkQueue |
| *Multi-valued* | No |

| | |
|---|---|
| *Required* | Yes |
| *Admin Action Required* | Restart the server for changes to take effect. |
| *Advanced* | No |
| *Read-Only* | No |

Chapter 3
# Properties

The following sections list **dsconfig** configuration properties by the initial letter in the property name. Follow the links for details.

## A

accept-backlog [HTTP Connection Handler ]

accept-backlog [LDAP Connection Handler ]

access-token-cache-enabled [HTTP OAuth2 Authorization Mechanism ]

access-token-cache-expiration [HTTP OAuth2 Authorization Mechanism ]

access-token-directory [HTTP OAuth2 File Based Authorization Mechanism ]

account-status-notification-handler [Password Policy ]

account-status-notification-type [Error Log Account Status Notification Handler ]

add-missing-rdn-attributes [Global Configuration ]

advertised-listen-address [Administration Connector ]

advertised-listen-address [Global Configuration ]

advertised-listen-address [HTTP Connection Handler ]

advertised-listen-address [LDAP Connection Handler ]

advertised-listen-address [Replication Server ]

allow-attribute-name-exceptions [Global Configuration ]

allow-attribute-types-with-no-sup-or-syntax [Core Schema ]

allow-expired-password-changes [Password Policy ]

allow-ldap-v2 [LDAP Connection Handler ]

allow-multiple-password-values [Password Policy ]

append [File Based HTTP Access Log Publisher ]

asynchronous [CSV File Access Log Publisher ]

asynchronous [CSV File HTTP Access Log Publisher ]

asynchronous [File Based Access Log Publisher ]

asynchronous [File Based Audit Log Publisher ]

asynchronous [File Based Debug Log Publisher ]

asynchronous [File Based Error Log Publisher ]

asynchronous [File Based HTTP Access Log Publisher ]

attribute [Backend Index ]

attribute-type [Collective Attribute Subentries Virtual Attribute ]

attribute-type [Entity Tag Virtual Attribute ]

attribute-type [entryDN Virtual Attribute ]

attribute-type [entryUUID Virtual Attribute ]

attribute-type [Governing Structure Rule Virtual Attribute ]

attribute-type [Has Subordinates Virtual Attribute ]

attribute-type [Is Member Of Virtual Attribute ]

attribute-type [Num Subordinates Virtual Attribute ]

attribute-type [Password Expiration Time Virtual Attribute ]

attribute-type [Password Policy Subentry Virtual Attribute ]

attribute-type [Referential Integrity Plugin ]

attribute-type [Seven Bit Clean Plugin ]

attribute-type [Structural Object Class Virtual Attribute ]

attribute-type [Subschema Subentry Virtual Attribute ]

attribute-type [Virtual Attribute ]

auth-password [Mail Server ]

auth-username [Mail Server ]

# B

# C

case-sensitive-validation [Dictionary Password Validator ]

case-sensitive-validation [Repeated Characters Password Validator ]

case-sensitive-validation [Unique Characters Password Validator ]

certificate-attribute [External SASL Mechanism Handler ]

certificate-mapper [External SASL Mechanism Handler ]

certificate-validation-policy [External SASL Mechanism Handler ]

changelog-enabled [Replication Server ]

changelog-enabled-excluded-domains [Replication Server ]

changetime-heartbeat-interval [Replication Synchronization Provider ]

character-set [Character Set Password Validator ]

character-set-ranges [Character Set Password Validator ]

check-references [Referential Integrity Plugin ]

check-references-filter-criteria [Referential Integrity Plugin ]

check-references-scope-criteria [Referential Integrity Plugin ]

check-schema [Global Configuration ]

check-substrings [Attribute Value Password Validator ]

check-substrings [Dictionary Password Validator ]

checksum-algorithm [Entity Tag Virtual Attribute ]

cipher-key-length [Crypto Manager ]

cipher-key-length [Pluggable Backend ]

cipher-key-length [Replication Server ]

cipher-transformation [Crypto Manager ]

cipher-transformation [Pluggable Backend ]

cipher-transformation [Replication Server ]

client-id [HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism ]

client-secret [HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism ]

community [SNMP Connection Handler ]

compact-encoding [Pluggable Backend ]

confidentiality-enabled [Backend Index ]

confidentiality-enabled [Pluggable Backend ]

confidentiality-enabled [Replication Server ]

config-directory [Rest2LDAP Endpoint ]

config-file [External Access Log Publisher ]

config-file [External HTTP Access Log Publisher ]

conflict-behavior [Collective Attribute Subentries Virtual Attribute ]

conflict-behavior [Entity Tag Virtual Attribute ]

conflict-behavior [entryDN Virtual Attribute ]

conflict-behavior [entryUUID Virtual Attribute ]

conflict-behavior [Governing Structure Rule Virtual Attribute ]

conflict-behavior [Has Subordinates Virtual Attribute ]

conflict-behavior [Is Member Of Virtual Attribute ]

conflict-behavior [Member Virtual Attribute ]

conflict-behavior [Num Subordinates Virtual Attribute ]

conflict-behavior [Password Expiration Time Virtual Attribute ]

conflict-behavior [Password Policy Subentry Virtual Attribute ]

conflict-behavior [Structural Object Class Virtual Attribute ]

conflict-behavior [Subschema Subentry Virtual Attribute ]

conflict-behavior [Virtual Attribute ]

connection-client-address-equal-to [Access Log Filtering Criteria ]

connection-client-address-equal-to [Global Access Control Policy ]

connection-client-address-not-equal-to [Access Log Filtering Criteria ]

connection-client-address-not-equal-to [Global Access Control Policy ]

