Hardening the CyberArk CPM and PVWA Servers

Version 10.4

CAHEPV-10-4-0-1

Table of Contents

Harden the CyberArk CPM and PVWA Servers

This section describes automatic and manual procedures for hardening CyberArk's CPM and PVWA servers. These procedures were tested and reviewed by CyberArk's Research and Development department and CyberArk's Security Team. The automatic procedure and the manual procedure complement each other and, therefore, both must be applied.

When the CPM and PVWA server environments are part of Active Directory domain ('In Domain'), the automatic hardening procedure is based on a prepared GPO (Group Policy Object) file. However, when the CPM and PVWA server environments are not a part of Active Directory domain ('Out of Domain'), it is based on an INF file.

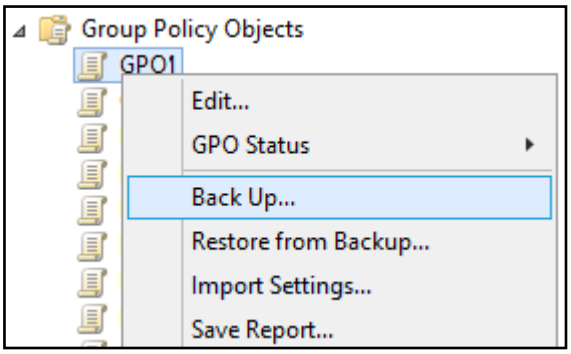
This section describes how to harden CyberArk's CPM and PVWA servers that are installed on Windows 2012R2 and Windows 2016 Servers in 'In Domain' deployments as well as in 'Out of Domain' deployments.

In this section:

'In Domain' Deployments

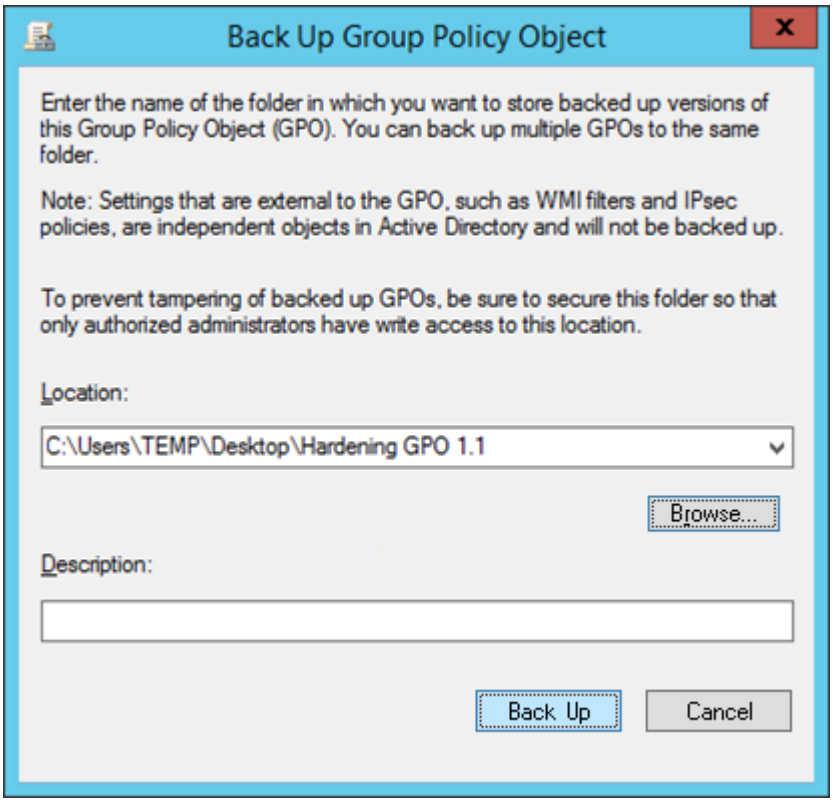
Backup the GPO file (In Domain)

1. In **Group Policy Objects**, right-click the same GPO and select **Back Up**.

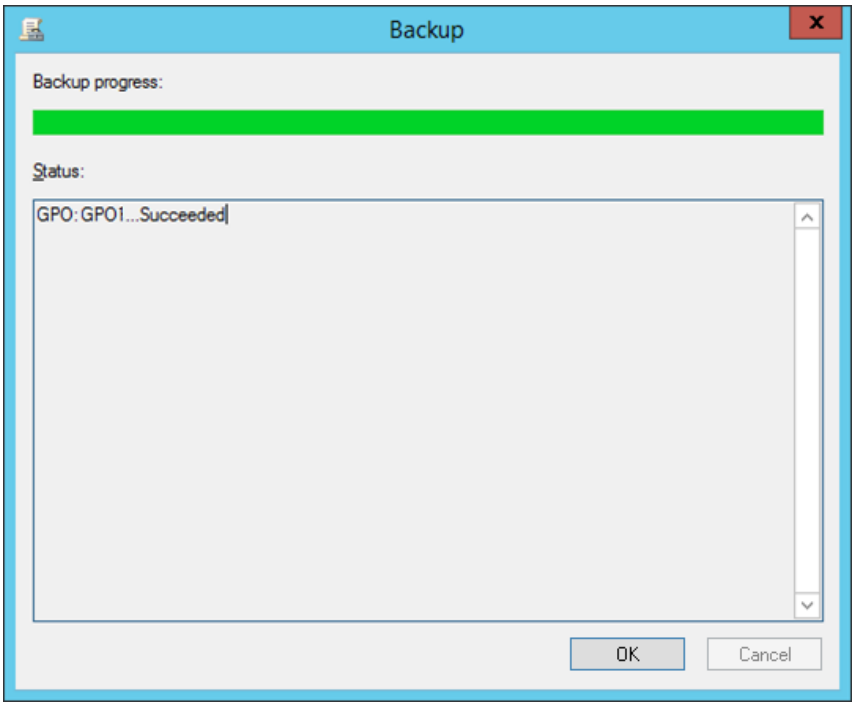


The Back Up Group Policy Object window appears.

2. Click **Browse** and navigate to the new target backup folder, then click **Back Up**.



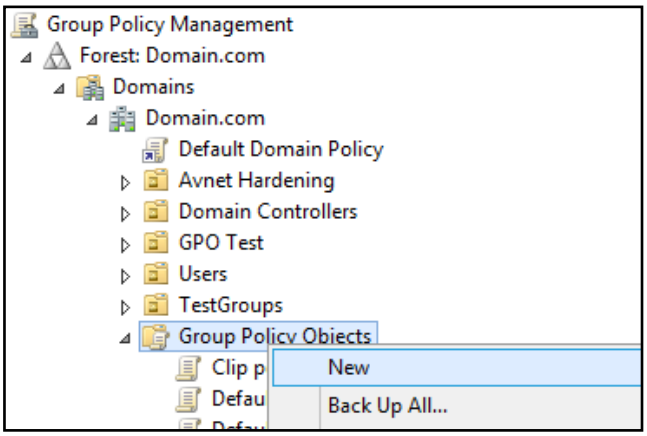
The Backup window appears and displays the backup progress.



3. When the backup has finished, click **OK**.

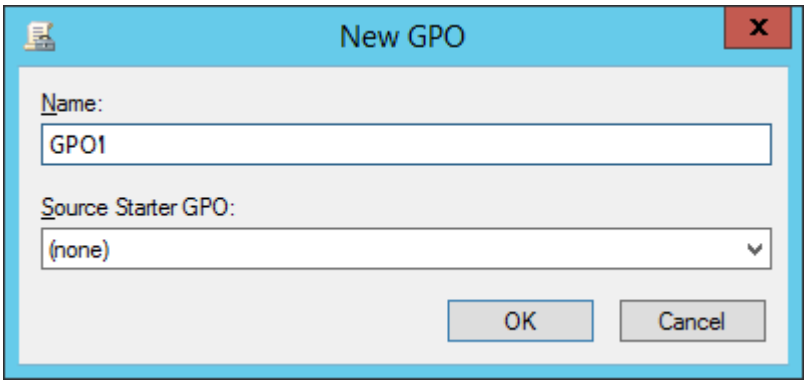
Import a GPO file to an Active Directory domain (In Domain)

1. Get the most recent Group Policy Object (GPO) backup. Create this backup manually from your GPO as described in Backing Up the GPO File (In Domain), page 10.
2. Open the **Group Policy Management Console** (GPMC.msc).
3. Create a new GPO that will inherit the settings of the latest GPO backup:
   - Display and right-click **Group Policy Objects** and select **New**.

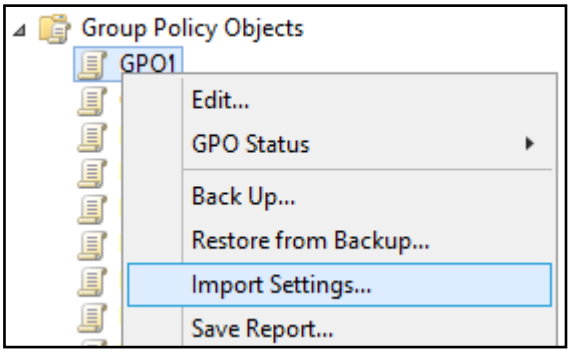


4. Specify a new name for the GPO, then click **OK**.

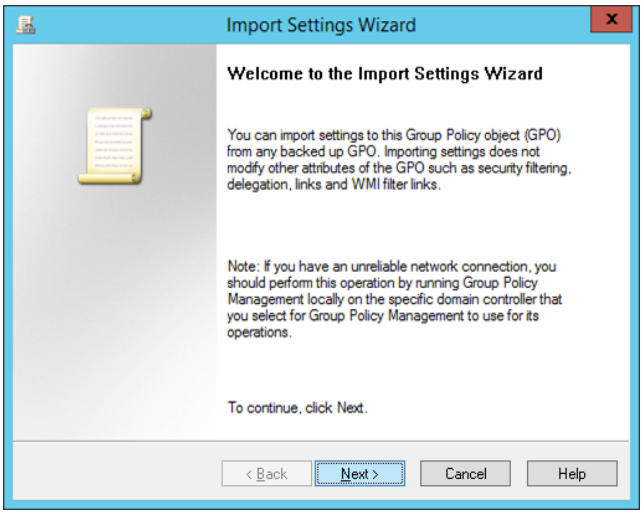
> **Note:**
> Specify a name that indicates the purpose of the GPO. This name is displayed to all users.



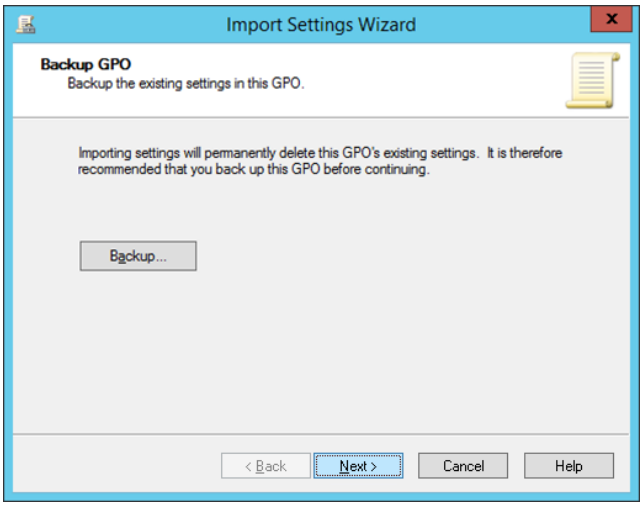
5. In the list of Group Policy Objects, right-click the new GPO and select **Import Settings…**.



The Import Settings Wizard appears.

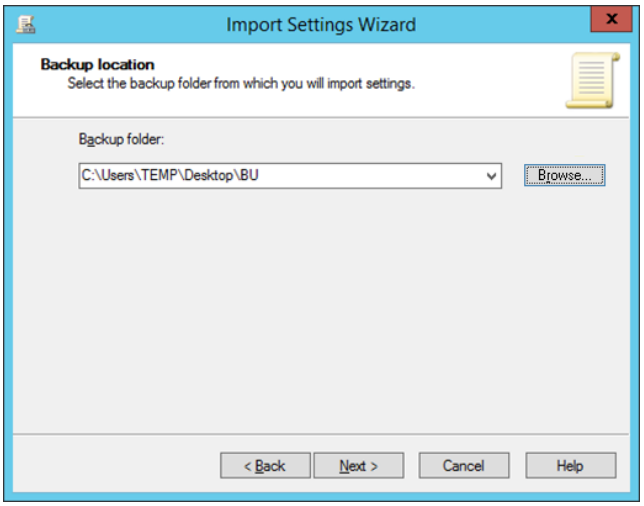


6. In the Welcome to the Import Settings Wizard window, click **Next**; the Backup GPO window appears.

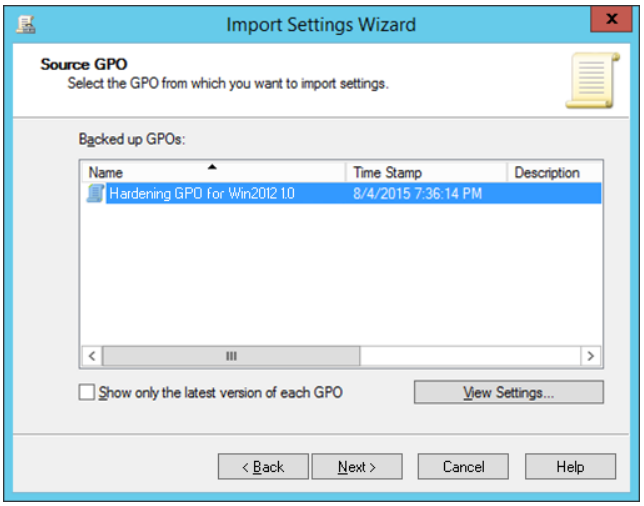


You do not have to configure backup as this GPO is new.

