SYSKEYOT ASSET DASHBOARD

SyskeyOT
Asset Dashboard

USER GUIDE

WWW.SYSKEYSOFTLABS.COM

Syskey Softlabs

support@syskeysoftlabs.com | sales@syskeysoftlabs.com

Copyright

Trademarks

Contents

Introduction

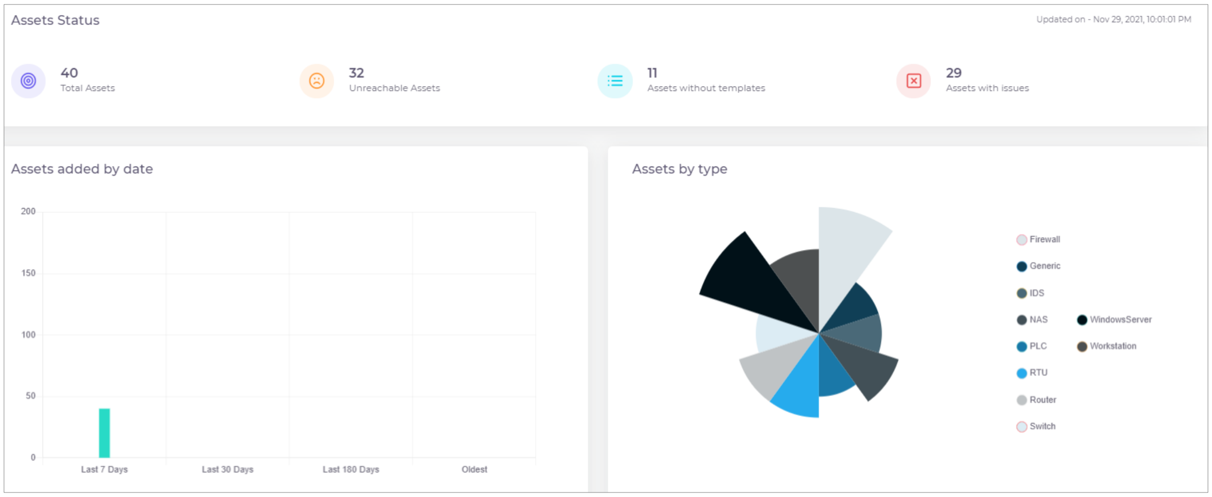
SysKeyOT Asset Dashboard automates asset management by discovering, tracking, and maintaining an inventory of assets in the network. Assets can be a PLC, RTU, IDS, server, router, firewall or any other network enabled device. Asset Manager collects asset data using various industrial standard protocols like IEC61850, SNMP, WMI/WinRM, and others.

The typical automated asset inventory workflow is:

1. Discover assets in the network through select probing.
2. Add discovered assets to inventory and apply templates and credentials to the discovered assets as required.
3. Run periodic automatic scans or manually scan the network to collect data from the assets.
4. Configure the baseline values for asset attributes such as the firmware version.
5. View the asset information and system alerts periodically to check for any issues and take corrective actions as required.

Assets Dashboard

The Assets Dashboard is your one-stop shop for asset data and includes information about assets status, number of unreachable assets, assets without templates and assets with issues. Graphical views of assets added by date and assets by type of network device are also available. The list of assts with issues including details of last scan is also displayed.



Assets Status

Updated on - Nov 29, 2021, 10:01:01 PM

40 Total Assets

32 Unreachable Assets

11 Assets without templates

29 Assets with issues

Discovery of Assets

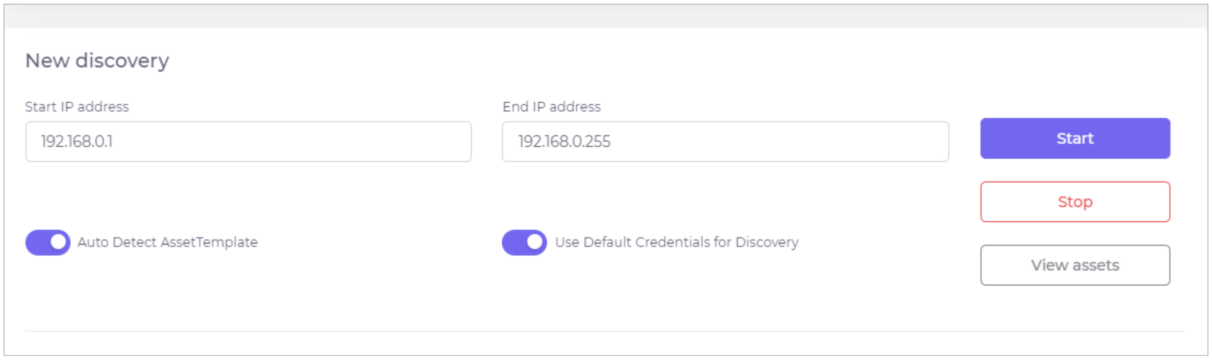
Assets can be added automatically by running a discovery probe over a network range or individual assets can be manually added.

