

Active Directory Federation Services Management Pack Guide

Microsoft Corporation

Published: October 2021

Send suggestions and comments about this document to systemcenterfeedback@microsoft.com Please include the Management Pack guide name with your feedback.

Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2017 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Revision History

| **Release Date** | **Changes** |
| --- | --- |
| October 2021 | Fixed: Duplicate instance issue,The MP has verified for Windows Server 2012 R2 & 2016 and above operating systems and branded as version agnostic  |
| June 2021 | Version agnostic support has been implemented Windows Server 2016 and above |
| November 2018 | Fixed a bug in the SQL Configuration Database Unavailable monitor so that it works with non-default SQL ports |
| July 2018 | Published updated guide to include missing revision history |
| May 2018 | Fixed a bug where the ADFS role would be undiscovered if the ADFS service was stopped. |
| March 2017 | AD FS MP 2016 Released; document updated to reflect the new MP version. |

Contents

[Introduction to the AD FS Management Pack 6](#_Toc74651282)

[Supported Configurations 6](#_Toc74651283)

[Getting Started 7](#_Toc74651284)

[Before You Import the Management Pack 7](#_Toc74651285)

[Files in This Management Pack 7](#_Toc74651286)

[How to Import the AD FS Management Pack 8](#_Toc74651287)

[Initial Configuration 8](#_Toc74651288)

[Create a New Management Pack for Customizations 8](#_Toc74651289)

[Perform Discoveries for Monitored Components 8](#_Toc74651290)

[Optional Configuration 9](#_Toc74651291)

[Security Considerations 10](#_Toc74651292)

[Low-Privilege Environments 10](#_Toc74651293)

[Understanding Management Pack Operations 10](#_Toc74651294)

[Objects That the AD FS Management Pack Discovers 10](#_Toc74651295)

[Classes 11](#_Toc74651296)

[Key Monitoring Scenarios 12](#_Toc74651297)

[Token-Issuance Failures Scenario 12](#_Toc74651298)

[Token-Acceptance Failures Scenario 18](#_Toc74651299)

[Trust Management Failures Scenario 21](#_Toc74651300)

[Windows Internal Database (WID) Synchronization Failures Scenario 23](#_Toc74651301)

[Certificate Management Failures Scenarios 24](#_Toc74651302)

[General Federation Server Failures Scenario 24](#_Toc74651303)

[Device Registration Service 27](#_Toc74651304)

[Known Issues 27](#_Toc74651305)

[Appendix: Scripts 28](#_Toc74651306)

Introduction to the AD FS Management Pack

The Active Directory Federation Services (AD FS) Management Packs provide both proactive and reactive monitoring of your AD FS deployment for the federation server. The management pack monitors events that the AD FS Windows service records in the AD FS event logs, and it monitors the performance data that the AD FS performance counters collect. It also monitors the overall health of the AD FS system and the federation passive application, and it provides alerts for critical issues and warning issues.

This management pack includes monitoring servers running the AD FS role on Windows Server 2016 and above. Due to the architectural changes in AD FS, this Management Pack will not be able to monitor earlier versions of AD FS servers. With this management pack, the discovery of servers running AD FS on Windows Server 2016 and above is enabled.

Document Version

This guide was written based on the 10.0.3.2 version of the AD FS Management Pack. Before you install the updated ADFS Management Pack (v10.0.3.2), remove any existing ADFS Management Packs.

Getting the Latest Management Pack and Documentation

You can find the AD FS Management Pack in the [System Center Marketplace](http://go.microsoft.com/fwlink/?LinkId=82105) (http://go.microsoft.com/fwlink/?LinkId=82105).

Supported Configurations

This management pack requires System Center Operations Manager 2016 and System Center Operations Manager 2019.