7. Click **Next**; the Backup location screen appears.

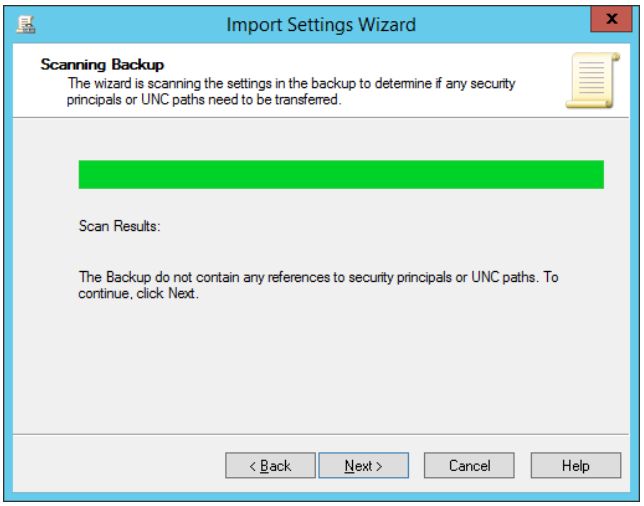


8. Click **Browse…** , and select the location of the folder where the hardening settings are stored, then click **Next**; the Source GPO window appears.

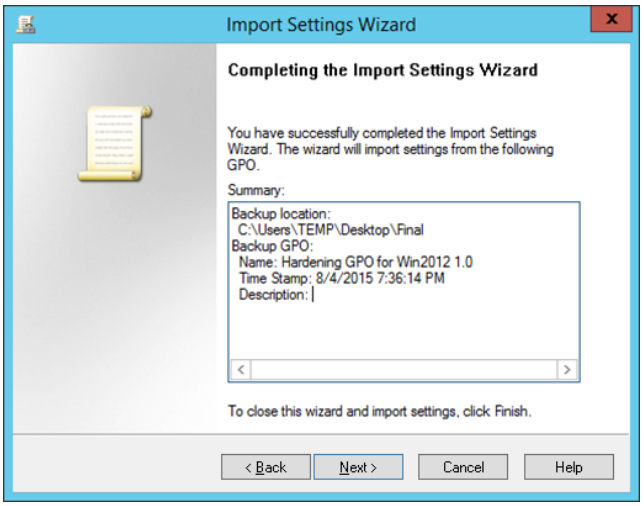


9. Select the displayed backed up GPO, then click **Next**; the Scanning Backup window appears.

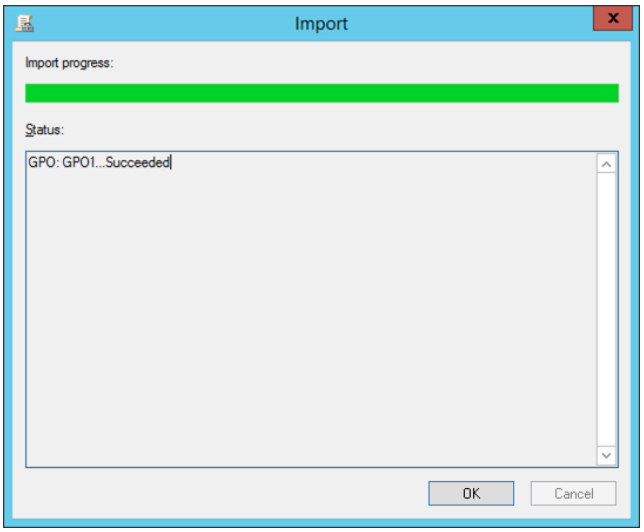
> **Note:**
> No references to domain/UNC paths should be found.



10. Click **Next**; the Completing the Import Settings Wizard window appears.



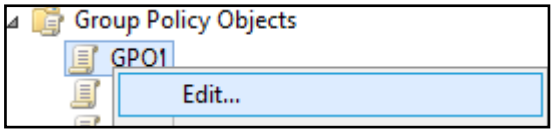
11. Click **Finish**; the Import window appears and shows the progress of the GPO import.



12. When the GPO import process has been completed, click **OK**.

Update the GPO file (In Domain)

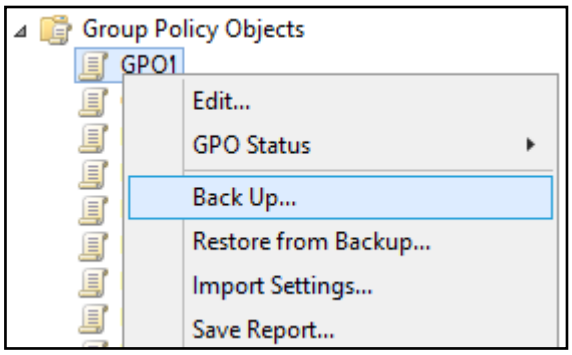
1. In **Group Policy Objects**, right-click the GPO that you created in the previous step and select **Edit**.



Note:
Do not add any domain specific settings to the GPO, and make sure that there are no domain specific settings in the GPO, unless configured manually by the customers. For example, "Domain\Domain Admins", "Domain\Connect", "Domain\AdminConnect".

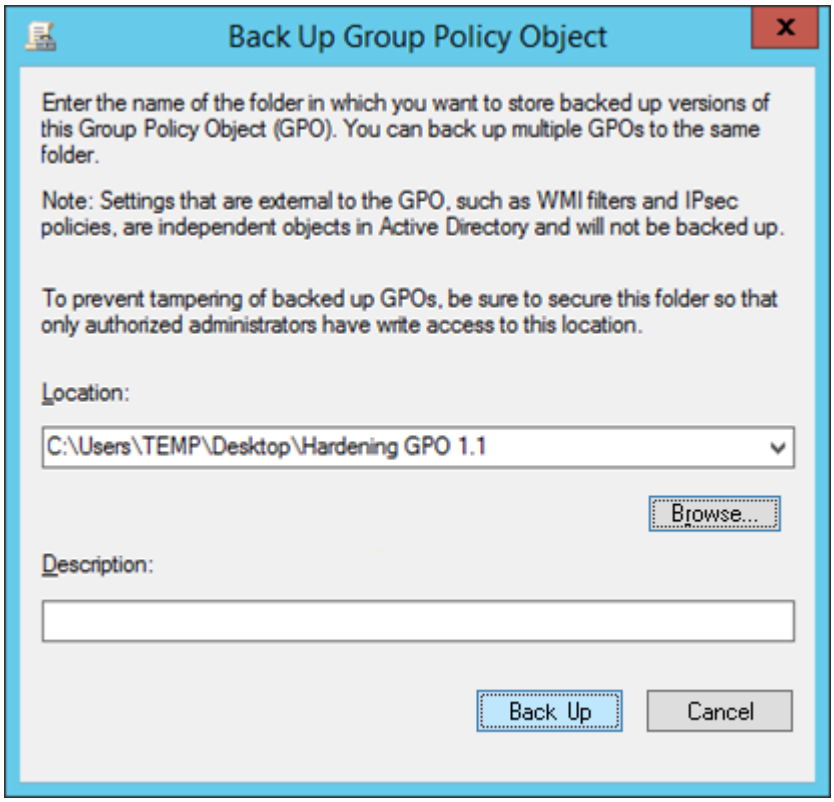
Backing Up the GPO File (In Domain)

1. In **Group Policy Objects**, right-click the same GPO and select **Back Up**.

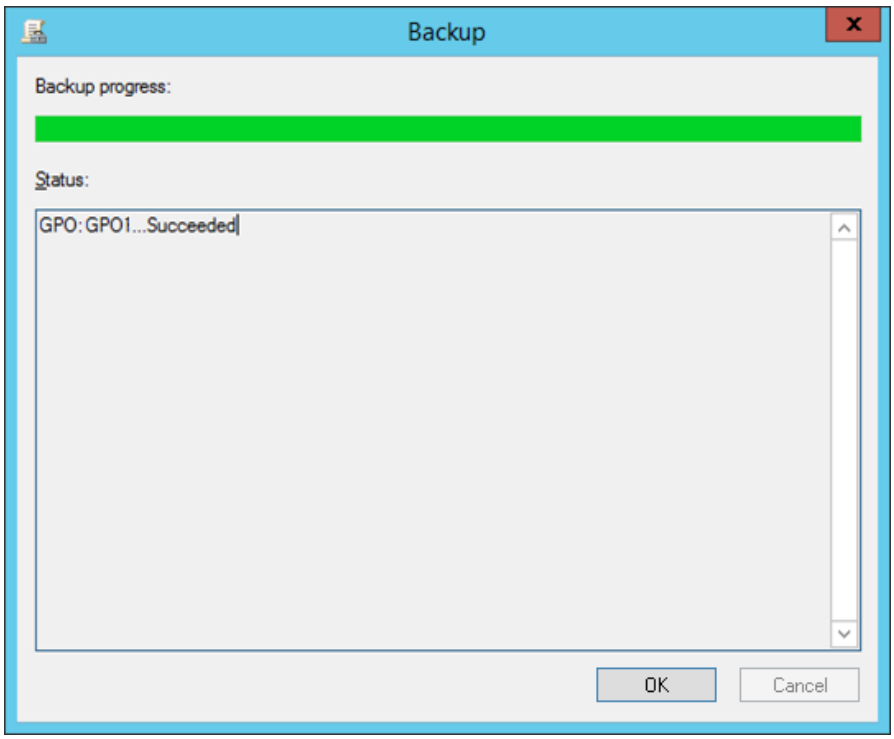


The Back Up Group Policy Object window appears.

2. Click **Browse** and navigate to the new target backup folder, then click **Back Up**.



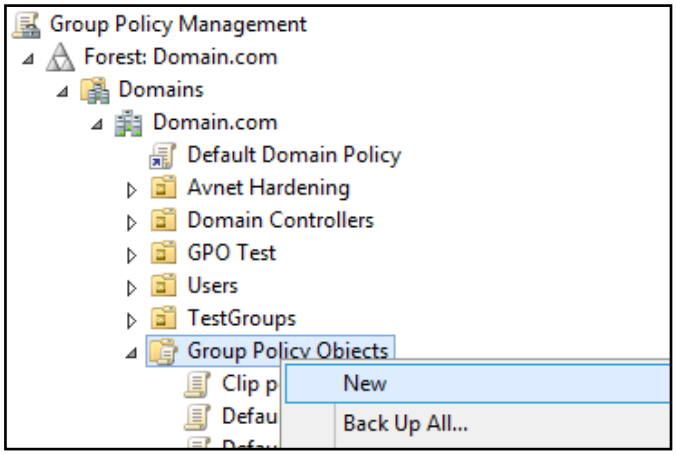
The Backup window appears and displays the backup progress.



3. When the backup has finished, click **OK**.

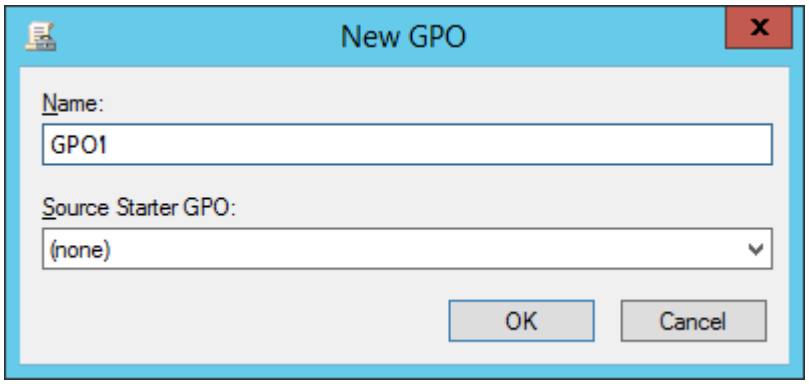
Importing a GPO file to an Active Directory Domain (In Domain)

1. Get the most recent Group Policy Object (GPO) backup. Create this backup manually from your GPO as described in Backing Up the GPO File (In Domain), page 10.
2. Open the **Group Policy Management Console** (GPMC.msc).
3. Create a new GPO that will inherit the settings of the latest GPO backup:
   - Display and right-click **Group Policy Objects** and select **New**.

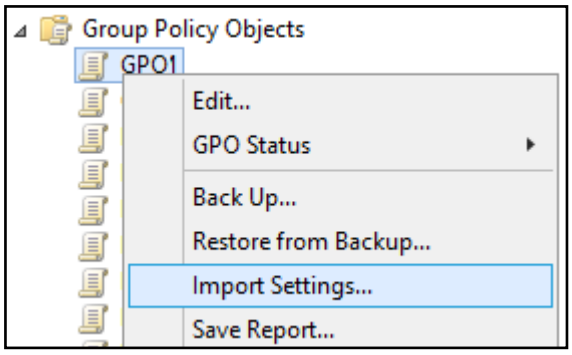


4. Specify a new name for the GPO, then click **OK**.

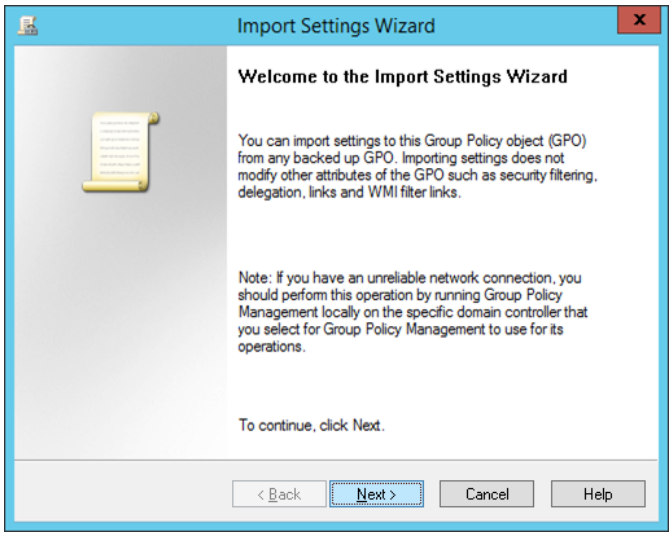
   Note: Specify a name that indicates the purpose of the GPO. This name is displayed to all users.