# D

db-durability [JE Backend ]

db-evictor-core-threads [JE Backend ]

db-evictor-keep-alive [JE Backend ]

db-evictor-max-threads [JE Backend ]

db-log-file-max [JE Backend ]

db-log-filecache-size [JE Backend ]

db-log-verifier-schedule [JE Backend ]

db-logging-file-handler-on [JE Backend ]

db-logging-level [JE Backend ]

db-num-cleaner-threads [JE Backend ]

db-num-lock-tables [JE Backend ]

db-run-cleaner [JE Backend ]

db-run-log-verifier [JE Backend ]

debug-exceptions-only [Debug Target ]

debug-scope [Debug Target ]

default-auth-password-storage-scheme [Password Policy Import Plugin ]

default-debug-exceptions-only [Debug Log Publisher ]

default-include-throwable-cause [Debug Log Publisher ]

default-omit-method-entry-arguments [Debug Log Publisher ]

default-omit-method-return-value [Debug Log Publisher ]

default-password-policy [Global Configuration ]

default-password-storage-scheme [Password Policy ]

default-severity [Error Log Publisher ]

default-throwable-stack-frames [Debug Log Publisher ]

default-user-password-storage-scheme [Password Policy Import Plugin ]

degraded-status-threshold [Replication Server ]

# E

enabled [Backend ]

enabled [Certificate Mapper ]

enabled [Connection Handler ]

enabled [Debug Target ]

enabled [Entry Cache ]

enabled [Extended Operation Handler ]

enabled [Group Implementation ]

enabled [HTTP Authorization Mechanism ]

enabled [HTTP Endpoint ]

enabled [Identity Mapper ]

enabled [Key Manager Provider ]

enabled [Log Publisher ]

enabled [Mail Server ]

enabled [Password Generator ]

enabled [Password Storage Scheme ]

enabled [Password Validator ]

enabled [Plugin ]

enabled [Replication Domain ]

enabled [SASL Mechanism Handler ]

enabled [Schema Provider ]

enabled [Synchronization Provider ]

enabled [Trust Manager Provider ]

enabled [Virtual Attribute ]

enabled-alert-type [Alert Handler ]

entries-compressed [Pluggable Backend ]

etime-resolution [Global Configuration ]

exclude-filter [FIFO Entry Cache ]

## F



## G

# H



# I

# J

java-class [Alert Handler ]

java-class [Alive HTTP endpoint ]

java-class [Anonymous SASL Mechanism Handler ]

java-class [Attribute Cleanup Plugin ]

java-class [Attribute Value Password Validator ]

java-class [Authentication Policy ]

java-class [Backend ]

java-class [Base64 Password Storage Scheme ]

java-class [Bcrypt Password Storage Scheme ]

java-class [Blind Trust Manager Provider ]

java-class [Blowfish Password Storage Scheme ]

java-class [Cancel Extended Operation Handler ]

java-class [Certificate Mapper ]

java-class [Change Number Control Plugin ]

java-class [Character Set Password Validator ]

java-class [Clear Password Storage Scheme ]

java-class [Collective Attribute Subentries Virtual Attribute ]

java-class [Connection Handler ]

java-class [Console Error Log Publisher ]

java-class [Core Schema ]

java-class [CRAM-MD5 SASL Mechanism Handler ]

java-class [Common REST Metrics HTTP Endpoint ]

java-class [Crypt Password Storage Scheme ]

java-class [CSV File Access Log Publisher ]

java-class [CSV File HTTP Access Log Publisher ]

java-class [Debug Log Publisher ]

java-class [Dictionary Password Validator ]

java-class [DIGEST-MD5 SASL Mechanism Handler ]

java-class [DSEE Compatible Access Control Handler ]

java-class [Dynamic Group Implementation ]

java-class [Entity Tag Virtual Attribute ]

java-class [Entry Cache ]

java-class [entryDN Virtual Attribute ]

java-class [entryUUID Plugin ]

java-class [entryUUID Virtual Attribute ]

java-class [Error Log Account Status Notification Handler ]

java-class [Error Log Publisher ]

java-class [Exact Match Identity Mapper ]

java-class [Extended Operation Handler ]

java-class [External Access Log Publisher ]

java-class [External HTTP Access Log Publisher ]

java-class [External SASL Mechanism Handler ]

java-class [FIFO Entry Cache ]

java-class [File Based Access Log Publisher ]

java-class [File Based Audit Log Publisher ]

java-class [File Based Debug Log Publisher ]

java-class [File Based Error Log Publisher ]