**refer below links:**

SCOM 2019 : [System requirements for System Center Operations Manager | Microsoft Docs](https://docs.microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-2019#microsoft-monitoring-agent-operating-system)

SCOM 2016 : [System requirements for System Center Operations Manager | Microsoft Docs](https://docs.microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-2016#software-requirements-for-operations-manager-components)

The Active Directory Federation Services (AD FS) Management Pack is supported on the operating system configurations in the following table.

| **Configuration** | **Support** |
| --- | --- |
| Windows Server 2016 and above | Yes |
| Windows Server 2012 and 2012 R2 | Yes |

All support is subject to the Microsoft overall [Help and Support](http://go.microsoft.com/fwlink/?Linkid=26134) (http://go.microsoft.com/fwlink/?Linkid=26134).

Getting Started

This section describes the actions that you should take before you import the Active Directory Federation Services (AD FS) Management Pack, any steps that you should take after you import the AD FS Management Pack, and information about customizations.

Before You Import the Management Pack

Before you import the Active Directory Federation Services (AD FS) Management Pack, take the following actions:

 Before you install the updated ADFS Management Pack (v10.0.3.2), remove any existing ADFS Management Packs.

 Install System Center Operations Manager 2016 or later.

Files in This Management Pack

The Active Directory Federation Services (AD FS) Management Pack includes the following files:

Microsoft System Center MP for ADFS.msi

Microsoft System Center MP for ADFS (CHS).msi

Microsoft System Center MP for ADFS (CHT).msi

Microsoft System Center MP for ADFS (CSY).msi

Microsoft System Center MP for ADFS (DEU).msi

Microsoft System Center MP for ADFS (ESN).msi

Microsoft System Center MP for ADFS (FRA).msi

Microsoft System Center MP for ADFS (HUN).msi

Microsoft System Center MP for ADFS (ITA).msi

Microsoft System Center MP for ADFS (JPN).msi

Microsoft System Center MP for ADFS (KOR).msi

Microsoft System Center MP for ADFS (NLD).msi

Microsoft System Center MP for ADFS (PLK).msi

Microsoft System Center MP for ADFS (PTB).msi

Microsoft System Center MP for ADFS (PTG).msi

Microsoft System Center MP for ADFS (RUS).msi

Microsoft System Center MP for ADFS (SVE).msi

Microsoft System Center MP for ADFS (TRK).msi

How to Import the AD FS Management Pack

For instructions about importing a management pack, see [How to install an Operations Manager Management Pack](https://technet.microsoft.com/en-us/library/hh212691%28v%3Dsc.12%29.aspx) (https://technet.microsoft.com/en-us/library/hh212691(v=sc.12).aspx).

After the Active Directory Federation Services (AD FS) Management Pack is imported, create a new management pack in which you store overrides and other customizations.

Initial Configuration

After the Active Directory Federation Services (AD FS) Management Pack is imported, follow these procedures to finish your initial configuration:

1. Create a new management pack in which to store overrides and other customizations.

2. Perform discoveries for monitored components.

Create a New Management Pack for Customizations

Most vendor management packs are sealed so that you cannot change any of the original settings in the management pack file. However, you can create customizations, such as overrides or new monitoring objects, and save them to a different management pack. By default, System Center Operations Manager saves all customizations to the Default Management Pack. As a best practice, you should instead create a separate management pack for each sealed management pack that you want to customize.

Creating a new management pack for storing overrides has the following advantages:

 It simplifies the process of exporting customizations that were created in your test and preproduction environments to your production environment. For example, instead of exporting the Default Management Pack that contains customizations from multiple management packs, you can export just the management pack that contains customizations of a single management pack.

 You can delete the original management pack without first having to delete the Default Management Pack. A management pack that contains customizations depends on the original management pack. This dependency requires you to delete the management pack with customizations before you can delete the original management pack. If all your customizations are saved to the Default Management Pack, you must delete the Default Management Pack before you can delete an original management pack.

 It is easier to track and update customizations to individual management packs.

For more information about management packs [What is an Operations Manager Management Pack](https://technet.microsoft.com/en-us/library/hh212794%28v%3Dsc.12%29.aspx) (https://technet.microsoft.com/en-us/library/hh212794(v=sc.12).aspx).