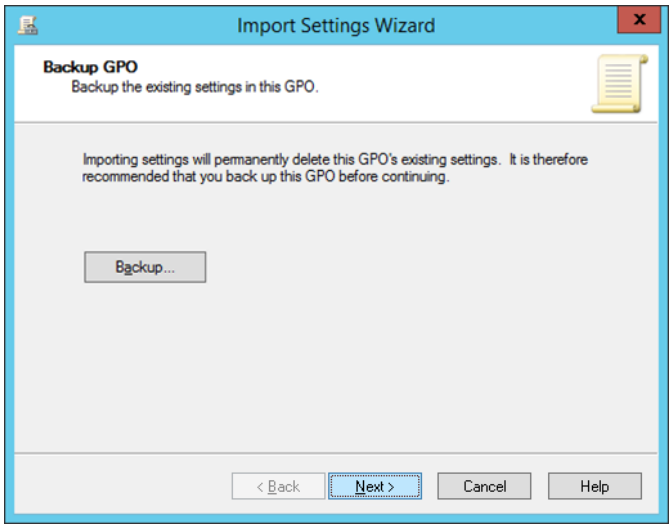
5. In the list of Group Policy Objects, right-click the new GPO and select **Import Settings...**.



The Import Settings Wizard appears.

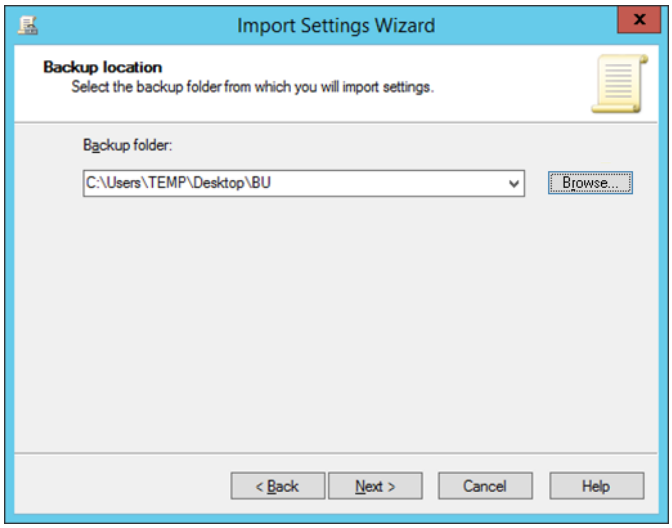


6. In the Welcome to the Import Settings Wizard window, click **Next**; the Backup GPO window appears.

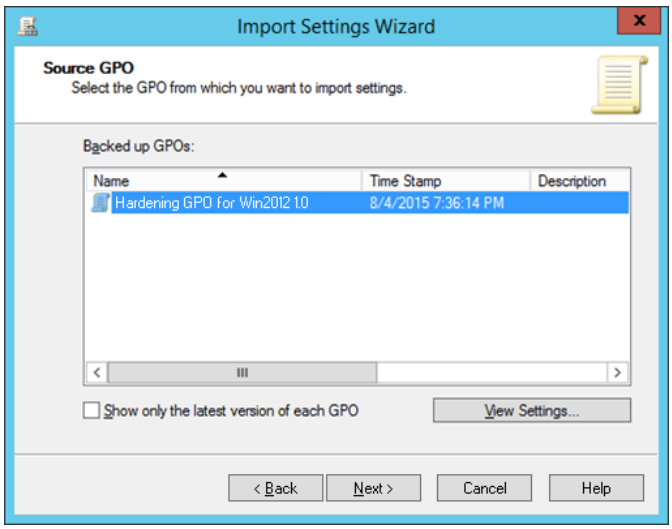


You do not have to configure backup as this GPO is new.

7. Click **Next**; the Backup location screen appears.

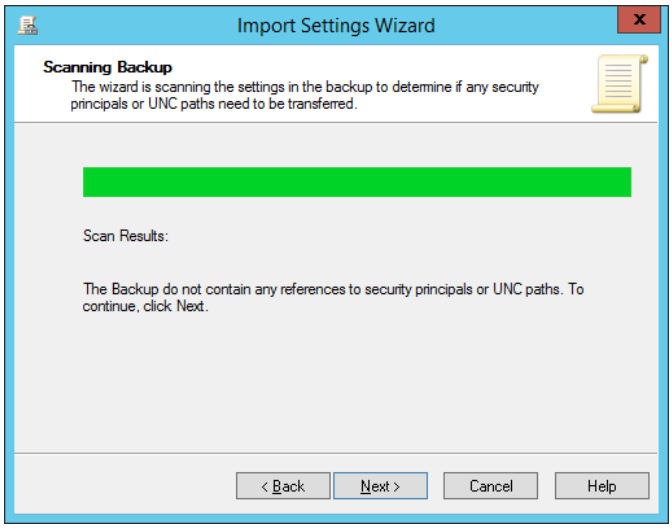


8. Click **Browse…** , and select the location of the folder where the hardening settings are stored, then click **Next**; the Source GPO window appears.

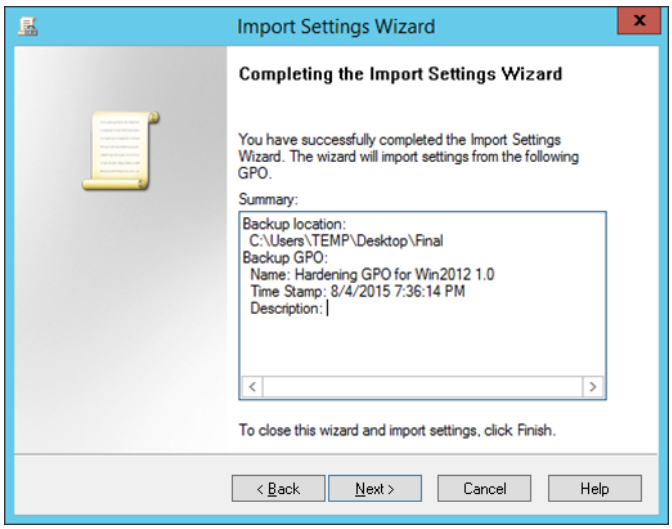


9. Select the displayed backed up GPO, then click **Next**; the Scanning Backup window appears.

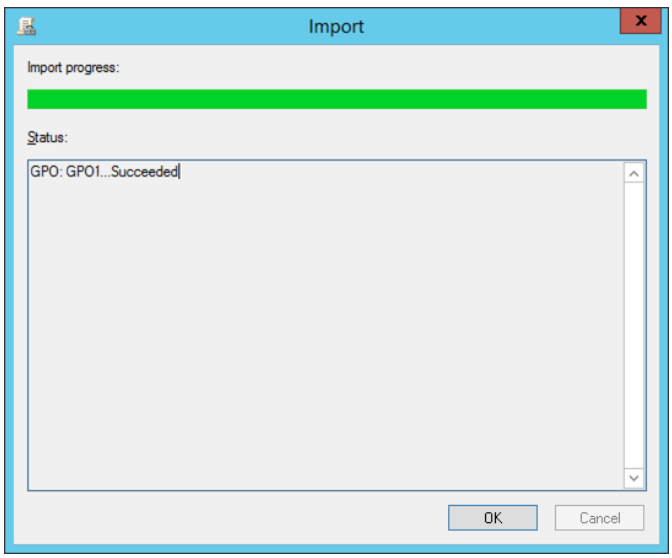
   Note: No references to domain/UNC paths should be found.



10. Click **Next**; the Completing the Import Settings Wizard window appears.



11. Click **Finish**; the Import window appears and shows the progress of the GPO import.



12. When the GPO import process has been completed, click **OK**.

'Out of Domain' Deployments

This section describes how to apply automatic hardening procedures in 'Out of Domain' deployments.

CyberArk offers two methods of implementation for hardening the CPM and PVWA servers:

1. Automatic implementation, page 17- This method uses PowerShell scripts
2. Manual implementation, page 19

Automatic implementation

This automatic method covers all post-installation and hardening steps that are required to secure your server. If the CPM and PVWA are both installed on the same server, run both scripts.

Note:
When installing PSM on the same machine as CPM and/or PVWA, run the CPM/PVWA hardening scripts before installing the PSM.

Harden the CPM server

1. In the Installation CD Image Automatic_Hardening folder (...\Central Policy Manager\Automatic_Hardening), locate the "CPM_Hardening.ps1" script.
2. Open PowerShell as Administrator and run this script.

   This script creates a **log file that lists all the steps** that were carried out (successful or failed). For each step, the log includes the value before the change and after the change.

   - The script log is created in the same folder as the script and is called "HardeningScript.log".
   - The steps performed by the script are explained below, in Manual implementation, page 19.

   This script also creates a **log file that analyzes the changes** made when the Hardening INF file is imported.

   - The log file is called "CYBR_Hardening_secedit.log".
   - After the script has finished running, each customer should review this log to verify that no errors occurred.
   - The steps performed when the Hardening INF file is imported are explained below, in Manual implementation, page 19.

After the script has finished running, review the log files to ensure that all hardening steps were completed successfully. If one of the steps failed, you can perform it manually using the steps described below, in Manual implementation, page 19.

Hardening the PVWA

1. In the Installation CD Image Automatic_Hardening folder (...\Password Vault Web Access\Automatic_Hardening) locate the "PVWA_Hardening.ps1" script.
2. Open PowerShell as Administrator and run this script.

   This script creates a **log file that lists all the steps** that were carried out (successful or failed). For each step, the log includes the value before the change and after the change.

   - The script log is created in the same folder as the script and is called "HardeningScript.log".

- The steps performed by the script are explained below, in Manual implementation, page 19.

This script also creates a **log file that analyzes the changes** made when the Hardening INF file is imported.

- The log file is called "CYBR_Hardening_secedit.log".
- The steps performed when the Hardening INF file is imported are explained below, in Manual implementation, page 19.

After running the scripts

1. Review the script logs to verify that no errors occurred and that all hardening steps were completed successfully. If one of the steps failed, you can perform it manually using the steps described below, in Manual implementation, page 19.
2. Restart the server machine.

Additional manual steps

The following additional manual steps harden your CPM/PVWA server even further:

- Update your Operating System, page 22
- Install an Anti-Virus Solution, page 22
- Restrict Network Protocols, page 22
- Rename Default Accounts, page 22
- Application Pool, page 25
- Secure PKI Authentication (PVWA Only), page 31
- Manual procedures, page 35
- Clear the "Log on as a service" configuration from all other users, as listed in Additional manual steps, page 47

Manual implementation

Import an INF file to the local machine

Tip:
This step is performed automatically using the PowerShell script.

1. Open MS Management Console by running **mmc.exe**.
2. Configure the export settings:
   If you are configuring a hardening environment, skip this step and go to step 3 where you configure the import settings.
   a. From **File**, select **Add/Remote Snap-ins**, and add the **Security Templates**.
   b. Right click, select **New template** and name it.
   c. Expand the template and configure it according to your hardening definitions.

Note:
Pay attention to the following:
- Only security settings are there. Other settings should be set manually.
- Audit settings also doesn't appear here, they must be set via the gpedit.msc

   d. Right click on the template and save it as an **inf** file.
3. Configure the import settings:
   - In the mmc, display **Add/Remove Snap-ins** and add **Security Configuration and Analysis**.
4. Create a new database:
   a. Right click **Security Configuration and Analysis** then, from the pop-up menu, select **Open Database**.
   b. Type the name of the new database or select an existing one, then click **Open**.
   c. Select the ini file of the hardening settings. For example, CyberArk_PAS_Local Security Templates.ini.
   d. Right click the imported file and select **Import template** , then select your ini file.
   e. Right click the imported file again, then select **Configure Computer Now**.
   f. Right click the imported file again, then select **Analyze Computer now**.
   g. Expand the **Console Root** and review the settings in **Local policies/User Rights Assignment** and **Local policies/Security Options**. Check the differences between the database and the computer and match the settings that were not imported. Note the green/red indications and the "Database Setting" vs. "Computer Setting".

Note:
Importing the local security policy will overwrite the local group policy. Use the above guide to make a backup of your current settings.

Importing an INF File to the Local Machine

1. Open MS Management Console by running **mmc.exe**.
2. Configure the export settings:
   - If you are configuring a hardening environment, skip this step and go to step 3 where you configure the import settings.
   - From **File**, select **Add/Remote Snap-ins**, and add the **Security Templates**.
1. Right click, new template, name it.
2. Expand it and configure it according to your hardening definitions

   Note: Pay attention to the following:

   Only security settings are there. Other settings should be set manually.

