

Release Notes

ON THIS PAGE

[Release Notes](#)

[What's New](#)

[What's New in Web Agent 5.9.1](#)

[What's New in Web Agent 5.9](#)

[Requirements](#)

[Supported Operating Systems and Web Servers](#)

[AM Requirements](#)

[OpenSSL Requirements](#)

[Other Requirements](#)

[Special Requests](#)

[Incompatible Changes](#)

[Incompatible Changes in Web Agent 5.9.1](#)

[Incompatible Changes in Web Agent 5.9](#)

[Deprecation](#)

[Deprecated Functionality in Web Agent 5.9.1](#)

[Deprecated Functionality in Web Agent 5.9](#)

[Removed](#)

[Removed Functionality in Web Agent 5.9.1](#)

[Removed Functionality in Web Agent 5.9](#)

[Fixes](#)

[Fixes in Web Agent 5.9.1](#)

[Fixes in Web Agent 5.9](#)

[Security advisories](#)

[Limitations](#)

[Limitations in Web Agent 5.9.1](#)

[Limitations in Web Agent 5.9](#)

Known Issues

Known Issues in Web Agent 5.9.1

Known Issues in Web Agent 5.9

Documentation

Appendix A: Release Levels and Interface Stability

ForgeRock product release levels

ForgeRock product stability labels

Getting support

Release Notes



What's New

Discover new features.



Requirements

Check Web Agent prerequisites.



Compatibility

Review incompatible changes.



Fixes

Review bug fixes, limitations, known issues.



Documentation

Track documentation changes.



Support

Get support and training.

ForgeRock® Identity Platform serves as the basis for our simple and comprehensive Identity and Access Management solution. We help our customers deepen their relationships with their customers, and improve the productivity and connectivity of their employees and partners. For more information about ForgeRock and about the platform, see <https://www.forgerock.com>.

The ForgeRock® Common REST API works across the platform to provide common ways to access web resources and collections of resources.

What's New

What's New in Web Agent 5.9.1

Pre-authentication Cookies Are Expired Immediately After Authentication

In previous releases, the pre-authentication cookie, `agent-authn-tx`, expired when it reached the age configured by [Profile Attributes Cookie Maxage](#). From this release, the pre-authentication cookie expires when the first of the following events occur:

- Authentication completes successfully
- It reaches the age configured by [Profile Attributes Cookie Maxage](#)

Expiring the cookie immediately after authentication reduces the amount of used header space, and prevents authentication errors and errors in applications that set headers.

URI Fragments Persisted in Custom Login Mode

When the value of [Enable Custom Login Mode](#) is `2`, URI fragments were previously lost during login. From this release, URI fragments in the browser are not lost after the custom login procedure.

Post Data Preservation: Use a Single Agent Profile for Multiple Agent Instances

In previous releases, to correctly configure post data preservation, a separate agent profile was required in AM for each agent instance. From this release, a single agent profile can be used for multiple agent instance.

Use this feature for scalable deployments, where resources are dynamically created or destroyed.

For more information, see [Create an Agent Profile for Multiple Agent Instances When POST Data Preservation is Enabled](#) and [Map One Agent Profile to Multiple Agent Instances When POST Data Preservation is Enabled](#).

NGINX Plus R25

The NGINX Plus R25 platform is available in this release.

What's New in Web Agent 5.9

Keep Session Cache After Configuration Change

Retain Session Cache After Configuration Change is a new property to stop the agent from purging the session cache each time the agent configuration is changed. Use this property to prevent the agent from flooding AM instances with requests, when the agent configuration changes regularly, and the changes do not affect the agent authorisation decisions.

Profile, Response, and Session Attributes Take Multiple Values

The following properties can now take multiple values:

- Profile Attribute Map
- Response Attribute Map
- Session Attribute Map

In previous releases, they could take only one value.

