

Active Directory and Group Policy Management Best Practices

November 2024

ACKNOWLEDGEMENTS

The Center for Internet Security (CIS) would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls® (CIS Controls®) and CIS Benchmarks™. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

As a nonprofit organization driven by its volunteers, we are always looking for new topics and assistance in creating cybersecurity guidance. If you are interested in volunteering, have questions/comments, or have identified ways to improve this guide, please write to us at benchmarkinfo@cisecurity.org.

All references to tools or other products in this guide are provided for informational purposes only, and do not represent endorsement by CIS of any company, product, or technology.

Editors

Justin Brown, CIS
Haemish Edgerton, GDIT
Caleb Eifert, CIS
Jennifer Jarose, CIS
Matt Woods, CIS

Contributors

Bill Hennings, CIS
Uzoma Ifeakanwa, CIS
Jordan Rakoske, CIS
Phil White, CIS

CONTENTS

Introduction	1
Audience	2
Domain Services Overview	3
Forest	3
Tree	4
Domain	4
Domain Controller	4
Site	4
Active Directory	5
Schema	5
Global Catalog	5
Replication	5
Group Policy Management	6
Organizational Unit (OU)	6
Security Groups	6
Administrative Template Files (ADMX/ADML)	6
Default Domain Policy and Default Domain Controller Policy	6
Best Practices	7
Domain, Forest, and Site	7
Active Directory	7
Forest-wide FSMO Roles	8
Domain-wide FSMO Roles	8
Schema	9
Global Catalog	10
Replication	10
Read-only Domain Controller (RODC)	11

Group Policy Management	11
Organization Unit (OU)	12
Computer and User Based Policies	12
Security Groups	12
Administrative Template Files (ADMX/ADML)	13
Default Domain Policy and Default Domain Controller Policy	18
Organizational Unit Naming and User and Computer Settings	21
Group Policy Management Hierarchy	26
Security Filtering	28
Allow	28
Deny	29
WMI Filtering	29
Group Policy Tools	31
Group Policy Results	31
Gpresult	31
Microsoft Policy Analyzer	31
Group Policy Modeling	32
Group Policy Update	33
Backup and Restoration	34
Change Management	36
CIS Build Kits	37
Conclusion	42
References	43
Appendix A Default Domain Policy vs CIS Recommendations	44
Appendix B Default Domain Controller Policy vs CIS Recommendations	45
Appendix C Links and Resources	46

Introduction

A properly thought out and designed Active Directory® (AD) structure can help with the cumbersome task of maintaining Domain Services for an environment. Microsoft® provides built-in tools that allow organizations to control the services necessary for maintenance and troubleshooting of an Active Directory environment. A wide range of information on this topic is available from various sources and of varying quality. This guide will focus on considerations while designing and building an Active Directory management program and best practices for Group Policy Management (GPM), and the relationship it has to the CIS Benchmarks™ (Benchmarks™) and CIS Build Kits (Build Kits). Note: This guide does not cover hybrid or Entra-joined AD scenarios.

Audience

This guide was written to address common questions brought up in the [CIS Microsoft Windows Benchmark Community](#) regarding Active Directory and Group Policy. This guide touches on many areas of Microsoft Active Directory and Group Policy Management, but due to the breadth and depth of this technology, this guide should be considered a general tutorial. This guide assumes that the reader has working knowledge of Active Directory and should not be used as a reference. Links are supplied at the end of this guide, which can be used as references for further information.

If you are interested in volunteering, have questions or comments, or have identified ways to improve this guide, please write to us at: benchmarkinfo@cisecurity.org or visit the [Community](#).

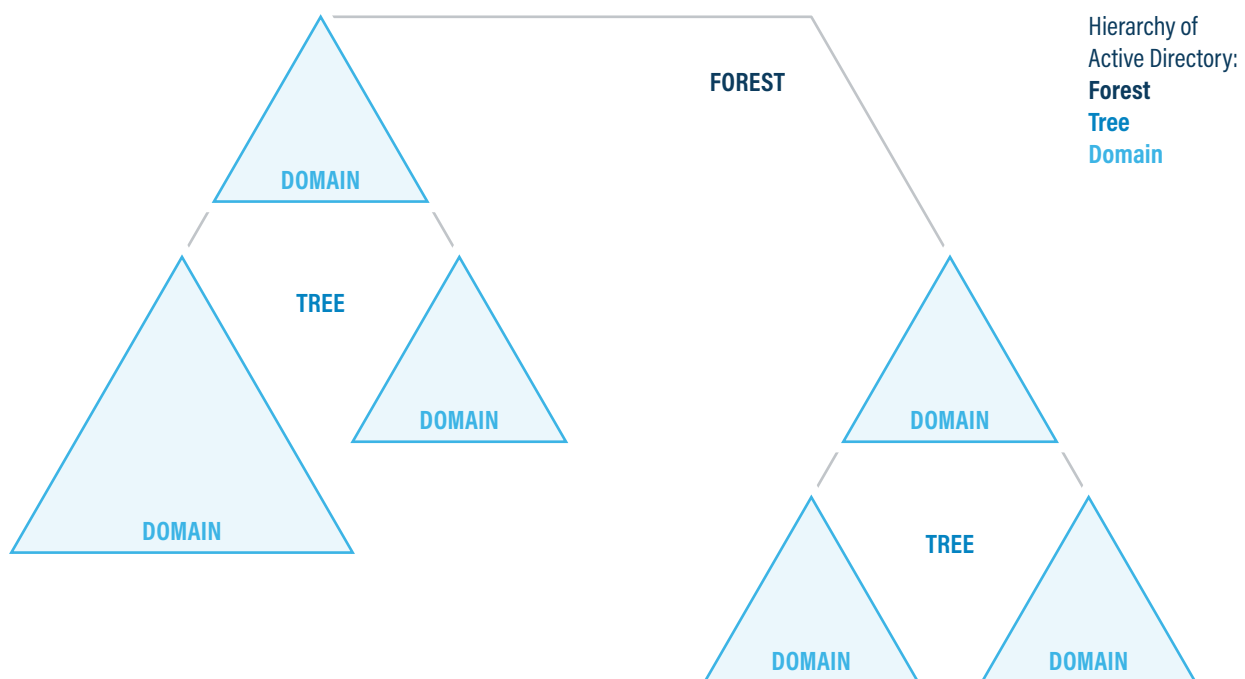
Domain Services Overview

Active Directory Domain Services (AD DS) is based on a hierarchical structure that stores information about objects, such as user and computer accounts, and network devices. This information is stored in a directory database containing information about the objects and their relationships. AD DS is accessed and administered through various tools, such as Active Directory Users and Computers (ADUC), Active Directory Administrative Center (ADAC), and PowerShell.

Forest

An Active Directory Forest sits at the top of the hierarchical structure of Active Directory and provides the means to manage one or more domains as a single unit. A forest shares resources like schema and the global catalog to all domains within it. The forest is made up of one or more trees and domains and is the main security boundary of Active Directory.

Figure 1 | Active Directory structure at the forest, tree, and domain levels.



Tree

An Active Directory tree is a grouping of domains within the forest. All domains within the same tree have a transitive trust relationship, so if a domain joins the tree, it automatically trusts all other domains. All domains within a tree share a common contiguous namespace.

Domain

An Active Directory domain is a logical grouping of objects that share administrative, security, and replication settings. Objects within the domain are defined as a single user, group, computer, or printer, etc.

Domain Controller

A Domain Controller (DC) is a networked server that provides the tools to administer domain services. Additionally, these servers respond to identity security requests, enforce security policies, and can manage software installations. All DCs share the same Active Directory database and replicate it so that any DC can respond to client queries.

Site

An Active Directory Site is a logical grouping of domain controllers. They mirror the actual network topology, organizing DCs based on the most efficient routes for AD-related network traffic. This helps ensure the most efficient replication, authentication, and service requests.

Active Directory


Active Directory acts as the central repository where all objects and their attributes are stored. Objects are single elements within the database such as a user, computer, group, or printer. Like the domain structure described above, AD is made up of several components, with the primary ones being:

Schema	The schema is a directory of how information should be stored in the database. It outlines the object classes and what type of information about those objects is collected. For example, a user is a class within the schema and holds attributes such as name, email address, group membership, etc.
Global Catalog	The Global Catalog provides information on all objects in the forest, including objects that are not part of a domain.
Replication	Replication is the process by which changes or updates to the directory database are distributed amongst the DCs in a domain.

Figure 2 | Example of an object and its attributes.

Test User Properties ? X

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile		COM+	Attribute Editor	
General	Address	Account	Profile	Telephones
				Organization



Test User

First name:

Initials:

Last name:

Display name:

Description:

Office:

Telephone number:

Other...

E-mail:

Web page:

Other...

OK

Cancel

Apply

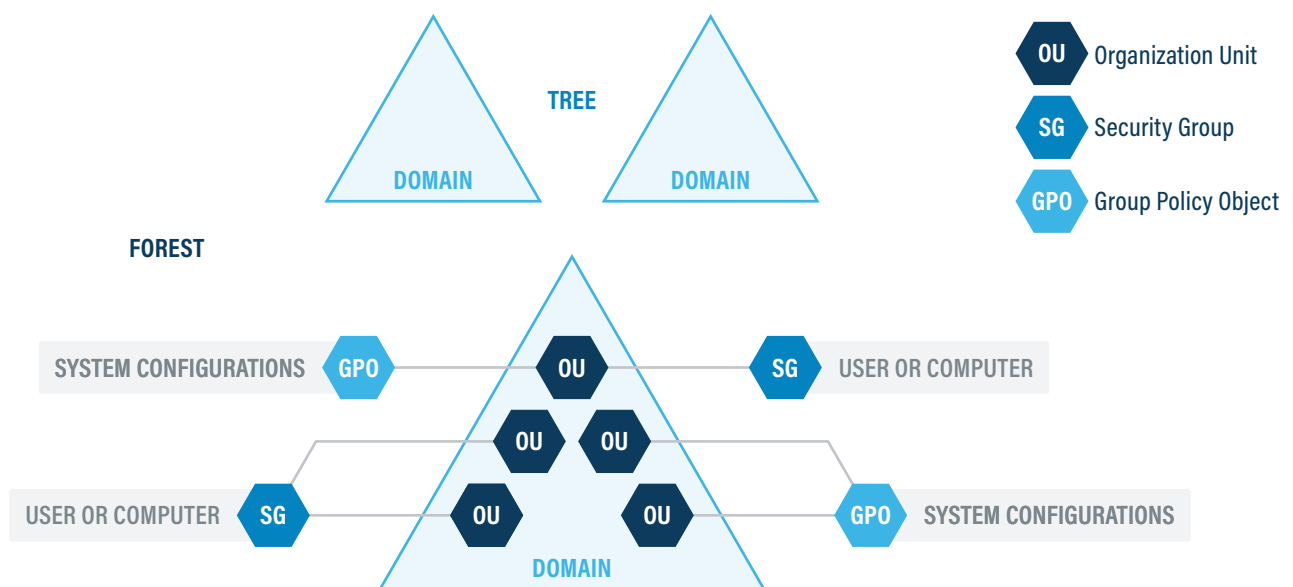
Help

Group Policy Management

The Group Policy Management Console (GPMC) is the primary tool used to organize, manage, and administer Group Policies within AD.

Organizational Unit (OU)	An Organizational Unit (OU) is a container within a domain that logically groups objects such as, users, computers, groups, and printers.
Security Groups	A Security Group is used to assign user rights or grant permissions to resources within an environment, allowing access to be managed collectively. A security group can contain objects, such as users, computers, and other security groups.
Administrative Template Files (ADMX/ADML)	Administrative Template files (ADMX/ADML) are a critical part of group policy and the primary means of supplying the operating system (OS) with configurations that are defined centrally via Group Policy Management.
Default Domain Policy and Default Domain Controller Policy	The Default Domain Policy (DDP) and Default Domain Controller Policy (DDCP) are default Group Policy Objects (GPOs) created automatically when Active Directory Domain Services are installed on the first server in the environment creating the first Domain Controller.

