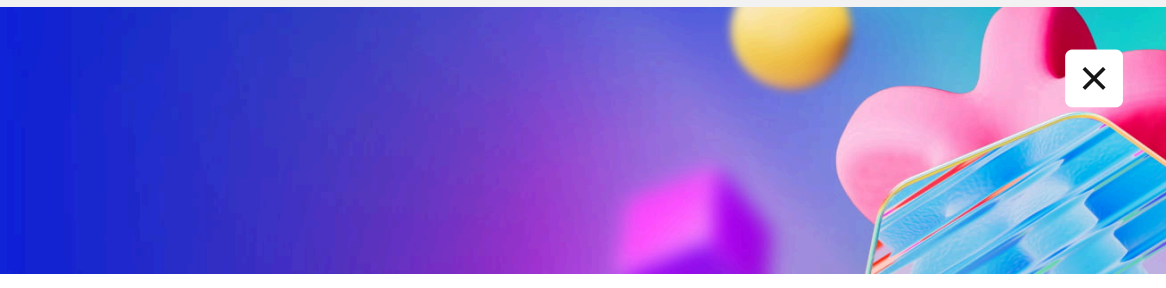

Security operations for infrastructure

Article • 10/23/2023 • 5 contributors

Feedback

In this article

Infrastructure has many components where vulnerabilities can occur if not properly configured. As part of your monitoring and alerting strategy for infrastructure, monitor and alert events in the following areas:

- Authentication and Authorization
- Hybrid Authentication components incl. Federation Servers
- Policies
- Subscriptions

Monitoring and alerting the components of your authentication infrastructure is critical. Any compromise can lead to a full compromise of the whole environment. Many enterprises that use Microsoft Entra ID operate in a hybrid authentication environment. Cloud and on-premises components should be included in your monitoring and alerting strategy. Having a hybrid authentication environment also introduces another attack vector to your environment.

We recommend all the components be considered Control Plane / Tier 0 assets, and the accounts used to manage them. Refer to Securing privileged assets (SPA) for guidance on designing and implementing your environment. This guidance includes recommendations for each of the hybrid authentication components that could potentially be used for a Microsoft Entra tenant.

A first step in being able to detect unexpected events and potential attacks is to establish a baseline. For all on-premises components listed in this article, see Privileged access deployment, which is part of the Securing privileged assets (SPA) guide.

Where to look

The log files you use for investigation and monitoring are:

- Microsoft Entra audit logs
- Sign-in logs
- Microsoft 365 Audit logs
- Azure Key Vault logs

From the Azure portal, you can view the Microsoft Entra audit logs and download as comma separated value (CSV) or JavaScript Object Notation (JSON) files. The Azure portal has several ways to integrate Microsoft Entra logs with other tools that allow for greater automation of monitoring and alerting:

- **Microsoft Sentinel** – Enables intelligent security analytics at the enterprise level by providing security information and event management (SIEM) capabilities.
- **Sigma rules** - Sigma is an evolving open standard for writing rules and templates that automated management tools can use to parse log files. Where Sigma templates exist for our recommended search criteria, we've added a link to the Sigma repo. The Sigma templates aren't written, tested, and managed by Microsoft. Rather, the repo and templates are created and collected by the worldwide IT security community.
- **Azure Monitor** – Enables automated monitoring and alerting of various conditions. Can create or use workbooks to combine data from different sources.
- **Azure Event Hubs** integrated with a SIEM - Microsoft Entra logs can be integrated to other SIEMs such as Splunk, ArcSight, QRadar and Sumo Logic via the Azure Event Hubs integration.
- **Microsoft Defender for Cloud Apps** – Enables you to discover and manage apps, govern across apps and resources, and check your cloud apps' compliance.
- **Securing workload identities with Microsoft Entra ID Protection** - Used to detect risk on workload identities across sign-in behavior and offline indicators of compromise.

The remainder of this article describes what to monitor and alert on. It is organized by the type of threat. Where there are pre-built solutions, you'll find links to them, after the table. Otherwise, you can build alerts using the preceding tools.