java-class [File Based HTTP Access Log Publisher ]

java-class [File Based Key Manager Provider ]

java-class [File Based Trust Manager Provider ]

java-class [File Count Log Retention Policy ]

java-class [Fingerprint Certificate Mapper ]

java-class [Fixed Time Log Rotation Policy ]

java-class [Free Disk Space Log Retention Policy ]

java-class [Get Connection ID Extended Operation Handler ]

java-class [Get Symmetric Key Extended Operation Handler ]

java-class [Governing Structure Rule Virtual Attribute ]

java-class [Graphite Monitor Reporter Plugin ]

java-class [Group Implementation ]

java-class [GSSAPI SASL Mechanism Handler ]

java-class [Has Subordinates Virtual Attribute ]

java-class [Healthy HTTP endpoint ]

java-class [HTTP Access Log Publisher ]

java-class [HTTP Anonymous Authorization Mechanism ]

java-class [HTTP Authorization Mechanism ]

java-class [HTTP Basic Authorization Mechanism ]

java-class [HTTP Connection Handler ]

java-class [HTTP Endpoint ]

java-class [HTTP OAuth2 CTS Authorization Mechanism ]

java-class [HTTP OAuth2 File Based Authorization Mechanism ]

java-class [HTTP OAuth2 OpenAM Authorization Mechanism ]

java-class [HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism ]

java-class [Identity Mapper ]

java-class [Is Member Of Virtual Attribute ]

java-class [JE Backend ]

java-class [JMX Alert Handler ]

java-class [JMX Connection Handler ]

java-class [JSON Equality Matching Rule ]

java-class [JSON File Based Access Log Publisher ]

java-class [JSON File Based HTTP Access Log Publisher ]

java-class [JSON Ordering Matching Rule ]

java-class [JSON Query Equality Matching Rule ]

java-class [Key Manager Provider ]

java-class [Last Mod Plugin ]

java-class [LDAP Attribute Description List Plugin ]

java-class [LDAP Connection Handler ]

java-class [LDAP Key Manager Provider ]

java-class [LDAP Pass Through Authentication Policy ]

java-class [LDAP Trust Manager Provider ]

java-class [LDIF Backend ]

java-class [LDIF Connection Handler ]

java-class [Length Based Password Validator ]

java-class [Log Publisher ]

java-class [Log Retention Policy ]

java-class [Log Rotation Policy ]

java-class [MD5 Password Storage Scheme ]

java-class [Member Virtual Attribute ]

java-class [Memory Backend ]

java-class [Monitor Backend ]

java-class [Null Backend ]

java-class [Num Subordinates Virtual Attribute ]

java-class [Password Expiration Time Virtual Attribute ]

java-class [Password Generator ]

java-class [Password Modify Extended Operation Handler ]

java-class [Password Policy Import Plugin ]

java-class [Password Policy ]

java-class [Password Policy State Extended Operation Handler ]

java-class [Password Policy Subentry Virtual Attribute ]

java-class [Password Storage Scheme ]

java-class [Password Validator ]

java-class [PBKDF2-HMAC-SHA256 Password Storage Scheme ]

java-class [PBKDF2-HMAC-SHA512 Password Storage Scheme ]

java-class [PBKDF2 Password Storage Scheme ]

java-class [PKCS#11 Key Manager Provider ]

java-class [PKCS#11 Trust Manager Provider ]

java-class [PKCS#5 V2.0 Scheme 2 Password Storage Scheme ]

java-class [Plain SASL Mechanism Handler ]

java-class [Plugin ]

java-class [Policy Based Access Control Handler ]

java-class [Prometheus HTTP Endpoint ]

java-class [Proxy Backend ]

java-class [Random Password Generator ]

java-class [RC4 Password Storage Scheme ]

java-class [Referential Integrity Plugin ]

java-class [Regular Expression Identity Mapper ]

java-class [Repeated Characters Password Validator ]

java-class [Replication Service Discovery Mechanism ]

java-class [Replication Synchronization Provider ]

java-class [Rest2LDAP Endpoint ]

java-class [Salted MD5 Password Storage Scheme ]

java-class [Salted SHA-1 Password Storage Scheme ]

java-class [Salted SHA-256 Password Storage Scheme ]

java-class [Salted SHA-384 Password Storage Scheme ]

java-class [Salted SHA-512 Password Storage Scheme ]

java-class [Samba Password Plugin ]

java-class [SASL Mechanism Handler ]

java-class [Schema Backend ]

java-class [Schema Provider ]

java-class [SCRAM-SHA-256 Password Storage Scheme ]

java-class [SCRAM-SHA-256 SASL Mechanism Handler ]

java-class [SCRAM-SHA-512 Password Storage Scheme ]

java-class [SCRAM-SHA-512 SASL Mechanism Handler ]

java-class [Service Discovery Mechanism ]

java-class [Seven Bit Clean Plugin ]

java-class [SHA-1 Password Storage Scheme ]

java-class [Similarity Based Password Validator ]

java-class [Size Limit Log Retention Policy ]