Figure 3 | Active Directory Structure at the Domain and Organization Unit levels.



Best Practices

When architecting an Active Directory structure, the design should be flexible and easily adaptable, so future growth is not inhibited. An Active Directory structure that is designed properly should exceed the current environment's needs and be well organized. For example, separating objects by their type (e.g., users, computers, groups) can be helpful for both assigning administrative roles to staff, and for organized group policy management.

Domain, Forest, and Site

The simplest option for organizations is to limit the forest to a single domain, unless a logical separation is needed (e.g., operating in different countries), or existing domains are migrated into a new structure.

When the first Domain Controller is created in the Domain, the first Active Directory Site is also automatically created containing this DC. When creating additional DCs, they can either be placed into the same site, or into a separate site, depending on network topology needs. Typically, the same site is used for DCs with fast (e.g., LAN) network speeds between them, and separate sites are used for DCs with slower links (e.g., WAN). A site can contain DCs from more than one domain, and a forest can contain more than one site. It is recommended that at least two domain controllers are present within each domain to provide redundancy.

Active Directory

Active Directory contains five flexible single-master operator (FSMO) roles that work together within Active Directory Domain Services and play an important part in the combined functions of AD DS.

Multiple FSMO roles can be installed on a single domain controller (single-master model), or they can be separated onto individual DCs (multi-master model). In a multi-master environment, each role can only be assigned to one DC at a time within the forest or domain, and it is responsible for the role it plays within AD DS. There are some situations where multiple roles can exist on the same DC.

If an FSMO role needs to be moved to another DC, and the current role holder is online, it can be gracefully transferred. This is the preferred way to move roles. However, if a domain controller containing an FSMO role goes down and cannot be recovered in a reasonable timeframe, the role can be seized by another DC in the environment, and it will take over the role moving forward.

If an FSMO role seizure and not a graceful transfer becomes necessary, the former FSMO role holder should never be brought back online. It should be erased, including its records (e.g., computer account and metadata) from the Domain because if it is brought back online, it would still believe it holds the role and cause conflict. Instead, the server should be wiped, rebuilt, and rejoined as a fresh domain controller, ideally with a different name, and without any FSMO role installed. At that point, a graceful transfer of the previous role could be done.

The following is a breakdown of activities that each FSMO role is responsible for within the domain.

Forest-wide FSMO Roles

- **Schema master role:** This role is responsible for writing updates to the directory schema. Schema is the attributes of objects within the database such as logon name, email address, or phone number. Once updates are performed, it then replicates the data to other DCs within the environment. Only one DC in a forest can hold the schema master role.
- **Domain naming master:** This role is responsible for adding and removing domains from the forest and ensuring that domain names are not duplicated within the tree. In addition, it is responsible for cross references to domains in external directories. Only one DC in a forest can hold the domain naming master role.

Domain-wide FSMO Roles

- **Relative ID (RID) master:** This role is responsible for processing relative ID (RID) pool requests. Each object in the Domain contains a security identifier (SID) assigned by a DC. Each SID is an identifier that is unique within each domain and a RID which provides uniqueness within the forest. This mitigates the risk of two objects having the same SID within a forest. This role is also responsible for moving objects from one domain to another. Only one DC in each domain can hold the RID master role.
- **Primary Domain Controller (PDC) emulator:** This role is considered authoritative within the domain and is responsible for authentication requests, password changes, and managing Group Policy Objects. It is also responsible for syncing time within the domain, as consistent time settings are critical to the concept of preferential replication. Active Directory only allows a maximum of a five-minute time variance between two domain computers to avoid replication errors. Only one DC in each domain can hold the PDC emulator role. The following functions are also controlled by the PDC emulator:
 - Replication of password changes performed by other DCs within the domain.
 - Authentication failures from other DCs within the domain are forwarded to the PDC emulator before a bad password failure message is reported to the user.
 - Account lockout enforcement.

- **Infrastructure master:** This role is responsible for updating globally unique identifiers (GUID), SIDs, and distinguished names (DN) in a cross-domain object reference. Only one DC in each domain can hold the infrastructure master role.

Schema

In some environments the extension of the schema could be necessary to store unique information about an object. AD schema is designed to be extended based on local requirements. When making changes to the schema, it is important to know that any changes made will be permanent. When deciding to extend it, first determine if this information is necessary across the environment, as all changes are global and will affect the entire forest. A risk associated with schema changes is the possibility of it conflicting with previous changes or default schema updates that might be made by Microsoft. To avoid this, it is best to use a unique naming convention for any local schema extensions. Only members of the Schema Admins group in the forest’s root domain can modify Active Directory Schema. Since this is rarely done, this group is best kept empty when not planning to modify the Schema.

Some Microsoft back-end products also require modifying the AD schema to create additional attributes and objects that are specific to their operation. Two common examples of this are Microsoft Exchange and Microsoft Teams.

The default schema is periodically modified by Microsoft to update object classes and attributes. For more information on Microsoft Active Directory schema updates, please visit: [Schema updates in Windows Server | Microsoft Learn](#).

Table 1 | Schema versions

Operating System	Schema Version
Windows Server 2025	91
Windows Server 2022	88
Windows Server 2019	88
Windows Server 2016	87

Schema outlines the object classes and what type of attributes are stored.

Global Catalog

The Global Catalog is a vital part of the functions performed by Active Directory. It is built automatically by the domain services replication system on the first DC created in the forest, as this DC would initially hold the Schema master role.

The Global Catalog holds a partial replica of every naming context within the database and a copy of every object in the directory, but only contains a small number of their attributes. This list is defined by Microsoft but can be modified to meet organizational needs. The two primary functions of the Global Catalog are providing logon capabilities and responding to Active Directory queries.

To provide logon capabilities, the Global Catalog provides the Domain Controller that processes authentication with the User Principal Name (UPN) in cases where the Domain Controller has no local knowledge of the user account. For example, if a user from Domain 1 ("user@domain1.sales.com") logs into a system located in Domain 2 ("domain2.manufacturing.com") for the first time, the authenticating DC will contact the Global Catalog to resolve the UPN before the authentication process is complete.

If universal groups are present in a multi-domain environment, the Global Catalog is the only source of information for these groups. When a logon request is made, the Global Catalog must be available to process the request. If it is unavailable, and cache credentials are preset on the device, the user can log in normally. If cached credentials are not available, only local resources will be available.

The Global Catalog is also responsible for validating object references to other domains within the forest and answers queries for user directory information throughout the forest. Indexing attributes within the Global Catalog can improve the performance of these queries. It is worth noting that indexes only apply to attributes and not classes, so when indexing is enabled, all attributes for that object are indexed, regardless of class.

Replication

Replication allows for changes to be made to objects in the Global Catalog and those changes are distributed to all other DCs within the domain. This creates redundancy in the environment and if one DC is down or unavailable, another DC can take over with no loss of information or functionality.

Replication within Active Directory provides several benefits that ensure availability, consistency, and load balancing across the tree. This means that if a DC becomes inoperable, the environment remains stable, and business continues as normal. Although there is the possibility of a replication collision, this is alleviated by the time stamp of the two objects, as the most recent timestamp will be accepted, and that object replicated. Some benefits of replication are:

- **Availability:** Replication ensures that if a specific DC is unavailable, users can still log on and access domain resources.
- **Consistency:** Replication ensures that if a change is made on one DC it will be reflected on all DCs in the domain, and that data remains consistent.

- **Load Balancing:** Replication ensures that user requests are distributed across DCs in the domain and reduces the load on any single DC.

Applications and appliances that rely on Lightweight Directory Access Protocol (LDAP) to connect to Active Directory will often only allow a connection to one specific DC. This negates AD redundancy for that resource, because if that specific DC goes offline the resource will cease to function even though other DCs are available.

Replication occurs through a built-in process called the Knowledge Consistency Checker (KCC) that runs on all DCs in the environment. The KCC is responsible for generating a replication topology for the forest. It will also adjust the replication topology to accommodate new, deleted, or moved DCs.

Replication on an object occurs frequently and typically as soon as a change is made. Upon detection of a change, the DC will send the updated information to its replication partner. If this does not occur, the KCC runs by default every 15 minutes and outstanding changes will be sent to the replication partner. Additionally, a full intra-site replication should occur every 180 minutes under a default configuration.

Replication delay values between Active Directory sites can be adjusted in the AD Sites & Services tool. The shortest inter-site value that can be configured with this tool is 15 minutes. With modern hardware and network connections, it is often acceptable to lower the inter-site replication times to this value. For an Active Directory Site with more than one DC (i.e., intra-site), replication linked DCs will replicate every five minutes.

Read-only Domain Controller (RODC)

A Read-only Domain Controller (RODC) has read-only partitions of the Active Directory Domain Services (AD DS) database. It can be deployed to a site where there is no network connectivity to hub sites or can be used in cases where AD DS remote access is necessary. Many RODC features can be helpful, including filtered attribute sets, administrator role separation, and Read-only Domain Name System (DNS). For more information on RODC, visit: [Planning Domain Controller Placement | Microsoft Learn](#).

Group Policy Management

The Group Policy Management Console (GPMC) is the main tool for creating, maintaining, and administering GPO settings. GPMC can help facilitate:

- Configurations for devices (desktops and servers), startup, and logon/logoff scripts.
- Security policies for password and account lockouts, system services, and local or host-based firewall settings.
- Access rules for network resources like devices, shared folders, printers, and applications.
- Software deployment such as the installation of software on specific devices.

The Central Store is a folder hosted on domain controllers whose purpose is to centrally store and replicate ADMX/ADML templates for use by all systems in a domain environment. ADMX templates and their corresponding ADML subfolder(s) and files are copied to the Policies\PolicyDefinitions folder in the SYSVOL share on a domain controller, which are then replicated to all domain controllers in the environment. This allows for consistency when creating policies and mitigates the need to manually push or copy new templates to devices. When using the Central Store, devices that receive GPOs do not need the ADMX/ADML files installed locally to properly process and configure the required settings. In Windows® XP and Windows Server® 2003 and earlier, ADM files were used and required that the files exist locally on the system receiving the policies. Another advantage of the Central Store is that domain controllers no longer store or replicate multiple copies of templates. Master files that can be used by multiple policies are established in the Store.

Organization Unit (OU)

When Active Directory is deployed, default containers are created for users, computers, and other objects. These containers provide a similar role to organizational units (OUs), but with less control and delegation abilities. For this reason, it is best to avoid using the default containers except for the built-in Active Directory objects. As a best practice, separate computer accounts, user accounts, and other objects into their own custom OUs and group them logically. Several strategies for organizing these objects are discussed later in this guide. This method allows for easier targeting of distinct policies to the proper objects within the domain.

Computer and User Based Policies

Computer-based policies (GPOs) apply to the device system-wide during startup. This happens before a user logs in to the system and is applied equally regardless of who logs onto that computer. Whereas User-based policies (GPOs) are assigned to user accounts and are applied to the user's profile during system login. Both policy types are refreshed regularly, about every 90 minutes, while a domain controller is reachable. A force sync on or to a device can also be performed for an immediate refresh. This is talked about in greater detail below.

Security Groups

There are two main functions of security groups within the forest and domain, assigning user rights and managing permissions. User Rights determine what actions members of a group can perform within the environment. For example, a user assigned to the Domain Admins group has permission to administer domain controllers. Whereas the Users group does not have permission to make changes to a system, but they can complete tasks such as running an application or shutting down the local computer.

Security groups can also be used to assign Permissions to domain resources like file shares and printers. These permissions determine who has access to the resource and what level of access is allowed, such as Read Only.

