Microsoft Intune Policy Import

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

The provided Windows 10 and Microsoft Edge device configuration profiles are meant to be used in conjunction with built-in Endpoint Security | Security baselines. Applying security baselines are outside the scope of the document, but administrators must apply MDM Security Baselines to managed devices to meet the required STIG configurations for Windows 10 devices.

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. For most environments, failure to test before implementation may lead to a loss of required functionality.

**IMPORTANT**: The provided Microsoft Intune policies are intended to be used in test environments or for evaluation purposes in production environments at this time.

1. The following modules must be present to complete steps to import JSON files.
   1. AzureAD
   2. MSGraphFunctions
   3. 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 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 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. Type “*Connect-MSGraph*”
   2. Enter tenant credentials to complete sign-on.

**NOTE**: May need to update authentication endpoints to authenticate with appropriate AzureGOV environment

To connect to an Azure US Government tenant: Type “ *Update-MSGraphEnvironment -authurl 'https://login.microsoftonline.us/common' -graphbaseurl 'https://dod-graph.microsoft.us' -graphresourceid 'https://dod-graph.microsoft.us' ”*

1. 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"*