java-class [Size Limit Log Rotation Policy ]

java-class [SMTP Account Status Notification Handler ]

java-class [SMTP Alert Handler ]

java-class [SNMP Connection Handler ]

java-class [Soft Reference Entry Cache ]

java-class [StartTLS Extended Operation Handler ]

java-class [Static Group Implementation ]

java-class [Static Service Discovery Mechanism ]

java-class [Structural Object Class Virtual Attribute ]

java-class [Subject Attribute To User Attribute Certificate Mapper ]

java-class [Subject DN To User Attribute Certificate Mapper ]

java-class [Subject Equals DN Certificate Mapper ]

java-class [Subschema Subentry Virtual Attribute ]

java-class [Synchronization Provider ]

java-class [Task Backend ]

java-class [Time Limit Log Rotation Policy ]

java-class [Traditional Work Queue ]

java-class [Triple-DES Password Storage Scheme ]

java-class [Trust Manager Provider ]

java-class [Unique Attribute Plugin ]

java-class [Unique Characters Password Validator ]

java-class [User Defined Virtual Attribute ]

java-class [Virtual Attribute ]

java-class [Virtual Static Group Implementation ]

java-class [Who Am I Extended Operation Handler ]

java-class [Work Queue ]

je-backend-shared-cache-enabled [Global Configuration ]

je-property [JE Backend ]

json-keys [JSON Equality Matching Rule ]

json-keys [JSON Ordering Matching Rule ]

json-validation-policy [Core Schema ]

# K

kdc-address [GSSAPI SASL Mechanism Handler ]

keep-stats [HTTP Connection Handler ]

keep-stats [LDAP Connection Handler ]

key-manager-provider [Administration Connector ]

key-manager-provider [Crypto Manager ]

key-manager-provider [HTTP Connection Handler ]

key-manager-provider [HTTP OAuth2 OpenAM Authorization Mechanism ]

key-manager-provider [HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism ]

key-manager-provider [JMX Connection Handler ]

key-manager-provider [LDAP Connection Handler ]

key-manager-provider [Proxy Backend ]

key-manager-provider [Replication Service Discovery Mechanism ]

key-manager-provider [Replication Synchronization Provider ]

key-manager-provider [Static Service Discovery Mechanism ]

key-store-file [CSV File Access Log Publisher ]

key-store-file [CSV File HTTP Access Log Publisher ]

key-store-file [File Based Key Manager Provider ]

key-store-pin [CSV File Access Log Publisher ]

key-store-pin [CSV File HTTP Access Log Publisher ]

key-store-pin [File Based Key Manager Provider ]

key-store-pin [LDAP Key Manager Provider ]

key-store-pin [PKCS#11 Key Manager Provider ]

key-store-type [File Based Key Manager Provider ]

key-store-type [PKCS#11 Key Manager Provider ]

key-wrapping-transformation [Crypto Manager ]

keytab [GSSAPI SASL Mechanism Handler ]

# L

last-login-time-attribute [Password Policy ]

log-directory [JSON File Based Access Log Publisher ]

log-directory [JSON File Based HTTP Access Log Publisher ]

log-field-blacklist [CSV File Access Log Publisher ]

log-field-blacklist [CSV File HTTP Access Log Publisher ]

log-field-blacklist [External Access Log Publisher ]

log-field-blacklist [External HTTP Access Log Publisher ]

log-field-blacklist [JSON File Based Access Log Publisher ]

log-field-blacklist [JSON File Based HTTP Access Log Publisher ]

log-field-whitelist [CSV File HTTP Access Log Publisher ]

log-field-whitelist [External HTTP Access Log Publisher ]

log-field-whitelist [JSON File Based HTTP Access Log Publisher ]

log-file [File Based Access Log Publisher ]

log-file [File Based Audit Log Publisher ]

log-file [File Based Debug Log Publisher ]

log-file [File Based Error Log Publisher ]

log-file [File Based HTTP Access Log Publisher ]

log-file [Referential Integrity Plugin ]

log-file-name-prefix [CSV File Access Log Publisher ]

log-file-name-prefix [CSV File HTTP Access Log Publisher ]

log-file-name-prefix [JSON File Based Access Log Publisher ]

log-file-name-prefix [JSON File Based HTTP Access Log Publisher ]

log-file-permissions [File Based Access Log Publisher ]

log-file-permissions [File Based Audit Log Publisher ]

log-file-permissions [File Based Debug Log Publisher ]

log-file-permissions [File Based Error Log Publisher ]

log-file-permissions [File Based HTTP Access Log Publisher ]