   Audit settings also doesn't appear here, they must be set via the gpedit.msc
3. Right click on the template and save it as an **inf** file.
3. Configure the import settings:
   - In the mmc, display **Add/Remove Snap-ins** and add **Security Configuration and Analysis**.
1. Create a new database:
1. Right click **Security Configuration and Analysis** then, from the pop-up menu, select **Open Database**.
2. Type the name of the new database or select an existing one, then click **Open**.
3. Select the ini file of the hardening settings. For example, CyberArk_PAS_Local Security Templates.ini.
2. Right click the imported file and select **Import template** , then select your ini file.
3. Right click the imported file again, then select **Configure Computer Now**.
4. Right click the imported file again, then select **Analyze Computer now**.
5. Expand the **Console Root** and review the settings in **Local policies/User Rights Assignment** and **Local policies/Security Options**. Check the differences between the database and the computer and match the settings that were not imported. Note the green/red indications and the "Database Setting" vs. "Computer Setting".

Note: Importing the local security policy will overwrite the local group policy. You can use the above guide to make a backup of your current settings.

General Configuration for all Deployments

This section describes configuration that must be performed in 'In Domain' deployments as well as in 'Out of Domain' deployments.

In this section:

Update your Operating System

Microsoft releases periodic updates (security updates and service packs) to address security issues that were discovered in Operating Systems. Make sure your Operating System is updated to the latest version.

You can install the updates in either of the following ways:

- Manually install updates and service packs
- Automatically install with Server Update Services (WSUS), which is located on a corporate network

Install an Anti-Virus Solution

In today's world, the pace of virus development is very fast. Servers without anti-virus protection are exposed to two risks:

- Server infected with viruses that might damage the server and the entire network
- Trojan horses that are planted to allow remote control of the server and to all the information on it

Install an Anti-Virus solution and update it as needed.

Restrict Network Protocols

Install only the required protocols and remove unnecessary ones. For example, only TCP/IP are necessary, and ensure that no additional protocols such as IPX or NetBEUI are allowed.

Rename Default Accounts

It is recommended to change the names of both the Administrator and the guest to names that will not testify about their permissions. It is also recommended to create a new locked and unprivileged Administrator user name as bait.

Validate Proper Server Roles

Tip:
This step is performed automatically using the PowerShell script.

To minimize your attack surface, as a best practice, make sure that only the minimum roles and features that are required are defined on the CPM and PVWA server(s). Remove all unnecessary roles and features.

- For information about installing and enabling the required roles and features for the PVWA and CPM, refer to the Privileged Access Security Installation Guide.

Note:

- Unless otherwise specified, the roles and features below are listed by specific name. There is no specified parent roles that assume the removal of children dependencies, and you should **only** remove the roles that are listed.
  However, when removing roles, you will sometimes be prompted to remove dependent features and/or roles, which is acceptable for the roles listed below. Always elect to remove these dependent features and/or roles when prompted (unless they are required by your environment for some reason).
- Removing the "SMB 1.0/CIFS File Sharing Support" feature will disable Windows accounts management and the discovery of Scheduled Task dependencies using the CPM Scanner in old target machines which only support SMB 1.0, e.g. Windows XP, Windows 2003.
  It is recommended to disable SMB 1.0 due to known security issues.

The following list enumerates the server roles and features that can be safely removed.

Roles

Application Server

- TCP Port Sharing
- Windows Process Activation Service Support
  - Named Pipes Activation
  - TCP Activation

Remote Access

- DirectAccess and VPN (RAS)
- Routing
- Web Application Proxy (With dependent features)

Web Server (IIS)

- Web Server
  - Health and Diagnostic
    - Logging Tools
    - Tracing

Security

- Centralized SSL Certificate Support
- Client Certificate Mapping Authentication

- Digest Authentication
- IIS Client Certificate Mapping Authentication
- IP and Domain Restrictions
- URL Authentication

Application Development

- Server Side Includes
- WebSocket Protocols

- Windows Deployment Services (with dependent features) – including all child roles

Features

- Group Policy Management
- IIS Hostable Web Core
- Ink and Handwriting Services
- Media foundation
- RAS Connection Mananger Administration Kit (CMAK)
- Remote Server Administration Tools – Including all child features.
- Telnet Client (in case CPM is not managing account using the telnet plugin)
- Windows Internal Database
- SMB 1.0/CIFS File Sharing Support

Note:
This feature is incompatible with old targets (e.g. Windows XP and 2003 which only support SMB 1.0).

IIS Hardening (PVWA Only)

Perform the following steps on the PVWA Server that runs the IIS:

In this section:

Shares

Tip:
This step is performed automatically using the PowerShell script.

IMPORTANT! Always backup your registry before making any changes to it.

It is recommended to disable all default shares on servers that run an IIS service.

Disable default shares:

1. Run regedit.
2. Change the following key:
   - HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
   - Value Name: AutoShareServer
   - Type: REG_DWORD
   - Value: 0
3. Restart the server service by running the following commands in a cmd console as the administrator:

```
net stop server
net start server
```

Re-enable administrative shares:

1. Run regedit.
2. Change the following key:
   - Value Name: AutoShareServer
   - Type: REG_DWORD
   - Value: 1
3. Restart the server service by running the following commands in a cmd console as the administrator

```
net stop server
net start server
```

Application Pool

It is important to remove all unnecessary application pools that are installed by default with the IIS server. In addition, all application pools must be configured as **Integrated**, since Classic mode has known vulnerabilities.

Keep the following application pools only:

- DefaultAppPool (Managed Pipeline Mode = Integrated)
- PasswordVaultWebAccess (Managed Pipeline Mode = Integrated)

Note:
The PVWA application pool name can be changed.

Remove all other application pools

1. From the run window, run **inetmgr**.
2. Expand your site node and open **Application Pools**.
3. Remove all application pools, except for the **DefaultAppPool** and **PasswordVaultWebAccessPool**

Note:
If the PVWA application pool name was changed, do not delete it.

4. Run iisreset.

Web Distributed Authoring and Versioning (WebDAV)

Tip:
This step is performed automatically using the PowerShell script.

WebDAV protocol enables users to create, change and move documents on a web server or web share. It has known vulnerabilities and should be disabled.

Disable WebDAV by removing the "WebDAV Publishing" server role:

- Web Server (IIS)
  - Web Server
    - Common HTTP Features
      - WebDAV Publishing

MIME Types

Tip:
This step is performed automatically using the PowerShell script.

It is recommended to remove all unnecessary file types to avoid the possibility of an attacker importing a malicious file into the website and getting the IIS service to run it.

Remove all MIME types except for the following:

.css, .csv, .dll, .dll.config, .eot, .gif, .htc, .htm, .html, .jar, .jpe, .jpeg, .jpg, .js, .json, .png, .svg, .swf, .ttf, .txt, .xls, .xlsx, .xml

This can be done in either of the following ways:

- From the IIS Manager:
  a. From the run window, run **inetmgr**.
  b. Click on the site node and open **MIME Types**.

Or

- Edit the applicationHost.config file:
  a. Open the %windir%\System32\inetsrv\config\applicationHost.config file.
  b. Remove the **mimeMap** elements of non-required MIME types.

SSL/TLS Settings

Tip:
This step is performed automatically using the PowerShell script.

It is important to keep your server SSL/TLS settings up to date. Among other settings, the different protocols and cipher suites can be vulnerable to different attacks on SSL/TLS.

IMPORTANT: It is important to understand that things are dynamic, and that best practices change as time progresses and new vulnerabilities are found. Sometimes, it is a matter of security vs. compatibility. For example, older clients such as Windows XP, Server 2003, and also Vista and Server 2008 (not R2) will not support TLS 1.2 and 1.1, which are considered to be the most secure protocols to date.

It is important to keep up to date with the latest recommendations and make changes to your server configuration as things evolve.

Some recommended references about securing SSL/TLS are:

- https://www.ssllab.com/projects/documentation/
- https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

The following guidelines are basic for SSL/TLS hardening:

- Always apply the latest software updates (Windows), since some vulnerabilities are implementation bugs.
- Disable SSL v2.0, since it is considered to be broken (see RFC6176).
- If possible, disable SSL v3.0 as it is considered insecure in some cases. It is vulnerable to the POODLE attack and can force a downgrade of the protocol, if used).

Note:
Disabling SSL v3.0 will break older clients such as Windows XP and or IE6/7.

- TLS 1.0 is very common and can be made relatively secure, but it requires configuration and in-depth understanding of the environment to work securely with all cipher suites. It also does not support all modern cipher suites that are supported by later versions. For example, it is vulnerable to the BEAST attack with some cipher suites. PCI DSS states that starting June 30 2016, SSL and TLS 1.0 are no longer to be used (PCI DSS Version 3.0 to 3.1).
- TLS 1.2 is considered secure at the moment, without any known vulnerabilities.

The problem with disabling SSL v3.0, and moreover TLS1.0 and TLS 1.1, is the resultant compatibility issues with older clients. This depends on your environment and on the supported clients.

Refer to https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/manage-ssl-protocols-in-ad-fs for the official documentation of the registry values that governs the SSL/TLS settings in the windows registry.

After you have finished the setting the following registry keys, restart the Windows machine (not just the IIS).

Disable SSL V2.0

1. From the run window, run regedit.
2. Add the following registry keys and values:
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 2.0\Client
     - Value Name: Enabled
       - Type: REG_DWORD
       - Value: 0
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 2.0\Client
     - Value Name: DisabledByDefault
       - Type: REG_DWORD
       - Value: 1
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 2.0\Server
     - Value Name: Enabled
       - Type: REG_DWORD
       - Value: 0
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 2.0\Server
     - Value Name: DisabledByDefault
       - Type: REG_DWORD
       - Value: 1

Disable SSL V3.0

1. From the run window, run regedit.
2. Add the following registry keys and values:
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 3.0\Client
     - Value Name: Enabled
       - Type: REG_DWORD
       - Value: 0
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 3.0\Client
     - Value Name: DisabledByDefault
       - Type: REG_DWORD
       - Value: 1
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 3.0\Server
     - Value Name: Enabled
       - Type: REG_DWORD
       - Value: 0
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 3.0\Server

- Value Name: DisabledByDefault
  - Type: REG_DWORD
  - Value: 1

Disable TLS 1.0

1. From the run window, run regedit.
2. Add the following registry keys and values:
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS1.0\Client
     - Value Name: Enabled
       - Type: REG_DWORD
       - Value: 0
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS1.0\Client
     - Value Name: DisabledByDefault
       - Type: REG_DWORD
       - Value: 1
   - HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS1.0\Server
     - Value Name: Enabled
       - Type: REG_DWORD
       - Value: 0
   - HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS1.0\Server
     - Value Name: DisabledByDefault
       - Type: REG_DWORD
       - Value: 1

Disable TLS 1.1

1. From the run window, run regedit.
2. Add the following registry keys and values:
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS1.1\Client
     - Value Name: Enabled
       - Type: REG_DWORD
       - Value: 0
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS1.1\Client
     - Value Name: DisabledByDefault
       - Type: REG_DWORD
       - Value: 1
   - HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS1.1\Server
     - Value Name: Enabled

        - Type: REG_DWORD
        - Value: 0
    - HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS1.1\Server
        - Value Name: DisabledByDefault
            - Type: REG_DWORD
            - Value: 1

Enable TLS 1.2

1. From the run window, run regedit.
2. Add the following registry keys and values:
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client
     - Value Name: DisabledByDefault
       - Type: REG_DWORD
       - Value: 0
   - HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server
     - Value Name: Enabled
       - Type: REG_DWORD
       - Value: ffffffff
3. To enable .NET Framework to use TLS1.2, add the following registry keys and values:
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319
     - Value Name: SchUseStrongCrypto
       - Type: REG_DWORD
       - Value: 00000001
   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319
     - Value Name: SchUseStrongCrypto
       - Type: REG_DWORD
       - Value: 00000001

After you have finished, restart the Windows machine (not just the IIS).

Secure PKI Authentication (PVWA Only)

Public Key Infrastructure (PKI) authentication is a common authentication for smart card or other client certificate authentication types to IIS applications. PVWA supports PKI authentication using different types of smart cards

Each PKI certificate is signed by a certificate authority and is trusted by the server. In order to make PKI authentication more secure, we recommend removing all other trusted CAs from the certificate store on the PVWA server, except the CA that the organization uses to verify the client's certificate.

In addition, as the machine’s certificate store can be updated via Windows Updates, make sure that no trusted CA was added after the Windows Updates installation.

Cryptography Mode Settings (CPM only)

CyberArk recommends configuring CPM to run with elevated FIPS cryptography mode to ensure that CPM complies with FIPS 140-2 including the random number generator to create secrets.

To configure CPM to use elevated FIPS cryptography mode, add a parameter to the **CyberArk Password Manager** service.

Do one of the following to set the mode:

From the registry

1. Open regedit.exe and go to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services**.
2. Select **CyberArk Password Manager**
3. Select the **ImagePath** subkey and change the value to:

```
"C:\Program Files (x86)\CyberArk\Password
Manager\PMEngine.exe" /SERVICE /ADVANCEDFIPSCRYPTOGRAPHY
```

4. Restart the **CyberArk Password Manager** service

From the command line

1. Open a cmd window
2. Run the following command:

```
sc config "CyberArk Password Manager" binPath=
"\"C:\Program Files (x86)\CyberArk\Password
Manager\PMEngine.exe\" /SERVICE
/ADVANCEDFIPSCRYPTOGRAPHY"
```

3. Restart the **CyberArk Password Manager** service

Cryptography Mode Settings for PVWA

CyberArk recommends configuring PVWA to run with elevated FIPS cryptography mode to ensure that PVWA complies with FIPS 140-2 including the random number generator to create secrets.

To configure PVWA to use elevated FIPS cryptography mode, add a parameter to the **web.config** file.

