Windows Security Hardening

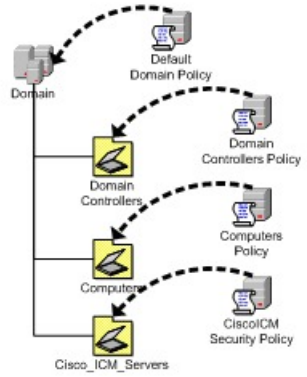
Windows Server Hardening

As a best practice, we recommend using the Microsoft security baseline and CIS benchmarks for secure configuration of ICM servers. Use the latest Microsoft security baseline and Level 1 CIS benchmark profile to lower the attack surface without impacting the functionality and performance.

Apply the security policy in the form of Group Policy Object (GPO) into a separate Organizational Unit(OU) that contains ICM servers. Name the OU as Cisco_ICM_Servers (or a similar clearly identifiable name) and ensure to name these servers in accordance with your corporate policy.

Create this OU either at the same level as the Computers' container or at the Cisco Unified ICM Root OU. If you are unfamiliar with the Active Directory, engage your Domain Administrator to assist you with Group Policy deployments.

Figure 1: Group Policy Deployments



After applying the security policy at the OU level, block any differing policies from being inherited at the Unified ICM/Unified Contact Center Enterprise Servers OU. You can override a blocking inheritance, a configuration option at the OU object level, by selecting the Enforced/No Override option at a higher hierarchy level. The application of group policies must follow a thought-out design that starts with the most common denominator. These group policies must be restrictive at the appropriate level in the hierarchy.

Cisco Unified Contact Center Enterprise Security Hardening for Windows Server

This section outlines the security baseline that is needed for hardening Windows Servers running ICM servers. This security baseline is essentially a collection of Microsoft group policy settings based on the Microsoft security baseline and Level 1 CIS benchmark profile.

To apply the security baseline in the domain controller, perform the following steps:

1. Download the security hardening templates applicable for the respective Windows version from the Microsoft and CIS benchmark URL. You can download these security hardening templates from https://www.microsoft.com/en-us/download/details.aspx?id=55319 and https://workbench.cisecurity.org/files?q=&tags=3.
2. Install the latest Administrative Templates (ADMX) for the Windows Server. These templates can be downloaded from the Microsoft website at https://www.microsoft.com/en-us/download/details.aspx?id=103667. You can install the `.msi installer` on any Windows node as per your IT policy. The windows server can be ICM or non ICM or Domain Controller.
3. Navigate to the installed location of administrative templates. Copy the below-mentioned template files to the domain controller SYSVOL folder.
   - Copy the *.admx files from the PolicyDefinitions folder to `\<Domain>\SYSVOL<Domain>\Policies\PolicyDefinitions`
   - Copy the *.adml files from the PolicyDefinitions<applicable-language> folder to `\<Domain>\SYSVOL<Domain>\Policies\PolicyDefinitions\en-US`

Note The domain controller automatically copies the admx and adml files to all the domain-joined machines.

Select the applicable language code (en-US) based on your deployment setting.

Create the PolicyDefinitions folder if it does not exist.

4. Create a Group Policy Object in the domain controller using the **Group Policy Management** console and import respective policy using the Import Setting Wizard in the console as per below details. This can be done directly on the ICM nodes based on the IT policy.
   - The downloaded Microsoft baseline (see Step-1) has Group Policy Object (GPO) for Windows Client, Windows Server, Common GPO for both Client and Server, Domain Controller, and Internet Explorer. We recommend you to import the GPO specific to Windows Server, Internet Explorer, and Common GPO for both Client and Server.
   - The downloaded CIS baseline (see Step-1) has GPO for Domain Controller, Microsoft, and User. We recommend importing only the MS-L1 and User-L1 GPO.
5. Create the custom GPO in the Domain Controller to override the policies outlined in the **Security Baseline Policy Exception for ICM**, and import the custom exception GPO using import setting wizard in the console. You can manually override the policies directly on the ICM nodes based on the IT policy.

6. Ensure that the exception policy imported (see Step-5) has higher priority such that the exception policy is applied after the Microsoft and CIS policies are applied.

Note Step 6 is applicable only on domain controllers.

7. Create the OU **Cisco_ICM_Servers** (or a similar identifiable name) under the domain. Map all the ICM machines to this OU. You can perform this step at any point, even before performing Step-1.
8. Link the created GPO (see Step-4 and Step-5) to the OU created (see Step-7).
9. Restart the ICM servers in the organizational unit or run the **gpupdate** command on the respective target ICM nodes to apply the security baseline.

Security Baseline Policy Exception for ICM

The following CIS baseline policies impact the ICM functionality.

The recommended values (outlined in the table below) are to be used for the exception policies to override the recommended values of CIS.