Authentication infrastructure

In hybrid environments that contain both on-premises and cloud-based resources and accounts, the Active Directory infrastructure is a key part of the authentication stack. The stack is also a target for attacks so must be configured to maintain a secure environment and must be monitored properly. Examples of current types of attacks used against your authentication infrastructure use Password Spray and Solorigate techniques. The following are links to articles we recommend:

- Securing privileged access overview – This article provides an overview of current techniques using Zero Trust techniques to create and maintain secure privileged access.
- Microsoft Defender for Identity monitored domain activities - This article provides a comprehensive list of activities to monitor and set alerts for.
- Microsoft Defender for Identity security alert tutorial - This article provides guidance on creating and implementing a security alert strategy.

The following are links to specific articles that focus on monitoring and alerting your authentication infrastructure:

- Understand and use Lateral Movement Paths with Microsoft Defender for Identity - Detection techniques to help identify when non-sensitive accounts are used to gain access to sensitive network accounts.
- Working with security alerts in Microsoft Defender for Identity - This article describes how to review and manage alerts after they're logged.

The following are specific things to look for:

Expand table

What to monitor	Risk level	Where	Notes
Extranet lockout trends	High	Microsoft Entra Connect Health	See, Monitor AD FS using Microsoft Entra Connect Health for tools and techniques to help detect extranet lock-out trends.
Failed sign-ins	High	Connect Health Portal	Export or download the Risky IP report and follow the guidance at Risky IP report (public preview) for next steps.

In privacy compliant	Low	Microsoft Entra Connect Health	Configure Microsoft Entra Connect Health to disable data collections and monitoring using the User privacy and Microsoft Entra Connect Health article.
Potential brute force attack on LDAP	Medium	Microsoft Defender for Identity	Use sensor to help detect potential brute force attacks against LDAP.
Account enumeration reconnaissance	Medium	Microsoft Defender for Identity	Use sensor to help perform account enumeration reconnaissance.
General correlation between Microsoft Entra ID and Azure AD FS	Medium	Microsoft Defender for Identity	Use capabilities to correlate activities between your Microsoft Entra ID and Azure AD FS environments.

Pass-through authentication monitoring

Microsoft Entra pass-through authentication signs users in by validating their passwords directly against on-premises Active Directory.

The following are specific things to look for:

Expand table

What to monitor	Risk level	Where	Filter/sub-filter	Notes
Microsoft Entra pass-through authentication errors	Medium	Application and Service Logs\Microsoft\AzureAdConnect\AuthenticationAgent\Admin	AADSTS80001 – Unable to connect to Active Directory	Ensure t agent se member same AI as the u whose p need to validate they car to Activ Director
Microsoft Entra pass-through authentication errors	Medium	Application and Service Logs\Microsoft\AzureAdConnect\AuthenticationAgent\Admin	AADSTS8002 - A timeout occurred connecting to Active Directory	Check t that Act Director available respond requests the ager
Microsoft Entra pass-through authentication errors	Medium	Application and Service Logs\Microsoft\AzureAdConnect\AuthenticationAgent\Admin	AADSTS80004 - The username passed to the agent was not valid	Ensure t is attem sign in v right us
Microsoft Entra pass-through authentication errors	Medium	Application and Service Logs\Microsoft\AzureAdConnect\AuthenticationAgent\Admin	AADSTS80005 - Validation encountered unpredictable WebException	A transi Retry th request. continue contact support
Microsoft Entra pass-through authentication errors	Medium	Application and Service Logs\Microsoft\AzureAdConnect\AuthenticationAgent\Admin	AADSTS80007 - An error occurred communicating with Active Directory	Check th logs for informat verify th Director operatin expecte
Microsoft Entra pass-through authentication errors	High	Win32 LogonUserA function API	Log on events 4624(s): An account was successfully logged on - correlate with –	Use with suspecte usernam the dom controlle authent requests

			4625(F): An account failed to log on	Guidanc LogonU function (winbase
Microsoft Entra pass-through authentication errors	Medium	PowerShell script of domain controller	See the query after the table.	Use the informat Microso Connect Troubles Pass-thr Authent guidanc

Kusto Copy

```
<QueryList>

<Query Id="0" Path="Security">

<Select Path="Security">*[EventData[Data[@Name='ProcessName'] and (Data='C:\Program Files

</Query>

</QueryList>
```

Monitoring for creation of new Microsoft Entra tenants

Organizations might need to monitor for and alert on the creation of new Microsoft Entra tenants when the action is initiated by identities from their organizational tenant. Monitoring for this scenario provides visibility on how many tenants are being created and could be accessed by end users.