Set the mode

1. Go to the application folder, usually located at **C:\inetpub\wwwroot\Passwordvault**
2. Open **web.config** file for editing.

3. Under the **<appsettings>** node, add the following key:

```
<add key="AdvancedFIPSCryptography" value="yes" />
```

4. Restart **IIS**.

Configure PVWA and CPM Servers in 'In Domain' Deployments

This section describes how to configure PVWA and CPM servers in 'In Domain' deployments.

Automatic procedures (handled by GPO and installation scripts)

Install the hardening GPO as described in Importing a GPO file to an Active Directory Domain (In Domain), page 12. The GPO should be imported during the installation process.

- You will receive the hardening package from CyberArk as a zipped file. Unzip this file so that you can import the hardening GPO.

Clipboard redirection

If you run the hardening script on the machine, clipboard redirection is disabled. If you want to enable the clipboard redirection on the machine for PSM functionality, do the following:

1. Go to **Windows > Start button > gpedit.msc**.
2. Open U**ser Configuration > Administrative Templates >Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection** and set **Do not allow clipboard redirection** to **Disabled**.
3. Restart the machine.

Manual procedures

Group policy and permissions

Policy	Setting
Create a domain/local user to use in the "PMEngine" (CPM) service	
Set permissions on the local folder for the CPM user and remove unnecessary permissions (Leave the CPM user, administrators group and SYSTEM)	▪ Set reader permissions on the following folders: ▪ [Drive]:\Python27 ▪ [Drive]:\Oracle ▪ [Drive]:\Program Files (x86)\CyberArk ▪ Set full permissions on the following folders: ▪ [Drive]:\Program Files (x86)\CyberArk\PasswordManager\Logs ▪ [Drive]:\Program Files (x86)\CyberArk\PasswordManager\tmp ▪ [Drive]:\Program Files (x86)\CyberArk\PasswordManager\bin ▪ [Drive]:\Program Files (x86)\CyberArk\PasswordManager\Vault\ user.ini ▪ [Drive]:\Program Files (x86)\ CyberArk\PasswordManager\Scanner\ Log ▪ Remove the "users" permissions from all the above folders and from all other unnecessary users and

Policy	Setting
	▪ groups. **Comments:** ▪ Stop the CPM, CPMScanner and Scheduled Task services. ▪ To remove user/groups from a folder, disable the permission inheritance on the folder (Folder properties → Security → Advanced → Change permissions: clear "Include inheritable permissions…" or click "Disable inheritance" before removing the user(s). ▪ Set the following reader permissions: Read & Execute, List folder content, Read. ▪ Set the following full permissions: Full Control, Read & Execute, List, Read, Modify, Write.
Remove unnecessary user/group permissions from the PVWA folders	▪ Remove all users/groups except for the built-in SYSTEM and Administrators group from the " [Drive:]\CyberArk" folder. **Comments:** ▪ By default, the "Password Vault Web Access" folder is in C:\CyberArk, unless this was changed during installation.
Create a domain/local user to use in the "CyberArk Scheduled Task" service (installed by the PVWA)	
Set permissions for the "CyberArk Scheduled Task" service and remove unnecessary permissions	▪ Set reader permissions for the service user on the following folder: "[Drive]:\CyberArk\ PasswordVaultWebAccess\Services". ▪ Set full permissions on "[Drive]:\CyberArk\ PasswordVaultWebAccess\Services\Logs". ▪ Remove the "users" permissions from the above folders and other unnecessary users and groups. **Comments:** ▪ To remove users/groups from a folder, disable permission inheritance on the folder (Folder properties → Security → Advanced → Change permissions: clear "Include inheritable permissions…" or click "Disable inheritance" before removing the user(s). ▪ Set the following reader permissions: Read & Execute, List folder content, Read. ▪ Set the following full permissions: Full Control, Read & Execute, List, Read, Modify, Write.
"Log on as a service" Group policy object:	Add the following users: ▪ NT SERVICE\ALL SERVICES

Policy	Setting
Computer Configuration/Policies/ Windows Settings/Security Settings/Local Policies/User Rights Assignment	▪ CPM service user ▪ Scheduled Task service user Remove any other users from the list. **Comments:** ▪ Allows CPM and "CyberArk Scheduled Task" service users to "Run as a service".
Service users	Open services.msc and set the proper user for the following services, : ▪ "CyberArk Password Manager" – CPM service user ▪ "CyberArk Central Policy Manager Scanner" – CPM service user ▪ "CyberArk Scheduled " Restart all services
"Accounts: Rename administrator account" Group policy object: Computer Configuration/Policies/ Windows Settings/Security Settings/Local Policies/ Security Options	It is recommended to change the Administrator's name and the guest's name to a name that will not testify to their permissions, and to create a new locked and unprivileged user name Administrator as bait. **Comments:** Apply this parameter according to the organizational security policy. **Vulnerability:** The administrators default name is known as a high privilege user. This user is a target for hacking attempts.
Only the following network protocols/services/clients are required for a CPM & PVWA machine: ▪ Client for Microsoft Network ▪ File and Printer Sharing for Microsoft Network ▪ Internet Protocol Version 4 (TCP/IPv4)	Remove/disable any other protocols/services/clients from your network connection properties. Unless specifically required, disable IPv6 too. **Comments:** The following were removed and tested: ▪ QoS Packet Scheduler ▪ Link-Layer Topology Discovery Mapper IO Driver ▪ Link-Layer Topology Discovery Responder
The following services are disabled in the policy settings: ▪ Routing and Remote Access ▪ Smart Card ▪ Smart Card Removal Policy ▪ SNMP Trap	By default, all these services are disabled. Disable other services that are not required. **Comments:** ▪ Check whether all enabled services are required. For example Smart card might be in use but customers. ▪ If you disable the Windows Error Reporting Service, your system will not be able to collect dumps.

Policy	Setting
▪ Special Administration Console Helper ▪ Windows Error Reporting Service ▪ WinHTTP Web Proxy Auto-Discovery Service	

Configure PVWA and CPM Servers in 'Out of Domain' Deployments

This section describes how to configure PVWA and CPM servers in 'Out of Domain' deployments.

Automatic procedures (Handled by INF files)

Tip:
This step is performed automatically using the PowerShell script

Install the hardening INF file as described in Importing an INF File to the Local Machine, page 20.

- You will receive the hardening package from CyberArk as a zipped file. Unzip this file so that you can import the hardening INF file.

Manual Procedures

Manually change the settings listed in the following sections.

Notes

- **IMPORTANT!** To manage COM+ usages, the CPM user requires the "Replace a process level token" permission, which by default is only given to the NETWORK_SERVICE and LOCAL_SERVICE users in the hardening process. If the CPM user doesn't have this permission, the following error will appear: "Error creating change password process using LogonAs activation method (error 1314)".

  This permission is given to the CPM user automatically for COM+ usages, but must be set manually for all other plug-ins that use the LogonAs method.
- Many of the "Advance Auditing Configuration" settings record both success and failure events.
  - If "Auditing for Success" is set, it can overload the system. If an overload is created, it is recommended to set "Auditing for Failure" only. These audit settings are in the following local Group Policy:
    Computer Configuration/Windows Settings/Security Settings/Advance Audit Policy Configuration
- The log file sizes in the "General Auditing Configuration" settings are set to 100032 KB. Make sure this is sufficient for your environment.
- The "Network access: Do not allow storage of passwords and credentials for network authentication" settings can affect local scheduled tasks that run with a user (logged on or not) and prevent it from running. These settings are in the following local Group Policy:
  Computer Configuration/Windows Settings/Security Settings/Local Policies\Security Options

Note:
These are local scheduled tasks, not to be confused with scheduled tasks that CPM manages on other machines.)

- The "Network security: Minimum session security for NTLM SSP based (including secure RPC) clients/servers" setting can deny access to Windows 2003/XP

- machines. These settings are in the following local Group Policy: Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options
- The "Shutdown: Clear virtual memory pagefile" prolongs shut down and restart processes, especially on computers with large paging files.
- Possible client and applications compatibility issues, as described in KB823659, can occur from setting the following:
  - In the Event log viewer:
    - Maximum security log size
    - Retention method for security log
  - Under "Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options":
    - Domain member: Require strong (Windows 2000 or later) session key
    - Network access: Do not allow anonymous enumeration of SAM accounts
    - Network access: Do not allow anonymous enumeration of SAM accounts and shares
    - Network security: LAN Manager authentication level
  - Under "Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignment":
    - Access this computer from the network
    - Bypass traverse checking
    - Enable computer and user accounts to be trusted for delegation

Screen Saver

Tip:
This step is performed automatically using the PowerShell script.

In the Local Group Policy, under User Configuration/Administrative Templates/Control Panel/Personalization:

Policy	Setting
Enable screen saver	Enabled
Force specific screen saver	Enabled (e.g.,"C:\Windows\System32\Ribbons.scr")
Password protect the screen saver	Enabled
Screen saver timeout	Enabled Seconds: 600

Advanced audit policy configuration

Tip:
This step is performed automatically using the PowerShell script

In the Local Group Policy

Under Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options:

Policy	Setting	Comments
Audit: Force audit policy subcategory settings to override audit policy category settings	Enabled	This setting enables the use of advanced auditing in the Operating System

In the Local Group Policy

Under Computer Configuration/Windows Settings/Security Settings/Advanced Audit Policy Configuration:

Policy	Setting	
Account Logon	Credential Validation	Success, Fail
	Other Account Logon Event	Success, Fail
Account Management	Application Group Management	Success, Fail
	Computer Account Management	Success, Fail
	Distribution Group Management	Success, Fail
	Other Account Management Events	Success, Fail
	Security Group Management	Success, Fail
	User Account Management	Success, Fail
Logon\Logoff	Account Lockout	Success, Fail
	Logoff	Success, Fail
	Logon	Success, Fail
	Network Policy Server	Success, Fail
	Other Logon\Logoff Event	Success, Fail
	Special Logon	Success, Fail

Policy	Setting	
Object Access	Application Generated	Success, Fail
	Certification Services	Success, Fail
	Detailed File Share	Fail
	File Share	Success, Fail
	File System	Success, Fail
	Kernel Object	Success, Fail
	Registry	Success, Fail
	Removable Storage	Success
	SAM	Success, Fail
	Comment: Operational aspects: Applying "Auditing for Success" can overload the system. If an overload is created, it is recommended to apply "Auditing for Failure" only.	
Policy Change	Audit Policy Change	Success, Fail
	Authentication Policy Change	Success, Fail
	Authorization Policy Change	Success, Fail
	Filtering Platform Policy Change	Success, Fail
	MPSSVC Rule –Level Policy Change	Success, Fail
Privilege Use	Non Sensitive Privilege Use	Success, Fail
	Sensitive Privilege Use	Fail
System	Other System Events	Success, Fail
	Security State Change	Success, Fail
	Security System Extension	Success, Fail
	System Integrity	Success, Fail

Remote desktop services

Tip:
This step is performed automatically using the PowerShell script.

In the Local Group Policy

Under User Configuration/Administrative Template/ Windows Components/Remote Desktop Services/Remote Desktop Session Host:

Note:
* Indicated settings are not available in the local policy settings.

Policy	Setting
Connections/Automatic reconnection*	Disabled
Connections/Configure keep-alive connection interval*	Enabled Keep-Alive interval:1
Connections/Deny logoff of an administrator logged in to the console session*	Enabled
Connections/Set rules for remote control of Remote Desktop Services user sessions	Enabled View Session without user's permission
Device and Resource Redirection/Do not allow Clipboard redirection	Enabled
Device and Resource Redirection/Do not allow COM port redirection*	Enabled
Device and Resource Redirection/Do not allow drive redirection*	Enabled
Device and Resource Redirection/Do not allow LPT port redirection*	Enabled
Device and Resource Redirection/Do not allow supported Plug and Play device redirection*	Enabled
Remote Session Environment/Remove "Disconnect" option from Shut Down dialog*	Enabled
Remote Session Environment/Remove Windows Security item from Start menu*	Enabled
Security/Do not allow local administrators to customize permissions*	Enabled
Security/Require secure RPC communication*	Enabled
Security/Set client connection encryption level*	Enabled Encryption Level: High Level
Session Time Limits/End session when time limits are reached	Enabled
Session Time Limits/Set time limit for active but idle Remote Desktop Services sessions	Enabled
Session Time Limits/Set time limit for disconnected sessions*	Enabled Session Time Limits/Set time limit for disconnected sessions*
Temporary Folders/Do not delete temp folders upon	Disabled

Policy	Setting
exit*	
Temporary Folders/Do not use temporary folders per session*	Disabled

General auditing configuration, registry and file system

Tip:
This step is performed automatically using the PowerShell script.

IMPORTANT! Always backup your registry before making changes.

