**Microsoft Intune Policy Import**

The following document will assist the administrator in importing the DISA Quarterly STIG Microsoft Intune Device Configurations profiles in their individual tenant.

Note that the configuration profiles provided must be evaluated in a local, representative test environment before implementation within production environments. The extensive variety of environments makes it impossible to test these configuration profiles for all potential enterprise software configurations. In co-management environments, administrators must migrate the appropriate workloads to apply MEM policies.

For most environments, failure to test before implementation may lead to a loss of required functionality. This document is not intended to be a deployment or configuration guide.

**IMPORTANT**: The provided Microsoft Intune policies are intended to be used in test environments or for evaluation purposes in production environments prior to enterprisewide deployment. It is recommended the following steps be completed on an approved hardened workstation or privileged access workstation (PAW).

The following steps walk through importing individual policies one at a time. This is the preferred method for established environments with existing STIG Intune polices in place.

**Device Configuration – Settings Catalog Profiles**

1. Extract the Intune STIG Policy Baseline to local system.
2. Sign in to the Microsoft Intune Portal with appropriate delegated administrative account, Intune Administrator, or built-in Policy and Profile manager role.
3. Open **Devices | Configuration** blade.
4. Select **+ Create**.
5. Select **Import Policy**.
6. Select **Browse for files** to browse to the location of extracted Intune policies. Only one policy can be imported at a time.
7. Select targeted policy, and then select **Open**.
8. Enter the appropriate value for **New Name.** A **Description** can be entered for operational needs.

**Note:** If an existing policy name is used, the import will be successful, and two policies will exist in Microsoft Intune portal with the same name. The new policy will not impact on the previously existing policy and the new policy will not have any assignments.

1. Select **Save**.
2. Select either **View Policy** or **Close**.
3. Repeat import of additional policies as needed.
4. To complete any operational modifications to imported policies, select desired policy and then edit configuration settings.

**Device Configuration – Preference File Profiles**

Administrators may modify the supporting preference files as needed to meet organization requirements. If new files are generated, when selecting property list file administrators will browse to the location of modified files.

1. Extract the Intune STIG Policy Baseline to the local system.
2. Sign-in to Microsoft Intune Portal with appropriate delegated administrative account, Intune Administrator, or built-in Policy and Profile manager role.
3. Open **Devices | macOS | Configuration** blade.

To create Google Chrome Preference Profile.

1. Select **+ Create**.
2. Select **+ New Policy**.
3. Select **Templates** under **Profile type**.
4. Select **Preference file** under **Template name** list.
5. Select **Create**.
6. Enter appropriate data for **Name, Description** as operational requirement mandates.
7. Select **Next**.
8. Enter **com.google.chrome** in the **Preference domain name** field, select the browse icon under the Property list file field, and browse to the location of extracted **Intune Baseline Support macOS directory.**
9. Select the **com.google.Chrome\_vDoD.plist** file.
10. Select **Open**.
11. Select **Review + Save**.
12. Select **Save**.

To create Microsoft Edge Preference Profile, complete the following steps:

1. Select **+ Create**.
2. Select **+ New Policy**.
3. Select **Templates** under **Profile type**.
4. Select **Preference file** under **Template name** list.
5. Select **Create**.
6. Enter appropriate data for **Name, Description** as operational requirement mandates.
7. Select **Next**.
8. Enter **com.microsoft.Edge** in the **Preference domain name** field, select the browse icon under the Property list file field, and browse to location of extracted **Intune Baseline Support macOS directory.**
9. Select the **com.microsoft.Edge\_vDoD.plist** file.
10. Select **Open**.
11. Select **Review + Save**.
12. Select **Save**.

To create Mozilla Firefox Preference Profile, complete the following steps:

1. Select **+ Create**.
2. Select **+ New Policy**.
3. Select **Templates** under **Profile type**.
4. Select **Preference file** under **Template name** list.
5. Select **Create**.
6. Enter appropriate data for **Name, Description** as operational requirement mandates.
7. Select **Next**.
8. Enter **org.mozilla.firefox** in the **Preference domain name** field, select the browse icon under the Property list file field, and browse to the location of extracted **Intune Baseline Support macOS directory.**
9. Select the **org.mozilla.firefox.xml** file.
10. Select **Open**.
11. Select **Review + Save**.
12. Select **Save.**

**Device Configuration – Custom Profiles**

**Note:** Provided PowerShell import scripts do not include the required AMDX ingest OMA-URI setting. Administrators must modify imported device configuration custom policy to add ADMX ingest to policy before deploying to endpoints.

Administrators may modify the supporting PowerShell files as needed to meet organization requirements. The location of import scripts is Intune STIG Policy Baselines\Support Files\Windows\PowerShell Scripts\CustomPolicyImport directory. If new files are generated, file administrators will browse to the location of modified files to execute PowerShell.

The following provide directions for administrators leveraging Microsoft Graph PowerShell to import custom profiles.