Reduced Authentication Requests to AM

The agent reads its configuration from AM in the following situations:

- When it connects to AM
- After a configuration change
- When it authenticates with AM

If the AM server is flooded with requests from the agent, it can become unresponsive, causing the agents to stop functioning normally and refuse access.

In previous releases, after a configuration update each request thread retrieved the new configuration, and re-authenticated with AM.

In this release, a single request thread retrieves the new configuration, and re-authenticates with AM only if necessary. Concurrent request threads wait for the time specified by TCP Receive Timeout for the retrieving request thread to complete, and then they use the new configuration.

Requirements

ForgeRock supports customers using the versions specified here. Other versions and alternative environments might work as well. When opening a support ticket for an issue, however, make sure you can also reproduce the problem on a combination covered here.

Supported Operating Systems and Web Servers

Operating Systems	OS Versions	Web Servers & Minimum Supported Versions
<ul style="list-style-type: none"> • Amazon Linux 2 • CentOS • Oracle Linux • Red Hat Enterprise Linux 	<ul style="list-style-type: none"> • 7 • 8 	<ul style="list-style-type: none"> • Apache HTTP Server 2.4 • IBM HTTP Server 9 • NGINX Plus R22⁽¹⁾ • NGINX Plus R23, R24, R25
<ul style="list-style-type: none"> • Ubuntu Linux 	<ul style="list-style-type: none"> • 18.04 LTS • 20.04 LTS 	<ul style="list-style-type: none"> • Apache HTTP Server 2.4 • IBM HTTP Server 9 • NGINX Plus R22⁽¹⁾ • NGINX Plus R23, R24, R25
<ul style="list-style-type: none"> • IBM AIX 	<ul style="list-style-type: none"> • 7 	<ul style="list-style-type: none"> • IBM HTTP Server 9
<ul style="list-style-type: none"> • Microsoft Windows Server 	<ul style="list-style-type: none"> • 2012 R2⁽¹⁾ 	<ul style="list-style-type: none"> • Apache HTTP Server 2.4⁽¹⁾ (2) • Microsoft IIS 8.5⁽¹⁾
	<ul style="list-style-type: none"> • 2016 	<ul style="list-style-type: none"> • Apache HTTP Server 2.4,⁽²⁾ • Microsoft IIS 10
	<ul style="list-style-type: none"> • 2019 	<ul style="list-style-type: none"> • Apache HTTP Server 2.4⁽²⁾ • Microsoft IIS 10

⁽¹⁾Support to be discontinued in a future release.

⁽²⁾The [Apache HTTP Server Project](#) does not offer binary releases for Microsoft Windows. The ForgeRock Apache HTTP Server web agent for Windows was tested against the binaries offered by [Apache Lounge](#)

IMPORTANT

32-bit architectures are not supported.

AM Requirements

- Web Agent 5.9.1 supports AM 6 and later.
- Web Agent 5.9.1 requires the WebSocket protocol to communicate with AM. Both the web server and the network infrastructure must support the WebSocket protocol.

For example, Apache HTTP server requires the `proxy_wstunnel_module` for proxying the WebSocket protocol.

Refer to your network infrastructure and web server documentation for more information about WebSocket support.

- If you are upgrading from a version earlier than 5, Web Agent 5 introduced notable changes in the configuration. For example, if you are using custom login pages, you must enable the `org.forgerock.openam.agents.config.allow.custom.login` property. For more information about changes introduced in Web Agent 5, refer to the Web Agent 5 Release Notes.

OpenSSL Requirements

Agents require OpenSSL or the Windows built-in Secure Channel API to be present. These libraries help to secure communications, for example, when connecting to AM using the WebSocket protocol.