# M

matching-rule-oid [JSON Equality Matching Rule ]

matching-rule-oid [JSON Ordering Matching Rule ]

matching-rule-oid [JSON Query Equality Matching Rule ]

max-allowed-client-connections [Global Configuration ]

max-blocked-write-time-limit [HTTP Connection Handler ]

max-blocked-write-time-limit [LDAP Connection Handler ]

max-concurrent-ops-per-connection [HTTP Connection Handler ]

max-consecutive-length [Repeated Characters Password Validator ]

max-entries [FIFO Entry Cache ]

max-internal-buffer-size [Global Configuration ]

max-memory-percent [FIFO Entry Cache ]

max-password-age [Password Policy ]

max-password-length [Length Based Password Validator ]

max-password-reset-age [Password Policy ]

max-psearches [Global Configuration ]

max-replication-delay-health-check [Replication Synchronization Provider ]

max-request-size [HTTP Connection Handler ]

max-request-size [LDAP Connection Handler ]

message-body [SMTP Alert Handler ]

message-subject [SMTP Account Status Notification Handler ]

message-subject [SMTP Alert Handler ]

message-template-file [SMTP Account Status Notification Handler ]

metric-name-prefix [Graphite Monitor Reporter Plugin ]

min-character-sets [Character Set Password Validator ]

min-password-age [Password Policy ]

min-password-difference [Similarity Based Password Validator ]

## N



## O



## P

password-format [Random Password Generator ]

password-generator [Password Policy ]

password-history-count [Password Policy ]

password-history-duration [Password Policy ]

password-validator [Password Policy ]

pbkdf2-iterations [PBKDF2 Password Storage Scheme ]

permission [Global Access Control Policy ]

plugin-order-intermediate-response [Plugin Root ]

plugin-order-ldif-import [Plugin Root ]

plugin-order-ldif-import-begin [Plugin Root ]

plugin-order-ldif-import-end [Plugin Root ]

plugin-order-post-connect [Plugin Root ]

plugin-order-post-disconnect [Plugin Root ]

plugin-order-post-operation-abandon [Plugin Root ]

plugin-order-post-operation-add [Plugin Root ]

plugin-order-post-operation-bind [Plugin Root ]

plugin-order-post-operation-compare [Plugin Root ]

plugin-order-post-operation-delete [Plugin Root ]

plugin-order-post-operation-extended [Plugin Root ]

plugin-order-post-operation-modify [Plugin Root ]

plugin-order-post-operation-modify-dn [Plugin Root ]

plugin-order-post-operation-search [Plugin Root ]

plugin-order-post-operation-unbind [Plugin Root ]

plugin-order-post-response-add [Plugin Root ]

plugin-order-post-response-bind [Plugin Root ]

plugin-order-post-response-compare [Plugin Root ]

plugin-order-post-response-delete [Plugin Root ]

plugin-order-post-response-extended [Plugin Root ]

plugin-order-post-response-modify [Plugin Root ]

plugin-order-post-response-modify-dn [Plugin Root ]

plugin-order-post-response-search [Plugin Root ]

plugin-order-post-synchronization-add [Plugin Root ]

plugin-order-post-synchronization-delete [Plugin Root ]

plugin-order-post-synchronization-modify [Plugin Root ]

plugin-order-post-synchronization-modify-dn [Plugin Root ]

plugin-order-pre-operation-add [Plugin Root ]

plugin-order-pre-operation-bind [Plugin Root ]

plugin-order-pre-operation-compare [Plugin Root ]

plugin-order-pre-operation-delete [Plugin Root ]

plugin-order-pre-operation-extended [Plugin Root ]

plugin-order-pre-operation-modify [Plugin Root ]

plugin-order-pre-operation-modify-dn [Plugin Root ]

plugin-order-pre-operation-search [Plugin Root ]

plugin-order-pre-parse-abandon [Plugin Root ]

plugin-order-pre-parse-add [Plugin Root ]

plugin-order-pre-parse-bind [Plugin Root ]

plugin-order-pre-parse-compare [Plugin Root ]

plugin-order-pre-parse-delete [Plugin Root ]

plugin-order-pre-parse-extended [Plugin Root ]

plugin-order-pre-parse-modify [Plugin Root ]

plugin-order-pre-parse-modify-dn [Plugin Root ]

plugin-order-pre-parse-search [Plugin Root ]

plugin-order-pre-parse-unbind [Plugin Root ]

plugin-order-search-result-entry [Plugin Root ]

plugin-order-search-result-reference [Plugin Root ]

plugin-order-shutdown [Plugin Root ]

plugin-order-startup [Plugin Root ]

plugin-order-subordinate-delete [Plugin Root ]

plugin-order-subordinate-modify-dn [Plugin Root ]

plugin-type [Attribute Cleanup Plugin ]

plugin-type [Change Number Control Plugin ]

plugin-type [entryUUID Plugin ]

plugin-type [Graphite Monitor Reporter Plugin ]

plugin-type [Last Mod Plugin ]

plugin-type [LDAP Attribute Description List Plugin ]

plugin-type [Password Policy Import Plugin ]

plugin-type [Plugin ]

plugin-type [Referential Integrity Plugin ]

plugin-type [Samba Password Plugin ]

plugin-type [Seven Bit Clean Plugin ]

plugin-type [Unique Attribute Plugin ]

poll-interval [LDIF Connection Handler ]

previous-last-login-time-format [Password Policy ]

primary-group-id [Replication Service Discovery Mechanism ]

primary-remote-ldap-server [LDAP Pass Through Authentication Policy ]

primary-server [Static Service Discovery Mechanism ]

principal-name [GSSAPI SASL Mechanism Handler ]

proxied-authorization-identity-mapper [Global Configuration ]