Expand table

What to monitor	Risk level	Where	Filter/sub-filter	Notes
Creation of a new Microsoft Entra tenant, using an identity from your tenant.	Medium	Microsoft Entra audit logs	Category: Directory Management Activity: Create Company	Target(s) shows the created TenantID

Private network connector

Microsoft Entra ID and Microsoft Entra application proxy give remote users a single sign-on (SSO) experience. Users securely connect to on-premises apps without a virtual private network (VPN) or dual-homed servers and firewall rules. If your Microsoft Entra private network connector server is compromised, attackers could alter the SSO experience or change access to published applications.

To configure monitoring for Application Proxy, see Troubleshoot Application Proxy problems and error messages. The data file that logs information can be found in Applications and Services Logs\Microsoft\Microsoft Entra private network\Connector\Admin. For a complete reference guide to audit activity, see Microsoft Entra audit activity reference. Specific things to monitor:

Expand table

What to monitor	Risk level	Where	Filter/sub-filter	Notes
Kerberos errors	Medium	Various tools	Medium	Kerberos authentication error guidance under Kerberos errors on Troubleshoot Application Proxy problems and error messages.
DC security issues	High	DC Security Audit logs	Event ID 4742(S): A computer account was changed -and- Flag – Trusted for Delegation	Investigate any flag change.

			-or- Flag – Trusted to Authenticate for Delegation	
Pass-the-ticket like attacks	High			Follow guidance in: Security principal reconnaissance (LDAP) (external ID 2038) Tutorial: Compromised credential alerts Understand and use Lateral Movement Paths with Microsoft Defender for Identity Understanding entity profiles

Legacy authentication settings

For multifactor authentication (MFA) to be effective, you also need to block legacy authentication. You then need to monitor your environment and alert on any use of legacy authentication. Legacy authentication protocols like POP, SMTP, IMAP, and MAPI can't enforce MFA. This makes these protocols the preferred entry points for attackers. For more information on tools that you can use to block legacy authentication, see New tools to block legacy authentication in your organization.

Legacy authentication is captured in the Microsoft Entra sign-in log as part of the detail of the event. You can use the Azure Monitor workbook to help with identifying legacy authentication usage. For more information, see Sign-ins using legacy authentication, which is part of How to use Azure Monitor Workbooks for Microsoft Entra reports. You can also use the Insecure protocols workbook for Microsoft Sentinel. For more information, see Microsoft Sentinel Insecure Protocols Workbook Implementation Guide. Specific activities to monitor include:

Expand table

What to monitor	Risk level	Where	Filter/sub-filter	Notes
Legacy authentications	High	Microsoft Entra sign-in log	ClientApp : POP ClientApp : IMAP ClientApp : MAPI ClientApp: SMTP ClientApp : ActiveSync go to EXO Other Clients = SharePoint and EWS	In federated domain environments, failed authentications aren't recorded and don't appear in the log.

Microsoft Entra Connect

Microsoft Entra Connect provides a centralized location that enables account and attribute synchronization between your on-premises and cloud-based Microsoft Entra environment. Microsoft Entra Connect is the Microsoft tool designed to meet and accomplish your hybrid identity goals. It provides the following features:

- Password hash synchronization - A sign-in method that synchronizes a hash of a user's on-premises AD password with Microsoft Entra ID.
- Synchronization - Responsible for creating users, groups, and other objects. And, making sure identity information for your on-premises users and groups matches the cloud. This synchronization also includes password hashes.
- Health Monitoring - Microsoft Entra Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity.

Synchronizing identity between your on-premises environment and your cloud environment introduces a new attack surface for your on-premises and cloud-based environment. We recommend:

- You treat your Microsoft Entra Connect primary and staging servers as Tier 0 Systems in your control plane.
- You follow a standard set of policies that govern each type of account and its usage in your environment.

- You install Microsoft Entra Connect and Connect Health. These primarily provide operational data for the environment.

Logging of Microsoft Entra Connect operations occurs in different ways:

- The Microsoft Entra Connect wizard logs data to `\ProgramData\AADConnect`. Each time the wizard is invoked, a timestamped trace log file is created. The trace log can be imported into Sentinel or other 3rd party security information and event management (SIEM) tools for analysis.
- Some operations initiate a PowerShell script to capture logging information. To collect this data, you must make sure script block logging in enabled.

