Microsoft Entra security operations for devices

Article • 10/23/2023 • 6 contributors

Feedback

In this article

Devices aren't commonly targeted in identity-based attacks, but *can* be used to satisfy and trick security controls, or to impersonate users. Devices can have one of four relationships with Microsoft Entra ID:

- Unregistered
- Microsoft Entra registered
- Microsoft Entra joined
- Microsoft Entra hybrid joined

Registered and joined devices are issued a Primary Refresh Token (PRT), which can be used as a primary authentication artifact, and in some cases as a multifactor authentication artifact. Attackers may try to register their own devices, use PRTs on legitimate devices to access business data, steal PRT-based tokens from legitimate user devices, or find misconfigurations in device-based controls in Microsoft Entra ID. With Microsoft Entra hybrid joined devices, the join process is initiated and controlled by administrators, reducing the available attack methods.

For more information on device integration methods, see Choose your integration methods in the article Plan your Microsoft Entra device deployment.

To reduce the risk of bad actors attacking your infrastructure through devices, monitor

- Device registration and Microsoft Entra join
- Non-compliant devices accessing applications
- BitLocker key retrieval
- Device administrator roles
- Sign-ins to virtual machines

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.

Much of what you'll monitor and alert on are the effects of your Conditional Access policies. You can use the Conditional Access insights and reporting workbook to examine the effects of one or more Conditional Access policies on your sign-ins, and the results of policies including device state. This workbook enables you to view a summary, and identify the effects over a specific time period. You can also use the workbook to investigate the sign-ins of a specific user.

The rest of this article describes what we recommend you monitor and alert on, and is organized by the type of threat. Where there are specific pre-built solutions we link to them or provide samples following the table. Otherwise, you can build alerts using the preceding tools.

Device registrations and joins outside policy

Microsoft Entra registered and Microsoft Entra joined devices possess primary refresh tokens (PRTs), which are the equivalent of a single authentication factor. These devices can at times contain strong authentication claims. For more information on when PRTs contain strong authentication claims, see When does a PRT get an MFA claim? To keep bad actors from registering or joining devices, require multi-factor authentication (MFA) to register or join devices. Then monitor for any devices registered or joined without MFA. You'll also need to watch for changes to MFA settings and policies, and device compliance policies.

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Device registration or join completed without MFA	Medium	Sign-in logs	Activity: successful authentication to Device Registration Service. And No MFA required	Alert when: Any device registered or joined without MFA Microsoft Sentinel template Sigma rules
Changes to the Device Registration MFA toggle in Microsoft Entra ID	High	Audit log	Activity: Set device registration policies	Look for: The toggle being set to off. There isn't audit log entry. Schedule periodic checks. Sigma rules
Changes to Conditional Access policies requiring domain joined or compliant device.	High	Audit log	Changes to Conditional Access policies	Alert when: Change to any policy requiring domain joined or compliant, changes to trusted locations, or accounts or devices added to MFA policy exceptions.

You can create an alert that notifies appropriate administrators when a device is registered or joined without MFA by using Microsoft Sentinel.

```
SigninLogs
| where ResourceDisplayName == "Device Registration Service"
| where ConditionalAccessStatus == "success"
| where AuthenticationRequirement <> "multiFactorAuthentication"
```

You can also use Microsoft Intune to set and monitor device compliance policies.

Non-compliant device sign-in

It might not be possible to block access to all cloud and software-as-a-service applications with Conditional Access policies requiring compliant devices.

Mobile device management (MDM) helps you keep Windows 10 devices compliant. With Windows version 1809, we released a security baseline of policies. Microsoft Entra ID can integrate with MDM to enforce device compliance with corporate policies, and can report a device's compliance status.

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Sign-ins by non-compliant devices	High	Sign-in logs	DeviceDetail.isCompliant == false	If requiring sign-in from compliant devices, alert when: any sign in by non-compliant devices, or any access without MFA or a trusted location. If working toward requiring devices, monitor for suspicious sign-ins. Sigma rules
Sign-ins by unknown devices	Low	Sign-in logs	DeviceDetail is empty, single factor authentication, or from a non-trusted location	Look for: any access from out of compliance devices, any access without MFA or trusted location Microsoft Sentinel template Sigma rules

Use LogAnalytics to query

Sign-ins by non-compliant devices

```
SigninLogs
| where DeviceDetail.isCompliant == false
| where ConditionalAccessStatus == "success"
```

Sign-ins by unknown devices

```
SigninLogs
| where isempty(DeviceDetail.deviceId)
| where AuthenticationRequirement == "singleFactorAuthentication"
```

```
| where ResultType == "0"
| where NetworkLocationDetails == "[]"
```

Stale devices

Stale devices include devices that haven't signed in for a specified time period. Devices can become stale when a user gets a new device or loses a device, or when a Microsoft Entra joined device is wiped or reprovisioned. Devices might also remain registered or joined when the user is no longer associated with the tenant. Stale devices should be removed so the primary refresh tokens (PRTs) cannot be used.