Each security group is also assigned a scope, which defines where permissions can be granted in the network. The three scopes are defined as:

- **Universal:** Accounts, domain, and universal groups from any domain in the same forest can be added to groups of this scope, and the group is also visible from any trusted domain. These groups are often used to define roles and manage permissions within the same forest.
Note: Avoid nesting multiple groups as a best practice.
- **Global:** Only accounts and global groups from the same domain can be added to groups of this scope but the group is visible from other trusted domains. Members of this group are usually based on the categorization of business roles (user group) and members often share similar network access requirements. Groups with a global scope are also often used to group computers together (computer group) by a common trait.
- **Domain Local:** This group scope can contain (as members) accounts from any trusted domain, universal groups in the same forest, and domain local groups in the same domain. However, groups of this scope are not visible from other trusted domains. This group can be assigned anywhere within the domain it was created and is often used to assign and manage permissions for access to resources (resource group).

Security Groups should be kept in separate OUs away from other objects and built-in groups. Permissions to resources should never be applied directly to a single object (computer or user), but rather through a group even if that group contains only a single user or computer. For example, if a user is delegated control over resetting user passwords, this should be achieved with a security group and assigned to a group that contains only users designated to reset passwords.

Administrative Template Files (ADMX/ADML)

ADMX/ADML templates were first introduced in Microsoft Windows Vista™ Service Pack 1 and Windows Server® 2008. The two sets of XML files work together and contain necessary information for the OS and GPM to process most end-point settings and their configuration. ADMX files are language agnostic and contain the registry key and desired value pair that will be used by the OS and GPM to enforce the policy on the target system. ADML files are language specific and allow for the management of the same set of configurations using multiple languages, while still ensuring that the underlying registry values remain the same, as defined in the matching ADMX file. ADMX template files are typically stored in the parent ProfileDefinitions folder, and the corresponding ADML template files are stored in a child subfolder that is named by the language /region tag (e.g., en-US for English (United States), fr-FR for French (France), etc.). A full list of language packs supported on Windows and their language/region tags are available from Microsoft at this link: [Available Language Packs for Windows | Microsoft Learn](#).

Figure 4 | AppPrivacy ADMX file

```
<policy name="LetAppsAccessCalendar"
  class="Machine"
  displayName="$(string.LetAppsAccessCalendar_Name)"
  explainText="$(string.LetAppsAccessCalendar_Explain)"
  presentation="$(presentation.LetAppsAccessCalendar)"
  key="Software\Policies\Microsoft\Windows\AppPrivacy">
  <parentCategory ref="AppPrivacy" />
  <supportedOn ref="windows:SUPPORTED_Windows_10_0"/>
  <elements>
    <enum id="LetAppsAccessCalendar_Enum" valueName="LetAppsAccessCalendar">
      <item displayName="$(string.UserInControl)">
        <value>
          <decimal value="0" />
        </value>
      </item>
      <item displayName="$(string.ForceAllow)">
        <value>
          <decimal value="1" />
        </value>
      </item>
      <item displayName="$(string.ForceDeny)">
        <value>
          <decimal value="2" />
        </value>
      </item>
    </enum>
    <multiText id="LetAppsAccessCalendar_UserInControlOfTheseApps_List"
  valueName="LetAppsAccessCalendar_UserInControlOfTheseApps" />
    <multiText id="LetAppsAccessCalendar_ForceAllowTheseApps_List"
  valueName="LetAppsAccessCalendar_ForceAllowTheseApps" />
    <multiText id="LetAppsAccessCalendar_ForceDenyTheseApps_List"
  valueName="LetAppsAccessCalendar_ForceDenyTheseApps" />
  </elements>
</policy>
```

Figure 5 | AppPrivacy en-US ADML file

```
</string>
  <string id="LetAppsAccessCalendar_Name">Let Windows apps access the calendar</string>
  <string id="LetAppsAccessCalendar_Explain">This policy setting specifies whether Windows apps can access the
calendar.
```

You can specify either a default setting for all apps or a per-app setting by specifying a Package Family Name. You can get the Package Family Name for an app by using the Get-AppPackage Windows PowerShell cmdlet. A per-app setting overrides the default setting.

If you choose the "User is in control" option, employees in your organization can decide whether Windows apps can access the calendar by using Settings > Privacy on the device.

If you choose the "Force Allow" option, Windows apps are allowed to access the calendar and employees in your organization cannot change it.

If you choose the "Force Deny" option, Windows apps are not allowed to access the calendar and employees in your organization cannot change it.

If you disable or do not configure this policy setting, employees in your organization can decide whether Windows apps can access the calendar by using Settings > Privacy on the device.

If an app is open when this Group Policy object is applied on a device, employees must restart the app or device for the policy changes to be applied to the app.

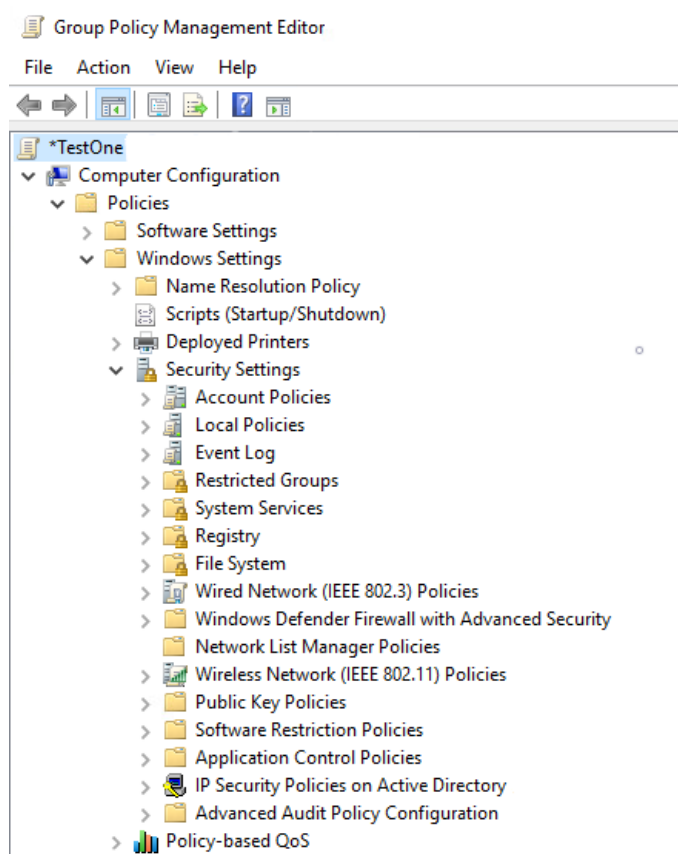
ADMX template packs for the Windows OS are typically updated by Microsoft annually in the second half of the year. Until late 2021, Microsoft maintained one current set of downloadable templates (Windows 10) for use with all OS versions. In late 2021, Microsoft introduced several sets of ADMX/ADML templates, (Windows 10, Windows 11, and a few months later Server 2022), which caused some confusion when using a Central Store. The Central Store is designed to hold only one version of a template at a time and cannot simultaneously accommodate the three sets mentioned above.

CIS evaluated all three sets of templates when they were released and found that the Windows 11 templates are inclusive of all GPO settings needed for the Windows Workstation and Server Benchmarks including older Windows versions. For this reason, CIS suggests using the latest available Windows 11 templates regardless of which Windows OS is being targeted. This ensures seamless central administration of templates. For versioning history of Microsoft's Administrative Templates, please visit: [Create and manage Central Store - Windows Client | Microsoft Learn](#).

In addition to the modern ADMX/ADML templates and built-in security templates, legacy ADM templates are still heavily used by some third-party vendors such as Adobe. ADM templates are Unicode formatted text files that Group Policy uses to describe the location of registry-based policy settings, just like ADMX files. However, they are not language-neutral like their successor and a copy of each ADM template must be kept with the GPO in the domain, which leads to redundant copies of the templates. This is true even when the same ADM template is used by multiple GPOs, and sometimes different versions of the ADM file are needed, as they are not synchronized or updated automatically between GPOs.

Built-in Security Templates: Each OS instance contains a native built-in security template, which is different than the downloadable ADMX/ADML templates. This security template contains security settings (Figure 7 below) which are specific to the OS version. For example, a Windows 11 system may have additional security settings that are not available in some Windows 10 versions. One example of this is the *Relax minimum password length limits* policy setting. This setting was introduced in Windows 10 Release 2004 and does not appear in previous versions of Windows 10. Occasionally, a new setting for the built-in security templates is introduced with a security update for older OS versions.

Figure 6 | Group Policy Management editor showing the built-in Security Template



References are made in the CIS Microsoft Windows Workstation and CIS Microsoft Windows Server Benchmarks when a setting only applies to a specific version of the OS. For example, Recommendation 1.1.6 (L1) *Ensure 'Relax minimum password length limits' is set to 'Enabled'* is only available within the native OS security template of Windows 10 Release 2004, Windows 11, and Server 2022 or newer. Therefore, we only recommend this setting for all releases of Windows 10, Windows 11, and Windows Server 2022 or later OSes. Applying these settings to older OS versions does not have any effect nor inhibit the system's functionality. OSes that do not support these settings will simply ignore them. One advantage of pre-applying the configuration is that it positions the system so if the setting becomes available via a future update it becomes immediately effective and in compliance.

In the CIS Windows Benchmarks, Sections 1-17 are obtained from the OS's built-in security template, and Sections 18 & 19 are obtained from downloadable ADMX templates.

Figure 7 | CIS Microsoft Windows 11 Benchmark Recommendation

1.1.6 (L1) *Ensure 'Relax minimum password length limits' is set to 'Enabled' (Automated)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether the minimum password length setting can be increased beyond the legacy limit of 14 characters. For more information, please see the following [Microsoft Security Blog](#).

The recommended configuration is:

Note: This setting only affects accounts that are local to the computer.

Rationale:

This setting allows for the use of longer passwords, which increases the security of the system. The Minimum password length setting is a security control that prevents users from creating passwords that are too short. If very long and increases the number of characters, it increases the security of the system.

Impact:

The Minimum password length setting is a security control that prevents users from creating passwords that are too short. If very long and increases the number of characters, it increases the security of the system.

Audit:

Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy > Relax minimum password length limits**. The **Relax minimum password length limits** setting should be set to **Enabled**.

REG_DWORD

HKLM\System

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies>Password Policy\Relax minimum password length limits

Note: This setting is only available within the built-in OS security template of Windows 10 Release 2004 and Server 2022 (or newer) and is not available via older versions of the OS, or via downloadable Administrative Templates (ADMX/ADML). Therefore, you must use a Windows 10 Release 2004 or Server 2022 system (or newer) to view or edit this setting with the Group Policy Management Console (GPMC) or Group Policy Management Editor (GPME).

Default Value:

Disabled. (The *Minimum password length* may be configured to a maximum of 14 characters.)

References:

- <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>
- <https://support.microsoft.com/en-us/topic/minimum-password-length-auditing-and-enforcement-on-certain-versions-of-windows-5ef7fecf-3325-f56b-cc10-4fd565aacc59>
- <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy>

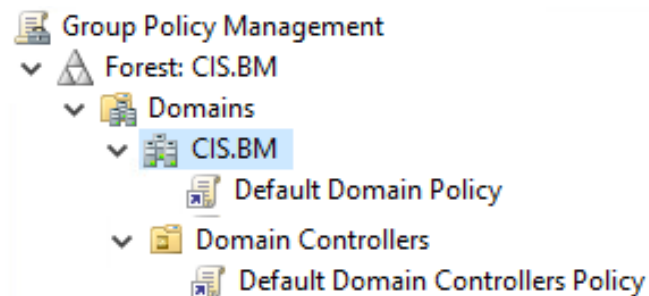
CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

Default Domain Policy and Default Domain Controller Policy

The Default Domain Policy (DDP) and Default Domain Controller Policy (DDCP) are the first GPOs in a new domain, provided automatically when the domain is created. The DDP sits at the top of the structural hierarchy and affects all Users and Computers in the Domain. Whereas the DDCP is only applied to Domain Controllers. These two policies contain Microsoft's default security settings such as account password criteria, account lockout thresholds, and Kerberos policies which establish a baseline level of domain security.

Figure 8 | Linked location of the Default Domain Policy and Default Domain Controller Policy



As a best practice, if a configuration needs to be updated for an existing setting within the default policies, such as to make it CIS-compliant, it should be updated within these policies and not in a separate GPO. All other new settings configured for the environment, but not originally contained within these policies, should be created in a new, separate GPO.