Operating Systems	OpenSSL Versions
<ul style="list-style-type: none">• CentOS• Red Hat Enterprise Linux• Oracle Linux• Ubuntu Linux	<ul style="list-style-type: none">• OpenSSL 1.0.x• OpenSSL 1.1.0• OpenSSL 1.1.1
<ul style="list-style-type: none">• Microsoft Windows Server	<ul style="list-style-type: none">• OpenSSL 1.0.x• OpenSSL 1.1.0• OpenSSL 1.1.1⁽¹⁾
<ul style="list-style-type: none">• IBM AIX	<ul style="list-style-type: none">• OpenSSL 0.9.8• OpenSSL 1.0.x• OpenSSL 1.1.0• OpenSSL 1.1.1

⁽¹⁾On Windows, Web Agent uses the Windows built-in Secure Channel API by default.

- OpenSSL 1.0.2 or later is required to support TLSv1.2. If you have to use an earlier, *weaker* cipher in your environment, configure the `org.forgerock.agents.config.tls.bootstrap` property with a security protocol other than TLSv1.2.
- OpenSSL 1.1.1 or later is required to support TLSv1.3.

Other Requirements

Before installing Web Agent on your platform, make sure that the system meets the following requirements:

Linux Systems

- Web Agent on Linux supports Glibc 2.17 and later versions, and is compatible with Glibc 2.14 and later versions. For Glibc versions before 2.14, contact [ForgeRock Support](#).
- Web Agent on Linux requires a minimum of 16 MB of shared memory for the session and policy cache, and the various worker processes. Additionally, it needs 32 KB shared memory for the logging system. Failure to provide enough shared memory may result in errors similar to the following:

```
2017-11-10 12:06:00.492 +0000  DEBUG [1:7521]
[source/shared.c:1451]am_shm_create2() about to create
block-clusters_0, size 1074008064
2017-11-10 12:06:00.492 +0000  ERROR
[1:7521]am_shm_create2(): ftruncate failed, error: 28
```

To configure additional shared memory for the session and policy cache, see [Environment Variables](#).

- If POST data preservation is enabled, the web agent requires additional free disk space in the web agent installation directory to store the POST data cache files.

Microsoft Windows Systems

- Before installing the IIS web agent, make sure that the optional Application Development component of Web Server (IIS) is installed. In the Windows Server 2012 Server Manager for example, Application Development is a component of Web Server (IIS) | Web Server.
- Web Agent on Windows requires a minimum of 16 MB of shared memory for the session and policy cache, and the various worker processes in the system page file. Additionally, it needs 32 KB shared memory for the logging system. Failure to provide enough shared memory may result in errors similar to the following:

```
2017-11-10 12:06:00.492 +0000    DEBUG [1:7521]
[source/shared.c:1451]am_shm_create2() about to create
block-clusters_0, size 1074008064
2017-11-10 12:06:00.492 +0000    ERROR
[1:7521]am_shm_create2(): ftruncate failed, error: 28
```

To configure additional shared memory for the session and policy cache, see [Environment Variables](#).

- If POST data preservation is enabled, the web agent requires additional free disk space in the web agent installation directory to store the POST data cache files.

Special Requests

If you need support for a combination not listed here, contact ForgeRock at info@forgerock.com.

Incompatible Changes

Incompatible Changes in Web Agent 5.9.1

No incompatible changes were introduced in this release.

Incompatible Changes in Web Agent 5.9

The following changes introduced in this release can impact your migration from Web Agent 5.8:

▼ [AM 5.x.x End-of-Service-Life](#)

AM 5.x.x has reached End-of-Service-Life (EOSL), and no is longer supported.

▼ [Error Logic for Login Time Out in Sessions](#)

The fix for [AMAGENTS-2717](#) changes the error logic that caused 403s to be seen on `agent/cdsso-redirect` or `agent/custom-login-response` when a user is redirected to authenticate, but then stays on the authentication page for longer than the default of 5 minutes.

This error could occur when a user logged out, was redirected for authentication by the agent, and then reopened the same browser the next day. Similarly, it could occur with a similar use case, on a mobile browser application.

Workarounds that were previously recommended, such as using non-default values for [Profile Attributes Cookie Maxage](#), [Enable POST Data Preservation](#), and [POST Data](#)

Entries Cache Period, are no longer necessary or advised.

