Oracle® Cloud

Known Issues for Oracle Cloud Identity and Access Management

16.3

E68445-07

August 2016

This document describes issues you might encounter when using shared identity management for Oracle Cloud services.

ORACLE

Oracle Cloud Known Issues for Oracle Cloud Identity and Access Management, 16.3

E68445-07

Contents

Preface

Known Issues for Oracle Cloud Identity Management describes the issues you might encounter with shared identity management for Oracle Cloud services.

Related Documents

There are several types of related resources available to you.

See Secure Platform Cloud Services documentation, videos, and tutorials.

Conventions

The following text conventions are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Known Issues and Deprecated Features

This section describes issues associated with Shared Identity Management for Oracle Cloud services.

There are no deprecated features/commands in this release.

Topics:

Supported Browsers

Oracle Cloud supports the following the minimum requirements for web browsers:

Web Browser	Version
Microsoft Internet Explorer	9 or 10 **Notes:** • Set Browser Mode to IE9 or IE10 • Set Document Mode to IE9 or IE10 standards
Google Chrome	29 and later
Mozilla Firefox	24 and later
Apple Safari	6

Known Issues

The following issues are present in Shared Identity Management for Oracle Cloud services.

Topics:

Updating NameID/ SSO Profile Requires Import Of Metadata

After importing partner metadata using the Self Service SSO configuration, you may run into problems updating the SSO profile or NameID mapping.

After you used **MyServices** > **Users** > **SSO Confguration** tab to import partner metadata, if you want to change the SSO Profile or NameID mapping, then you must re-import the partner metadata.

However, after re-importing the partner metadata, the previous settings of SSO Profile / NameID are rolled back to default values.

Workaround

The Oracle Identity Federation REST APIs support update via `PUT`. Use the `PUT` operation and update only the provided fields.

After Importing Metadata, SSO Is Disabled Automatically

When using the Self Service **SSO Configuration** tab, if you re-import new partner metadata, SSO is disabled automatically.

As an indication, the message `SSO is disabled` appears at the bottom of screen.

Whenever you upload a new configuration, you must test the new configuration before enabling SSO.

SSO Configuration Breaks

SSO configuration breaks if a corrupted identity metadata file or a new certificate file is uploaded.

Issue

The SSO Configuration may break if you:

- Uploaded a corrupted Identity Provider metadata file
- Uploaded a new Certificate file to an existing SSO Configuration
- Tried importing an Identity Provider metadata file without specifying the SingleLogout endpoint

If there is a existing SSO configuration in place, and you update the Signing Certificate, by choosing **Enter identity provider metadata manually**, and upload the certificate file, the SSO configuration becomes unavailable, as if there was no configuration in place.

If you have uploaded a corrupted metadata file, during the first configuration, then also the SSO configuration becomes unusable. And because you cannot update the metadata, as mentioned above, the SSO configuration cannot be reconfigured either.

Any attempt to re-create the configuration fails.

Probable Reason

When invoking the Oracle Identity Federation REST API to create or update a partner, the MyServices console sets the `SigningCert` or `EncryptionCert` to the exact content of the file, instead of converting to the Base64 encoded value of the binary certificate.

Workaround

If the certificate is PEM encoded, before you upload the file, ensure that the file does not contain either of the following lines:

```
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
```

If the certificate contains these lines, remove them.

If the certificate is in binary format, the MyServices console does not support uploading this format.

If you are trying to import Identity Provider metadata without specifying the SingleLogout endpoint, edit and add the `SingleLogoutService` element to your Identity Provider metadata.xml file and then import it.