General auditing configuration

Policy	Setting
Event log size and retention	1. Run eventvwr.msc, open "Windows logs", for each of the following items: ▪ Application ▪ Security ▪ System 2. Right click Properties. 3. Set the "Maximum log size (KB)" to 100032. 4. Make sure that "Overwrite events as needed" is selected.
Registry Audits	1. For the following: ▪ HKLM\SOFTWARE ▪ HKLM\SYSTEM 2. Run regedit.exe. 3. Right click the registry key (e.g. HKLM\SOFTWARE) and open the Permissions window. 4. Click Advanced and then Auditing. 5. Select Principal and specify "Everyone", then click OK. 6. Select the following: ▪ Type="Success" ▪ Applies to="This key and sub keys" 7. Click "Show advanced permissions", select check "Set Value", then click OK. 8. Add another auditing entry (add). 9. Select Principal and specify "Everyone", then click OK. 10. Select the following: ▪ Type="All" ▪ Applies to="This key and sub keys"

Policy	Setting
	11. Click "Show advanced permissions" and select the following: ▪ Create Subkey ▪ Create Link ▪ Delete ▪ Write DAC ▪ Read Control 12. Click OK. 13. Click Apply and OK.
Registry permissions	1. Run regedit.exe. 2. Right click the following key: "HKLM\System\CurrentControlSet\Control\ SecurePipeServers\Winreg" and select "Permissions". 3. Make sure that only the Administrators group has all permissions ("Full control"). 4. Remove all other groups and/or users. 5. Click OK.
File System Hardening	1. For the following folders: ▪ %SystemRoot%\System32\Config ▪ %SystemRoot%\System32\Config\RegBack 2. Set the relevant permissions: a. Right click the folder, and select Properties → Security → Edit. b. Make sure that only the "Administrators" and "SYSTEM" have all permissions ("Full control"). c. Remove all other groups and/or users. 3. Set auditing: a. Right click the folder, and select Properties → Security → b. Advanced → Auditing. c. Click Add, then select a principal, and add "Everyone". d. Select Type="Fail", then click "Show advanced permissions", and make sure that at least the following are checked: ▪ Traverse Folder\ Execute File ▪ List Folder\ Read Data ▪ Read Attributes ▪ Read Extended Attribute. e. Click OK. f. In the same way as described above, add audit of type="All" and select the following: ▪ Create Files\ Write Data ▪ Create Folders\ Append Data ▪ Write Attributes ▪ Write Extended Attributes

Policy	Setting
	▪ Delete Subfolders And Files ▪ Delete ▪ Change Permissions ▪ Take Ownership. g. Click OK.

Additional manual steps

Additional steps

Tip:
Most of the steps listed in the following table are performed automatically using the PowerShell script. The steps that are NOT performed automatically are marked below.

Policy	Setting
Create a domain/local user to use in the "PMEngine" (CPM) service.	
Set permissions on the local folder for the CPM user and remove unnecessary permissions (Leave the CPM user, administrators group and SYSTEM).	▪ Set reader permissions on the following folders: ▪ [Drive]:\Python27 ▪ [Drive]:\Oracle ▪ [Drive]:\Program Files (x86)\CyberArk ▪ Set full permissions on the following folders: ▪ [Drive]:\Program Files (x86)\CyberArk\PasswordManager\Logs ▪ [Drive]:\Program Files (x86)\CyberArk\PasswordManager\tmp ▪ [Drive]:\Program Files (x86)\CyberArk\PasswordManager\bin ▪ [Drive]:\Program Files (x86)\ CyberArk\PasswordManager\Vault\user.ini ▪ [Drive]:\Program Files (x86)\CyberArk\PasswordManager\Scanner \Log ▪ Remove the "users" permissions from all aforementioned folders and other unnecessary users and groups. **Comments** ▪ Stop the CPM, CPMScanner and Scheduled task services. ▪ To remove user/groups from a folder, disable permission inheritance for the folder: ▪ Folder properties → Security → Advanced.

Policy	Setting
	▪ Change the permissions: ▪ Clear "Include inheritable permissions…" or ▪ Click "Disable inheritance" ▪ Reader permissions = Read & Execute, List folder content, Read. ▪ Full permissions = Full Control, Read & Execute, List, Read, Modify, Write.
Remove unnecessary user/group permissions from the PVWA folders.	From the "[Drive:]\CyberArk" folder, remove all users/groups except for the built-in SYSTEM and Administrators group. **Comments** ▪ By default, the PVWA is installed in C:\CyberArk. Make sure you know where the "Password Vault Web Access" folder is.
Create a domain/local user to use in the "CyberArk Scheduled Task" service (installed by the PVWA)	
Set permissions for the "CyberArk Scheduled Task" service and remove unnecessary permissions.	▪ Set reader permissions for the service user on: "[Drive]:\CyberArk\PasswordVault WebAccess\Services". ▪ Set full permissions on: "[Drive]:\CyberArk\PasswordVault WebAccess\Services\Log". ▪ Remove the "users" permissions from the above folders and from other unnecessary users and groups. **Comments** ▪ To remove user/groups from a folder, disable permission inheritance for the folder: ▪ Folder properties → Security → Advanced. ▪ Change the permissions: ▪ Clear "Include inheritable permissions…" or ▪ Click "Disable inheritance" ▪ Reader permissions = Read & Execute, List folder content, Read. ▪ Full permissions = Full Control, Read & Execute, List, Read, Modify, Write.
"Log on as a service" Local group policy:	▪ Add the following users: ▪ NT SERVICE\ALL SERVICES ▪ CPM service user

Policy	Setting
Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignment	▪ Scheduled Task service user ▪ Clear the "Log on as a service" configuration from all other users  **Tip:** This setting is not performed automatically using the PowerShell script. Set it manually. **Comments** ▪ Allow CPM and "CyberArk Scheduled Task" service users to "Run as a service".
Service users	▪ Open services.msc and set the correct user for each of the services, by right clicking "Log on": ▪ "CyberArk Password Manager" – CPM service user ▪ "CyberArk Central Policy Manager Scanner" - CPM service user ▪ "CyberArk Scheduled Tasks" ▪ Restart all services
"Accounts: Rename administrator account" Local group policy: Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options  **Tip:** This step is not performed automatically using the PowerShell script. Set it manually.	It is recommended to change both the Administrator name and the guest names to a name that will not testify to their permissions, and to create a new locked and unprivileged user called Administrator as bait. **Comments** ▪ Apply this parameter according to the organization security policy. **Vulnerability** ▪ The administrators default name is known as a high privilege user. This user is a target for hacking attempts. **Operational aspects** ▪ None
Only the following network protocols/Services/Clients are required for a CPM & PVWA machine: ▪ Client for Microsoft Network ▪ File and Printer Sharing for Microsoft Network	▪ Remove/disable any other protocols/services/clients from your network connection properties. ▪ Unless specifically required, also disable IPv6. **Comments** The following were removed and tested: ▪ QoS Packet Scheduler

Policy	Setting
▪ Internet Protocol Version 4 (TCP/IPv4)  **Tip:** This step is not performed automatically using the PowerShell script. Set it manually.	▪ Link-Layer Topology Discovery Mapper IO Driver ▪ Link-Layer Topology Discovery Responder
The following services are disabled in the policy settings: ▪ Routing and Remote Access ▪ Smart Card ▪ Smart Card Removal Policy ▪ SNMP Trap ▪ Special Administration Console Helper ▪ Windows Error Reporting Service ▪ WinHTTP Web Proxy Auto-Discovery Service	▪ By default, all of these services are disabled. ▪ Disable any other services that are not required. **Comments** ▪ Review all services and make sure they are not required. For example, Smart card might be in use by customers. ▪ If the Windows Error Reporting Service is disabled, the system will not be able to collect dumps.

GPO Settings

Policy	Value	Reason
User Configuration → Policies → Administrative Templates → Control Panel/Personalization		
Enable screen saver	Enabled	**Vulnerability:** There is no protection against a user with physical and remote desktop access to the server. **Severity of the damage:** Medium **Operational aspects:** None
Force specific screen saver	Enabled	
Password protect the screen saver	Enabled	
Screen saver timeout	Enabled Seconds: 600	
Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies /Security Options		
Audit: Force audit policy subcategory settings to override audit policy category settings	Enabled	This setting enables the use of advance auditing in the operating system
Computer Configuration → Policies → Windows Settings → Security Settings → Advance Audit Policy Configuration → Logon Account		

Policy	Value	Reason
Credential Validation	Success, Fail	**Vulnerability:** Lack of information on unauthorized user login attempt. Lack of this type of information will prevent identification of intruders to the system, as well as inability to check access to the server or its resources. **Severity of the damage:** Medium **Operational aspects:** None
Other Account Logon Event	Success, Fail	
Computer Configuration → Policies → Windows Settings → Security Settings → Advance Audit Policy Configuration → Account Management		

Policy	Value	Reason
Application Group Management	Success, Fail	**Vulnerability:** Lack of information on user management in the system (addition and removal of users). Lack of this type of information will prevent identification of intruders to the system, as well as inability to check access to the server or its resources. **Severity of the damage:** Medium **Operational aspects:** None
Computer Account Management	Success, Fail	
Distribution Group Management	Success, Fail	
Other Account Management Events	Success, Fail	
Security Group Management	Success, Fail	
User Account Management	Success, Fail	
Computer Configuration → Policies → Windows Settings → Security Settings → Advance Audit Policy Configuration → Logon\Logoff		

Policy	Value	Reason
Account Lockout	Success, Fail	**Vulnerability:** Lack of information on unauthorized user login attempt. Lack of this type of information will prevent identification of intruders to the system, as well as inability to check access to the server or its resources. **Severity of the damage:** Medium **Operational aspects:** None
Logoff	Success, Fail	
Logon	Success, Fail	
Network Policy Server	Success, Fail	
Other Logon\Logoff Event	Success, Fail	
Special Logon	Success, Fail	
Computer Configuration → Policies → Windows Settings → Security Settings → Advance Audit Policy Configuration → Object Access		

Policy	Value	Reason
Application Generated	Success, Fail	**Vulnerability:** Lack of information on access to sensitive files and folders in the system. Lack of this type of information will prevent identification of intruders to the system, as well as inability to check access to the server or its resources. **Severity of the damage:** Medium **Operational aspects:** Applying Auditing for Success can overload the system. In case an overload is created, it is recommended to apply the auditing for Failure only.
Certification Services	Success, Fail	
Detailed File Share	Fail	
File Share	Success, Fail	
File System	Success, Fail	
Kernel Object	Success, Fail	
Registry	Success, Fail	
Removable Storage	Success	
SAM	Success, Fail	
Computer Configuration → Policies → Windows Settings → Security Settings → Advance Audit Policy Configuration → Policy Change		

Policy	Value	Reason
Audit Policy Change	Success, Fail	**Vulnerability:** Lack of information on changes in the policy. Lack of this type of information will prevent identification of intruders to the system, as well as inability to check access to the server or its resources. **Severity of the damage:** Medium **Operational aspects:** None
Authentication Policy Change	Success, Fail	
Authorization Policy Change	Success, Fail	
Filtering Platform Policy Change	Success, Fail	
MPSSVC Rule –Level Policy Change	Success, Fail	
Computer Configuration → Policies → Windows Settings → Security Settings → Advance Audit Policy Configuration → Privilege Use		
Non Sensitive Privilege Use	Success, Fail	**Vulnerability:** Lack of information on the use of system authorizations. Lack of this type of information will prevent identification of intruders to the system, as well as inability to check access to the server or its resources. **Severity of the damage:** Medium **Operational aspects:** None
Sensitive Privilege Use	Fail	
Computer Configuration → Policies → Windows Settings → Security Settings →		

Policy	Value	Reason
Advance Audit Policy Configuration → System		
Other System Events	Success, Fail	**Vulnerability:** Lack of information on system start-up, shutdown and system changes. Lack of this type of information will prevent identification of intruders to the system, as well as inability to check access to the server or its resources. **Severity of the damage:** Medium **Operational aspects:** None
Security State Change	Success, Fail	
Security System Extension	Success, Fail	
System Integrity	Success, Fail	
Computer Configuration → Policies → Windows Settings → Security Settings → Event Log		
Maximum application log size	100032 KB	**Vulnerability:** There is a risk that many log records will not be saved due to the file's size. **Severity of the damage:** Medium **Operational aspects:** None
Maximum security log size	100032 KB	
Maximum system log size	100032 KB	
Prevent local guests group from accessing application log	Enabled	
Prevent local guests group from accessing security log	Enabled	
Prevent local guests group from accessing system log	Enabled	
Retention method for application log	As needed	
Retention method for security log	As needed	
Retention method for system log	As needed	
Computer Configuration → Policies → Windows Settings → Security Settings → Registry		
Audit the following registry keys: . HKLM\SYSTEM	Auditing should be applied according to the following parameters:	

Policy	Value	Reason
. HKLM\SOFTWARE	**Audit - Success only:** Set Value **Audit - All:** Create Subkey, Create Link, Delete, Read Permissions, Change Permissions	
Computer Configuration → Policies → Windows Settings → Security Settings → Registry		
Hklm\ System\ CurrentControlSet\ Control\ SecurePipeServers\ Winreg	Administrators – Full Control	**Vulnerability:** Ability to remotely access data on the system by an unauthorized user. **Severity of the damage:** Low **Operational aspects:** None
Computer Configuration → Policies → Windows Settings → Security Settings → File System		
Set permissions and audit to the following folders: . %SystemRoot%\System32 \Config, . %SystemRoot%\System32\Con fig \RegBack	Permissions and auditing should be applied according to the following parameters: **Audit – Failure only:** Traverse Folder\ Execute File, List Folder\ Read Data, Read Attributes, Read Extended Attribute. **Audit - All:** Create Files\ Write Data, Create Folders\ Append Data, Write Attributes, Write Extended Attributes, Delete Subfolders And Files, Delete, Change Permissions, Take Ownership. **Permissions:** Administrator, System -	**Vulnerability:** Lack of information on delete, change of authorizations, gain ownership of sensitive files, or any attempt to do so, will prevent the ability to identify unauthorized access and therefore will make it difficult to prevent such attempts. **Severity of the damage:** Medium **Operational**

