Release Notes

/ ForgeRock Token Validation Microservice 1.0.2

Latest update: 1.0.2

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

Abstract

Notes on prerequisites, fixes, and known issues for the ForgeRock® Token Validation Microservice.

Table of Contents

Preface

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.

Chapter 1
What's New

The ForgeRock Token Validation Microservice (TVMS) is delivered as part of the ForgeRock Identity Platform to introspect and validate OAuth 2.0 access_tokens in service-to-service deployments. For information about the features of TVMS, see the User Guide.

New Features

New Features in TVMS 1.0.2

The following new features were introduced in this release:

Deterministic ECDSA for JWT Signatures

When elliptic curve keys are used for signing, and Bouncy Castle is installed, by default JWTs are signed with a deterministic ECDSA. In previous releases, JWTs were signed with a non-deterministic ECDSA, which is less secure.

The new system property `org.forgerock.secrets.preferdeterministicecdsa` is by default `true`. To use the less secure algorithm, set the property to `false`.

New Features in TVMS 1.0.1

No new features were introduced in this release.

New Features in TVMS 1.0.0

No new features were introduced in this release.

Product Improvements

This section lists improvements introduced in TVMS.

Product Improvements in TVMS 1.0.2

Correct Maintenance of Cookies With `sameSite` Flag

Cookies that arrive at TVMS with the `sameSite` flag set are correctly maintained.

Ping Endpoint

A ping endpoint is available after TVMS startup to check whether the service is available. When TVMS is installed and running as described in "*Starting and Stopping TVMS*" in the *User Guide*, the endpoint is at `http://mstokval.example.com:9090/ping`.

Warning If Decoded Secret Starts or Ends in a Non-ASCII Character

TVMS logs a warning when the decoded value of a BASE64-encoded secret starts or ends with a non-ASCII character.

If a text editor adds a carriage return to the end of a plain string value before it is encoded, non-ASCII characters can be added to the BASE64-encoded value. When the decoded value is used as part of a username/password exchange, it can then cause an authentication error.

New Functions

The functions `encodeBase64url` and `decodeBase64url` are added to facilitate URL-safe and filename-safe encoding and decoding.

Global Log Level Configurable Through A Variable

To make it easier to deploy TVMS without modifying the default configuration, the global log level is now defined as a variable in the default `logback.xml`. To change the global log level, set an environment variable or system property.

Product Improvements in TVMS 1.0.1

No improvements were introduced in this release.

Product Improvements in TVMS 1.0.0

No improvements were introduced in this release.

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*.

Chapter 2

Before You Install

This chapter describes the requirements for running TVMS.

Tip

If you have a request to support a component or combination not listed here, contact ForgeRock at info@forgerock.com.

Downloading the TVMS Software

Download the product software from the ForgeRock BackStage download site:

- TVMS .zip file, `MicroserviceTokenValidation-1.0.2.zip`

Java Requirements

The following table lists supported Java versions:

JDK Requirements

Vendor	Versions
Oracle JDK	11 or later versions
OpenJDK	11 or later versions

For the latest security fixes, ForgeRock recommends that you use the most recent update.

Authorization Server Requirements

Use an OAuth 2.0 authentication server, such as ForgeRock Access Management. For information about downloading and using AM, see AM's *Release Notes*.

If you use AM, AM version 6 or later is required.

The examples in the TVMS User Guide use AM, and assume that it is reachable on `http://openam.example.com:8088/openam`.

Chapter 3

Compatibility With Other Releases

This chapter describes important changes to existing functionality, deprecated functionality, and removed functionality in TVMS.

Important Changes to Existing Functionality

This section lists important changes to existing functionality in TVMS.

Important Changes in TVMS 1.0.2

KeyStore and KeyStoreSecretStore Default Type Based On Keystore Extension

Oracle recommends the use of PKCS12 keystores. From Java 9, Oracle has provided more support for PKCS12. From Java 11, Oracle has changed the default keystore to PKCS12.

Following this lead, the default type for KeyStore and KeyStoreSecretStore is now based on the keystore extension. If the keystore extension is not recognized, the default type is PKCS12. In previous releases, the default type was the one used by the platform.

To ensure backward-compatibility, where keys are generated using a non-PKCS12 type (for example, JKS), specify `type` in KeyStore or `storeType` in KeyStoreSecretStore.

For information, see "KeyStore" in the *Configuration Reference* and "KeyStoreSecretStore" in the *Configuration Reference*.

Important Changes in TVMS 1.0.1

gracefulStop In ScheduledExecutorService

When `gracefulStop` is `true`, the ScheduledExecutorService now removes submitted jobs and attempts to end running jobs, after respecting the `gracePeriod`. In previous releases, when `gracefulStop` was true, it did not remove or end jobs.

Important Changes in TVMS 1.0.0

No important changes to existing functionality were made in this release.

Deprecated Functionality

There is no deprecated functionality in TVMS, as defined in "ForgeRock Product Stability Labels".

Removed Functionality

This section lists removed functionality in TVMS, as defined in "ForgeRock Product Stability Labels".

Removed Functionality in TVMS 1.0.2

No functionality was removed in TVMS 1.0.2.

