# Microsoft Intune Policy Deployment Model

The following outlines the 2 models of deploying the DISA Quarterly STIG Microsoft Intune Device Configurations profile to assist an administrator in their individual tenant. This document is not intended to be an implementation guide. It is intended to provide details of Intune policies contained within the package and how these policies can be leveraged to meet STIG requirements on managed endpoints.

The DISA Quarterly STIG Microsoft Intune Baseline package contains multiple device configuration profiles, Administrative Templates, Baselines, and Settings Catalog.

* **Administrative Templates**: On Windows 10/11 devices, these templates are ADMX settings that you configure. If you're familiar with ADMX policies or group policy objects (GPO), then using administrative templates is a natural step to Microsoft Intune.

|  |  |  |
| --- | --- | --- |
| Policy | Details | Use Cases |
| DoD Adobe Acrobat Pro DC Continuous STIG v2r1 Administrative Template | Contains STIG configurations for Adobe Acrobat Pro DC Continuous.  Requires Adobe ADMX template to be imported.  ADMX templates are available in STIG Baseline ADMX Templates directory. | Intune Standalone  Co-Management |
| DoD Adobe Acrobat Reader DC Continuous STIG v2r1 Administrative Template | Contains STIG configurations for Adobe Acrobat Reader DC Continuous.  Requires Adobe ADMX template to be imported.  ADMX templates are available in STIG Baseline ADMX Templates directory. | Intune Standalone  Co-Management |
| DoD Microsoft 365 STIG v2r8 Administrative Template | Contains STIG configurations for M365 Apps. Policy also applies to Office 2016 and Office 2019 products. | Intune Standalone  Co-Management |
| DoD Microsoft Defender AntiVirus STIG r2v4 Administrative Template | Contains STIG configurations for Microsoft Defender Antivirus. | Intune Standalone  Co-Management |
| DoD Microsoft Edge STIG v1r6 Administrative Template | Contains STIG configurations NOT in Edge Security Baseline. | \*Intune Standalone |
| DoD Mozilla Firefox STIG v6r4 Administrative Template | Contains STIG configurations for Mozilla Firefox.  Requires Mozilla and Firefox ADMX templates to be imported.  ADMX templates are available in STIG Baseline ADMX Templates directory. | Intune Standalone  Co-Management |
| DoD Windows 10 STIG v2r5 Administrative Templates\_ECC\_Removed | Contains STIG configurations NOT in Windows 10 and Internet Explorer 11 Security Baseline.  STIG ID WN10-CC-000052 is not configured within policy due to an input error during import of JSON file. Administrator must configure setting after importing JSON. This is noted in the known issues. | \*Intune Standalone |
| DoD Google Chrome STIG v2r8 Administrative Template | Contains STIG configurations for Google Chrome.  Requires Google ADMX template to be imported.  ADMX templates are available in STIG Baseline ADMX Templates directory. | Intune Standalone  Co-Management |

\*- Requires DoD Windows 10 STIG v2r5 and Internet Explorer 11 STIG v2r3 Security Baseline and Microsoft Edge Security Baseline to be applied to endpoints.

For more information, see [Administrative Templates](https://learn.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows)

* **Baselines**: On Windows 10/11 devices, these baselines include preconfigured security settings. These are preloaded security policy using recommendations by Microsoft security teams. The security baselines are the starting point from DISA STIG.

|  |  |  |
| --- | --- | --- |
| Policy | Details | Use Cases |
| 034ccd46-190c-4afc-adf1-ad7cc11262eb\_DoD Windows 10 STIG v2r5 and Internet Explorer 11 STIG v2r3 Security Baseline | Contains Windows 10/11 and Internet Explorer MS Security Baseline configurations.  Baseline is NOT all Windows OS STIG settings. Baseline profiles must be used in conjunction with additional device configuration profiles. | Intune Standalone  \*Co-Management |
| a8d6fa0e-1e66-455b-bb51-8ce0dde1559e\_DoD Microsoft Edge STIG Computer v1r6 Security Baseline | Contains Microsoft Edge MS Security Baseline configurations.  Baseline is NOT all Microsoft Edge STIG settings. Baseline profiles must be used in conjunction with DoD Microsoft Edge STIG v1r6 Administrative Template profile. | Intune Standalone  \*Co-Management |

\*- Requires appropriate workloads be migrated within MECM. MECM workload configuration is outside scope of this document.

For more information, see [Security baselines](https://learn.microsoft.com/en-us/mem/intune/protect/security-baselines).

* **Settings Catalog**: On Windows 10/11 devices, use the settings catalog to see all the available settings, and in one location. For example, you can see all the settings that apply to BitLocker and create a policy that just focuses on BitLocker. On macOS devices, use the settings catalog to configure Microsoft Edge version 77 and later settings.

For more information, see [Settings catalog](https://learn.microsoft.com/en-us/mem/intune/configuration/settings-catalog).