Policy	Value	Reason
	Full	**aspects:** None
Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies/Security Options		
Accounts: Administrator account status	Enabled	
Accounts: Guest account status	Disabled	
Accounts: Limit local account use of blank passwords to console logon only	Enabled	
Accounts: Rename administrator account	It is recommended to change both the Administrator and the guest names to a name that will not testify about their permissions, and also to create a new locked and unprivileged user name Administrator as bate	**Comment:** Apply this parameter according to the organization security policy. **Vulnerability:** The administrators default name is known as a high privilege user. This user is a target for hacking attempts. **Severity of the damage:** Medium **Operational aspects:** None
Audit: Audit the use of Backup and Restore privilege.	Enabled	**Vulnerability:** The system does not monitor backup and restore activities of files, therefore it does not allow exposing unusual activities in this area. **Severity of the damage:**

Policy	Value	Reason
		Low **Operational aspects:** None
Devices: Allowed to format and eject removable media	Administrator	**Vulnerability:** Users may be able to move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control, and view or modify any file. The fact that most removable storage devices will eject media by pressing a mechanical button diminishes the advantage of this policy setting. **Severity of the damage:** Low **Operational aspects:** None
Devices: Prevent users from installing printer drivers	Enabled	**Vulnerability:** A malicious user could install inappropriate printer drivers in a deliberate attempt to damage the computer, or a user might accidentally

Policy	Value	Reason
		install malicious software that masquerades as a printer driver. **Severity of the damage:** Low **Operational aspects:** None
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled	**Vulnerability:** A remote user could potentially access a mounted CD that contains sensitive information. This risk is small, because CD drives are not automatically made available as shared drives; administrators must deliberately choose to share the drive. However, administrators may want to deny network users the ability to view data or run applications from removable media on the server. **Severity of the damage:** Low **Operational aspects:** None
Devices: Restrict floppy access to locally logged-on user only	Enabled	**Vulnerability:**

Policy	Value	Reason
		A remote user could potentially access a mounted floppy that contains sensitive information. This risk is small, because floppy drives are not automatically made available as shared drives; administrators must deliberately choose to share the drive. However, administrators may want to deny network users the ability to view data or run applications from removable media on the server. **Severity of the damage:** Low **Operational aspects:** None
Domain member: Disable machine account password changes	Disabled	**Vulnerability:** Computers that cannot automatically change their account password are at risk from an attacker who could determine the password for the computer's domain account. **Severity of the damage:**

Policy	Value	Reason
		Low **Operational aspects:** None
Domain member: Maximum machine account password age	30 days	**Vulnerability:** Setting this parameter to 0 will allow an attacker to execute Brute Force attacks to find the computer account password. **Severity of the damage:** Low **Operational aspects:** None
Domain member: Require strong (Windows 2000 or later) session key	Enabled	**Vulnerability:** Session keys that are used to establish secure channel communications between domain controllers and member computers are much stronger in Windows 2000 than they were in previous Windows operating systems. **Severity of the damage:** Low **Operational aspects:** None
Interactive logon: Do not display last user name	Enabled	**Vulnerability:**

Policy	Value	Reason
		An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Terminal Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute force attack to try to log on. **Severity of the damage:** Low **Operational aspects:** None
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	**Vulnerability:** If users are not required to press CTRL+ALT+DEL, they are susceptible to attacks that attempt to intercept their passwords, If this setting is enabled, an attacker could install a Trojan horse program that looks like the standard logon dialog box in the Windows operating

Policy	Value	Reason
		system, and capture the user's password. **Severity of the damage:** Low **Operational aspects:** None
Interactive logon: Number of previous logons to cache (in case domain controller is not available).	0	**Vulnerability:** Users who access the server console will have their logon credentials cached on that server. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to attempt to determine user passwords. **Severity of the damage:** Medium **Operational aspects:** The local Administrator password should be known in case of DC unavailability
Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled	**Vulnerability:** By default, the computer caches in memory the credentials of any users who

Policy	Value	Reason
		are authenticated locally. The computer uses these cached credentials to authenticate anyone who attempts to unlock the console. When cached credentials are used, any changes that have recently been made to the account—such as user rights assignments, account lockout, or the account being disabled—are not considered or applied after the account is authenticated. User privileges are not updated, and (more important) disabled accounts are still able to unlock the console of the computer. **Severity of the damage:** Medium **Operational aspects:** The local Administrator password should be known in case of DC unavailability
Microsoft network client: Send unencrypted password to third-party	Disabled	**Vulnerability:**

Policy	Value	Reason
SMB servers.		The server can transmit passwords in plaintext across the network to other computers that offer SMB services. These other computers might not use any of the SMB security mechanisms that are included with Windows Server 2003 and above. **Severity of the damage:** Medium **Operational aspects:** None
Microsoft network server: Amount of idle time required before suspending session	15 minutes	**Vulnerability:** Each SMB session consumes server resources, and numerous null sessions will slow the server or possibly cause it to fail. An attacker could repeatedly establish SMB sessions until the server's SMB services become slow or unresponsive. **Severity of the damage:** Medium **Operational aspects:** None
Microsoft network server: Attempt	Disabled	**Vulnerability:**

Policy	Value	Reason
S4U2Self to obtain claim information		Enabling this policy setting allows you take advantage of features in Windows Server 2012 and Windows 8 for specific scenarios to use claims-enabled tokens to access files or folders that have claim-based access control policy applied on Windows operating systems prior to Windows Server 2012 and Windows 8. **Severity of the damage:** Medium **Operational aspects:** None
Microsoft network server: Server SPN target name validation level	Off	**Vulnerability:** This policy setting controls the level of validation that a server with shared folders or printers performs on the service principal name (SPN) that is provided by the client computer when the client computer establishes a session by using the SMB protocol. The

Policy	Value	Reason
		level of validation can help prevent a class of attacks against SMB servers (referred to as SMB relay attacks). This setting will affect both SMB1 and SMB2. **Severity of the damage:** Low **Operational aspects:** None
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	**Vulnerability:** An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks. **Severity of the damage:** Medium **Operational aspects:** None
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled	**Vulnerability:** An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess

Policy	Value	Reason
		passwords or perform social-engineering attacks. **Severity of the damage:** Medium **Operational aspects:** None
Network access: Do not allow storage of passwords and credentials for network authentication.	Enabled	**Vulnerability:** Passwords that are cached can be accessed by the user when logged on to the computer. Although this information may sound obvious, a problem can arise if the user unknowingly runs malicious software that reads the passwords and forwards them to another, unauthorized user. **Severity of the damage:** Medium **Operational aspects:** This parameter could affect windows schedule task services
Network access: Let Everyone permissions apply to anonymous users	Disabled	**Vulnerability:** The system will allow all users, including users who have not

Policy	Value	Reason
		identified themselves in the Domain, perform operations of reading information related to user accounts and the names of the shares. **Severity of the damage:** Medium **Operational aspects:** None
Network access: Named Pipes that can be accessed anonymously	List has been deleted	**Vulnerability:** Ability to remotely access data on the system by an unauthorized user. **Severity of the damage:** Low **Operational aspects:** None
Network access: Remotely accessible registry paths	List has been deleted	**Vulnerability:** An attacker could use information in the registry to facilitate unauthorized activities. To reduce the risk of such an attack, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorized

Policy	Value	Reason
		users. **Severity of the damage:** Low **Operational aspects:** None
Network access: Remotely accessible registry paths and subpaths	List has been deleted	**Vulnerability:** An attacker could use information in the registry to facilitate unauthorized activities. To reduce the risk of such an attack, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorized users. **Severity of the damage:** Low **Operational aspects:** None
Network access: Restrict anonymous access to Named Pipes and Shares.	Enabled	**Vulnerability:** Null sessions are a weakness that can be exploited through shared folders on computers environment. **Severity of the damage:** Low **Operational aspects:** None

Policy	Value	Reason
Network access: Shares that can be accessed anonymously	List has been deleted	**Vulnerability:** Any shared folders that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data. **Severity of the damage:** Medium **Operational aspects:** None
Network access: Sharing and security model for local accounts	Classic - Local users authenticate as themselves	**Vulnerability:** With the Guest only model, any user who can authenticate to the server over the network does so with guest privileges, which means that they will not have write access to shared resources on that server. Although this restriction does increase security, it makes it more difficult for authorized users to access shared resources on the server because ACLs on those resources must include access control entries (ACEs) for the Guest account. With the Classic model, local

Policy	Value	Reason
		accounts should be password protected. Otherwise, if Guest access is enabled, anyone can use those user accounts to access shared system resources. **Severity of the damage:** Low **Operational aspects:** None
Network security: Do not store LAN Manager hash value on next password change	Enabled	**Vulnerability:** The SAM file can be targeted by attackers who seek access to user name and password hashes. Such attacks use special tools to discover passwords, which can then be used to impersonate users and gain access to resources on your network. **Severity of the damage:** Medium **Operational aspects:** None
Network security: Force logoff when logon hours expire	Enabled	**Vulnerability:** Users can remain connected to the computer outside

Policy	Value	Reason
		of their allotted logon hours. **Severity of the damage:** Low **Operational aspects:** None
Network security: LAN Manager authentication level	Send NTLMv2 Responses Only/Refuse LM & NTLM	**Vulnerability:** The system allows identification of users in the old LM and NTLM protocols. The old identification protocols are vulnerable to attacks. **Severity of the damage:** Medium **Operational aspects:** These parameters could effect on legacy system if the system don't support NTLMv2
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security Require 128-bit encryption	**Vulnerability:** Network traffic that uses the NTLM Security Support Provider (NTLM SSP) might be exposed such that an attacker who has gained access to the network can create man-in-the-middle attacks. **Severity of the**

Policy	Value	Reason
		damage: Medium **Operational aspects:** None
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security Require 128-bit encryption	**Vulnerability:** Network traffic that uses the NTLM Security Support Provider (NTLM SSP) might be exposed such that an attacker who has gained access to the network can create man-in-the-middle attacks. **Severity of the damage:** Medium **Operational aspects:** None
Recovery console: Allow automatic administrative logon	Disabled	**Vulnerability:** The Recovery Console can be very useful when you need to troubleshoot and repair computers that do not start. However, it is dangerous to allow automatic logon to the console. Anyone could walk up to the server, disconnect the power to shut it down, restart it, select Recover Console from the Restart menu,

Policy	Value	Reason
		and then assume full control of the server. **Severity of the damage:** Medium **Operational aspects:** None
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	**Vulnerability:** An attacker who can cause the system to restart into the Recovery Console could steal sensitive data and leave no audit or access trail. **Severity of the damage:** Low **Operational aspects:** None
Shutdown: Allow system to be shut down without having to log on	Disabled	**Vulnerability:** Users who can access the console locally could shut down the computer. **Severity of the damage:** Low **Operational aspects:** None
Shutdown: Clear virtual memory pagefile	Enabled	**Vulnerability:** Important information that is kept in real memory may be

Policy	Value	Reason
		written periodically to the paging file to help the operating system handle multitasking functions. An attacker who has physical access to a server that has been shut down could view the contents of the paging file. The attacker could move the system volume into a different computer and then analyze the contents of the paging file. Although this process is time consuming, it could expose data that is cached from random access memory (RAM) to the paging file. **Severity of the damage:** Low **Operational aspects:** It takes longer to shut down and restart the computer, especially on computers with large paging files.
System Settings: Optional subsystems	No one	**Vulnerability:** The POSIX

Policy	Value	Reason
		subsystem introduces a security risk that relates to processes that can potentially persist across logons. If a user starts a process and then logs out, there is a potential that the next user who logs on to the computer could access the previous user's process. This would allow the second user to take actions on the process by using the privileges of the first user. **Severity of the damage:** Low **Operational aspects:** None
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Enable	**Vulnerability:** Without the use of software restriction policies, users and computers might be exposed to the running of unauthorized software, such as viruses and Trojans horses. **Severity of the damage:** Medium **Operational**

Policy	Value	Reason
		aspects: None
User Account Control: Use Admin Approval Mode for the built-in Administrator account	Enable	**Vulnerability:** Malicious software running under elevated credentials without the user or administrator being aware of its activity. **Severity of the damage:** Medium **Operational aspects:** None
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disable	**Vulnerability:** Without the use of software restriction policies, users and computers might be exposed to the running of unauthorized software, such as viruses and Trojans horses. **Severity of the damage:** Medium **Operational aspects:** None
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for non-Windows binaries	**Vulnerability:** Malicious programs running under elevated credentials without the user or administrator being aware of their activity.