Figure 9 | Example of the Default Domain Policy

Default Domain Policy	
Data collected on: 10/17/2024 11:54:28 AM	
General	
Computer Configuration (Enabled)	
Policies	
Windows Settings	
Security Settings	
Account Policies/Password Policy	
Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Account Policies/Account Lockout Policy	
Policy	Setting
Account lockout threshold	0 invalid logon attempts
Account Policies/Kerberos Policy	
Local Policies/Security Options	
Network Access	
Policy	Setting
Network access: Allow anonymous SID/Name translation	Disabled
Network Security	
Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled
Public Key Policies/Encrypting File System	
Certificates	

In the Microsoft Windows Benchmarks, recommendations for settings within the DDP and DDCP contain a note to ensure these settings are configured properly. For a comparison of default Microsoft Windows Server 2019 and 2022 policies to the CIS recommended configured state, see [Appendix A](#) and [B](#).

Figure 10 | Example of a Windows Benchmark note regarding the Default Domain Policy

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines the number of renewed, unique passwords that must be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for stand-alone systems is 0 passwords, but the default setting when joined to a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password.

The recommended state for this setting is: **24 or more password(s)**.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are separate from Group Policy and most easily configured using Active Directory Administrative Center.

If the default policies become corrupt or the policy needs to be reverted to its original state, there is a built-in command line tool *dcgppfix* (Windows\System32\dcgppfix.exe) that is available with all versions of Windows Server. This tool can recreate the Default Domain Policy and Default Domain Controller Policy GPOs. This tool does not restore or recreate any other policies within the domain and is only intended for use in disaster recovery scenarios. Backups of all other policies are still required.

One small but important recommendation for the DDP is to change the *Allow users to encrypt files using Encrypting File System (EFS)* setting to Disabled when building a new domain. This ensures that the EFS is disabled from the start on all domain-joined computers. EFS makes files more difficult to backup or recover when the user loses access to or deletes them. With modern disk encryption tools such as BitLocker, the entire drive can be encrypted rather than targeting individual files. Encrypting files with EFS may result in them not being able to be recovered and/or decrypted. If the existing domain has this feature Enabled, investigate if any users are currently using EFS and decrypt the files before changing this setting to avoid unexpected data loss.

Figure 11 | Example the EFS Policy when Disabled

Default Domain Policy	
Data collected on: 10/17/2024 11:49:13 AM	
General	
Computer Configuration (Enabled)	
Policies	
Windows Settings	
Security Settings	
Account Policies/Password Policy	
Account Policies/Account Lockout Policy	
Account Policies/Kerberos Policy	
Local Policies/Security Options	
Public Key Policies/Encrypting File System	
Properties	
Policy	Setting
Allow users to encrypt files using Encrypting File System (EFS)	Disabled
Encrypt the contents of the user's Documents folder	Disabled
Require a smart card for EFS	Disabled
Create caching-capable user key from smart card	Disabled
Enable pagefile encryption	Disabled
Display key backup notifications when user key is created or changed	Disabled
Allow EFS to generate self-signed certificates when a certification authority is not available	Disabled
Key size for self-signed certificates	Disabled
EFS template for automatic certificate requests	Disabled
Cache timeout	Disabled
Clear cache when user locks workstation	Disabled
Certificates	

Organizational Unit Naming and User and Computer Settings

Organizational Units play a key role in organizing and managing objects such as computers and users within the domain. Access control lists (ACLs) can be used for delegation of authority and permits the owner of the object to transfer full or limited administrative control to other users or groups. They can also be used to separate objects from each other and restrict access to resources via Group Policy assignments.

A well thought out OU design can decrease issues with implementing and managing group policies, delegating permissions, auditing, and can simplify administrative tasks such as bulk changes and reporting.

There are several predominant ways to organize Active Directory: location based, logical or departmental based, and a mix of the two. Each of these models has its own advantages and the decision regarding which to use should be thoughtfully planned and tested before a design is implemented.

For optimal Group Policy management, it is recommended to start at the top level of Active Directory by separating all objects via type, such as Domain Users, Domain Computers, and Domain Groups. It is also a good idea to create a separate OU for more privileged user accounts like admins, service accounts, etc., and manage them separately from standard user accounts. Within each of these object type-based OUs additional sub-OUs can be created as needed. One example of this would be creating Member Servers and Workstations OUs inside of Domain Computers to apply targeted group policies more easily to the respective computer types.

Beyond object-type separation, there are some other OU structure considerations to consider, which may affect the design of the OU structure:

In a location or geographically based structure, each OU is based on the device's physical location. This model is best for organizations that have multiple locations and the need to apply specific policies locally. For example, one office might contain devices used for software development and need exceptions to policies the rest of the organization does not require. Another location might contain devices open for public use and access to these systems would require tighter control.

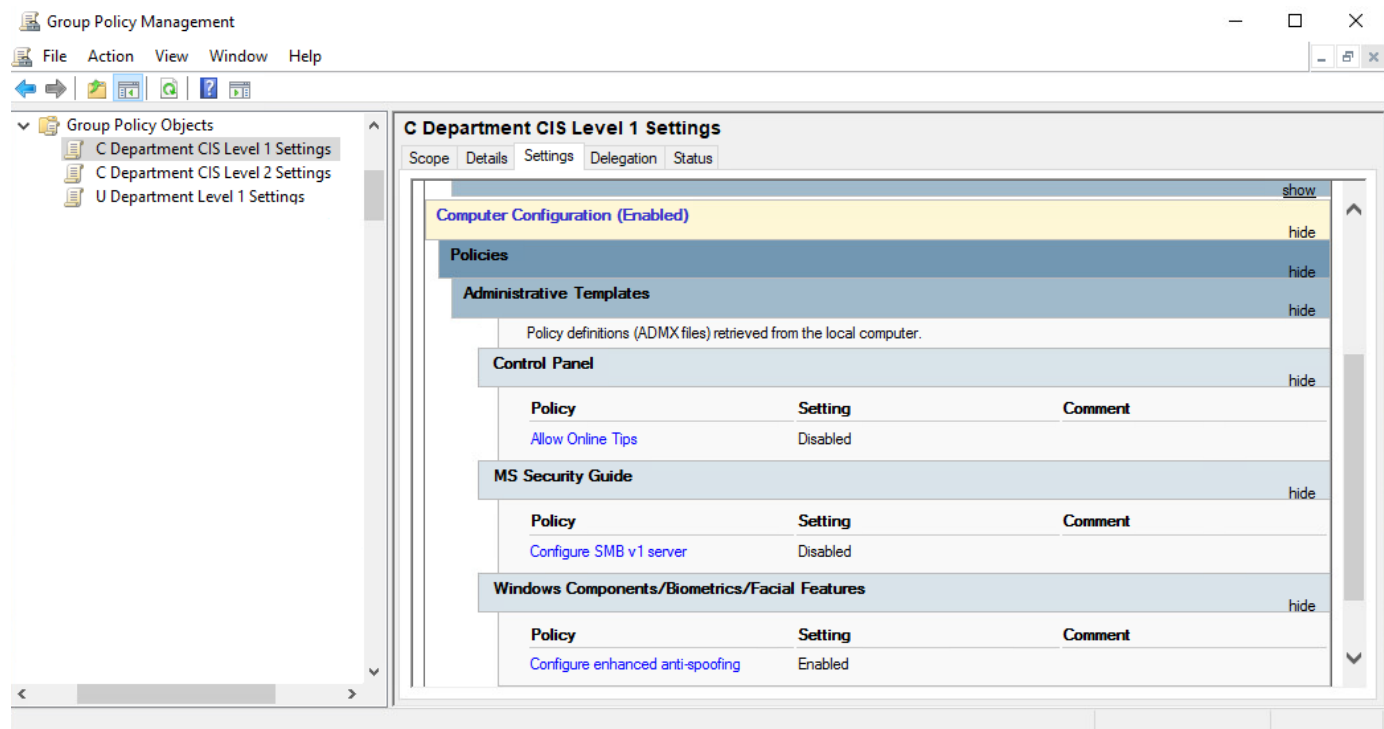
In a logical or departmental-based structure, each OU is based on the logical component of the organization like Human Resources (HR), Finance, or Support. This structure allows for granularity of GPOs and security filtering by job function. For example, Support employees might need access to Remote Desktop, whereas an accountant in Finance would not.

A hybrid of the two, location and departmental based, allows for the separation of locations and sub-OUs that contain departments within the location. This model allows for even more granular policies to be strategically pushed and controlled for each department within that locale. This allows for the most organized and logical approach to Active Directory organization. The examples used above are also valid for this structure, but instead of being a department or function, departments or functions could be distributed across many locations.

Within this structure, consideration of whether to use monolithic (few larger) or distributed (many smaller) group policies is a decision that each organization should evaluate when designing and architecting the Active Directory environment.

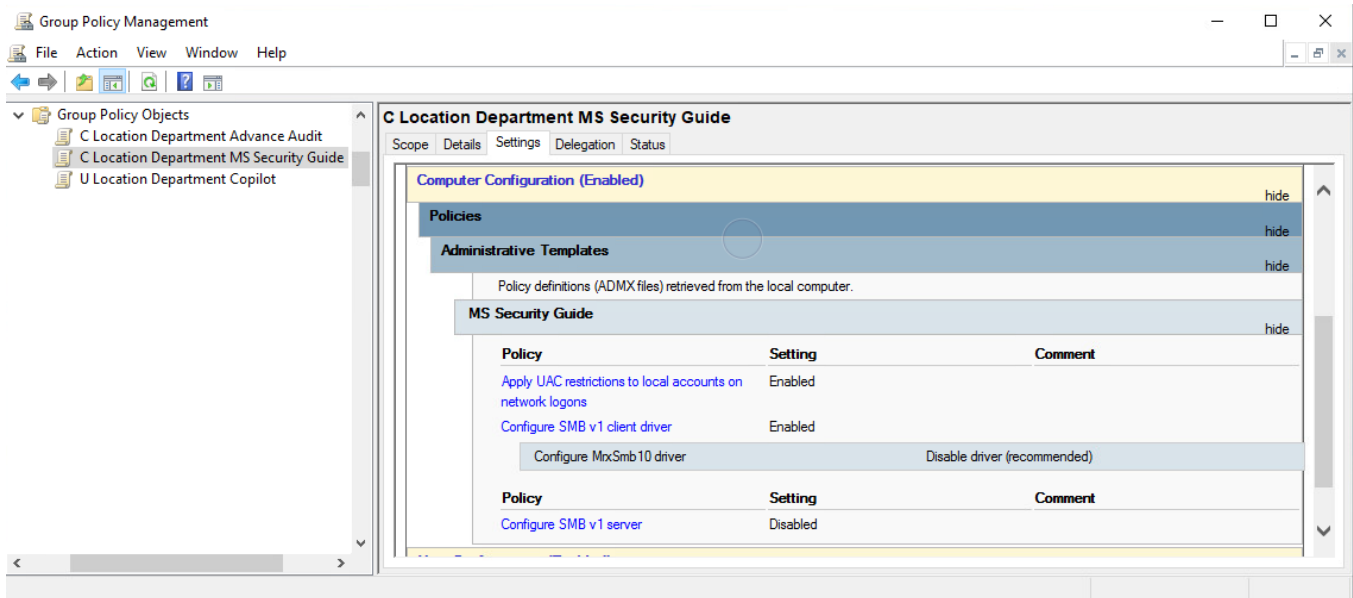
For smaller organizations, a monolithic structure is lower maintenance and tracking of policies is less complex. In this design, granularity is sacrificed, and more exceptions and security filtering could be needed.

Figure 12 | Example of monolithic policies within a location-based structure



For larger organizations (enterprise level), the use of distributed policies may be more practical as custom configurations for locations and/or departments might be required. This allows granular policies to be applied for each location and/or department within that location, necessitating fewer exceptions. All policies should be grouped by similar settings and a procedure should be put in place to determine how policies are created and maintained.