On macOS, continue using the [preference file](https://learn.microsoft.com/en-us/mem/intune/configuration/preference-file-settings-macos) to:

* + Configure earlier versions of Microsoft Edge
  + Configure Edge browser settings that aren’t in settings catalog

|  |  |  |
| --- | --- | --- |
| Policy | Details | Use Cases |
| DoD Google Chrome STIG v2r8 Settings Catalog | Contains STIG configurations for Google Chrome. | Intune Standalone  Co-Management |
| DoD Internet Explorer 11 STIG v2r3 Settings Catalog | Contains STIG configurations for Internet Explorer 11. | \*Intune Standalone  Co-Management |
| DoD Microsoft 365 STIG v2r8 Settings Catalog | Contains STIG configurations for M365 Apps.  Policy also applies to Office 2016 and Office 2019 products. | Intune Standalone  Co-Management |
| DoD Microsoft Defender Antivirus STIG Computer v2r4 Settings Catalog | Contains STIG configurations for Microsoft Defender Antivirus. | Intune Standalone  Co-Management |
| DoD Microsoft Edge STIG 1vr6 - macOS | Contains STIG configurations for Microsoft Edge on macOS. | Intune Standalone |
| DoD Microsoft Edge STIG v1r6 Settings Catalog | Contains STIG configurations for Microsoft Edge. | \*Intune Standalone  Co-Management |
| DoD Windows 10 STIG v2r5 Settings Catalog | Contain STIG configurations for Windows 10. | \*Intune Standalone  Co-Management |
| DoD Windows 11 STIG v1r2 Settings Catalog | Contain STIG configurations for Windows 11. | \*Intune Standalone  Co-Management |
| DoD Windows Firewall STIG v1r7 Settings Catalog | Contain STIG configurations for Windows Firewall. This does NOT contain Domain Profile configurations. | Intune Standalone  Co-Management |
| Set Execution Policy\_ Non-STIG | Contain PowerShell execution policy to allow accompanying Desired State Configuration policy to run. | Intune Standalone  Co-Management |

\*- Settings catalog profiles would not be used in a cloud-only scenario when Security Baselines are applied.

* **Custom Profiles**: Custom profiles are used for device settings and features that aren't built into Intune. Custom settings are configured differently for each platform. For example, to control features on Android and Windows devices, you can enter Open Mobile Alliance Uniform Resource Identifier (OMA-URI) values.

|  |  |  |
| --- | --- | --- |
| Policy | Details | Use Cases |
| DoD Adobe Acrobat Pro DC Continuous STIG v2r1 Custom Profile | Contains STIG configurations for Adobe Acrobat Pro DC Continuous.  If DoD Adobe Acrobat Pro DC Continuous STIG v2r1 Administrative Template is used, there is no need to use custom profile. | Intune Standalone  Co-Management |
| DoD Adobe Acrobat Reader DC Continuous STIG v2r1 Custom Profile | Contains STIG configurations for Adobe Acrobat Reader DC Continuous.  If DoD Adobe Acrobat Reader DC Continuous STIG v2r1 Administrative Template is used, there is no need to use custom profile. | Intune Standalone  Co-Management |
| DoD Google Chrome STIG v2r8 - macOS | Contains STIG configurations for Google Chrome on macOS | Intune Standalone |
| DoD Google Chrome STIG v2r8 Custom Profile | Contains STIG configurations for Google Chrome.  If DoD Google Chrome STIG v2r8 Administrative Template is used, there is no need to use custom profile. | Intune Standalone  Co-Management |
| DoD Mozilla Firefox STIG v6r4 - macOS | Contains STIG configurations for Mozilla Firefox on macOS | Intune Standalone |
| DoD Mozilla Firefox STIG v6r4 Custom Profile | Contain STIG configurations for Mozilla Firefox.  If DoD Mozilla Firefox STIG v6r4 Administrative Template is used, there is no need to use custom profile. | Intune Standalone  Co-Management |
| DoD Windows 10 STIG v2r5 Custom Profile | Contains additional STIG configurations for Windows 10.  Applies to both Windows 10 and Windows 11 endpoints. | \*Intune Standalone |

\*- Requires DoD Windows 10 STIG v2r5 and Internet Explorer 11 STIG v2r3 Security Baseline and Microsoft Edge Security Baseline to be applied to endpoints.

* **Endpoint Protection Profiles**: Device configuration profiles to manage common Endpoint protection security features on devices.

|  |  |  |
| --- | --- | --- |
| Policy | Details | Use Cases |
| DoD Windows 10 STIG v2r5 Endpoint Protection Profile | Contains additional STIG configurations for Windows 10.  Applies to both Windows 10 and Windows 11 endpoints. | \*Intune Standalone  Co-Management |

\*- Requires DoD Windows 10 STIG v2r5 and Internet Explorer 11 STIG v2r3 Security Baseline to be applied to endpoints.

# Intune Standalone

A cloud-based solution that provides the compliance, configuration, Windows Update, and app features in Intune. Windows Update and application features are outside the scope of this document. To achieve a STIG complaint Windows 10/11 endpoints, you must deploy the provided Security Baseline profiles and supporting additional device configuration profiles. There are 2 provided Security Baseline profiles that are meant to be used in conjunction with several other device configuration profiles to achieve a STIG complaint endpoint.