Perform Discoveries for Monitored Components

You must configure the Agent or Operation Manager server so that it has the permission to perform discoveries for the components that are monitored. When you do this, ensure that both the Agent and Operation Manager have the Allow this server/agent to act as proxy and discover managed objects on other computers option enabled.

To configure the Agent

|  |
| --- |
| 1. Open the Operations Console of the Operation Manager. 2. In the left panel, click the Administration tab. 3. Click Device Management, and then click Agent Managed. 4. In the right panel, click the agent that you want to configure, and then click Properties.5. On the Agent Properties page, click the Security tab.6. Make sure that the Allow this agent to act as a proxy and discover managed objects on other computers check box is selected.  |

To configure the Operation Manager

|  |
| --- |
| 1. Open the Operations Console of the Operation Manager. 2. In the left panel, click the Administration tab. 3. Click Device Management, and then click Management Servers.4. In the right panel, click the agent that you want to configure, and then click Properties.5. On the Management Server Properties page, click the Security tab.6. Make sure that the Allow this server to act as a proxy and discover managed objects on other computers check box is selected. |

Optional Configuration

Enable monitoring of authorization rules

Depending on how Active Directory Federation Services (AD FS) was deployed in your organization, you may want to enable the ability to monitor how authorization claim rules are working in your organization. Microsoft assumes that administrators, before putting AD FS into production, configured the user authorization claim rules properly, and any denial of access that users experience is a result of the authorization claim rules that were configured.

The following rules are disabled by default in the AD FS management pack:

 On Behalf Of Authorization Error

 Caller Authorization Error

 Act As Authorization Error

You can enable these rules by performing the following procedure.

To enable rules

|  |
| --- |
| 1. Open the Operations Console of the Operation Manager. 2. Click the Authoring tab in the left panel. 3. Click Management Pack Objects, and then click Rules. 4. In the list of rules, locate the rule that you want to enable under Type: Token Issuance, right-click the rule, point to Overrides, point to Override the Rule, and then click For all objects of class: Token issuance.  |

Security Considerations

You may need to customize your Active Directory Federation Services (AD FS) Management Pack. Certain accounts cannot be run in a low-privilege environment, or they must have minimum permissions.

Low-Privilege Environments

So that each of the client-side monitoring scripts can run successfully, the Action Account must be a member of the Administrators group or a Local System account on the Agent computer on which Active Directory Federation Services (AD FS) is running.

Understanding Management Pack Operations

This section provides additional information about the types of objects that the Active Directory Federation Services (AD FS) Management Pack discovers and about the classes that are involved. It also explains the concepts that are introduced in the [Key Monitoring Scenarios](#z41b39ab2469e474089e673236a7bd714) section.

Objects That the AD FS Management Pack Discovers

The Active Directory Federation Services (AD FS) Management Pack discovers the object types in the following table for the federation server role.

| **Role** | **Object type** |
| --- | --- |
| Federation server | Federation Server Seed |
| Federation server | AD FS |
| Federation server | Federation Service |
| Federation server | Federation Server |
| Federation server | Authentication |
| Federation server | Certificate Management |
| Federation server | Trust Management |
| Federation server | On-premises Device Registration Service |
| Federation server | WID Sync |
| Federation server | Artifact Service |
| Federation server | Token Acceptance |
| Federation server | Token Issuance |

The Federation Server Seed object type is discovered when the federation server is installed on the monitored computer.

For information about discovering objects, [Objects the Management Pack Discovers](https://technet.microsoft.com/en-us/library/dd767419.aspx) (<https://technet.microsoft.com/en-us/library/dd767419.aspx>).

Classes

The following diagram shows the classes that are defined in the Active Directory Federation Services (AD FS) Management Pack.