Policy	Value	Reason
		This setting raises awareness to the user that a program requires the use of elevated privilege operations and requires that the user be able to supply administrative credentials in order for the program to run. **Severity of the damage:** Medium **Operational aspects:** None
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials on the secure desktop	**Vulnerability:** Malicious programs running under elevated credentials without the user or administrator being aware of their activity. This setting raises awareness to the user that a program requires the use of elevated privilege operations and requires that the user be able to supply administrative credentials in order for the program to run. **Severity of the**

Policy	Value	Reason
		damage: Low **Operational aspects:** None
User Account Control: Only elevate UIAccess applications that are installed in secure locations Severity of the damage: Low Operational aspects: None	Enable	**Vulnerability:** UIAccess Integrity allows an application to bypass User Interface Privilege Isolation (UIPI) restrictions when an application is elevated in privilege from a standard user to an administrator. **Severity of the damage:** Low **Operational aspects:** None
User Account Control: Run all administrator in admin approval mode	Enable	**Vulnerability:** This is the setting that turns on or off UAC. If this setting is disabled, UAC will not be used and any security benefits and risk mitigations that are dependent on UAC will not be present on the system. **Severity of the damage:** Medium **Operational aspects:** None

Policy	Value	Reason
User Account Control: Switch to the secure desktop when prompting for elevation	Enable	**Vulnerability:** Elevation prompt dialog boxes can be spoofed, causing users to disclose their passwords to malicious software. **Severity of the damage:** Medium **Operational aspects:** None
User Account Control: Virtualize file and registry write failures to per-user locations	Enable	**Severity of the damage:** Low **Operational aspects:** None
Microsoft network server: Server SPN target name validation level	Disabled	**Vulnerability:** Without the use of software restriction policies, users and computers might be exposed to the running of unauthorized software, such as viruses and Trojans horses. **Severity of the damage:** Low **Operational aspects:** None
Computer Configuration → Policies → Windows Settings → Security Settings → System Services		

Policy	Value	Reason
Routing and Remote Access	Disabled	**Vulnerability:** Unnecessary services are expose the server to vulnerabilities and increasing the attack surface **Severity of the damage:** Medium **Operational aspects:** Before disabling any of the services, make sure that it is not depended on by other system or service.
Smart Card	Disabled	
Smart Card Removal Policy	Disabled	
SNMP Trap	Disabled	
Special Administration Console Helper	Disabled	
Windows Error Reporting Service	Disabled	
WinHTTP Web Proxy Auto-Discovery Service	Disabled	
Windows Firewall	Enabled	
Computer Configuration → Policies → Admininstrative Tamplates → Windows Components → Remote Desktop Services → Remote Desktop Session Host		

Policy	Value	Reason
Automatic reconnection	Disabled	**Vulnerability:** An unlimited number of open connections can cause denial of Service attack on the Terminal Services. If a disconnected session kept alive that can lead a session hijacking by an attacker. Clipboard mapping enables the client to transfer a virus or a malicious application to the server as well as copy configuration or sensitive data from the server back to the client machine. There is a risk of infecting to the whole network or damaging the system. **Severity of the damage:** Medium **Operational aspects:** None
Configure keep-alive connection interval	Enabled Keep-Alive interval:1	
Deny logoff of an administrator logged in to the console session	Enabled	
Set rules for remote control of Remote Desktop Services user sessions	Enabled View Session without user's permission	
Do not allow Clipboard redirection	Disabled	
Do not allow COM port redirection	Enabled	
Do not allow drive redirection	Enabled	
Do not allow LPT port redirection	Enabled	
Do not allow supported Plug and Play device redirection	Enabled	
Remove "Disconnect" option from Shut Down dialog	Enabled	
Remove Windows Security item from Start menu	Enabled	
Do not allow local administrators to customize permissions	Enabled	
Require secure RPC communication	Enabled	
Set client connection encryption level	Enabled Encryption Level: High Level	
End session when time limits are reached	Enabled	
Set time limit for active but idle Remote Desktop Services sessions	Enabled	
Set time limit for disconnected sessions	Enabled Remote App session logoff delay: 15	
Do not delete temp folders upon exit	Disabled	
Do not use temporary folders per session	Disabled	
Computer Configuration → Policies → Windows Settings → Security Settings → User Rights Assignment		
Access Credential Manager as a trusted caller		**Vulnerability:**

Policy	Value	Reason
		If an account is given this right, the user of the account can create an application that calls into Credential Manager and is then provided the credentials for another user. **Severity of the damage:** Medium **Operational aspects:** None
Access this computer from the network	BUILTIN\Administrators	**Vulnerability:** This right allows the users to use the SMB communications protocol in front of the server. This protocol allows access to the operating resources, such as: sharing and remote system administration using the operating system's built-in tools. **Severity of the damage:** Medium **Operational aspects:** None
Act as part of the operating system		**Vulnerability:** Users with the Act as part of the operating system user right can

Policy	Value	Reason
		take complete control of the computer and erase evidence of their activities. **Severity of the damage:** Medium **Operational aspects:** None
Adjust memory quotas for a process	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, BUILTIN\Administrators	**Vulnerability:** A user with the Adjust memory quotas for a process user right can reduce the amount of memory that is available to any process, which could cause business-critical network applications to become slow or to fail. This privilege could be used to start a denial-of-service (DoS) attack. **Severity of the damage:** Medium **Operational aspects:** None
Allow log on locally	BUILTIN\Administrators	**Vulnerability:** Any account with the Allow log on locally user right can log on at the console of the computer. If you do not restrict this user right to

Policy	Value	Reason
		legitimate users who must log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges. **Severity of the damage:** Medium **Operational aspects:** None
Allow log on through Terminal Services	BUILTIN\Administrators	**Vulnerability:** Any account with the Allow log on through Remote Desktop Services user right can log on to the remote console of the computer. If you do not restrict this user right to legitimate users who must log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges. **Severity of the damage:** Medium **Operational aspects:** None
Back up files and directories	BUILTIN\Administrators	**Vulnerability:**

Policy	Value	Reason
		Users who can back up data from a computer could take the backup media to a non-domain computer on which they have administrative privileges and restore the data. They could take ownership of the files and view any unencrypted data that is contained within the backup set. **Severity of the damage:** Medium **Operational aspects:** None
Bypass traverse checking	NT AUTHORITY\ NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators	**Vulnerability:** This right allows the user to access files and partitions although he is not authorized to view files and change them. **Severity of the damage:** Medium **Operational aspects:** None
Change the system time	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE	**Vulnerability:** Users who can change the time on a computer could cause several problems. For

Policy	Value	Reason
		example, time stamps on event log entries could be made inaccurate, an attacker who changes a computer's time may cause that computer to be unable to obtain or grant Kerberos protocol tickets. **Severity of the damage:** Medium **Operational aspects:** None
Change the time zone	BUILTIN\Administrator	**Vulnerability:** Changing the time zone represents little vulnerability because the system time is not affected. This setting merely enables users to display their preferred time zone while being synchronized with domain controllers in different time zones. **Severity of the damage:** Low **Operational aspects:** None
Create a token object		**Vulnerability:** A user account

Policy	Value	Reason
		that is given this user right has complete control over the system, and it can lead to the system being compromised. **Severity of the damage:** High **Operational aspects:** None
Create global objects	NT AUTHORITY\SERVICE, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, BUILTIN\Administrators	**Vulnerability:** Users who can create global objects could affect processes that run under other users' sessions. This capability could lead to a variety of problems, such as application failure or data corruption. **Severity of the damage:** Medium **Operational aspects:** None
Create permanent shared objects		**Vulnerability:** Users who have the Create permanent shared objects user right could create new shared objects and expose sensitive data to the network. **Severity of the**

Policy	Value	Reason
		damage: Medium **Operational aspects:** None
Create symbolic links	Administrators	**Vulnerability:** Users who have the Create symbolic links user right could inadvertently or maliciously expose your system to symbolic link attacks. Symbolic link attacks can be used to change the permissions on a file, to corrupt data, to destroy data, or as a DoS attack. **Severity of the damage:** Low **Operational aspects:** None
Debug programs	BUILTIN\Administrator	**Vulnerability:** The Debug programs user right can be exploited to capture sensitive computer information from system memory or to access and modify kernel or application structures. Some attack tools exploit this user right to extract hashed

Policy	Value	Reason
		passwords and other private security information or to insert rootkit code. **Severity of the damage:** Low **Operational aspects:** None
Deny access to this computer from the network	BUILTIN\Guests	**Vulnerability:** Users who can log on to the computer over the network can enumerate lists of account names, group names, and shared resources. Users with permission to access shared folders and files can connect over the network and possibly view or modify data. **Severity of the damage:** Medium **Operational aspects:** None
Deny log on as a batch job	BUILTIN\Guests	**Vulnerability:** Accounts that have the Deny log on as a batch job user right could be used to schedule jobs that could consume excessive computer

Policy	Value	Reason
		resources and cause a DoS condition. **Severity of the damage:** Medium **Operational aspects:** None
Deny log on as a service	BUILTIN\Guests	**Vulnerability:** Accounts that can log on as a service could be used to configure and start new unauthorized services, such as a keylogger or other malicious software. **Severity of the damage:** Medium **Operational aspects:** None
Deny log on locally	BUILTIN\Guests	**Vulnerability:** Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who must log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Policy	Value	Reason
		Severity of the damage: Medium **Operational aspects:** None
Deny log on through Terminal Services	BUILTIN\Guests	**Vulnerability:** Any account with the right to log on through Remote Desktop Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, malicious users might download and run software that elevates their privileges. **Severity of the damage:** Medium **Operational aspects:** None
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators	**Vulnerability:** Misuse of the **Enable computer and user accounts to be trusted for delegation** user right could allow unauthorized users to impersonate other users on the network. An attacker could

Policy	Value	Reason
		exploit this privilege to gain access to network resources and make it difficult to determine what has happened after a security incident. **Severity of the damage:** Medium **Operational aspects:** None
Force shutdown from a remote system	BUILTIN\Administrators	**Vulnerability:** Any user who can shut down a computer could cause a DoS condition to occur. Therefore, this user right should be tightly restricted. **Severity of the damage:** Low **Operational aspects:** None
Generate security audits	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE	**Vulnerability:** Accounts that can write to the Security log could be used by an attacker to fill that log with meaningless events. If the computer is configured to overwrite events as needed, attackers could

Policy	Value	Reason
		use this method to remove evidence of their unauthorized activities. If the computer is configured to shut down when it is unable to write to the Security log and it is not configured to automatically back up the log files, this method could be used to create a DoS condition. **Severity of the damage:** Low **Operational aspects:** None
Increase scheduling priority	BUILTIN\Administrators	**Vulnerability:** Increasing the working set size for a process decreases the amount of physical memory that is available to the rest of the system. **Severity of the damage:** Low **Operational aspects:** None
Load and unload device drivers	BUILTIN\Administrators	**Vulnerability:** Device drivers run as highly privileged code. A user who has

Policy	Value	Reason
		the Load and unload device drivers user right could unintentionally install malicious software that masquerades as a device driver. **Severity of the damage:** Low **Operational aspects:** None
Lock pages in memory	BUILTIN\Administrators	**Vulnerability:** Users with the Lock pages in memory user right could assign physical memory to several processes, which could leave little or no RAM for other processes and result in a DoS condition. **Severity of the damage:** Low **Operational aspects:** None
Log on as a service	*Domain\CPM_ ServiceUser NT SERVICE\ALL SERVICES	**Vulnerability:** Accounts that can log on as a service could be used to configure and start new unauthorized services, such as a keylogger or other malicious software.

Policy	Value	Reason
		Severity of the damage: Medium **Operational aspects:** None
Manage auditing and security log	BUILTIN\Administrators	**Vulnerability:** Anyone with the Manage auditing and security log user right can clear the Security log to erase important evidence of unauthorized activity. **Severity of the damage:** Medium **Operational aspects:** None
Modify an object label		**Vulnerability:** Anyone with the Modify an object label user right can change the integrity level of a file or process so that it becomes elevated or decreased to a point where it can be deleted by lower-level processes. Either of these states effectively circumvents the protection offered by Windows Integrity Controls and makes your system

Policy	Value	Reason
		vulnerable to attacks by malicious software. **Severity of the damage:** Low **Operational aspects:** None
Modify firmware environment values	BUILTIN\Administrators	**Vulnerability:** Anyone who is assigned the Modify firmware environment values user right could configure the settings of a hardware component to cause it to fail, which could lead to data corruption or a DoS condition. **Severity of the damage:** Medium **Operational aspects:** None
Perform volume maintenance tasks	BUILTIN\Administrators	**Vulnerability:** A user who is assigned the Perform volume maintenance tasks user right could delete a volume, which could result in the loss of data or a DoS condition. Also, disk maintenance tasks can be

Policy	Value	Reason
		used to modify data on the disk such as user rights assignments that might lead to escalation of privileges. **Severity of the damage:** Low **Operational aspects:** None
Profile single process	BUILTIN\Administrators	**Vulnerability:** The Profile single process user right presents a moderate vulnerability. Attackers with this user right could monitor a computer's performance to help identify critical processes that they might want to attack directly. Attackers may be able to determine what processes run on the computer so that they could identify countermeasures that they may need to avoid, such as antivirus software or an intrusion-detection system. They could also identify other users who are logged on to a

Policy	Value	Reason
		computer. **Severity of the damage:** Low **Operational aspects:** None
Replace a process level token	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE	**Vulnerability:** Users with the **Replace a process level token** user right can start processes as other users whose credentials they know. **Severity of the damage:** Low **Operational aspects:** IMPORTANT! If you need to manage COM+ Usages you must give the cpm user the permission to "Replace a process level token", which by default is only given to the NETWORK_ SERVICE and LOCAL_ SERVICE users in the hardening process. otherwise you will experience the following error: "Error creating change password

Policy	Value	Reason
		process using LogonAs activation method (error 1314)", this is also true for other methods that uses LogonAs if such exist (the only one out of the box is COM+).
Restore files and directories	BUILTIN\Administrators	**Vulnerability:** An attacker with the Restore files and directories user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data, data corruption, or a denial-of-service condition. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install programs that provide continued access to the computer.

Policy	Value	Reason
		Severity of the damage: Medium **Operational aspects:** None
Shut down the system	BUILTIN\Administrators	**Vulnerability:** The ability to shut down the server should be limited to a very small number of trusted administrators. **Severity of the damage:** Low **Operational aspects:** None
Take ownership of files or other objects	BUILTIN\Administrators	**Vulnerability:** Any users with the Take ownership of files or other objects user right can take control of any object, regardless of the permissions on that object, and then make any changes that they want to make that object. Such changes could result in exposure of data, corruption of data, or a DoS condition. **Severity of the damage:** High **Operational aspects:**

Policy	Value	Reason
		None