For a cloud-only deployment model, the following policies should be applied to your endpoints.

1. 034ccd46-190c-4afc-adf1-ad7cc11262eb\_DoD Windows 10 STIG v2r5 and Internet Explorer 11 STIG v2r3 Security Baseline
2. a8d6fa0e-1e66-455b-bb51-8ce0dde1559e\_DoD Microsoft Edge STIG Computer v1r6 Security Baseline
3. DoD Windows 10 STIG v2r5 Endpoint Protection Profile
4. DoD Windows 10 STIG v2r5 Custom Profile
5. DoD Windows 10 STIG v2r5 Administrative Templates\_ECC\_Removed – STIG IG WN10-CC-000052 to be configured after import.
6. DoD Microsoft Edge STIG v1r6 Administrative Template
7. DoD Adobe Acrobat Pro DC Continuous STIG v2r1 Custom Profile (if required)
8. DoD Adobe Acrobat Reader DC Continuous STIG v2r1 Custom Profile (if required)
9. DoD Google Chrome STIG v2r8 Custom Profile (if required)
10. DoD Mozilla Firefox STIG v6r4 Custom Profile (if required)
11. DoD Microsoft 365 STIG v2r8 Administrative Template (applies to Office 2016 & Office 2019)
12. DoD Microsoft Defender AntiVirus STIG r2v4 Administrative Template

As new profile types become available the specified profile types can be swapped out. For example, the DoD Google Chrome STIG v2r8 Custom Profile could be replaced with either the DoD Google Chrome STIG v2r8 Settings Catalog profile or the DoD Google Chrome STIG v2r8 Administrative Template. For new deployments, it is recommended to use the Setting Catalog profiles as much as possible.

# Configuration Manager (Co-Management)

The features of Configuration Manager (on-premises) combined with the cloud. you can:

* Manage on-premises devices, including Windows Server.
* Manage partner or third-party software updates.
* Create custom task sequences when deploying operating systems.
* Deploy and manage many app types.

For a co-management model, there are dependencies on what workloads have been migrated to Intune. For this example, we are assuming the Endpoint Security workload is NOT migrated therefore it is not possible to leverage the pre-staged Security Baseline profiles or the Endpoint Protection profiles. In this case the following policies should be applied to your endpoints:

1. DoD Windows 10 STIG v2r5 Settings Catalog or DoD Windows 11 STIG v1r2 Settings Catalog
2. DoD Internet Explorer 11 STIG v2r3 Settings Catalog
3. DoD Microsoft Edge STIG v1r6 Settings Catalog
4. DoD Windows Firewall STIG v1r7 Settings Catalog
5. DoD Microsoft Defender Antivirus STIG Computer v2r4 Settings Catalog
6. DoD Google Chrome STIG v2r8 Settings Catalog (if required)
7. DoD Mozilla Firefox STIG v6r4 Custom Profile
8. DoD Microsoft 365 STIG v2r8 Settings Catalog (applies to Office 2016 & Office 2019)
9. DoD Adobe Acrobat Pro DC Continuous STIG v2r1 Custom Profile (if required)
10. DoD Adobe Acrobat Reader DC Continuous STIG v2r1 Custom Profile (if required)

As new profile types become available the specified profile types can be swapped out. For example, the DoD Adobe Acrobat Pro DC Continuous STIG v2r1 Custom Profile could be replaced with the DoD Adobe Acrobat Pro DC Continuous STIG v2r1 Administrative Template. The appropriate actions to import third-party ADMX files in environment must be completed. For new deployments, it is recommended to use the Setting Catalog profiles as much as possible.

# Additional Configurations

In either deployment model there are STIG required configurations that are not natively available in Intune. To account for these settings, there are PowerShell scripts available to complete configuration of your endpoints.

|  |  |  |
| --- | --- | --- |
| PowerShell Script | Details | Use Cases |
| Additional STIG Cleanup Items.ps1 | Removes PowerShellv2 Feature and disabled Secondary Logon service.  Note: These settings are now incorporated in the STIG DSC.ps1 and will be removed from future Intune Policy Baselines. | Intune Standalone  Co-Management  To be removed |
| DoD .NET Framework Disable RC4 Cipher STIG.ps1 | Configures .NET Framework STIG configurations.  Note: These settings are now incorporated in the STIG DSC.ps1 and will be removed from future Intune Policy Baselines. | Intune Standalone  Co-Management  To be removed |
| Removes Internet Explorer 11.ps1 | Removes IE 11 if present on system. | Intune Standalone  Co-Management |
| Set STIG Pre-requisites.ps1 | Sets up pre-requisites for running DSC to cover STIG gaps.  Sets the Data Execution Prevention policy to OptOut. | Intune Standalone  Co-Management |
| STIG DSC.ps1 | Configures additional STIG items not available within Intune. | Intune Standalone  Co-Management |

# STIG Checklist Files

To assist administrator to identify what profile contains individual STIG items, there are STIG checklist files provided with notes of what profile contains the individual STIG item. These checklist files can be found under the Support Files | Checklist Files directory within the DISA STIG Baseline Package.

Graphical user interface, text, application, email

Description automatically generated