Abstract classes

Abstract classes have no instances, and they exist only to act as a base class for other classes. With this in mind, the class Microsoft.ActiveDirectoryFederationServices.2016.FederationServer, and all the classes that it hosts, inherit from an abstract class named Microsoft.ActiveDirectoryFederationServices.2016.FederationServerBase.

Both Microsoft.ActiveDirectoryFederationServices.2016.FederationServer and Microsoft.ActiveDirectoryFederationServices.2016.FederationServerBase inherit from another abstract class named Microsoft.ActiveDirectoryFederationServices.2016.ActiveDirectoryFederationServices.2016Base.

Key Monitoring Scenarios



The following tables list the subscenarios for monitors/rules that the Active Directory Federation Services (AD FS) Management Pack has implemented for key higher-level monitoring scenarios. If there are failures in those scenarios or if a success event indicates a warning, an alert is generated.

In some cases, the alerts are suppressed so that only one alert is generated when many failures/warnings with the same root cause occur. (See the Alert suppression column in the tables in this section.) For event-based monitors/rules, the event is counted before generating an alert for the intermittent failures. (See the Event counting column in the tables in this section.)

Note

Alert suppression applies only to rules. Event counting applies to only monitors.

Token-Issuance Failures Scenario

The monitors/rules in the following table monitor the token-issuance failures that are observed on the Federation Service for warning events that are related to token issuance.