Figure 13 | Example of distributed policies within a location-based structure



Regardless of the chosen design, a clear policy naming convention should be used. Group Policy Objects within GPMC all live together without a strict structure and enforcing a clear and meaningful naming policy helps with organization and is vital to the management of these policies. While GPO names have few limitations, the chosen naming convention should be consistent throughout the domain. Some aspects of the convention might differ if a logical versus a departmental-based structure is used.

One way to aid with naming conventions and the organization of policies is by using a multi-part naming system. This multi-part naming supports a location-based, department-based and hybrid model.

- **First part: “Type”** | Determine if this will be a User or Computer Policy. Typically, a capital U is used to depict user settings, and a capital C is used for computer settings. In addition, a capital A could be used to depict accounts with elevated privileges.
- **Second part: “Location”** | Determine which location (or a delimiter like ALL for organization-wide) this policy will apply. For example, if all offices are in one state, then the name of the city/town could be used. If there are locations throughout multiple states, the state abbreviation followed by the town/city could be used. Also, office locations might already have a recognized name; in this case, use what is already in place. Even under a purely department model, adding the location better positions the architecture for future growth or necessary subdivisions.
- **Third part: “Department”** | Determine which department (or a delimiter like ALL for organization-wide) this policy will apply, for example HR or Support. Like the location delimiter above, defining the department in a purely location model allows for future growth without breaking the naming convention.

- **Fourth part: “Policy”** | Create a short descriptive name for what this policy addresses. For example, if the GPO is being created to ensure systems have advanced auditing turned on, the fourth part could be named “Advanced Audit.”

Each of these parts can be combined in any order to produce a name that is useful and meaningful within the organization. Dashes (RFC complaint) can be used to separate the parts of the name, or they can be left out if desired. GPO names can contain letters, numbers, and special characters and must be no longer than 255 characters in length. Keep in mind that the longer the GPO name, the more difficult it will be to view it in GPME. Examples of different naming conventions are below in Table 2.

GPOs contain a comment field that can store information about the policy such as the owning administrator’s name, what type of object it applies to, a description of the policy, and its purpose. This ensures that GPOs are transparent and easy to manage and maintain.

Table 2 | Example of naming conventions

Type	Location	Department	Policy	Completed Name
C	ALL	FIN	Firewall Open Port 1234	C-ALL-FIN-Firewall Open Port 1234
C	DRYDEN	SUP	MS Security Guide	C-DRYDEN-SUP-MS Security Guide
C	GENOA	HR	MS Security Guide	C-GENOA-HR-MS Security Guide
C	GENOA	SUP	MS Security Guide	C-GENOA-SUP-MS Security Guide
U	DRYDEN	SUP	Cloud Content	U-DRYDEN-SUP-Cloud Content
U	GENOA	SUP	Copilot	U-GENOA-SUP-Copilot

Location	Department	Policy	Type	Completed Name
ALL	FIN	Firewall Open Port 1234	C	ALL-FIN-Firewall Open Port 1234-C
DRYDEN	SUP	MS Security Guide	C	DRYDEN-SUP-MS Security Guide-C
GENOA	HR	MS Security Guide	C	GENOA-HR-MS Security Guide-C
GENOA	SUP	MS Security Guide	C	GENOA-SUP-MS-Security Guide-C
DRYDEN	SUP	Cloud Content	U	DRYDEN-SUP-Cloud Content-U
GENOA	SUP	Copilot	U	GENOA-SUP-Copilot-U

In the end, the naming convention used should work for the organization and allow administrators to easily identify the users or systems where the policy applies.

With the MS16-072 (June 14, 2016) security update, Microsoft changed the behavior of how Group Policy processes user-based GPOs. Since then, the targeted user or group of users have access to the GPO, but the computer processing the GPO explicitly needs Read rights to it. Therefore, when creating a user-based GPO, the permissions of the GPO need to be updated to permit Domain Computers to have Read permission. Without granting this right to a user-based GPO, it will not be processed by the user accounts. The GPO does not need to have Domain Computers in Security Filtering because that grants both Read permission and Apply group policy permission.

Group Policy Management Hierarchy

It is extremely important where GPOs are linked within the hierarchy as they are processed in a specific order. Policies that are initially applied within the hierarchy will be overwritten by later policies. An effortless way to remember the order in which they are processed is the acronym LSDOU, which stands for Local, Site, Domain, and Organizational Unit.

- **Local:** GPOs that are set locally (either manually or via a tool) apply to the system first and have the lowest precedence. These policies are overwritten by Site, Domain, and OU settings.
- **Site:** GPOs applied at the Site level affect the domains contained in it. These policies are overwritten by Domain and OU settings.
- **Domain:** GPOs at this level affect all OUs within the domain. These policies are overwritten by the direct OU settings.
- **Organizational Unit:** GPOs applied at the OU level and the closest to the object take precedence over all other policies.

If the GPO is set to Enforced, it changes the processing order of LSDO. The Enforce option takes precedence over GPOs lower in the order, reversing SDOU for those GPOs to OUDS. These GPOs are always processed last, ensuring they supersede non-enforced GPOs, which can contain the same settings. GPOs set to Enforced cannot be blocked using the Block Inheritance feature on an OU.

Multiple GPOs can be applied to the same object at the same level, and in this case the GPO with the lowest link order has precedence. (Figure 14 below). If the same setting exists in two GPOs and linked to the same OU, a lower link order value will take precedence.

Figure 14 | Example of link order.

	Link Order	GPO	Enforced	Link Enabled	GPO Status
▼ CISWorkstation					
C Department CIS Level 1 Settings	1	C Department CIS Level 1 Settings	No	Yes	Enabled
C Department CIS Level 2 Settings	2	C Department CIS Level 2 Settings	No	Yes	Enabled

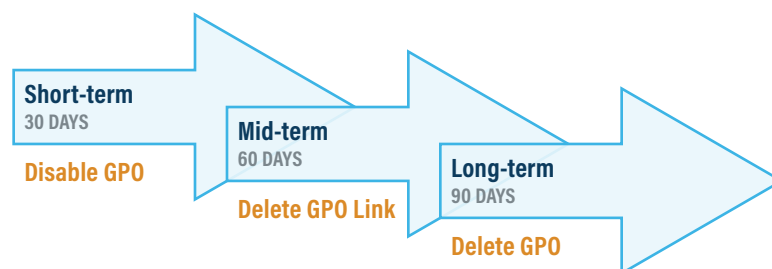
As a best practice, policies should rarely be applied at the root of the domain. This is typically done when there is a clear need to have a domain-wide GPO that applies to everything including domain controllers. In most cases, applying GPOs at the OU level is more desirable as this allows the targeting toward specific types of systems or users which facilitates implementation and troubleshooting.

There is one exception to the LSDO rule, which is loopback processing. This setting causes local group policy to be applied again at the end of the group policy refresh process. This setting should be used with caution and only when necessary because it allows anyone with local admin rights to override domain group policy settings. Instead, it is better to build a custom domain group policy for the use case settings and apply this policy to the system. Some adjusting may be needed to have it take precedence over other policies that would cause an issue for that system. Unique use cases can include a kiosk device that needs to be locked down for public use, or a case where a vendor product is dependent on local policy.

When policies are no longer useful, it is often recommended to delete the policy from the database rather than disabling it. CIS recommends a more staged approach and a three-step procedure: Disable, Unlink, then Delete. Taking this precaution ensures that accidental deletion of a necessary policy is avoided. Depending on the organization, when to disable, delete the link, and delete the policy should be discussed and policies and procedures put into place. Below is an example timeline for each step. Note: Dates are cumulative:

- **Short-term (30 Days):** Keep the GPO in place and disable it.
- **Mid-term (60 Days/Disable date +30):** Unlink the GPO from the OU where it is applied.
Note: When unlinking the GPO from an OU in GPME, the option needed to perform this is labeled delete.
- **Long-term (90 Days/Unlink date +30):** Delete the GPO from Active Directory.

Figure 15 | Example of a GPO deletion policy.



Security Filtering

OUs handle most cases where selectively applying GPOs to specific users or computers is desired. If more granularity is required, security filtering can be assigned to GPOs to further allow or deny specific policies from being applied to users, computers, or groups. There are cases where this is beneficial if an object must stay in an OU for organizational purposes but requires deviations from the GPOs applied to that OU.

There are two primary methods for filtering a GPO:

- **Allow:** Requires adding the object to the security filtering list on the GPO.
- **Deny:** Requires utilizing the delegation tab to explicitly deny permissions and is used to block a targeted exception/exclusion group from otherwise receiving the GPO (opt out).

Allow

To use security filtering with the allow method, either create a new security group or use an existing one. If an existing group is used, ensure that only needed objects are present.

To apply security filtering to a GPO using a security group:

- 1 Open GPMC and select the GPO to be changed.
- 2 Under the Scope tab, navigate to Security Filtering, select *Authenticated Users*, and click **Remove*.
- 3 Click *Add*, select the appropriate security group, click OK.
- 4 For user-based GPOs only:
 - a Click to change to the *Delegation* tab, then *Add Domain Computers* with *Read* permissions into the *Delegation* object.

When removing *Authenticated Users* from security filtering, the console will display a dialog message advising to add either *Authenticated Users* or *Domain Computers* with *Read* permissions. This is done in the *Delegation* tab and is a requirement for user-based GPOs. Without Step 4 above, a user-based GPO will not be applied to users or groups defined under Security Filtering, rendering it ineffective. However, the step is unnecessary for computer-based GPOs, as they automatically receive *Read* permissions alongside the *Apply group policy* permissions when added to Security Filtering.

Deny

As with other ACLs, deny takes precedence over allow. To prevent certain groups, users, or computers from receiving a GPO use the Delegation tab:

- 1 Open GPMC and select the GPO to be changed.
- 2 Under the *Delegation* tab, click the *Advanced* button at the bottom right.
- 3 Click *Add*, enter the appropriate user, computer, or security group, and click *OK*.
- 4 Select the principal that was just added, in the *Deny* column, click to place a check mark for the *Apply group policy* permissions, and click *OK*.
- 5 Answer *Yes* to the warning that appears for the Deny permissions taking precedence.

WMI Filtering

Windows Management Instrumentation (WMI) filtering is like security filtering; the key difference is that it allows for the filtering of computer objects based on attributes selected in a WMI query and it is dynamically updated. WMI filtering allows organizations to filter for things like OS versions, registry settings, processor architecture, etc.

While WMI filters are useful, overuse can cause delays during computer startup and user login, especially when using the Win32_Product class. This class validates every installed MSI package on the system and is therefore extremely resource intensive. In general, security filtering is a better option than WMI filtering, but certain use cases make WMI filtering a preferable option. Both filtering methods can be used in tandem for better refinement.

Creating and managing WMI filters is accomplished in GPMC. However, knowledge of the WMI Query Language (WQL) is needed to create these filters.

To create a WMI filter:

- 1 Open GPMC and expand the domain.
- 2 Right click WMI Filters, click *New*.
- 3 Enter a name and description.
- 4 Click *Add* to create the query.
- 5 Once completed, click *OK* to save the query to the filter.
- 6 Click *Save* to save the filter itself.

Figure 16 | Example of a WMI filter creation.

The screenshot shows a dialog box titled "CIS Filter Test" with a close button (X) in the top right corner. It contains the following fields and controls:

- Name:** A text box containing "WMI Filter Test".
- Description:** A text box containing "Only Apply to Domain Controllers".
- Queries:** A table with two columns: "Namespace" and "Query".

Namespace	Query
root\CIMv2	SELECT * FROM Win32_OperatingSystem WHERE ProductType="2"
- Buttons:** "Add", "Remove", and "Edit" buttons are located to the right of the Queries table. "Save" and "Cancel" buttons are at the bottom right of the dialog.

To link the WMI filter to a GPO:

- 1 Select the target GPO and click the Scope tab.
- 2 Choose the appropriate WMI filter from the drop-down menu
- 3 Click Yes.

Figure 17 | Example of a WMI filter linked to a GPO.