# Q



# R

# S

smtp-property [Mail Server ]

smtp-server [Mail Server ]

solve-conflicts [Replication Synchronization Provider ]

sort-order [Backend VLV Index ]

source-address [LDAP Pass Through Authentication Policy ]

source-address [Replication Synchronization Provider ]

ssl-cert-nickname [Administration Connector ]

ssl-cert-nickname [HTTP Connection Handler ]

ssl-cert-nickname [HTTP OAuth2 OpenAM Authorization Mechanism ]

ssl-cert-nickname [HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism ]

ssl-cert-nickname [JMX Connection Handler ]

ssl-cert-nickname [LDAP Connection Handler ]

ssl-cert-nickname [Proxy Backend ]

ssl-cert-nickname [Replication Service Discovery Mechanism ]

ssl-cert-nickname [Replication Synchronization Provider ]

ssl-cert-nickname [Static Service Discovery Mechanism ]

ssl-cipher-suite [Administration Connector ]

ssl-cipher-suite [HTTP Connection Handler ]

ssl-cipher-suite [HTTP OAuth2 OpenAM Authorization Mechanism ]

ssl-cipher-suite [HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism ]

ssl-cipher-suite [LDAP Connection Handler ]

ssl-cipher-suite [LDAP Pass Through Authentication Policy ]

ssl-cipher-suite [Replication Service Discovery Mechanism ]

ssl-cipher-suite [Replication Synchronization Provider ]

ssl-cipher-suite [Static Service Discovery Mechanism ]

ssl-client-auth-policy [HTTP Connection Handler ]

ssl-client-auth-policy [LDAP Connection Handler ]

# T

tamper-evident [CSV File HTTP Access Log Publisher ]

task-backing-file [Task Backend ]

task-retention-time [Task Backend ]

test-reversed-password [Attribute Value Password Validator ]

test-reversed-password [Dictionary Password Validator ]

throwable-stack-frames [Debug Target ]

time-interval [File Based Access Log Publisher ]

time-interval [File Based Audit Log Publisher ]

time-interval [File Based Debug Log Publisher ]

time-interval [File Based Error Log Publisher ]

time-interval [File Based HTTP Access Log Publisher ]

time-limit [Global Configuration ]

time-of-day [Fixed Time Log Rotation Policy ]

token-info-url [HTTP OAuth2 OpenAM Authorization Mechanism ]

token-introspection-url [HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism ]

trap-port [SNMP Connection Handler ]

traps-community [SNMP Connection Handler ]

traps-destination [SNMP Connection Handler ]

trust-manager-provider [Administration Connector ]

trust-manager-provider [HTTP Connection Handler ]

trust-manager-provider [HTTP OAuth2 OpenAM Authorization Mechanism ]

trust-manager-provider [HTTP OAuth2 Token Introspection (RFC 7662) Authorization Mechanism ]

trust-manager-provider [LDAP Connection Handler ]

trust-manager-provider [LDAP Pass Through Authentication Policy ]

trust-manager-provider [Mail Server ]

trust-manager-provider [Replication Service Discovery Mechanism ]

# U

# V



# W

writability-mode [Global Configuration ]

writability-mode [LDIF Backend ]

writability-mode [Local Backend ]

writability-mode [Memory Backend ]

writability-mode [Monitor Backend ]

writability-mode [Null Backend ]

writability-mode [Pluggable Backend ]

writability-mode [Schema Backend ]

writability-mode [Task Backend ]

Chapter 4

# Duration Syntax

Durations are specified with positive integers and unit specifiers. Unit specifiers include the following:

- `ms`: milliseconds
- `s`: seconds
- `m`: minutes
- `h`: hours
- `d`: days
- `w`: weeks
- `y`: years

A duration of 1 week can be specified as `1w`. A duration of 1 week, 1 day, 1 hour, 1 minute, and 1 second can be specified as `1w1d1h1m1s`.

Whitespace surrounding the value and the unit specifier is not significant. For example, `5d` is equivalent to `5 d`.

Not all properties taking a duration allow all unit specifiers. For example, milliseconds are not allowed if durations smaller than one second are not permitted.

Some properties limit minimum or maximum durations.

An unlimited duration is specified using `unlimited` (recommended for readability) or `-1`.

Chapter 5

# Size Syntax

Sizes are specified with non-negative integers and unit specifiers, which are not case-sensitive. Unit specifiers include the following:

- `b`, `bytes`
- `kb`, `kilobytes` (x1000)
- `kib`, `kibibytes` (x1024)
- `mb`, `megabytes` (x1000x1000)
- `mib`, `mebibytes` (x1024x1024)
- `gb`, `gigabytes` (x1000x1000x1000)
- `gib`, `gibibytes` (x1024x1024x1024)
- `tb`, `terabytes` (x1000x1000x1000x1000)
- `tib`, `tebibytes` (x1024x1024x1024x1024)
- `unlimited`, `-1` (if allowed, explicitly set no upper limit)

For example, you can specify a size of 1,000,000 bytes as `1MB`. To specify a size of 1,048,576 bytes, you can use `1MiB` or `1 mib`.

