



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

Accept

Reject

Manage cookies

Microsoft Ignite

Register now >

Nov 19–22, 2024



Learn

Discover >

Product documentation >

Development languages >

Topics >

Search Sign in

Microsoft Entra

Microsoft Entra ID

External ID

Global Secure Access

ID Governance

Permissions Management

More >

Admin center

Filter by title

Learn / Microsoft Entra / Microsoft Entra ID / Hybrid /



Connect sync reference

What is connect sync?

Tutorials

Concepts

How-to guides

Installation and upgrade

Plan and design

Manage Microsoft Entra Connect

Manage Pass-through authentication

Manage Federation Services

Managing federation with Microsoft Entra Connect

Multiple domain support for federating

Federate multiple instances of Microsoft Entra ID with single instance of AD FS

Renew federation certificates for M365 and Microsoft Entra ID

Update the SSL certificate for AD FS

Manage the AD FS trust with Microsoft Entra ID

Configure group claims for applications

Change hash algorithm for M365 RP

Use a SAML 2.0 server as your Idp

Emergency rotation of AD FS certificates

Monitor changes to federation configuration in your Microsoft Entra ID

Article • 11/06/2023 • 5 contributors

Feedback

In this article

[Set up alerts to monitor the trust relationship](#)

[Next steps](#)

When you federate your on-premises environment with Microsoft Entra ID, you establish a trust relationship between the on-premises identity provider and Microsoft Entra ID.

Due to this established trust, Microsoft Entra ID honors the security token issued by the on-premises identity provider post authentication, to grant access to resources protected by Microsoft Entra ID.

Therefore, it's critical that this trust (federation configuration) is monitored closely, and any unusual or suspicious activity is captured.

To monitor the trust relationship, we recommend you set up alerts to be notified when changes are made to the federation configuration.

Set up alerts to monitor the trust relationship

Follow these steps to set up alerts to monitor the trust relationship:

- > Manage Microsoft Entra Connect Health
- > Manage Microsoft Entra Connect Sync
- > Troubleshoot
- > Reference

 Download PDF

1. [Configure Microsoft Entra audit logs](#) to flow to an Azure Log Analytics Workspace.
2. [Create an alert rule](#) that triggers based on Microsoft Entra ID log query.
3. [Add an action group](#) to the alert rule that gets notified when the alert condition is met.

After the environment is configured, the data flows as follows:

1. Microsoft Entra logs are populated per the activity in the tenant.
2. The log information flows to the Azure Log Analytics workspace.
3. A background job from Azure Monitor executes the log query based on the configuration of the Alert Rule in the configuration step (2) above.

```
AuditLogs
| extend TargetResource = parse_json(TargetResources)
| where ActivityDisplayName contains "Set federation settings on domain" or Ac
| project TimeGenerated, SourceSystem, TargetResource[0].displayName, AADTenan
```

4. If the result of the query matches the alert logic (that is, the number of results is greater than or equal to 1), then the action group kicks in. Let's assume that it kicked in, so the flow continues in step 5.
5. Notification is sent to the action group selected while configuring the alert.

Note

In addition to setting up alerts, we recommend periodically reviewing the configured domains within your Microsoft Entra tenant and removing any stale, unrecognized, or suspicious domains.

Next steps

- [Integrate Microsoft Entra logs with Azure Monitor logs](#)
- [Create, view, and manage log alerts using Azure Monitor](#)
- [Manage AD FS trust with Microsoft Entra ID using Microsoft Entra Connect](#)
- [Best practices for securing Active Directory Federation Services](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