To prevent problems, remove such workarounds from your configuration. If you have not customized these properties, no change is required.

Deprecation

Deprecation is defined in [Release Levels and Interface Stability](#).

Deprecated Functionality in Web Agent 5.9.1

No additional functionality was deprecated in this release.

Deprecated Functionality in Web Agent 5.9

The following objects are deprecated:

Deprecated In	Object	Description
Web Agent 5.9	Monitoring endpoint	Described in Monitoring
	Disable Keep Alive (deprecated)	Whole object
	Maximum Number of Initialization Retries (deprecated)	Whole object
	Time to Wait Between Initialization Retries (deprecated)	Whole object
	Rotate Local Audit Log (deprecated)	Whole object

Removed

Removed is defined in [Release Levels and Interface Stability](#).

Removed Functionality in Web Agent 5.9.1

No additional functionality was removed in this release.

Removed Functionality in Web Agent 5.9

The following properties have been removed:

- `com.forgerock.agents.accept.ipdp.cookie`
- `com.forgerock.agents.config.pdpuri.prefix`
- `com.forgerock.agents.ext.url.validation.default.url.set`
- `com.forgerock.agents.ext.url.validation.level`
- `com.forgerock.agents.ext.url.validation.ping.interval`
- `com.forgerock.agents.ext.url.validation.ping.miss.count`
- `com.forgerock.agents.ext.url.validation.ping.ok.count`
- `com.forgerock.agents.init.retry.max`
- `com.forgerock.agents.init.retry.wait`
- `com.sun.identity.agents.config.anonymous.user.id`
- `com.sun.identity.agents.config.cdsso.cdcservlet.url`
- `com.sun.identity.agents.config.cdsso.enable`
- `com.sun.identity.agents.config.cleanup.interval`
- `com.sun.identity.agents.config.convert.mbyte.enable`
- `com.sun.identity.agents.config.debug.file.rotate`
- `com.sun.identity.agents.config.domino.check.name.database`
- `com.sun.identity.agents.config.domino.ltpa.config.name`
- `com.sun.identity.agents.config.domino.ltpa.cookie.name`
- `com.sun.identity.agents.config.domino.ltpa.enable`
- `com.sun.identity.agents.config.domino.ltpa.org.name`
- `com.sun.identity.agents.config.ignore.preferred.naming.url`
- `com.sun.identity.agents.config.ignore.server.check`
- `com.sun.identity.agents.config.iis.auth.type`
- `com.sun.identity.agents.config.iis.filter.priority`
- `com.sun.identity.agents.config.iis.owa.enable`
- `com.sun.identity.agents.config.iis.owa.enable.change.protocol`
- `com.sun.identity.agents.config.iis.owa.enable.session.timeout.url`
- `com.sun.identity.agents.config.load.balancer.enable`
- `com.sun.identity.agents.config.locale`
- `com.sun.identity.agents.config.override.notification.url`
- `com.sun.identity.agents.config.poll.primary.server`
- `com.sun.identity.agents.config.proxy.override.host.port`

- `com.sun.identity.agents.config.remote.log.interval`
- `com.sun.identity.agents.config.remote.logfile`
- `com.sun.identity.client.notification.url`
- `org.forgerock.agents.config.cdsso.deny.cleanup.disable`

Fixes

For information about security issues fixed in this release, see Security Advisories.

Fixes in Web Agent 5.9.1

The following issues were fixed in this release:

- [AMAGENTS-4788](#): Agent doesn't delete session tracking cookie when running in `accept.sso.token` mode
- [AMAGENTS-4716](#): Agent does not handle SSO tracking cookie enclosed in double quotes
- [AMAGENTS-4687](#): Web Agent 5.9.0 crash if configuration fetch fails.
- [AMAGENTS-4545](#): nginx agent can crash if graceful restart (reload) is used with load testing.
- [AMAGENTS-4539](#): IIS Web Agent doesn't log reason why PDP file deletion fails.