| **Subscenario** | **Rule/monitor name** | **Alert suppression** | **Event counting** |
| --- | --- | --- | --- |
| Artifact: Failed to connect to the artifact database. | Artifact Database Connection Open Error | N/A | No |
| Artifact: Failed to get artifacts from the artifact database. | Artifact Database Get Error | N/A | No |
| Artifact: Failed to add artifacts to the artifact database. | Artifact Database Add Error | N/A | No |
| Artifact: Failed to remove artifacts from the artifact database. | Artifact Database Remove Error | N/A | If the same failures happen at least 30 times within an hour |
| Artifact: The Artifact service failed to start. | Artifact Service Startup Exception | N/A | No |
| Artifact: The SAML artifact resolution service is not enabled for the relying party. | Artifact Requested But Disabled Error | Suppress if the failures are with the same relying party | N/A |
| Artifact resolution request: The SAML artifact resolution endpoint is not configured, or it is disabled. | Artifact Resolution Endpoint Not Configured Error | Suppress if the same failures happen | N/A |
| Artifact resolution request: The SAML artifact resolution request specified an issuer that is not configured for the relying party. | Artifact Resolution Service Identity Not Found Error | Suppress if the failures are with the same relying party | N/A |
| Artifact resolution request: The SAML artifact resolution request failed. | Artifact Resolution Failed | N/A | No |
| Artifact resolution request: The Federation Service was unable to issue a token because the SAML artifact could not be resolved. Artifact resolution request that was made to the claims provider trust failed. | SAML Artifact Resolution Request Error | Suppress if the failures are with the same claims provider | N/A |
| Artifact resolution request: Claims provider does not have a SAML artifact resolution endpoint with the specified index configured. Artifact resolution failed. | SAML Artifact Resolution Endpoint Not Found Error | Suppress if the failures are with the same claims provider | N/A |
| Assertion Consumer Service: The SAML request specified an assertion consumer service index that is not configured on the relying party. | Unmatched Assertion Consumer Service Index | Suppress if the failures are with the same relying party and the same assertion consumer service index | N/A |
| Assertion Consumer Service: The assertion consumer service protocol binding endpoint specified in the SAML request is not configured on the relying party. | Unmatched Assertion Consumer Service Protocol Binding | Suppress if the failures are with the same relying party and the same assertion consumer service protocol binding | N/A |
| Assertion Consumer Service: The assertion consumer service URL specified in the SAML request is not configured on the relying party. | Unmatched Assertion Consumer Service URL | Suppress if the failures are with the same relying party and the same assertion consumer service URL | N/A |
| Assertion Consumer Service: The assertion consumer service endpoint specified in the SAML request is not configured on the relying party. | Assertion Consumer Service Endpoint Was Not Configured | Suppress if the failures are with the same relying party | N/A |
| Assertion Consumer Service: The relying party is not configured with SAML assertion consumer services. | Configuration Missing SAML Assertion Consumer Services Error | Suppress if the failures are with the same relying party | N/A |
| Attribute store: The attribute store that is configured in the Federation Service could not be loaded. | Attribute Store Load Failure | Suppress if the failures are with the same attribute store | N/A |
| Attribute store: An error occurred during an attempt to execute a query to the SQL attribute store. | SQL Attribute Store Query Execution Error | Suppress if the failures are with the same SQL attribute store and the same query | N/A |
| Attribute store: A processing error occurred in the attribute store or in the attribute store rule. | Attribute Store Rule Processing Error | N/A | No |
| Authorization: The Federation Service could not authorize token issuance for the caller on behalf of the subject to the relying party. | On Behalf Of Authorization Error | Suppress if the failures are with the same caller, the same subject, and the same relying party | N/A |
| Authorization: The Federation Service could not authorize token issuance for the caller to the relying party. | Caller Authorization Error | Suppress if the failures are with the same caller and the same relying party | N/A |
| Certificate: The token-signing certificate for the relying party is not valid. | Relying Party Signing Certificate Is Not Valid | Suppress if the failures are with the same relying party and the same thumbprint | N/A |
| Certificate: The service account that the AD FS Windows Service uses does not have permission to the private key of its token-signing certificates and/or its token-decrypting certificates. | Certificate Private Key Inaccessible Error | N/A | No |
| Certificate: An error occurred during an attempt to build the certificate chain for the relying party trust using the encryption certificate that was identified by a thumbprint. | Relying Party Encryption Certificate Error | Suppress if the failures are with the same relying party and with the same thumbprint | N/A |
| Domain controller: The Federation Service failed to find a domain controller in the domain. | LDAP Lookup Error | Suppress if the failures are with the same domain controller | N/A |
| Endpoint: The WS-Metadata Exchange (MEX) endpoint that is used for authentication over SOAP and HTTP protocols is not reachable. | MEX Endpoint Is Unreachable | N/A | N/A |
| Federation passive: A communication error occurred during an attempt to get a token from the Federation Service. | Federation Passive Service Communication Error | N/A | No |
| Global catalog server: The Federation Service failed to connect to a global catalog server. | Global Catalog Server Connection Error | Suppress if the failures are with the same global catalog server | N/A |
| Global catalog server: The Federation Service failed to query a global catalog server. | LDAP Global Catalog Server Error | Suppress if the failures are with the same global catalog server | N/A |
| LDAP server: The Federation Service failed to connect to an LDAP server. | LDAP Connection Error | Suppress if the failures are with the same LDAP server | N/A |
| LDAP server: The Federation Service failed to query an LDAP server. | LDAP Server Query Error | Suppress if the failures are with the same LDAP server | N/A |
| NameID policy: The federation server cannot process the SAML authentication request because the NameID policy that was specified in the authentication request cannot be satisfied. | Unsupported NameID Policy | Suppress if the failures are with the same relying party and the same NameID policy | N/A |
| SAML request: The Federation Service encountered an error while processing the SAML authentication request. | SAML Request Processing Error | N/A | No |
| Security: The token that was used to authenticate the user or the request is signed with the signature algorithm, which is not the expected signature algorithm. | Weak Signature Algorithm Error | Suppress if the failures are with the same issuer | N/A |
| Security: The SAML artifact resolution request is signed with the signature algorithm, which is not the expected signature algorithm. | Weak Signature Algorithm Error in Artifact Resolution Request | Suppress if the failures are with the same relying party | N/A |
| Security: The SAML request is signed with the signature algorithm, which is not the expected signature algorithm. | Weak Signature Algorithm Error in SAML Request | Suppress if the same failures happen | N/A |
| Security: The Federation Service could not satisfy a token request because the authentication type requirement for the relying party was not met. | Invalid Authentication Type | Suppress if the failures are with the same relying party and the same authentication type | N/A |
| Signature verification: The verification of the SAML message signature from message issuer failed. | SAML Request Signature Verification Error | Suppress if the failures are with the same message issuer | N/A |
| Signature verification: The artifact resolution service could not verify the request signature. | Artifact Resolution Service Signature Verification Error | Suppress if the same failures happen | N/A |
| WS-Trust request: The Federation Service encountered an error during an attempt to process the WS-Trust request. | WS-Trust Request Processing Error | N/A | No |