Policy	CIS/Microsoft Baseline	Recommended Setting	Remarks
Ensure 'Perform volume maintenance tasks' is set to 'Administrators'	CIS	Administrators, NT Service/MSSQLServer	The ICM database engine runs as service **MSSQLSERVER**. The **NT SERVICE/MSSQLSERVER** login is used by the service to connect to the database engine. This policy impacts on this connectivity. Hence, include the **NT SERVICE/MSSQLSERVER** setting in addition to the **Administrators** setting.
Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'	CIS	Yes	This setting has an impact on operations of duplex CCE systems. For example, it impacts the private interface between the duplex router process.

Policy	CIS/Microsoft Baseline	Recommended Setting	Remarks
Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'	CIS	Disabled	This policy impacts the CCE functionality. For example, patch install is impacted. Applications such as snmp, msgagent etc., are blocked. You can enable this only after configuring the appropriate rules under the setting **Configure Attack Surface Reduction rules: Set the state for each ASR rule**. These include adding trusted/known applications with path in the exception list. The list of impacted application differs, so the recommendation is to set the value to **`Disabled`**.
Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: Semi-Annual Channel, 180 or more days'	CIS	Disabled	Automatic updates interrupt the functionality during automatic restarts.
Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'	CIS	Disabled	Automatic updates interrupt the functionality during automatic restarts.
Ensure 'Configure Automatic Updates' is set to 'Enabled'	CIS	Disabled	Automatic updates interrupts the functionality during automatic restarts.
Ensure 'No auto restart with logged-in users for scheduled automatic updates installations' is set to 'Disabled'	CIS	Enabled	Automatic updates interrupt the functionality during automatic restarts.

The following policies are optional. You can enable these policies as per the IT policy after considering the remarks column carefully.

Policy	CIS/Microsoft Baseline	Recommended Setting	Remarks
Ensure 'Allow log on locally' is set to 'Administrators'	CIS	BUILTIN\Users, BUILTIN\Administrators	After you apply the policy, the Domain only accounts cannot log in to the machine and perform operations. We recommend you to add **`BUILTIN\Users`** and **`BUILTIN\Administrators`**. You can enable this policy based on the IT policy and operational requirements.
Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only)	CIS	Guests	This policy may have operational impacts specifically for day 0/1 activities. We recommend setting the value to **Guests**. You can override this policy based on the IT policy and operational requirements.
Ensure 'Deny log on through Remote Desktop Services is set to 'Guests, Local account' (MS only)	CIS	Guests	This policy may have operational impacts specifically for day 0/1 activities. We recommend you setting the value to **Guests**. You can override this policy based on the IT policy and operational requirements.
'Prevent ignoring certificate errors' to be set as 'Enabled'	Microsoft	Disabled	CCE web applications such as Websetup cannot be accessed using Internet Explorer. Accessing these web applications with other supported browsers like Mozilla Firefox and Google Chrome will not be impacted due to this policy. We recommend setting the value to **`Disabled`**.
'Turn on Enhanced Protected Mode' to be set as 'Enabled'	Microsoft	Disabled	CCE web applications such as Websetup cannot be accessed using Internet Explorer. Accessing these web applications with other supported browsers like Mozilla Firefox and Google Chrome will not be impacted due to this policy. We recommend setting the value to **`Disabled`**.

Policy	CIS/Microsoft Baseline	Recommended Setting	Remarks
Ensure 'Accounts: Administrator account status' is set to 'Disabled' (MS only)	CIS	Enabled	This policy has operational impacts. For example, if a member server goes out of domain for any reason, with this policy in place ,we need to use unrecommended safe mode login to add back the member server to the domain. Other operations will have similar impact too.

Enable the following policies after you install the ICM server. Refer to the Remarks column for the deviations observed.

Policy	CIS/Microsoft Baseline	Recommended Setting	Remarks
Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	CIS	Administrators, Local Service, Network Service	IIS default user **`IIS Apppool\DefaultAppPool`** is added automatically to this policy after starting the IIS services. However, the CIS benchmark scans mark this policy as not compliant because of the presence of IIS default user.
Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	CIS	Local Service, Network Service	IIS default user **`IIS Apppool\DefaultAppPool`** is added automatically to this policy after starting the IIS services. However, the CIS benchmark scans mark this policy as not compliant because of the presence of IIS default user.
Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	CIS	Local Service, Network Service	IIS default user **`IIS Apppool\DefaultAppPool`** is added automatically to this policy after starting the IIS services. However, the CIS benchmark scans mark this policy as not compliant because of the presence of IIS default user.

Note The CIS benchmark versions **1.2.1 for Windows Server 2019, version 1.3.0 for Windows Server 2016, Microsoft baseline Windows Server 2019 version 1809, and Microsoft baseline Windows Server 2016 version 1607** are validated. Before applying the higher version of CIS and Microsoft benchmark, analyze the additional policies introduced in the new version for the impact on ICM functionality and performance. We recommend the GPOs must be tailored according to your organization's need. We recommend rolling out the GPOs to a small group of systems, preferably in a lab environment before rolling out into production.

In addition to the GPO settings, disable the following settings in Windows Server:

- NetBIOS
- SMBv1

Windows Security Hardening