Removed Functionality in TVMS 1.0.1

No functionality was removed in TVMS 1.0.1.

Removed Functionality in TVMS 1.0.0

No functionality was removed in TVMS 1.0.0.

Chapter 4

Fixes, Limitations, and Known Issues

This chapter lists the status of key issues and limitations in TVMS. TVMS issues are tracked at https://bugster.forgerock.org/jira/browse/MICSVC.

Key Fixes

This section lists key fixes in TVMS.

Key Fixes in TVMS 1.0.2

- MICSVC-122: JAVA_HOME can't be defined in env.sh
- MICSVC-135: TV: scope field is different when validating a stateless access token
- OPENIG-3755: IG's decodeBase64 function returns null on JWTs generated by IG or AM
- OPENIG-4048: Update Jackson Databind to 2.10

Key Fixes in TVMS 1.0.1

- OPENIG-3820: Path/QueryString with %encoded values are forwarded in a decoded way
- MICSVC-118: Remove default-config.json
- The port number in the default `admin.json` was changed to 9090

Key Fixes in TVMS 1.0.0

No important issues were fixed in this release.

Limitations

This section lists limitations that apply to TVMS.

Limitations in TVMS 1.0.2

CacheTimeout For The JwkSetSecretStore Cannot Be Disabled Or Lower Than 10 Seconds

The `cacheTimeout` property cannot be disabled in the JwkSetSecretStore. The minimum value is 10 seconds. If a lower value is set, the `cacheTimeout` is forced to 10 seconds.

Streaming Mode Not Available

The ClientHandler cannot stream responses from a proxied application to the user agent. Responses are processed in non-streaming mode only, after the entire entity content is available. Consequently, only the non-streaming mode is available, which does not support Server-Sent Events (SSE) or very large files.

TVMS Scripts Can Access Anything in Their Environment (OPENIG-3274)

TVMS scripts are not sandboxed, but instead have access to anything in their environment. You must make sure that the scripts that TVMS loads are safe.

Log File of Audit Events Can be Overwritten (OPENIG-813)

The log file of audit events can be overwritten when the log file is rotated.

When `CsvAuditEventHandler` is used to log audit events, the log file is overwritten if it is rotated before the file suffix, `rotationFileSuffix`, changes. By default, `rotationFileSuffix` is defined as a date in the format `_yyyy-MM-dd`.

Log files are rotated when one of the following limits is reached: `maxFileSize`, `rotationInterval`, or `rotationTimes`.

Set the log rotation parameters so that the log is not likely to rotate before `rotationFileSuffix` changes.

For Mutual Authentication in HTTPS Cannot Specify Which Certificate to Present (OPENIG-221)

TVMS can check server certificates for HTTPS. However, for mutual authentication, the client certificate must be the first certificate in the KeyStore.

Known Issues

This section lists important known issues in TVMS.

Known Issues in TVMS 1.0.2

- OPENIG-659: CryptoHeaderFilter - error on handling header value with incorrect length
- MICSVC-122: JAVA_HOME can't be defined in env.sh

Chapter 5
Documentation Changes

The following table lists important changes to the documentation:

Documentation Changes

Release	Date	Description
1.0.2	August 2022	Examples of how to introspect access tokens from the the ForgeRock Identity Cloud have been added to the User Guide.
1.0.2	November 2019	The Configuration Reference has been added to the documentation set, and the Reference section removed from the User Guide. Information about the ProtectionFilter is added in "Provided Objects" in the *Configuration Reference*. The filter was available in previous versions of TVMS but was not documented.
1.0.1	August 2019	Update to the lists of important changes, fixes, limitations, and known issues in the Release Notes.
1.0.0	July 2019	The first release of TVMS.

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 release level is reflected in the version number. 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)	• 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)	• Bring minor features, and bug fixes

Release Label	Version Numbers	Characteristics
		• 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 .p reflects a Patch version.	• 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	This documented feature or interface is expected to undergo backwards-compatible changes only for major releases. Changes may be announced at least one minor release before they take effect.
Evolving	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. 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.
Legacy	This feature or interface has been replaced with an improved version, and is no longer receiving development effort from ForgeRock. You should migrate to the newer version, however the existing functionality will remain. Legacy features or interfaces will be marked as *Deprecated* if they are scheduled to be removed from the product.

Stability Label	Definition
Deprecated	This feature or interface is deprecated and likely to be removed in a future release. For previously stable features or interfaces, the change was likely announced in a previous release. Deprecated features or interfaces will be removed from ForgeRock products.
Removed	This feature or interface was deprecated in a previous release and has now been removed from the product.
Technology Preview	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. DO NOT DEPLOY A TECHNOLOGY PREVIEW INTO A PRODUCTION ENVIRONMENT. 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. 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. Technology previews are provided on an “AS-IS” basis for evaluation purposes only and ForgeRock accepts no liability or obligations for the use thereof.
Internal/Undocumented	Internal and undocumented features or interfaces can change without notice. If you depend on one of these features or interfaces, contact ForgeRock support or email info@forgerock.com to discuss your needs.

Appendix B. 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 community members, 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.