Monitoring configuration changes

Microsoft Entra ID uses Microsoft SQL Server Data Engine or SQL to store Microsoft Entra Connect configuration information. Therefore, monitoring and auditing of the log files associated with configuration should be included in your monitoring and auditing strategy. Specifically, include the following tables in your monitoring and alerting strategy.

Expand table

What to monitor	Where	Notes
mms_management_agent	SQL service audit records	See SQL Server Audit Records
mms_partition	SQL service audit records	See SQL Server Audit Records
mms_run_profile	SQL service audit records	See SQL Server Audit Records
mms_server_configuration	SQL service audit records	See SQL Server Audit Records
mms_synchronization_rule	SQL service audit records	See SQL Server Audit Records

For information on what and how to monitor configuration information refer to:

- For SQL server, see SQL Server Audit Records.
- For Microsoft Sentinel, see Connect to Windows servers to collect security events.
- For information on configuring and using Microsoft Entra Connect, see What is Microsoft Entra Connect?

Monitoring and troubleshooting synchronization

One function of Microsoft Entra Connect is to synchronize hash synchronization between a user's on-premises password and Microsoft Entra ID. If passwords aren't synchronizing as expected, the synchronization might affect a subset of users or all users. Use the following to help verify proper operation or troubleshoot issues:

- Information for checking and troubleshooting hash synchronization, see Troubleshoot password hash synchronization with Microsoft Entra Connect Sync.
- Modifications to the connector spaces, see Troubleshoot Microsoft Entra Connect objects and attributes.

Important resources on monitoring

Expand table

What to monitor	Resources
Hash synchronization validation	See Troubleshoot password hash synchronization with Microsoft Entra Connect Sync
Modifications to the connector spaces	see Troubleshoot Microsoft Entra Connect objects and attributes
Modifications to rules you configured	Monitor changes to: filtering, domain and OU, attribute, and group-based changes
SQL and MSDE changes	Changes to logging parameters and addition of custom functions

Monitor the following:

Expand table

What to monitor	Risk level	Where	Filter/sub-filter	Notes
Scheduler changes	High	PowerShell	Set-ADSyncScheduler	Look for modifications to schedule
Changes to scheduled tasks	High	Microsoft Entra audit logs	Activity = 4699(S): A scheduled task was deleted -or- Activity = 4701(s): A scheduled task was disabled -or- Activity = 4702(s): A scheduled task was updated	Monitor all

- For more information on logging PowerShell script operations, see Enabling Script Block Logging, which is part of the PowerShell reference documentation.
- For more information on configuring PowerShell logging for analysis by Splunk, refer to Get Data into Splunk User Behavior Analytics.

Monitoring seamless single sign-on

Microsoft Entra seamless single sign-on (Seamless SSO) automatically signs in users when they are on their corporate desktops that are connected to your corporate network. Seamless SSO provides your users with easy access to your cloud-based applications without other on-premises components. SSO uses the pass-through authentication and password hash synchronization capabilities provided by Microsoft Entra Connect.

Monitoring single sign-on and Kerberos activity can help you detect general credential theft attack patterns. Monitor using the following information:

Expand table

What to monitor	Risk level	Where	Filter/sub-filter	Notes
Errors associated with SSO and Kerberos validation failures	Medium	Microsoft Entra sign-in log		Single sign-on list of error codes at Single sign-on.
Query for troubleshooting errors	Medium	PowerShell	See query following table. check in each forest with SSO enabled.	Check in each forest with SSO enabled.
Kerberos-related events	High	Microsoft Defender for Identity monitoring		Review guidance available at Microsoft Defender for Identity Lateral Movement Paths (LMPs)

Kusto Copy

```
<QueryList>

<Query Id="0" Path="Security">

<Select Path="Security">*[EventData[Data[@Name='ServiceName'] and (Data='AZUREADSSOACC$')

</Query>

</QueryList>
```

Password protection policies

If you deploy Microsoft Entra Password Protection, monitoring and reporting are essential tasks. The following links provide details to help you understand various monitoring techniques, including where each service logs information and how to report on the use of Microsoft Entra Password Protection.