Token-Acceptance Failures Scenario

The monitors/rules in the following table monitor the token acceptance failures in the Federation Service and other warning events. Some of the failures will cause token issuance to fail as well.

| **Subscenario** | **Rule/monitor name** | **Alert suppression** | **Event counting** |
| --- | --- | --- | --- |
| Artifact resolution request: The claims provider trust does not have the SAML artifact resolution service endpoint configured. SAML artifact resolution failed. | Missing Artifact Resolution Service Endpoint | Suppress if the failures are with the same claims provider | N/A |
| Certificate: The token-signing certificate for the claims provider is not valid. | Claims Provider Signing Certificate Is Not Valid | Suppress if the failures are with the same claims provider and the same thumbprint | N/A |
| Certificate: Cannot find the certificate that is used to validate the token/message signature that was obtained from the claims provider. Token acceptance and token issuance failed. | Claims Provider Signing Certificate Cannot Be Found | Suppress if the failures are with the same claims provider | N/A |
| Certificate: The encryption certificate of the claims provider is not valid. SAML logout failed. | Claims Provider Encryption Certificate Is Not Valid | Suppress if the failures are with the same claims provider | N/A |
| Federation passive: An error occurred during the processing of the SAML logout request. | SAML Logout Error | Suppress if the failures are with the same logout initiator identity and caller identity | N/A |
| Federation passive: The SAML Single Logout request does not correspond to the logged-in session participant. | SAML Logout Name Identifier Not Found Error | Suppress if the failures are with the same requester and the same name identifier | N/A |
| Signature verification: Failed to verify the signature of the artifact response from claims provider. | Artifact Response Failed Signature Check | Suppress if the failures are with the same claims provider | N/A |
| Token reply detection: The SAML artifact resolution service encountered an error while trying to perform a token replay detection. Token replay detection failed. | Token Replay Detection Error | N/A | No |
| Token validation: The token issuer that the key identifies does not match any known claims provider trusts that have been configured for this Federation Service. | Unmatched Token Issuer | Suppress if the failures are with the same claims provider | N/A |
| Token validation: The NotBefore attribute for the token that was received has a value that is set to a future time that has not yet occurred. | Security Token Not Yet Valid Error | Suppress if the same failures happen | N/A |
| Token validation: The audience URI that is specified in the token does not match acceptable identifiers of this Federation Service. | Invalid Audience URI | Suppress if the same failures happen | N/A |
| Token validation: Token validation failed. | Security Token Validation Error | N/A | No |
| Token validation: A security token was rejected because the specified IssueInstant was before the allowed time period. | Invalid Issuance Instant Error | N/A | No |

Trust Management Failures Scenario

The monitors/rules in the following table monitor the trust management failures in the Federation Service and other warning events.