The screenshot shows the "WMI Filtering" section of a Group Policy Object (GPO) configuration. It includes the following elements:

- Section Header:** "WMI Filtering".
- Text:** "This GPO is linked to the following WMI filter:".
- Drop-down Menu:** A menu showing "<none>" as the selected option, with a list of available filters below it, including "WMI Filter Test".
- Button:** An "Open" button located to the right of the drop-down menu.

A single WMI filter can be applied to multiple GPOs, but each GPO can only have one WMI filter applied to it. However, a WMI filter can be written with multiple conditions.

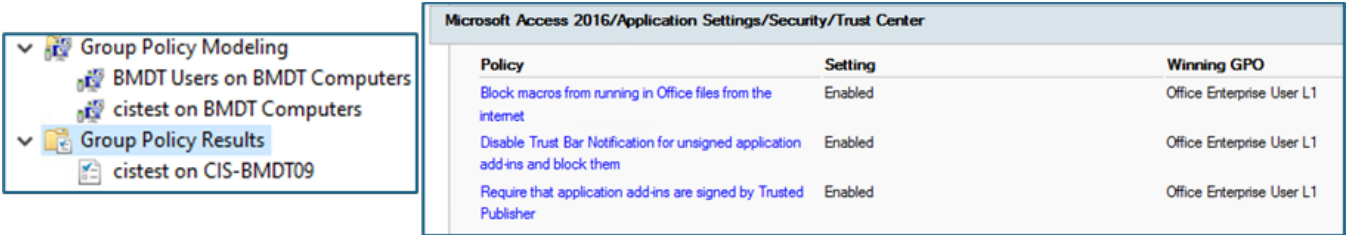
Group Policy Tools

Active Directory has several built-in tools that simplify the testing process and help facilitate troubleshooting of Group Policy. A few of these tools are discussed below.

Group Policy Results

Group Policy Results Wizard is a GPMC feature available on the Domain Controller that displays every setting applied to a system formatted in HTML. In the context of Benchmarks, it helps determine whether a GPO assigned to an OU has been effectively applied to a user or device. This tool is particularly useful for navigating filtering and precedence of GPOs. In the case of conflicts, it shows the winning policy and displays the individual configured settings within each GPO.

Figure 18 | Example of Group Policy Results and HTML view.



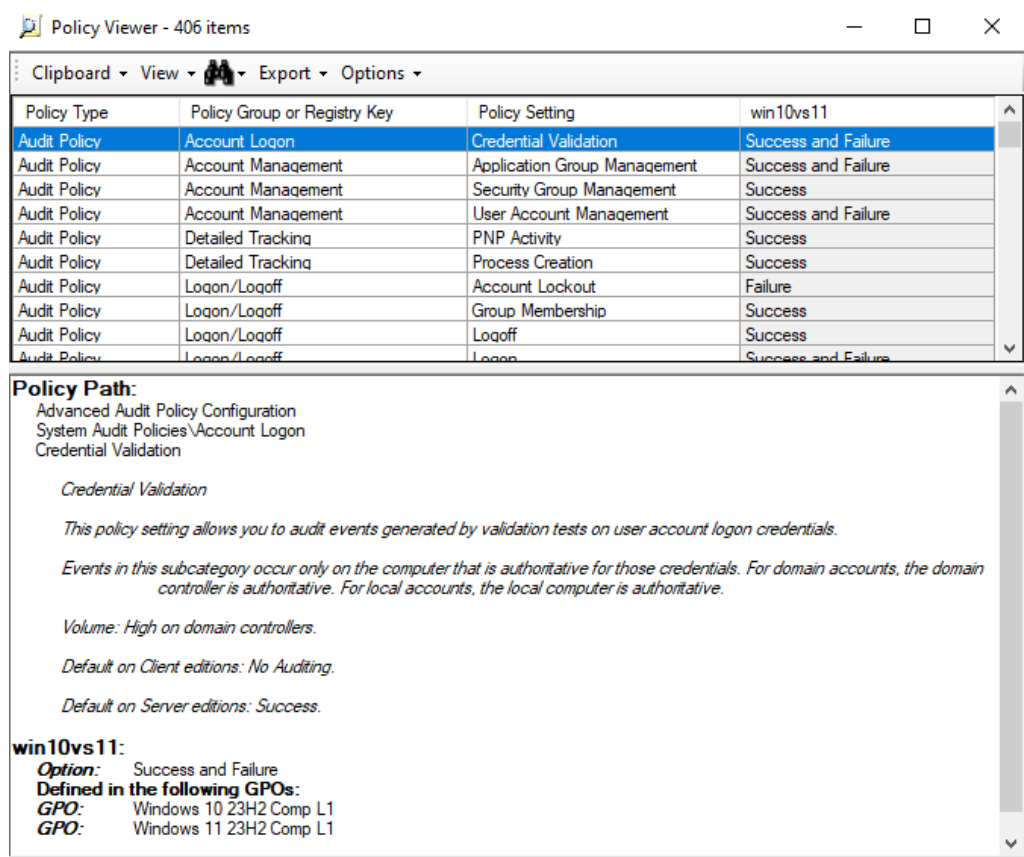
Gpresult

The *gpresult* command is a command-line interface (CLI) tool available on every domain-joined system and displays the Resultant Set of Policy (RSOP) for a user or computer. It can generate either a text report or a more comprehensive HTML report like those created in GPMC. While *gpresult* can be used remotely or locally, it is typically run on a local system via the Command Prompt to determine which policies have been applied. The *gpresult* command requires local administrative rights to report on GPOs applied to the local computer but does not require special privilege for reporting on GPOs applied to the logged-in user account.

Microsoft Policy Analyzer

Microsoft Policy Analyzer (Policy Analyzer) is a tool available as part of the [Microsoft Security Compliance Toolkit](#) that can analyze and compare sets of GPOs. It highlights redundant settings or inconsistencies and can compare GPOs against the current local policy and local registry settings. Results can easily be exported to a Microsoft Excel spreadsheet for further analysis. This tool is particularly useful for comparing the differences between two versions of CIS Build Kits or a CIS Build Kit versus what is currently enforced in an environment. Below is an example of GPOs for the Level1 Profiles from the CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 and the CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0.

Figure 19 | Example of CIS Microsoft Windows 10 Benchmark v3.0.0 and CIS Microsoft Windows 10 Benchmark v3.0.0 Build Kit Policies.



Policy Viewer - 406 items

Clipboard View Export Options

Policy Type	Policy Group or Registry Key	Policy Setting	win10vs11
Audit Policy	Account Logon	Credential Validation	Success and Failure
Audit Policy	Account Management	Application Group Management	Success and Failure
Audit Policy	Account Management	Security Group Management	Success
Audit Policy	Account Management	User Account Management	Success and Failure
Audit Policy	Detailed Tracking	PNP Activity	Success
Audit Policy	Detailed Tracking	Process Creation	Success
Audit Policy	Logon/Logoff	Account Lockout	Failure
Audit Policy	Logon/Logoff	Group Membership	Success
Audit Policy	Logon/Logoff	Logoff	Success
Audit Policy	Logon/Logoff	Logon	Success and Failure

Policy Path:
Advanced Audit Policy Configuration
System Audit Policies\Account Logon
Credential Validation

Credential Validation

This policy setting allows you to audit events generated by validation tests on user account logon credentials.

Events in this subcategory occur only on the computer that is authoritative for those credentials. For domain accounts, the domain controller is authoritative. For local accounts, the local computer is authoritative.

Volume: High on domain controllers.

Default on Client editions: No Auditing.

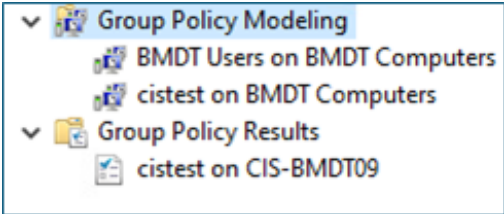
Default on Server editions: Success.

win10vs11:
Option: Success and Failure
Defined in the following GPOs:
GPO: Windows 10 23H2 Comp L1
GPO: Windows 11 23H2 Comp L1

Group Policy Modeling

The Group Policy Modeling Wizard is a feature of GPMC on each domain controller that creates a series of ‘what if’ scenarios for Group Policy. Unlike Group Policy Results, it simulates the net effect of GPOs based on chosen conditions. This powerful tool is ideal for testing before deploying policies or moving users and computers to different OUs. However, be aware it does not consider any local policies applied to the system and in some situations, this can cause a difference between the simulation and actual results if the local policy would take precedence.

Figure 20 | Group Policy Modeling.

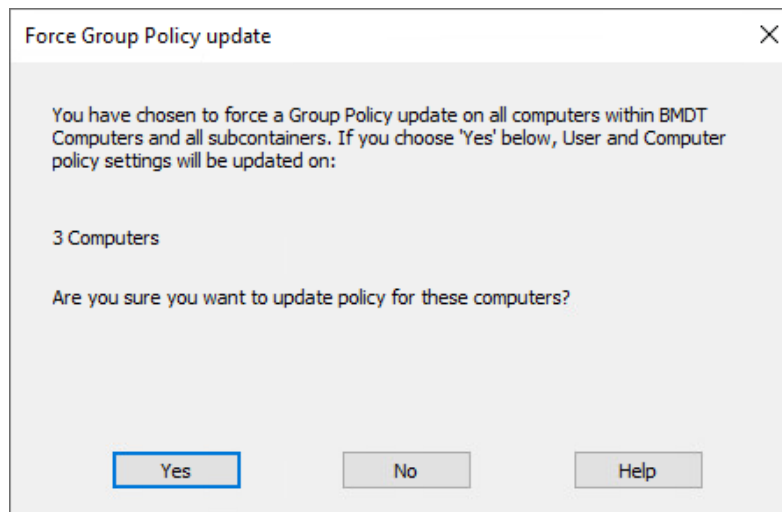


Group Policy Update

Group policy is periodically refreshed in the background to apply new or changed policies. This refresh is triggered whenever a new GPO is linked, unlinked, an ACL changes, or an object is moved in or out of an OU. A manual refresh is sometimes helpful for troubleshooting and testing. This can be done through the GPMC or via the command line using *gpupdate*. Windows clients automatically refresh group policy in the background about every 90 minutes, provided a DC is reachable.

To perform a remote update of group policy using GPMC, right-click on the appropriate OU and select *Group Policy Update*. If the OU contains computer objects, a dialog box will guide the administrator through the process. Note that User Settings will not be applied until a user logs in to the system.

Figure 21 | Example of forcing a group policy update from GPMC.



To manually refresh policies using *gpupdate*, run this command from a CLI such as CMD.exe or PowerShell. The *gpupdate* command can be run locally on the target computer or remotely from another system. When possible, avoid using the */force* switch unless there is a specific need. The */force* switch will force all GPOs to be reapplied from a DC which can increase system congestion unnecessarily. Running *gpupdate* without the */force* switch will apply only to the parts of the policy that have changed since the last Group Policy refresh. When the Group Policy Update feature mentioned above is used, the */force* switch, is automatically applied, so all GPOs will be reapplied. Unlike the *gpresult* command, the *gpupdate* command does not require elevated rights to operate. Both computer and user GPOs will be refreshed, provided a domain controller is reachable, for any user running this command.

To ensure that group policy refresh remains enabled, it is important that the following recommendation is applied to each device as detailed in the Windows Workstation and Server OS Benchmarks.

18.9.19.7 (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting prevents Group Policy from being updated while the computer is in use. This policy setting applies to Group Policy for computers, users and Domain Controllers.

The recommended state for this setting is: **Disabled**.