To import DoD Adobe Acrobat Pro DC Continuous STIG v2r1 Custom Profile, complete the following steps:

1. Extract the **Intune STIG Policy Baseline** to local system.
2. Open **Windows PowerShell** with appropriate delegated administrative account.
3. Enter **connect-mgGraph -environment usgov -tenantid APPROPRIATE TenantID**
4. Sign-in with appropriate delegated administrative account, Intune Administrator, or built-in Policy and Profile manager role.
5. Change location to Intune STIG Policy Baselines\Support Files\Windows\PowerShell Scripts\CustomPolicyImport directory or location of modified script.
6. Enter **.\Import\_DoDAdobeAcrobatProDCContinuousSTIGv2r1CustomProfile.ps1** and press **Enter**.
7. Sign-in to Microsoft Intune Portal with appropriate delegated administrative account, Intune Administrator, or built-in Policy and Profile manager role.
8. Open **Devices** | **Windows** | **Configuration** blade.
9. Locate the newly created custom policy **DoD Adobe Acrobat Pro DC Continuous STIG v2r1 Custom Profile** either by using search or scroll through list.
10. Select the custom policy **DoD Adobe Acrobat Pro DC Continuous STIG v2r1 Custom Profile**.
11. Select **Edit** under **Configuration settings** section.
12. Review imported **OMA-URI Settings** to ensure appropriate organizational settings are properly configured.
13. Select **Add**.
14. Enter **Acrobat Pro DC Continuous ADMX Ingest** in the **Name** field.
15. Enter appropriate organizational requirements in **Description** field.
16. Enter **./Device/Vendor/MSFT/Policy/ConfigOperations/ADMXInstall/Adobe Acrobat Pro DC Continuous/Policy/AcrobatProDCContinuousADMX** in **OMA-URI** field.
17. Select **String** from **Data Type** dropdown list.
18. Open the **AcrobatProDCContinuous.admx** file. The file is in the **DISA STIG GPO Package\ADMX Templates\Adobe** directory.
19. Select **ALL TEXT** and **Copy** to clipboard.
20. Paste the copied AMDX contents in the **Value** field.
21. Select **Save**.
22. Select **Review + save**.
23. Select **Save**.

To import the DoD Adobe Acrobat Reader DC Continuous STIG v2r1 Custom Profile, complete the following steps:

1. Enter **.\Import\_DoDAdobeAcrobatReaderDCContinuousSTIGv2r1CustomProfile.ps1** and press **Enter**.
2. Sign in to the Microsoft Intune Portal with appropriate delegated administrative account, Intune Administrator, or built-in Policy and Profile manager role.
3. Open **Devices** **|** **Windows** **|** **Configuration** blade.
4. Locate the newly created custom policy **DoD Adobe Acrobat Reader DC Continuous STIG v2r1 Custom Profile** either by using search or scroll through list.
5. Select the custom policy **DoD Adobe Acrobat Reader DC Continuous STIG v2r1 Custom Profile**.
6. Select **Edit** under **Configuration settings** section.
7. Review imported **OMA-URI Settings** to ensure appropriate organizational settings are properly configured.
8. Select **Add**.
9. Enter **Acrobat Reader DC Continuous ADMX Ingest** in the **Name** field.
10. Enter appropriate organizational requirements in **Description** field.
11. Enter **./Device/Vendor/MSFT/Policy/ConfigOperations/ADMXInstall/Adobe Acrobat Reader DC Continuous/Policy/AcrobatDCContinuousADMX** in **OMA-URI** field.
12. Select **String** from **Data Type** dropdown list.
13. Open the **AcrobatDCContinuous.admx** file. The file is in the **DISA STIG GPO Package\ADMX Templates\Adobe** directory.
14. Select **ALL TEXT** and **Copy** to clipboard.
15. Paste the copied AMDX contents in the **Value** field.
16. Select **Save**.
17. Select **Review + save**.
18. Select **Save**.

To import DoD Mozilla Firefox STIG v6r6 Custom Profile, complete the following steps:

1. Enter **.\Import\_DoDMozillaFirefoxSTIGv6r6CustomProfile.ps1** and press **Enter**.
2. Sign in to the Microsoft Intune Portal with appropriate delegated administrative account, Intune Administrator, or built-in Policy and Profile manager role.
3. Open **Devices** | **Windows** | **Configuration** blade.
4. Locate the newly created custom policy **DoD Mozilla Firefox STIG v6r6 Custom Profile** either by using search or scrolling through list.
5. Select the custom policy **DoD Mozilla Firefox STIG v6r6 Custom Profile**.
6. Select **Edit** under **Configuration settings** section.
7. Review imported **OMA-URI Settings** to ensure appropriate organizational settings are properly configured.
8. Select **Add**.
9. Enter **Mozilla Firefox ADMX Ingest** in the **Name** field.
10. Enter appropriate organizational requirements in **Description** field.
11. Enter **./Device/Vendor/MSFT/Policy/ConfigOperations/ADMXInstall/Firefox/Policy/FirefoxADMX** in **OMA-URI** field.
12. Select **String** from **Data Type** dropdown list.
13. Open the **firefox.admx** file. The file is in the **DISA STIG GPO Package\ADMX Templates\Mozilla** directory.
14. Select **ALL TEXT** and **Copy** to clipboard.
15. Paste the copied AMDX contents in the **Value** field.
16. Select **Save**.
17. Select **Review + save**.
18. Select **Save**.

When importing Disable Internet Explorer 11 Custom Profile, only the import script needs to be imported as there is no additional ADMX ingest required to execute.

1. Enter **.\Import\_DisableInternetExplorer11CustomProfile.ps1** and press **Enter**.
2. Sign in to the Microsoft Intune Portal with appropriate delegated administrative account, Intune Administrator, or built-in Policy and Profile manager role.
3. Open **Devices** | **Windows** | **Configuration** blade.
4. Locate the newly created custom policy **Disable Internet Explorer 11** either by using search or scrolling through list.
5. Review settings.