CIS Microsoft Intune MDM Service Desktop & Mobile STIG Benchmark

v1.0.0 – 04-22-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

Microsoft Intune MDM Service Desktop & Mobile Secure Technical Implementation Guide (STIG)
Version: 1 Release: 1 Benchmark
Date: 22 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Intune MDM Service Desktop & Mobile and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Microsoft Intune MDM Service Desktop & Mobile

Recommendations

1 STIG RULES

Microsoft Intune MDM

Microsoft Intune MDM Service Desktop & Mobile Secure Technical Implementation Guide (STIG)

Version: 1 Release: 1 Benchmark

Date: 22 Apr 2025

CLASSIFICATION unclassified

1.1 MSIN-25-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Microsoft Intune service must initiate a session lock after a 15-minute period of inactivity.

```
GROUP ID: V-273867
RULE ID: SV-273867r1101448
```

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their application session prior to vacating the vicinity, applications need to be able to identify when a user's application session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled. This is typically at the operating system level and results in a system lock but may be at the application level where the application interface window is secured instead.

Satisfies: SRG-APP-000003-UEM-000003, SRG-APP-000295-UEM-000169

Audit:

To verify the inactivity timeout is configured for 15 minutes or less, follow the steps outlined below:

1. Sign in to portal.office365.com (or .us if the user is a GCCH or DOD tenant).
2. Navigate to Admin >> Settings >> Org Settings >> Security and Privacy (tab on top of page) >> Idle Session Timeout.
3. Select the check box to enable "Turn on to set the period of inactivity".
4. Select custom option, then verify it has been set to 15.

If the inactivity timeout is not set to 15 minutes or less, this is a finding.

Remediation:

Sign in to portal.office365.com (or .us if the user is a GCCH or DOD tenant).

1. Navigate to Admin >> Settings >> Org Settings >> Security and Privacy (tab on top of page) >> Idle Session Timeout.
2. Select the check box to enable "Turn on to set the period of inactivity".
3. Select custom option, then enter "15".
4. Select "Save".

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

1.2 MSIN-25-000370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Microsoft Intune service must be configured to transfer Intune logs to another server for storage, analysis, and reporting at least every seven days.

```
GROUP ID: V-273868
RULE ID: SV-273868r1101588
```

Rationale:

Note: UEM server logs include logs of UEM events and logs transferred to Microsoft Intune service by UEM agents of managed devices.

Protection of log data includes ensuring log data is not accidentally lost or deleted. Backing up audit records to a different system or onto separate media than the system being audited on an organizationally defined frequency helps ensure, in the event of a catastrophic system failure, the audit records will be retained.

This helps to ensure a compromise of the information system being audited does not also result in a compromise of the audit records.

This requirement only applies to applications that have a native backup capability for audit records. Operating system backup requirements cover applications that do not provide native backup functions.

Satisfies: SRG-APP-000125-UEM-000074, SRG-APP-000275-UEM-000157, SRG-APP-000358-UEM-000228

Audit:

Verify the site has configured Intune to off-load Intune logs to a third-party log management server or to an Azure log storage and monitoring service like Azure monitor. Verification procedures are determined by the method used at the site. Ask the site Intune Administrator how logs are managed by the site and demonstrate that Intune logs are being off-loaded.
If site is off-loading Intune logs to the Azure monitor, do the following (refer to https://learn.microsoft.com/en-us/mem/intune-service/fundamentals/review-logs-using-azure-monitor):

1. Sign in to the Microsoft Intune admin center.
2. Select Reports >> Diagnostics settings.
3. Verify logs are being sent to the Azure monitor:
   a. A storage account has been configured.
   b. A Stream has been configured to stream logs to the Azure Event Hubs.
   c. Intune logs have been configured to be sent to Log Analytics.

If the site is not transferring Intune audit logs to a third-party audit log management server or to an Azure audit log storage and monitoring service, this is a finding.