Rationale:

This setting ensures that group policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with the key not existing.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:DisableBgndGroupPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Group Policy\Turn off background refresh of Group Policy
```

Note: This Group Policy path is provided by the Group Policy template **GroupPolicy.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Backup and Restoration

Regularly backing up GPOs is highly encouraged and should be part of an ongoing operations and disaster recovery plan. This can help facilitate a quick recovery if the domain is compromised or the GPO becomes corrupt. Manually recreating GPOs and going through the necessary planning, testing, and deployment can be costly and time consuming for organizations. GPMC has a built-in feature for archiving, restoring, copying, and migrating of GPOs. For more information on this process visit, [Backup and restore Group Policy in Windows | Microsoft Learn](#).

Backups should be created at least quarterly and stored on a separate system and preferably on a separate network. This ensures continuity and a clean restoration if a breach or corruption occurs. Backups can be done one of two ways, singularly (one GPO), or for all GPOs with the domain. The process is similar for both methods, as detailed below.

To back up one GPO in the domain:

- Right-click the desired GPO and select *Back Up*.
- Navigate to the path where the backup will be stored and enter a description.
- Click *Back Up*

To backup all GPOs in the domain:

- Right-click Group Policy Objects container and select *Back Up All*.
- Navigate to the path where the backup will be stored and enter a description.
- Click *Back Up*.
- After the backup operation is complete, a summary will be displayed.

Restoring deleted and backed up GPOs to a domain is just as simple as the backup process above.

To restore a GPO to a domain:

- Create a new GPO or navigate to the existing GPO to be restored, right-click, select *Restore from Backup*.
- Click *Next*, navigate to the location where the backup is located.
- Select the backup copy to be restored, click *Next*.
- Click *Finish* to restore the GPO.

To restore a deleted GPO:

- Right-click the Group Policy Objects container and select *Manage Backups*.
- From the Manage Backups dialog box, select *Browse* and navigate to the GPO to be restored from the backed-up GPOs.
 - Select *OK* to confirm the restore operation.
 - After the backup operation is complete, a summary will be displayed.

Change Management

Change management is a necessary part of basic system security; it can also minimize user connectivity issues and plays a key role in a healthy Active Directory ecosystem. An effective change management process facilitates the tracking of when, why, and who modified a policy. Having a reliable process in place will aid in performing a roll-back in the least disruptive manner possible.

Microsoft's Advanced Group Policy Management (AGPM) works with GPMC to provide change control for GPOs and is part of the Microsoft Desktop Optimization Pack (MDOP). AGPM stores a copy of each GPO in a centralized archive. This allows administrators to check GPOs in and out and modify them offline, so the active GPO is not affected. After being checked back in, the changes can be reviewed, approved, and deployed to production. A versioned copy of each GPO is saved in the archive to allow rolling back to an earlier version if unanticipated issues arise.

Warning: For AGPM to be effective, all Domain Administrators must use the AGPM snap-in to ensure consistent change control. If they bypass it by using GPMC or another tool, there will be no versioning nor accountability of the changes made.

Role-based delegation in AGPM allows domain administrators (AGPM Administrators) to delegate roles to individuals to specific GPOs without granting access to the entire domain GPO library. This also helps enterprises satisfy separation of duties requirements by providing edit, review, and approval roles.

AGPM specific defined roles are:

- **GPM Administrator:** Has full control and contains the permission set of all other roles.
- **Approver:** Can deploy GPOs to the production environment.
- **Editor:** Can edit GPOs, but not deploy them to production.
- **Reviewer:** Can review the GPOs settings in a report, all other roles have this ability too.

CIS Build Kits

CIS Build Kits (Build Kits) assist in the automated hardening of systems and are designed to correspond to the Benchmarks Remediation section. Build Kits for Microsoft Windows OSes are based on GPOs and are intended for use with on-prem (GPMC) and stand-alone systems (LGPO) only. Build Kits will remediate the system to the recommended state described by the Benchmark and are an excellent resource to accelerate the adoption of a Benchmark. Build Kits are created for:

- Automating the implementation of Benchmark Recommendations.
- Tailoring for an organization's specific security needs.
- Build Kits are available for Microsoft Windows Workstation and Server, Microsoft Intune, Microsoft Office and Edge, Apple macOS, various Linux distributions, Mozilla Firefox, and more.

Separate Build Kits are created for domain-joined and stand-alone systems due to the difference in recommendations within these Benchmarks. Download the correct Build Kit for the type of system to be configured.

For CIS group policy-based Benchmarks, Build Kits are intended to be applied to the system using GPME. Included with each Build Kit are README files containing valuable information about the Build Kit and instructions on how to properly apply them.

Figure 23 | Example of the Windows 11 README document.

Introduction

The purpose of this document is to describe the components of the CIS Microsoft Windows Build Kit and provide instructions on how to implement it. Build Kits are designed to cover most of the benchmark recommended settings, except for those which cannot be managed through group policy. **These templates can be modified in alignment with organizational defined policies.**

Note: Prior to applying a Build Kit, ensure that the most recent Microsoft Windows 11 Administrative Templates (applicable to both workstation and server OS versions) have been downloaded directly from Microsoft and installed on the system.

WARNING: Reviewing the content within the corresponding Benchmark PDF or Word document is imperative for an overall successful application of the Build Kit. Some settings may need an exception due to unique operational requirements.










Applying the Build Kit to a system without proper testing and review may result in a negative impact within the environment.

It is acceptable if 100% of the benchmark is not applied, as it is the responsibility and decision of each organization to determine which settings are applicable to their unique needs.

The Windows Workstation Benchmarks and Build Kits are made for **domain-joined** systems and not stand-alone/cloud systems.

Build Kits for group policy-based Benchmarks are made up of GPOs aligned to the Profiles contained within the Benchmark. For each Profile, a GPO is created based on the type of settings it contains. Build Kits for smaller Benchmarks, like Mozilla Firefox, typically contain only two GPOs (Level 1 and Level 2) while others, like Microsoft Windows 11 contain multiple separate GPOs. For example, if the *COMP-L1*, *SERVICES-L1*, and *USER-L1* Build Kits are applied to the system they contain all the necessary configurations to comply with the Microsoft Windows 11 Level 1 Profile for the Windows Workstation OS Benchmark.

Figure 24 | Example of the CIS Windows Server 2022 Build Kit.

Name	Date modified
 BITLOCKER	6/26/2024 8:49 AM
 COMP-L1	6/26/2024 8:49 AM
 COMP-L2	6/26/2024 8:49 AM
 IPv6 Template	6/26/2024 8:49 AM
 SERVICES-L1	6/26/2024 8:49 AM
 SERVICES-L2	6/26/2024 8:49 AM
 USER-L1	6/26/2024 8:49 AM
 USER-L2	6/26/2024 8:49 AM
 Windows11ReadMe.pdf	2/9/2024 8:21 AM

For domain-joined (on-prem) systems, the individual GPOs need to be imported into GPM for the proper domain. All policies should be analyzed, and changes made to align with organizational requirements before linking to a production environment. Although Benchmarks are made with a variety of environmental needs in mind, extensive testing in a non-production environment must be done prior to use in a production environment.

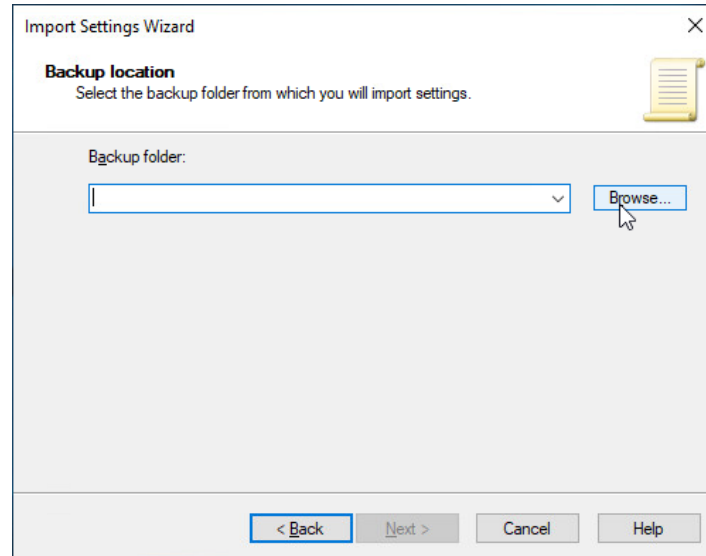
Only one GPO from the Build Kit can be imported into the new GPO in GPME. Ex: COMP-L1 and SERVICES-L1 cannot be imported into a single GPO. Each time an *Import Settings* command is run, the contents of the target GPO are erased and completely replaced by the imported settings. Care should be taken to not overwrite a GPO that still contains desired settings when using this feature. It is suggested to create a new GPO to import settings. This is a limitation of Active Directory and is not considered a best practice.

Prior to applying a Build Kit, ensure that the most recent version of the required Microsoft Windows 11 Administrative Templates has been downloaded directly from Microsoft and installed on the system.

To import a Build Kit into Group Policy Manager:

- 1 Download and unzip the Build Kit to a local folder on the Domain Controller.
- 2 Create a new GPO in the domain.
- 3 Right-click on the GPO that was created and click *Import Settings*.
- 4 Continue to click *Next* until reaching *Backup Location*.
- 5 Click *Browse* and select the folder that contains GPO to be imported.
- 6 Click *Finish*.

Figure 25 | Backup location section mentioned in step 4 of import process.



Applying a Build Kit for stand-alone systems can be done in several ways. The README file included with the Build Kit contains three examples of how to manage and apply policies using the command-line utility Local Group Policy Object Utility (LGPO.exe). This tool was created by Microsoft to automate the management of local group policy and is easy to use. Although CIS mentions LGPO for these examples, it is up to the organization to decide how best to automate and deploy Build Kits within the environment.

Since the LGPO tool is a command-line utility, the import process for stand-alone systems is different when compared to domain-joined systems. The LGPO PDF file included with the tool details its use and the various parameters available. To import a Build Kit, there is only one command needed as shown below in Figure 25. Before running LGPO any necessary changes should be made to align the Build Kit GPO with organizational requirements and testing should be done in a non-production environment before applying it to a production system.

Figure 26 | CLI for the LGPO.exe tool.