Fixes in Web Agent 5.9

The following issues were fixed in this release:

- [AMAGENTS-4501](#): Web Agent session cache invalidated on configuration change
- [AMAGENTS-4460](#): Response attributes for not enforced urls can be duplicated
- [AMAGENTS-4417](#): Address Agent session timeout, when AM doesn't return 401 with `getSessionInfo`
- [AMAGENTS-4340](#): Log level inappropriate when agent reconnects after its token expires
- [AMAGENTS-4298](#): Validator segmentation fault with `validate_session_profile` test
- [AMAGENTS-4292](#): WPA is failing to complete authentication when there is no `Content-Length` header set on `authn POST` from AM
- [AMAGENTS-4216](#): When fragment redirection is enabled, the Agent ignores the query string
- [AMAGENTS-4188](#): Agent crash with local (not central) configuration.

- [AMAGENTS-4165](#): Agent will not translate http to https in agent/cdsso-oauth2 redirect in SSL offloading case on nginx
- [AMAGENTS-4101](#): Inconsistent behavior for JSON request between web agent 4.2.1.2 and 5.7.0 for content-type header
- [AMAGENTS-4064](#): Fragments don't work in a ssl terminated environment
- [AMAGENTS-3165](#): Seg Fault if policy evaluation realm properties are null in local configuration.
- [AMAGENTS-2717](#): Timed out Login Session results in 403 Forbidden Error

Security advisories

ForgeRock issues security advisories in collaboration with our customers and the open source community to address any security vulnerabilities transparently and rapidly.

ForgeRock's security advisory policy governs the process on how security issues are submitted, received, and evaluated as well as the timeline for the issuance of security advisories and patches.

For details of all the security advisories across ForgeRock products, see [Security Advisories](#) in the *Knowledge Base library*.

Limitations

Limitations in Web Agent 5.9.1

No additional limitations were introduced in this release.

Limitations in Web Agent 5.9

The following limitations in this release are inherent to the design, not bugs to be fixed:

▼ [Custom Login Redirection Mode Requires AM 6 or Later](#)

Redirect of users to a specific AM instance, an AM site, or website other than AM, requires AM 6 or later versions. For more information, see [Login Redirection and Login Conditional Redirection](#).

▼ [Ignore Path Info Properties Is not Supported for NGINX Plus Agent](#)

The NGINX Plus web agent does not support the following ignore path info properties:

- `com.sun.identity.agents.config.ignore.path.info`
- `com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list`

▼ [IIS Web Agents May Fail to Install When IIS Configuration Is Locked](#)

Installing web agents in IIS may fail with an error similar to the following:

```
Creating configuration...
Error: failed to create module entry for
MACHINE/WEBROOT/APPHOST/AgentSite/ (error 0x80070021, line:
1823).
The process cannot access the file because another process has
locked a portion of the file. (error: 0x21).
Installation failed.
```

This error message means the **agentadmin.exe** command cannot access some IIS configuration files because they are locked.

To work around this issue, perform the following steps:

1. Open the IIS Manager and select the Configuration Editor.
2. Unlock the IIS `system.webServer/modules` module.
3. Retry the web agent installation.

NOTE:Unlocking the `system.webServer/modules` module should allow the installation to finish. However, you may need to unlock other modules depending on your environment.

▼ [Apache HTTP Server Authentication Functionality Not Supported](#)

The web agent replaces authentication functionality provided by Apache, for example, the `mod_auth_*` modules. Integration with built-in Apache `httpd` authentication directives, such as `AuthName`, `FilesMatch`, and `Require` is not supported.

▼ [IIS Web Agent With Client-Based Sessions Returning HTTP 403 Errors When Accessing Protected Resources](#)

IIS web agents configured for client-based sessions will return HTTP 403 errors when trying to access a protected resource if `com.sun.identity.client.notification.url` is configured.