Whitespace surrounding the value and the unit specifier is not significant. For example, `5gb` is equivalent to ` 5 gb `.

Some properties limit minimum or maximum sizes.

Chapter 6

# Property Value Substitution

Property value substitution enables you to achieve the following:

- Define a configuration that is specific to a single instance. For example, set the location of the keystore on a particular host.
- Define a configuration whose parameters vary between different environments. For example, change hostnames and passwords for test, development, and production environments.
- Disable certain capabilities on specific servers. For example, disable a database backend and its replication agreement for one set of replicas while enabling it on another set of replicas. This makes it possible to use the same configuration for environments with different data sets.

Property value substitution uses *configuration expressions* to introduce variables into the server configuration. You set configuration expressions as the values of configuration properties. The effective property values can be evaluated in a number of ways.

**Note**

DS servers only resolve configuration expressions in the `config/config.ldif` file on LDAP attributes whose names start with `ds-cfg-*`. These correspond to configuration properties listed in this reference.

DS servers do not resolve configuration expressions anywhere else.

DS servers resolve expressions at startup to determine the configuration. DS commands that read the configuration in offline mode also resolve expressions at startup. When you use expressions in the configuration, you must make their values available before starting the server and also when running such commands.

Configuration expressions share their syntax and underlying implementation with other platform software. Configuration expressions have the following characteristics:

- To distinguish them from static values, expression tokens are preceded by an ampersand and enclosed in braces. For example: `&{listen.port}`. The expression token in the example is `listen.port`. The `.` serves as the separator character.
- You can use a default value in an expression by including it after a vertical bar following the token.

  For example, the following expression sets the default listen port value to 1389: `&{listen.port|1389}`.
- A configuration property can include a mix of static values and expressions.

For example, suppose `hostname` is set to `directory`. Then `&{hostname}.example.com` evaluates to `directory.example.com`.

- You can define *nested* properties (that is, a property definition within another property definition).

  For example, suppose `listen.port` is set to `&{port.prefix}389`, and `port.prefix` is set to `2`. Then `&{listen.port}` evaluates to `2389`.

- You can read the value of an expression token from a file.

  For example, if the cleartext password is stored in `/path/to/password.txt`, the following expression resolves to the cleartext password: `&{file:/path/to/password.txt}`.

  You specify the file either by its absolute path, or by a path relative to the DS instance directory. In other words, if the DS instance directory is `/path/to/opendj`, then `/path/to/opendj/config/keystore` and `config/keystore` reference the same file.

DS servers define the following expression tokens by default. You can use these in expressions without explicitly setting their values beforehand:

**`ds.instance.dir`**

The file system directory holding the instance files required to run an instance of a server.

By default, the files are co-located with the product tools, libraries, and configuration files. You can change the location by using the `setup --instancePath` option.

This evaluates to a directory, such as `/path/to/my-instance`.

**`ds.install.dir`**

The file system directory where the server files are installed.

This evaluates to a directory, such as `/path/to/opendj`.

# Expression Evaluation and Order of Precedence

You must define expression values before starting the DS server that uses them. When evaluated, an expression must return the appropriate type for the configuration property. For example, the `listen-port` property takes an integer. If you set it using an expression, the result of the evaluated expression must be an integer. If the type is wrong, the server fails to start due to a syntax error.

If the expression cannot be resolved, and there is no default value in the configuration expression, DS also fails to start.

Expression resolvers evaluate expression tokens to literal values.

Expression resolvers get values from the following sources:

1. **Environment variables**

   You set an environment variable to hold the value.

   For example: `export LISTEN_PORT=1389`.

   The environment variable name must be composed of uppercase characters and underscores. The name maps to the expression token as follows:

   - Uppercase characters are lower cased.
   - Underscores, `_`, are replaced with `.` characters.

   In other words, the value of `LISTEN_PORT` replaces `&{listen.port}` in the server configuration.

2. **Java system properties**

   You set a Java system property to hold the value.

   Java system property names must match expression tokens exactly. In other words, the value of the `listen.port` system property replaces `&{listen.port}` in the server configuration.

   Java system properties can be set in a number of ways. One way of setting system properties for DS servers is to pass them through the `OPENDJ_JAVA_ARGS` environment variable.

   For example: `export OPENDJ_JAVA_ARGS="-Dlisten.port=1389"`

3. **Expressions files (optional)**

   You set a key in a `.json` or `.properties` file to hold the value. This optional mechanism is set using the `DS_ENVCONFIG_DIRS` environment variable, or the `ds.envconfig.dirs` Java system property.

   Keys in `.properties` files must match expression tokens exactly. In other words, the value of the `listen.port` key replaces `&{listen.port}` in the server configuration.

   The following example properties file sets the listen port:

   ```
   listen.port=1389
   ```

   JSON expression files can contain nested objects.

   JSON field names map to expression tokens as follows:

   - The JSON path name matches the expression token.
   - The `.` character serves as the JSON path separator character.