| **Subscenario** | **Rule/monitor name** | **Alert suppression** | **Event counting** |
| --- | --- | --- | --- |
| Auto-update: The automatic update of federation metadata for one or more trust configurations has been disabled while automatic monitoring has been enabled. Any future changes that are made in the partner organizations will no longer be committed automatically to the trust configurations on this Federation Service. | Automatic Update of the Trust Was Disabled | N/A | No |
| Auto-update: The trust monitoring service automatically updated the trust successfully with the partner's published changes. However, some metadata was ignored. | Successful Auto-Update with Warning | Suppress if the failures are with the same trust | N/A |
| Auto-update: The trust monitoring service detected changes in the federation metadata of the trust, but it did not apply the changes automatically on the trust partner. | Auto-Update Skipped with Warning | Suppress if the failures are with the same trust | N/A |
| Configuration database operation: The AD FS trust monitoring service encountered an error while writing to an object in the AD FS configuration database. | Trust Monitoring Write Error | N/A | If the same failure happens more than 3 times within 5 days |
| Configuration database operation: An error occurred during an attempt to read data that is stored in the AD FS configuration database. Trust monitoring was aborted temporarily, but another attempt will be made automatically based on the monitoring interval value that was set for all trusts. | Trust Monitoring Read Error | N/A | If the same failure happens more than 3 times within 5 days |
| Federation metadata: The Federation Service failed to retrieve the federation metadata document. | Trust Monitoring Retrieval Error | N/A | If the same failure happens more than 3 times within 5 days |
| Federation metadata: The Federation Service failed to create the federation metadata document. | Failed to Create Federation Metadata Document | N/A | No |
| Federation metadata: The Federation Service was unable to listen for requests to read the federation metadata document as the result of an unexpected error. | Error Listening for Federation Metadata Requests | N/A | No |
| Federation metadata: The trust monitoring service failed to read the federation metadata document. | Federation Metadata Parsing Error | N/A | If the same failure happens more than 3 times within 5 days |
| Federation metadata: The trust monitoring service failed to process the data in the metadata document. | Federation Metadata Processing Error | N/A | If the same failure happens more than 3 times within 5 days |
| Generic error: An error occurred during the monitoring for a trust. Trust monitoring was aborted temporarily, but another attempt will be made automatically based on the monitoring interval value that was set for all trusts. | Trust Monitoring Generic Error | N/A | If the same failure happens more than 3 times within 5 days |

Windows Internal Database (WID) Synchronization Failures Scenario

The monitors/rules in the following table monitor the Windows Internal Database (WID) synchronization failures on the federation server computer in the farm scenario.

| **Subscenario** | **Rule/monitor name** | **Alert suppression** | **Event counting** |
| --- | --- | --- | --- |
| Synchronization of the data that is stored on the primary federation server with the data on a secondary federation server did not occur. | AD FS Configuration Database Sync Error | N/A | If the same failures happen at least 3 times within 30 minutes |
| AD FS 2.0 detected that the Federation Service has more than 100 trusts configured and that the data in the AD FS configuration database for this Federation Service is stored and synchronized using the Windows Internal Database technology. | Synchronization Threshold Violation | Suppress if the same failures happen | N/A |

Certificate Management Failures Scenarios

The monitors/rules in the following table monitor the certificate management failures in the Federation Service.

| **Subscenario** | **Rule/monitor name** | **Alert suppression** | **Event counting** |
| --- | --- | --- | --- |
| The Federation Service failed to load additional certificates. | Additional Certificate Load Error | Suppress if the failures are with the same thumbprint | No |
| Certificate monitoring failed. | Certificate Monitoring Failure | N/A | No |

General Federation Server Failures Scenario

The monitors/rules in the following table monitor the startup failures and other operation or configuration failures on the federation server computer or in the Federation Service.