The domain controller (DC) agent and proxy services both log event log messages. All PowerShell cmdlets described below are only available on the proxy server (see the AzureADPasswordProtection PowerShell

module). The DC agent software doesn't install a PowerShell module.

Detailed information for planning and implementing on-premises password protection is available at Plan and deploy on-premises Microsoft Entra Password Protection. For monitoring details, see Monitor on-premises Microsoft Entra Password Protection. On each domain controller, the DC agent service software writes the results of each individual password validation operation (and other status) to the following local event log:

- \Applications and Services Logs\Microsoft\AzureADPasswordProtection\DCAgent\Admin
- \Applications and Services Logs\Microsoft\AzureADPasswordProtection\DCAgent\Operational
- \Applications and Services Logs\Microsoft\AzureADPasswordProtection\DCAgent\Trace

The DC agent Admin log is the primary source of information for how the software is behaving. By default, the Trace log is off and must be enabled before data is logged. To troubleshoot application proxy problems and error messages, detailed information is available at Troubleshoot Microsoft Entra application proxy. Information for these events is logged in:

- Applications and Services Logs\Microsoft\Microsoft Entra private network\Connector\Admin
- Microsoft Entra audit log, Category Application Proxy

Complete reference for Microsoft Entra audit activities is available at Microsoft Entra audit activity reference.

Conditional Access

In Microsoft Entra ID, you can protect access to your resources by configuring Conditional Access policies. As an IT administrator, you want to ensure your Conditional Access policies work as expected to ensure that your resources are protected. Monitoring and alerting on changes to the Conditional Access service ensures policies defined by your organization for access to data are enforced. Microsoft Entra logs when changes are made to Conditional Access and also provides workbooks to ensure your policies are providing the expected coverage.

Workbook Links

- Conditional Access insights and reporting
- Conditional Access gap analysis workbook

Monitor changes to Conditional Access policies using the following information:

Expand table

What to monitor	Risk level	Where	Filter/sub-filter	Notes
New Conditional Access Policy created by non-approved actors	Medium	Microsoft Entra audit logs	Activity: Add Conditional Access policy Category: Policy Initiated by (actor): User Principal Name	Monitor and alert on Conditional Access changes. Is Initiated by (actor): approved to make changes to Conditional Access? Microsoft Sentinel template Sigma rules
Conditional Access Policy removed by non-approved actors	Medium	Microsoft Entra audit logs	Activity: Delete Conditional Access policy Category: Policy Initiated by (actor): User Principal Name	Monitor and alert on Conditional Access changes. Is Initiated by (actor): approved to make changes to Conditional Access? Microsoft Sentinel template Sigma rules

Conditional Access Policy updated by non-approved actors	Medium	Microsoft Entra audit logs	Activity: Update Conditional Access policy Category: Policy Initiated by (actor): User Principal Name	Monitor and alert on Conditional Access changes. Is Initiated by (actor): approved to make changes to Conditional Access? Review Modified Properties and compare “old” vs “new” value Microsoft Sentinel template Sigma rules
Removal of a user from a group used to scope critical Conditional Access policies	Medium	Microsoft Entra audit logs	Activity: Remove member from group Category: GroupManagement Target: User Principal Name	Montior and Alert for groups used to scope critical Conditional Access Policies. "Target" is the user that has been removed. Sigma rules
Addition of a user to a group used to scope critical Conditional Access policies	Low	Microsoft Entra audit logs	Activity: Add member to group Category: GroupManagement Target: User Principal Name	Montior and Alert for groups used to scope critical Conditional Access Policies. "Target" is the user that has been added. Sigma rules

Next steps

Microsoft Entra security operations overview

Security operations for user accounts

Security operations for consumer accounts

Security operations for privileged accounts

Security operations for Privileged Identity Management

Security operations for applications

Security operations for devices

Feedback

Was this page helpful? Yes No

Provide product feedback

Additional resources

Training

Module
Plan, implement, and administer Conditional Access - Training

Conditional Access gives a fine granularity of control over which users can do specific activities, access which resources, and how to ensure data and systems are safe.

Certification
Microsoft Certified: Identity and Access Administrator Associate - Certifications

Demonstrate the features of Microsoft Entra ID to modernize identity solutions, implement hybrid solutions, and implement identity governance.