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Last sign-in date	Low	Graph API	approximateLastSignInDateTime	Use Graph API or PowerShell to identify and remove stale devices.

BitLocker key retrieval

Attackers who have compromised a user's device may retrieve the BitLocker keys in Microsoft Entra ID. It's uncommon for users to retrieve keys, and should be monitored and investigated.

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Key retrieval	Medium	Audit logs	OperationName == "Read BitLocker key"	Look for: key retrieval, other anomalous behavior by users retrieving keys. Microsoft Sentinel template Sigma rules

In LogAnalytics create a query such as

```
AuditLogs
| where OperationName == "Read BitLocker key"
```

Device administrator roles

The Microsoft Entra Joined Device Local Administrator and the Global Administrator roles automatically get local administrator rights on all Microsoft Entra joined devices. It's important to monitor who has these rights to keep your environment safe.

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Users added to global or device admin roles	High	Audit logs	Activity type = Add member to role.	Look for: new users added to these Microsoft Entra roles, subsequent anomalous behavior by machines or users. Microsoft Sentinel template Sigma rules

Non-Azure AD sign-ins to virtual machines

Sign-ins to Windows or LINUX virtual machines (VMs) should be monitored for sign-ins by accounts other than Microsoft Entra accounts.

Microsoft Entra sign-in for LINUX

Microsoft Entra sign-in for LINUX allows organizations to sign in to their Azure LINUX VMs using Microsoft Entra accounts over secure shell protocol (SSH).

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Non-Azure AD account signing in, especially over SSH	High	Local authentication logs	Ubuntu: monitor /var/log/auth.log for SSH use RedHat: monitor /var/log/sssd/ for SSH use	Look for: entries where non-Azure AD accounts are successfully connecting to VMs. See following example.

Ubuntu example:

May 9 23:49:39 ubuntu1804 aad_certhandler[3915]: Version: 1.0.015570001; user: localusertest01

May 9 23:49:39 ubuntu1804 aad_certhandler[3915]: User 'localusertest01' is not a Microsoft Entra user; returning empty result.

May 9 23:49:43 ubuntu1804 aad_certhandler[3916]: Version: 1.0.015570001; user: localusertest01

May 9 23:49:43 ubuntu1804 aad_certhandler[3916]: User 'localusertest01' is not a Microsoft Entra user; returning empty result.

May 9 23:49:43 ubuntu1804 sshd[3909]: Accepted publicly for localusertest01 from 192.168.0.15 port 53582 ssh2: RSA SHA256:MiROf6f9u1w8J+46AXR1WmPjDhNWJEoXp4HMm9lvJAQ

May 9 23:49:43 ubuntu1804 sshd[3909]: pam_unix(sshd:session): session opened for user localusertest01 by (uid=0).

You can set policy for LINUX VM sign-ins, and detect and flag Linux VMs that have non-approved local accounts added. To learn more, see using Azure Policy to ensure standards and assess compliance.

Microsoft Entra sign-ins for Windows Server

Microsoft Entra sign-in for Windows allows your organization to sign in to your Azure Windows 2019+ VMs using Microsoft Entra accounts over remote desktop protocol (RDP).

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Non-Azure AD account sign-in, especially over RDP	High	Windows Server event logs	Interactive Login to Windows VM	Event 528, log-on type 10 (RemoteInteractive). Shows when a user signs in over Terminal Services or Remote Desktop.

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 infrastructure

Feedback

Was this page helpful? Yes No

Provide product feedback

Additional resources

Training

Module
Monitor and maintain Microsoft Entra ID - Training

Audit and diagnostic logs within Microsoft Entra ID provide a rich view into how users are accessing your Azure solution. Learn to monitor, troubleshoot, and analyze sign-in data.

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.