| **Subscenario** | **Rule/monitor name** | **Alert suppression** | **Event counting** |
| --- | --- | --- | --- |
| Certificate: The private key for the token-signing or token-decrypting certificate that is in the AD FS configuration database could not be accessed by the AD FS service account. | AD FS  Windows Service Failed to Start Because of a Private Key | N/A | No |
| Certificate: The certificate that is configured in the Federation Service configuration could not be found. The AD FS Windows Service failed to start. | AD FS Windows Service Failed to Start Because of Missing Certificate | N/A | No |
| Certificate: The certificate that is identified by the thumbprint could not be found in the certificate store of Localmachine "My" store. | Certificate Load Warning | Suppress if the failures are with the same certificate | No |
| Certificate: An error occurred during an attempt to build the certificate chain for the configuration certificate that is identified by the thumbprint.  | Certificate Validation Failure | Suppress if the failures are with the same thumbprint | No |
| Certificate: AD FS detected that one or more certificates in the AD FS configuration database must be updated manually because they are expired or will expire soon. | Configuration Has Expired Certificates Warning | N/A | No |
| Certificate: AD FS detected that one or more of your trusts require their certificates to be updated manually because they are expired or will expire soon. | Trusts Have Expired Certificates Warning | N/A | No |
| Certificate: The AD FS Windows Service failed to start because one of the configured certificates is not valid or has expired. | AD FS Windows Service Failed to Start Because of Invalid Certificate | N/A | No |
| Configuration: The required element in the AD FS service configuration file was missing. The AD FS Windows Service failed to start. | AD FS Windows Service Failed to Start Because of a Missing Configuration Value | N/A | No |
| Configuration: The federation server failed to refresh its cache. | Service Configuration Reload Error | N/A | If the failures happen at least 3 times within 1 hour |
| Configuration database: The AD FS configuration database that is stored in SQL Server is unavailable. | SQL Configuration Database Unavailable | N/A | No |
| Configuration database: The AD FS configuration database could not be loaded correctly. The AD FS Windows Service failed to start. | AD FS Windows Service Failed to Start Because of Configuration Load Error | N/A | No |
| Configuration database: Synchronization from the AD FS configuration database failed. | Synchronization from Configuration Database Failed | N/A | No |
| Configuration database: Failed to register notification to the SQL database with the connection string for the cache type. | SQL Notification Registration Error | N/A | No |
| Service: The AD FS Windows Service was stopped on the federation server. | AD FS Windows Service Stopped on the Federation Server | N/A | No |
| Service restart: An error occurred during an attempt to restart the subservice. | Service Host Restart Error | N/A | No |
| SPN registration: The SPN of the AD FS service account is not registered correctly in Active Directory. | SPN Not Registered | N/A | No |
| Unexpected exception: The Federation Service encountered an unexpected exception error that resulted in the AD FS Windows Service being stopped. | Unhandled Exception Error | N/A | No |

Device Registration Service

The monitors/rules in the following table monitor the health of the running status and privilege level checks for the Device Registration Service.

|  |  |  |  |
| --- | --- | --- | --- |
| Subscenario | Rule/monitor name | Alert suppression | Event counting |
| Service it is up and running. | Is DRS Service Running  | N/A | No |
| Error in the access rights to the audit when the Device Registration Service attempts to access it for the write operations | Insufficient privileges writing to audit log | N/A | No |

Known Issues

This section describes the known issues that are related to setting up the Active Directory Federation Services (AD FS) Management Pack. If you cannot set up the management pack properly, you may have to:

 Run the commands net stop healthservice and net start healthservice at a command prompt on the MOM computer in situations in which you have reimported the management pack.

 Disable IP version 6 (IPV6) on the agent computer that is running AD FS. For more information, see [How to disable certain Internet Protocol version 6 (IPv6) components in Windows Vista, Windows 7, and Windows Server 2008](http://go.microsoft.com/fwlink/?LinkID=192761).

Appendix: Scripts

The following table describes all the scripts that are included in the Active Directory Federation Services (AD FS) Management Pack.

| **Script** | **Purpose** | **Rule/Task** |
| --- | --- | --- |
| FederationServerDiscovery.ps1 | Runs on the federation server computer and checks for federation server discovery | Federation Server discovery |
| FederationServerRemoteSQLServerPing.ps1 | Runs on the federation server computer and does a network ping on the SQL Server computer that hosts the AD FS configuration database | SQL Configuration Database Unavailable |
| FederationServerSPNCheck.ps1 | Runs on the federation server and checks if the correct SPN is configured for the AD FS service account | SPN Not Registered |
| FederationServerMEXEndpointCheck.ps1 | Runs on the federation server computer and queries the MEX endpoint in the Federation Service | MEX Endpoint Is Unreachable |