**Microsoft Intune Policy Import**

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

It must be noted that the configuration profiles provided should 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 enterprise-wide 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 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 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** browse to the location of extracted Intune policies. Only one policy can be imported at a time. Select targeted policy and select **Open**.
7. 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 2 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. Complete any operational modifications to imported policies by selecting desired policy and edit configuration settings.

**Device Configuration – Preference File Profiles**

Administrators may modify the provided 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 local system.
2. Sign-in Microsoft Intune Portal with appropriate delegated administrative account, Intune Administrator or built-in Policy and Profile manager role.
3. Open **Devices | macOS | Configuration profiles** 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 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.

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.

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 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**

**Automated Import – All JSON Files from Intune Backup**

The following provides an example of importing all STIG policies at once. This method can be used to establish a new MDM environment or in the event of a recovery.

**NOTE:** The following leveraged Microsoft Graph and IntuneBackupandRestore module.

1. The following modules must be present to complete steps to import JSON files.
   1. AzureAD
   2. MSGraphFunctions
   3. Microsoft.Graph.Intune
   4. IntuneBackupandRestore
2. To view installed modules
   1. Open PowerShell and run “**Get-InstalledModule**”
3. To install one or all required modules. In the same PowerShell instance:
   1. AzureAD: type “***Install-Module -Name AzureAD***”
   2. MSGraphFunctions: type “***Install-Module -Name MSGraphFunctions****”*
   3. IntuneBackupAndRestore: type “***Install-Module -Name IntuneBackupAndRestore***”
   4. If previously installed IntuneBackupAndRestore, type *“****Update-Module -Name IntuneBackupAndRestore****”*
   5. As of version 2.0.0, the IntuneBackupAndRestore PowerShell Module requires Microsoft.Graph.Intune, type ***“Install-module -Name Microsoft.Graph.Intune****”*
   6. Type *“****Import-Module -Name IntuneBackupAndRestore****”*
4. If not a Global Administrator (GA), a GA must have previously consented on behalf of the organization for required Microsoft Intune PowerShell permissions prior to completing the following steps. If running as a GA, you will be prompted to consent on behalf of your organization during sign-on.
5. Connect to Microsoft Graph
   1. If in GCC High, type “***Update-MSGraphEnvironment -AuthUrl 'https://login.microsoftonline.us/common' -GraphBaseUrl 'https://graph.microsoft.us' -GraphResourceId 'https://graph.microsoft.us' -SchemaVersion 'v1.0'***”
   2. If in DoD, type “***Update-MSGraphEnvironment -AuthUrl 'https://login.microsoftonline.us/common' -GraphBaseUrl 'https://dod-graph.microsoft.us' -GraphResourceId 'https://dod-graph.microsoft.us' -SchemaVersion 'v1.0'*”**
   3. Type “***Connect-MSGraph***”
   4. Enter tenant credentials to complete sign-on.
6. To restore configuration profile
   1. The following command will recursively parse the Microsoft Intune Policies directory and restore all found JSON files. Restore will not overwrite existing configurations but create new with the same name. Administrator may delete or move any JSON files from folder structure to prevent duplicate configurations from being created.
   2. Type “***Start-IntuneRestoreConfig -path "<location of DISA quarterly package>\Microsoft Intune Policies****"*