Remediation:

There are many methods for off-loading Intune logs, including downloading to a third-party log management server and sending logs to Azure Storage, Event Hubs, or Log Analytics, which are all part of Diagnostics Settings in Intune. Procedures will vary depending on which log management process is used at the site.
If the site is sending logs to Azure Monitor, follow the setup procedures found here: https://learn.microsoft.com/en-us/mem/intune-service/fundamentals/review-logs-using-azure-monitor

1. Sign in to the Microsoft Intune admin center.
2. Select Reports >> Diagnostics settings. The first time opening it, turn it on. Otherwise, add a setting.
   If the Azure subscription is not shown, navigate to the top right corner, select the signed in account, and choose "Switch directory". Enter the Azure subscription account, if necessary.
3. Enter the following properties:

- Name: Enter a name for the diagnostic settings. This setting includes all the properties entered. For example, enter Route audit logs to storage account.
- Archive to a storage account: Saves the log data to an Azure Storage account. To save or archive the data, choose this option, then select "Configure". Choose an existing storage account from the list, then click "OK".
- Stream to an event hub: Streams the logs to Azure Event Hubs. To have analytics on log data using SIEM tools such as Splunk and QRadar, choose this option, then select "Configure". Choose an existing Event Hubs namespace and policy from the list, then click "OK".
- Send to Log Analytics: Sends the data to Azure Log Analytics. To use visualizations, monitoring and alerting for logs, choose this option, then select "Configure". Create a new workspace and enter the workspace details or choose an existing workspace from the list, then click "OK".
- LOG > AuditLogs: Choose this option to send the Intune audit logs to the storage account, Event Hubs, or Log Analytics. The audit logs show the history of every task that generates a change in Intune, including who did it and when. For more information, go to IntuneAuditLogs.
  Note: If using a storage account, enter how many days to keep the data (retention). To keep data forever, set Retention (days) to "0".
- LOG > OperationalLogs: Operational logs show the success or failure of users and devices that enroll in Intune, and details on noncompliant devices. Choose this option to send the enrollment logs to the storage account, Event Hubs, or Log Analytics. For more information, go to IntuneOperationalLogs.
  To use a storage account, enter how many days to keep the data (retention). To keep data forever, set Retention (days) to "0".
- LOG > DeviceComplianceOrg: Device compliance organizational logs show the organizational report for Device Compliance in Intune and details of noncompliant devices. Choose this option to send the compliance logs to the storage account, Event Hubs, or Log Analytics. For more information, go to

IntuneDeviceComplianceOrg.
To use a storage account, enter how many days to keep the data (retention). To keep data forever, set Retention (days) to "0".

- LOG > IntuneDevices: The Intune Device log shows device inventory and status information for Intune enrolled and managed devices. Choose this option to send the IntuneDevices logs to your storage account, Event Hubs, or Log Analytics. For more reference information, go to IntuneDevices.
  Note: To use a storage account, enter how many days to keep the data (retention). To keep data forever, set Retention (days) to "0".

4. Save the changes. The setting is shown in the list. Once the settings are created, settings can be changed by selecting Edit setting >> Save.

Additional Information:

CCI-001348 Store audit records on an organization-defined frequency in a repository that is part of a physically different system or system component than the system or component being audited.

- NIST SP 800-53::AU-9 (2)
- NIST SP 800-53A::AU-9 (2).1 (iii)
- NIST SP 800-53 Revision 4::AU-9 (2)
- NIST SP 800-53 Revision 5::AU-9 (2)

CCI-001294 Alert organization-defined personnel or roles of failed security verification tests.

- NIST SP 800-53::SI-6 (1)
- NIST SP 800-53A::SI-6 (1).1
- NIST SP 800-53 Revision 4::SI-6 c
- NIST SP 800-53 Revision 5::SI-6 c

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	MSIN-25-000030 (Manual)	☐	☐
1.2	MSIN-25-000370 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 28, 2025	1.0.0	Initial CIS Release