```
LGPO.exe /g C:\GPOs\{73T152BB-92DE-831A-4HE9-0A95B18F8438}
```

Some best practices that are encouraged are:

- Download and install the most recent version of the Microsoft Windows 11 Templates directly from Microsoft.
- Read all documentation provided with the Build Kit and the Benchmark.
- Document exceptions to Recommendations that are not being adopted or when the recommended state is changed.
- Thoroughly test before pushing policies to a production environment.

It is acceptable and expected that some exceptions to recommendations will be needed. Each environment is different, and therefore exceptions will be needed. Exceptions should be discussed with, and approved by the organization's Security Department, and clearly documented in case questions arise or for auditing purposes.

Conclusion

As with everything in the information technology ecosystem, best practices like those described above should be followed. Starting with the fundamentals in this guide will reduce the burden of managing and maintaining an Active Directory environment. Creating an organized and process driven system and abiding by it will allow for ease of troubleshooting, maintenance, and future growth within the ecosystem.

References

- [Active Directory Flexible Single Master Operation \(FSMO\) roles in Windows – Windows Server | Microsoft Learn](#)
- [Assign Security Group Filters to the GPO | Microsoft Learn](#)
- [Backup and restore Group Policy in Windows | Microsoft Learn](#)
- [Create and manage Central Store - Windows Client | Microsoft Learn](#)
- [Create WMI Filters for the GPO | Microsoft Learn](#)
- [dcpofix | Microsoft Learn](#)
- [Download Microsoft Security Compliance Toolkit 1.0 from Official Microsoft Download Center](#)
- [Group Policy Modeling and Results in Windows | Microsoft Learn](#)
- [Group Policy overview for Windows | Microsoft Learn](#)
- [MS16-072: Security update for Group Policy: June 14, 2016 – Microsoft Support](#)
- [Never a dull moment with Group Policy \(or what to do about MS16-072\) \(mdmandgpanswers.com\)](#)
- [Planning Domain Controller Placement | Microsoft Learn](#)
- [Schema updates in Windows Server | Microsoft Learn](#)
- [Understanding the Global Catalog | Microsoft Learn](#)

APPENDIX A

Default Domain Policy vs CIS Recommendations

Figure 27 | Default DDP state as provided by Microsoft® versus CIS® recommended state.

Default Domain Policy Unique ID: (31B2F340-016D-11D2-945F-00C04FB984F9)			
Location Policy	Server 2019 Default State	Server 2022 Default State	CIS Configured State
Computer Configuration			
<i>Account Policies\Password Policy</i>			
Enforce password history	24 passwords remembered	24 passwords remembered	24 passwords remembered
Maximum password age	42 days	42 days	365 or fewer days, but not
Minimum password age	1 day	1 day	1 day
Minimum password length	7 characters	7 characters	14 or more characters
Password must meet complexity requirements	Enabled	Enabled	Enabled
Store passwords using reversible encryption	Disabled	Disabled	Disabled
<i>Account Policies\Account Lockout Policy</i>			
Account lockout duration	Not configured	Not configured	15 or more minutes
Account lockout threshold	0 invalid logon attempts	0 invalid logon attempts	5 or fewer invalid logon attempt(s), but not 0
Reset account lockout counter after	Not configured	Not configured	15 or more minutes
<i>Account Policies\Kerberos Policy</i>			
Enforce user logon restrictions	Enabled	Enabled	Enabled
Maximum lifetime for service ticket	600 minutes	600 minutes	600 minutes
Maximum lifetime for user ticket	10 hours	10 hours	10 hours
Maximum lifetime for user ticket renewal	7 days	7 days	7 days
Maximum tolerance for computer clock synchronization	5 minutes	5 minutes	5 minutes
<i>Local Policies\Security Options\Network Access</i>			
Network access: Allow anonymous SID/Name translation	Disabled	Disabled	Disabled
<i>Local Policies\Security Options\Network Security</i>			
Network security: Do not store LAN Manager hash value on next password change	Enabled	Enabled	Enabled
Network security: Force logoff when logon hours expire	Disabled	Disabled	Enabled
<i>Public Key Policies\Autoenrollment settings</i>			
Enroll certificates automatically	Not configured	Not configured	N/A
Renew expired certificates, update pending certificates, and remove revoked certificates	Not configured	Not configured	N/A
Update certificates that use certificate templates	Not configured	Not configured	N/A
<i>Public Key Policies\Encrypting File System\Properties</i>			
Allow users to encrypt files using Encrypting File System (EFS)	Not configured	Not configured	N/A
<i>Public Key Policies\Encrypting File System\Certificates</i>			
Issued To / Issued By / Expiration Date / Intended Purposes	Administrator / Administrator / <100 years> / File Recovery	Administrator / Administrator / <100 years> / File Recovery	Administrator / Administrator / <100 years> / File Recovery
<i>Public Key Policies\Trusted Root Certification Authorities\Properties</i>			
Allow users to select new root certification authorities (CAs) to trust	Not configured	Not configured	N/A
Client computers can trust the following certificate stores	Not configured	Not configured	N/A
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Not configured	Not configured	N/A
User Configuration			
<i>Client Installation Wizard options</i>			
Custom Setup	Not configured	Not configured	N/A
Restart Setup	Not configured	Not configured	N/A
Tools	Not configured	Not configured	N/A

APPENDIX B

Default Domain Controller Policy vs CIS Recommendations

Figure 28 | Default DDCP state as provided by Microsoft® versus CIS® recommended state.

Default Domain Controller Policy Unique ID: [6AC1786C-816F-11D2-945F-00C04FB94F9]				
Location & Policy	Server 2019 Default State	Server 2022 Default State	CIS Configured State	
Computer Configuration				
<i>Local Policies\Audit Policy</i>				
Audit account logon events	Not configured	Not configured	N/A	
Audit account management	Not configured	Not configured	N/A	
Audit directory service access	Not configured	Not configured	N/A	
Audit logon events	Not configured	Not configured	N/A	
Audit object access	Not configured	Not configured	N/A	
Audit policy change	Not configured	Not configured	N/A	
Audit privilege use	Not configured	Not configured	N/A	
Audit process tracking	Not configured	Not configured	N/A	
Audit system events	Not configured	Not configured	N/A	
<i>Local Policies\User Rights Assignment</i>				
Access this computer from the network	BUILTIN\Pre-Windows 2000 Compatible Access NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS NT AUTHORITY\Authenticated Users BUILTIN\Administrators Everyone	BUILTIN\Pre-Windows 2000 Compatible Access NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS NT AUTHORITY\Authenticated Users BUILTIN\Administrators Everyone	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS NT AUTHORITY\Authenticated Users BUILTIN\Administrators	
Act as part of the operating system	Not configured	Not configured	No one	
Add workstations to domain	NT AUTHORITY\Authenticated Users BUILTIN\Administrators	NT AUTHORITY\Authenticated Users BUILTIN\Administrators	BUILTIN\Administrators	
Adjust memory quotas for a process	NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\LOCAL SERVICE NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\LOCAL SERVICE	
Allow log on locally	BUILTIN\Print Operators BUILTIN\Server Operators BUILTIN\Account Operators BUILTIN\Backup Operators BUILTIN\Administrators BUILTIN\Server Operators BUILTIN\Backup Operators BUILTIN\Administrators	BUILTIN\Print Operators BUILTIN\Server Operators BUILTIN\Account Operators BUILTIN\Backup Operators BUILTIN\Administrators BUILTIN\Server Operators BUILTIN\Backup Operators BUILTIN\Administrators	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS BUILTIN\Administrators	
Back up files and directories	BUILTIN\Server Operators BUILTIN\Backup Operators BUILTIN\Administrators	BUILTIN\Server Operators BUILTIN\Backup Operators BUILTIN\Administrators	BUILTIN\Administrators	
Bypass traverse checking	BUILTIN\Pre-Windows 2000 Compatible Access NT AUTHORITY\Authenticated Users BUILTIN\Administrators NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\LOCAL SERVICE Everyone	BUILTIN\Pre-Windows 2000 Compatible Access NT AUTHORITY\Authenticated Users BUILTIN\Administrators NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\LOCAL SERVICE Everyone	BUILTIN\Pre-Windows 2000 Compatible Access NT AUTHORITY\Authenticated Users BUILTIN\Administrators NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\LOCAL SERVICE Everyone	
Change the system time	BUILTIN\Server Operators BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE	BUILTIN\Server Operators BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE	
Create a pagefile	NT AUTHORITY\Authenticated Users	NT AUTHORITY\Authenticated Users	BUILTIN\Administrators	
Create a token object	Not configured	Not configured	No one	
Create permanent shared objects	Not configured	Not configured	No one	
Debug programs	BUILTIN\Administrators	BUILTIN\Administrators	BUILTIN\Administrators	
Deny access to this computer from the network	Not configured	Not configured	Guests	
Deny log on as a batch job	Not configured	Not configured	Guests	
Deny log on as a service	Not configured	Not configured	Guests	
Deny log on locally	Not configured	Not configured	Guests	
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators	BUILTIN\Administrators	BUILTIN\Administrators	
Force shutdown from a remote system	BUILTIN\Server Operators BUILTIN\Administrators	BUILTIN\Server Operators BUILTIN\Administrators	BUILTIN\Administrators	
Generate security audits	NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\LOCAL SERVICE Window Manager\Window Manager Group	NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\LOCAL SERVICE Window Manager\Window Manager Group	NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\LOCAL SERVICE Window Manager\Window Manager Group	
Increase scheduling priority	BUILTIN\Administrators	BUILTIN\Administrators	BUILTIN\Administrators	
Load and unload device drivers	BUILTIN\Print Operators BUILTIN\Administrators	BUILTIN\Print Operators BUILTIN\Administrators	BUILTIN\Administrators	
Lock pages in memory	Not configured	Not configured	No one	
Log on as a batch job	BUILTIN\Performance Log Users BUILTIN\Backup Operators BUILTIN\Administrators	BUILTIN\Performance Log Users BUILTIN\Backup Operators BUILTIN\Administrators	BUILTIN\Administrators	
Log on as a service	Not configured	Not configured	N/A	
Manage auditing and security log	BUILTIN\Administrators	BUILTIN\Administrators	BUILTIN\Administrators	
Modify firmware environment values	BUILTIN\Administrators	BUILTIN\Administrators	BUILTIN\Administrators	
Profile single process	BUILTIN\Administrators	BUILTIN\Administrators	BUILTIN\Administrators	
Profile system performance	NT SERVICE\vd\ServiceHost BUILTIN\Administrators	NT SERVICE\vd\ServiceHost BUILTIN\Administrators	NT SERVICE\vd\ServiceHost BUILTIN\Administrators	
Remove computer from docking	BUILTIN\Administrators	BUILTIN\Administrators	BUILTIN\Administrators	
Replace a process level token	NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\LOCAL SERVICE	NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\LOCAL SERVICE	NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\LOCAL SERVICE	
Restore files and directories	BUILTIN\Server Operators BUILTIN\Backup Operators BUILTIN\Administrators BUILTIN\Print Operators	BUILTIN\Server Operators BUILTIN\Backup Operators BUILTIN\Administrators BUILTIN\Print Operators	BUILTIN\Administrators	
Shut down the system	BUILTIN\Server Operators BUILTIN\Backup Operators BUILTIN\Administrators	BUILTIN\Server Operators BUILTIN\Backup Operators BUILTIN\Administrators	BUILTIN\Administrators	
Synchronize directory service data	Not configured	Not configured	No one	
Take ownership of files or other	BUILTIN\Administrators	BUILTIN\Administrators	BUILTIN\Administrators	
<i>Local Policies\Security Options\Domain Controller</i>				
Domain controller: LDAP server signing requirements	None	None	Require Signing	
<i>Local Policies\Security Options\Domain Member</i>				
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Enabled	Enabled	
<i>Local Policies\Security Options\Microsoft Network Server</i>				
Microsoft network server: Digitally sign communications (always)	Enabled	Enabled	Enabled	
Microsoft network server: Digitally sign communications (if client agrees)	Enabled	Enabled	Enabled	
<i>Local Policies\Security Options\Network Security</i>				
Network security: LAN Manager authentication level	Not configured	Not configured	Send NTLMv2 response only. Refuse LM & NTLM	

Links and Resources

No-cost Resources and Tools

CIS Benchmarks™ (PDF) | Secure configuration guidelines that cover 75 vendor product families, including operating systems, cloud platforms, databases, applications, networking devices, mobile devices, and container service

CIS Critical Security Controls® (CIS Controls®) v8.1 | Prioritized set of Controls to mitigate the most prevalent cyber attacks against systems and networks

CIS-CAT® Lite | Tool that assists with the assessment of secure configurations of select CIS Benchmarks

CIS Community Defense Model 2.0 | A guide that leverages the open availability of comprehensive summaries of attacks and security incidents, and the industry-endorsed ecosystem that is developing around the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Model

CIS Controls Assessment Specification | A tool that provides details on what to measure for each CIS Safeguard to verify that they are properly implemented

CIS Controls Navigator | An online dashboard that enables users to learn more about the CIS Controls and CIS Safeguards and see how they map to other security standards

CIS Controls Self Assessment Tool (CSAT) | Tool that assesses, measures, and tracks the implementation of the CIS Controls and is designed for non-commercial use

CIS Risk Assessment Method (CIS RAM) | An information security risk assessment method that helps enterprises implement and assess their security posture against the CIS Controls

CIS White Papers | Download guides, security framework mappings, and other documents to assist with cybersecurity best practices

CIS WorkBench | Platform that integrates the CIS Controls and CIS Benchmarks communities, allowing for greater collaboration between experts and users

Paid Resources and Tools

CIS SecureSuite® Membership* | Provides enterprises access to integrated cybersecurity tools and resources including CIS-CAT Pro®, our configuration assessment tool, CIS Build Kits, full format CIS Benchmarks™ and Controls®, and more

CIS Hardened Images® | Virtual machine images pre-configured to the CIS Benchmarks

CIS Penetration Testing | A service that simulates a real-world cyber attack

CIS Vulnerability Assessments | A service that assists in identifying critical system weaknesses

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.



 www.cisecurity.org

 info@cisecurity.org

 518-266-3460

 Center for Internet Security

 CenterforIntSec

 @CISecurity

 TheCISecurity

 cisecurity