The `com.sun.identity.client.notification.url` property is removed in this release. Earlier versions of Web Agent use it to specify the notification listener for the agent. However, to provide backwards-compatibility with earlier versions of the agents, AM populates this property when creating the agent profile.

The value of this property should be removed for all agent installations, and must be removed for IIS web agents configured for client-based sessions.

▼ [Default Welcome Page Showing After Upgrade Instead of Custom Error Pages](#)

After upgrading, you may see the default Apache welcome pages instead of custom error pages defined by the Apache `ErrorDocument` directive.

If you encounter this issue, check your Apache `ErrorDocument` configuration. If the custom error pages are not in the document root of the Apache server, you should enclose the `ErrorDocument` directives in `Directory` elements. For example:

```
<Directory "/web/docs">
  ErrorDocument 403 myCustom403Error.html
</Directory>
```

Refer to the Apache documentation for more details on the `ErrorDocument` directive.

▼ [CA Certificate File Name Property not Honored when Client Authentication is not Required in Secure Channel Environments](#)

If you are using the Windows built-in Secure Channel API but your environment does not require client authentication, instead of setting the CA certificate friendly name in the CA Certificate File Name Property, set it in the Public Client Certificate File Name property. For example:

```
com.forgerock.agents.config.cert.ca.file =
com.forgerock.agents.config.cert.file = CA-cert-friendly-name
com.sun.identity.agents.config.trust.server.certs = false
```

▼ [Install IIS Web Agents on Child Applications Before Installing in Parent Application](#)

In an IIS environment where you need to protect a parent application and a child application with different web agent configurations, you must install the web agent on the child application before installing the web agent in the parent. Trying to install a web agent on a child that is already protected will result in error.

Known Issues

Known issues are tracked at <https://bugster.forgerock.org/jira/browse/AMAGENTS>.

Known Issues in Web Agent 5.9.1

The following additional issue remained open at the time of this release:

- AMAGENTS-5068: performance issue in AMAGENTS-4716 fix
- AMAGENTS-4795: POST Data Sticky Load Balancing Cookie Name configuration option isn't working

Known Issues in Web Agent 5.9

The following important issue remained open at the time of this release:

- AMAGENTS-4527: The web agent might not behave correctly after its token expires when session attribute allow-listing is used.
- AMAGENTS-4897: config.fallback.mode doesn't work for not-enforced url configuration

Documentation

Date	Description
December 2022	Information about the deprecated agent monitoring endpoint has been added to Monitoring .
July 2022	AMAGENTS-4897 and AMAGENTS-5068 added to the lists of known issues.
January 2022	Maintenance release of Web Agent 5.9.1 software.
September 2021	Initial release of Web Agent 5.9 software.
	The following changes have been made to the documentation, in addition to changes for product features: <ul style="list-style-type: none">• The Installation Guide and Maintenance Guide have been added to this release. Information about installation, auditing, monitoring and notifications, has been removed from the User Guide.• Information in the Properties Reference has been reorganized.• Agent Authenticators are no longer supported, and related information has been removed from the documentation.

Appendix A: Release Levels and Interface Stability

This appendix includes ForgeRock definitions for product release levels and interface stability.

ForgeRock product release levels

ForgeRock defines Major, Minor, Maintenance, and Patch product release levels. The version number reflects release level. The release level tells you what sort of compatibility changes to expect.

Release level definitions

Release Label	Version Numbers	Characteristics
Major	Version: x[.0.0] (trailing 0s are optional)	<ul style="list-style-type: none">• Bring major new features, minor features, and bug fixes.• Can include changes even to Stable interfaces.• Can remove previously Deprecated functionality, and in rare cases remove Evolving functionality that has not been explicitly Deprecated.• Include changes present in previous Minor and Maintenance releases.
Minor	Version: x.y[.0] (trailing 0s are optional)	<ul style="list-style-type: none">• Bring minor features, and bug fixes.• Can include backwards-compatible changes to Stable interfaces in the same Major release, and incompatible changes to Evolving interfaces.• Can remove previously Deprecated functionality.• Include changes present in previous Minor and Maintenance releases.
Maintenance, Patch	Version: x.y.z[.p] The optional <i>p</i> reflects a Patch version.	<ul style="list-style-type: none">• Bring bug fixes• Are intended to be fully compatible with previous versions from the same Minor release.