   The following example JSON file sets the listen address and listen port:

```
{
  "listen": {
    "address": "192.168.0.10",
    "port": "1389"
  }
}
```

In other words, the value of the `listen/port` field replaces `&{listen.port}` in the server configuration.

In order to use expression files, set the environment variable, `DS_ENVCONFIG_DIRS`, or the Java system property, `ds.envconfig.dirs`, to a comma-separated list of the directories containing the expression files.

Note the following constraints when using expression files:

- Although DS browses the directories in the specified order, within a directory DS scans the files in a non-deterministic order.
- DS reads all files with `.json` and `.properties` extensions.
- DS does not scan subdirectories.
- Do not define the same configuration token more than once in a file, as you cannot know in advance which value will be used.
- You cannot define the same configuration token in more than one file in a single directory.

  If the same token occurs in more than one file in a single directory, an error occurs.
- If the same token occurs once in several files which are located in different directories, the first value that DS reads is used.

The preceding list reflects the order of precedence:

- Environment variables override system properties, default token settings, and settings in any expression files.
- System properties override default token settings, and any settings in expression files.
- If `DS_ENVCONFIG_DIRS` or `ds.envconfig.dirs` is set, then the server uses settings found in expression files.
- Default token settings (`ds.config.dir`, `ds.instance.dir`, `ds.install.dir`).

For an embedded DS server, it is possible to change the expression resolvers, in the server configuration.

# Using Multivalued Expressions

A single expression token can evaluate to multiple property values. Such expressions are useful with multivalued properties.

For example, suppose you choose to set a connection handler's `ssl-cipher-suite` property. Instead of listing cipher suites individually, you use an `ssl.cipher.suites` token that takes multiple values. The following example commands set the token value in the environment, stop the server, use the expression in the LDAP connection handler configuration while the server is offline, and then start the server again:

```
$ export SSL_CIPHER_SUITES=\
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,\
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,\
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,\
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,\
TLS_EMPTY_RENEGOTIATION_INFO_SCSV
$ stop-ds --quiet
$ dsconfig \
 set-connection-handler-prop \
 --offline \
 --handler-name LDAPS \
 --add ssl-protocol:TLSv1.2 \
 --add ssl-cipher-suite:'&{ssl.cipher.suites}' \
 --no-prompt
$ start-ds --quiet
```

Multiple values are separated by commas in environment variables, system properties, and properties files. They are formatted as arrays in JSON files.

Use one of the following alternatives to set the value of the `ssl.cipher.suites` token. When the server evaluates `&{ssl.cipher.suites}`, the result is the following property values:

```
ssl-cipher-suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ssl-cipher-suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ssl-cipher-suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ssl-cipher-suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ssl-cipher-suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV
```

#### Environment Variable

```
export SSL_CIPHER_SUITES=\
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,\
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,\
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,\
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,\
TLS_EMPTY_RENEGOTIATION_INFO_SCSV
```

#### System Property

```
export OPENDJ_JAVA_ARGS="-Dssl.cipher.suites=\
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,\
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,\
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,\
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,\
TLS_EMPTY_RENEGOTIATION_INFO_SCSV"
```

**Properties File**

```
ssl.cipher.suites=\
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,\
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,\
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,\
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,\
TLS_EMPTY_RENEGOTIATION_INFO_SCSV
```

**JSON File**

```
{
  "ssl.cipher.suites": [
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_EMPTY_RENEGOTIATION_INFO_SCSV"
  ]
}
```

Alternative JSON file that sets `ssl.protocol` as well:

```
{
 "ssl": {
   "protocol": "TLSv1.2",
   "cipher.suites": [
     "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
     "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
     "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
     "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
     "TLS_EMPTY_RENEGOTIATION_INFO_SCSV"
   ]
 }
}
```

In order to fully use the settings in this file, you would have to change the example to include the additional expression: `--add ssl-protocol:'&{ssl.protocol}'`.

# Debugging Expressions

You can debug configuration expressions. Create a debug target for `org.forgerock.config.resolvers`. The following example demonstrates the process:

```
$ dsconfig \
 create-debug-target \
 --hostname localhost \
 --port 4444 \
 --bindDN uid=admin \
 --bindPassword password \
 --publisher-name "File-Based Debug Logger" \
 --type generic \
 --target-name org.forgerock.config.resolvers \
 --set enabled:true \
 --usePkcs12TrustStore /path/to/opendj/config/keystore \
 --trustStorePasswordFile /path/to/opendj/config/keystore.pin \
 --no-prompt
$ dsconfig \
 set-log-publisher-prop \
 --hostname localhost \
 --port 4444 \
 --bindDN uid=admin \
 --bindPassword password \
 --publisher-name "File-Based Debug Logger" \
 --set enabled:true \
 --usePkcs12TrustStore /path/to/opendj/config/keystore \
 --trustStorePasswordFile /path/to/opendj/config/keystore.pin \
 --no-prompt
$ stop-ds --restart --quiet
```

When the server starts, it logs debugging messages for configuration expressions. Do not leave debug logging enabled in production systems.