ForgeRock product stability labels

ForgeRock products support many features, protocols, APIs, GUIs, and command-line interfaces. Some of these are standard and very stable. Others offer new functionality that is continuing to evolve.

ForgeRock acknowledges that you invest in these features and interfaces, and therefore must know when and how ForgeRock expects them to change. For that reason, ForgeRock defines stability labels and uses these definitions in ForgeRock products.

ForgeRock stability label definitions

Stability Label	Definition
Stable	<p>This documented feature or interface is expected to undergo backwards-compatible changes only for major releases.</p> <p>Changes may be announced at least one minor release before they take effect.</p>
Evolving	<p>This documented feature or interface is continuing to evolve and so is expected to change, potentially in backwards-incompatible ways even in a minor release. Changes are documented at the time of product release.</p> <p>While new protocols and APIs are still in the process of standardization, they are Evolving. This applies for example to recent Internet-Draft implementations, and also to newly developed functionality.</p>
Legacy	<p>This feature or interface has been replaced with an improved version, and is no longer receiving development effort from ForgeRock.</p> <p>You should migrate to the newer version, however the existing functionality will remain.</p> <p>Legacy features or interfaces will be marked as <i>Deprecated</i> if they are scheduled to be removed from the product.</p>
Deprecated	<p>This feature or interface is deprecated, and likely to be removed in a future release.</p> <p>For previously stable features or interfaces, the change was likely announced in a previous release.</p> <p>Deprecated features or interfaces will be removed from ForgeRock products.</p>

Stability Label	Definition
Removed	This feature or interface was deprecated in a previous release, and has now been removed from the product.
Technology Preview	<p>Technology previews provide access to new features that are considered as new technology that is not yet supported. Technology preview features may be functionally incomplete, and the function as implemented is subject to change without notice.</p> <p><i>DO NOT DEPLOY A TECHNOLOGY PREVIEW INTO A PRODUCTION ENVIRONMENT.</i></p> <p>Customers are encouraged to test drive the technology preview features in a non-production environment, and are welcome to make comments and suggestions about the features in the associated forums.</p> <p>ForgeRock does not guarantee that a technology preview feature will be present in future releases, the final complete version of the feature is liable to change between preview and the final version. Once a technology preview moves into the completed version, said feature will become part of the ForgeRock platform.</p> <p>Technology previews are provided on an “AS-IS” basis for evaluation purposes only, and ForgeRock accepts no liability or obligations for the use thereof.</p>
Internal/Undocumented	<p>Internal and undocumented features or interfaces can change without notice.</p> <p>If you depend on one of these features or interfaces, contact ForgeRock support or email info@forgerock.com to discuss your needs.</p>

Getting support

ForgeRock provides support services, professional services, training through ForgeRock University, and partner services to assist you in setting up and maintaining your deployments. For a general overview of these services, see <https://www.forgerock.com>.

ForgeRock has staff members around the globe who support our international customers and partners. For details on ForgeRock’s support offering, including support plans and service level agreements (SLAs), visit <https://www.forgerock.com/support>.

ForgeRock publishes comprehensive documentation online:

- The ForgeRock Knowledge Base offers a large and increasing number of up-to-date, practical articles that help you deploy and manage ForgeRock software.

While many articles are visible to everyone, ForgeRock customers have access to much more, including advanced information for customers using ForgeRock software in a mission-critical capacity.

- ForgeRock product documentation, such as this document, aims to be technically accurate and complete with respect to the software documented. It is visible to everyone and covers all product features and examples of how to use them.

Copyright © 2010-2023 ForgeRock, all rights reserved.