How to Run Discovery

You can run a discovery operation to locate assets within a range of IP addresses. Asset Manager supports authenticated discovery, where discovered assets are authenticated using stored credentials.

Procedure:

1. Go to **Discovery**.



New discovery

Start IP address: 192.168.0.1

End IP address: 192.168.0.255

Auto Detect AssetTemplate

Use Default Credentials for Discovery

2. Enter the Start and End IP addresses of the range.
3. By default, assets are auto detected and auto assigned suitable templates. Disable the option **Auto Detect Asset Template** to manually assign templates.
4. The assets are authenticated using the default credentials available in the application, which helps to quickly identify new Windows devices. Disable the option **Use Default Credentials for Discovery** to manually authenticate the assets.
5. Click **Start** to begin the discovery.

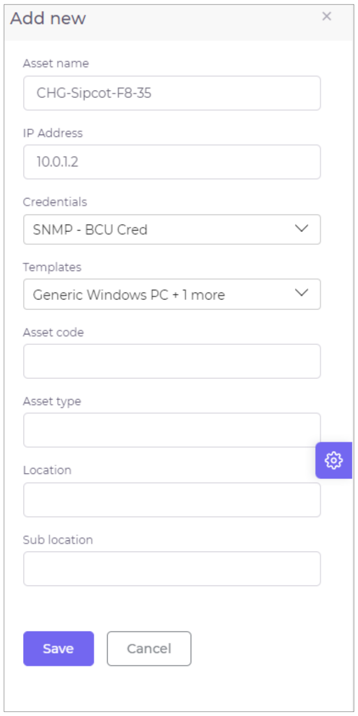
   The discovery progress and status are displayed along with details of the discovered assets. You can also view the list of skipped assets along with the reason for skipping.

How to Add Assets Manually

You can manually add an asset to scan. This is useful if you wish to add a non-network device to the application.

Procedure:

1. Go to **Assets** and click **Add new**.



Add new ×

Asset name: CHG-Sipcot-F8-35

IP Address: 10.0.1.2

Credentials: SNMP - BCU Cred

Templates: Generic Windows PC + 1 more

Asset code:

Asset type:

Location:

Sub location:

2. Enter the name of the asset.
3. Optionally, you can also specify the IP address, asset code, asset type, location and sub location of the asset.
4. Select the credentials to authenticate the asset and a scan template.

The device is added to the inventory with the specified attributes. After the asset is added to the inventory, you can perform operations such as scan, export and so on from the Assets page.

Templates

An asset template is set of preconfigured attributes that can be used during the scan to collect asset information for a particular type of device. By default, the following templates are available.

- Default – Default template that is automatically applied to any discovered device. This template defines common attributes such as name, station, type, model and so on.
- Generic IEC Device – Template for IEC devices based on IEC61850 protocol Name Plate and Physical Name definition.
- Generic Windows PC – Template for Windows servers and PCs based on Windows instrumentation definition.

An administrator can edit the preconfigured templates and can define additional custom templates. Templates can be customized to suit different customer needs. Templates can be reused across different installations by exporting and importing templates. Templates can also be assigned to an asset to collect data based on different configuration settings.

Template Fields

You can add custom fields to the templates. By default, the following three types of fields are available:

- TopLevel – A root level field on the Asset page such as Status.
- Baseline – A baseline parameter for the top-level field that is used for comparison such as version check.
- Sub Module – A sub-module is any data in tabular format. For example, all installed programs of Windows computer, installed patches, all sub MIBs under a primary MIB.

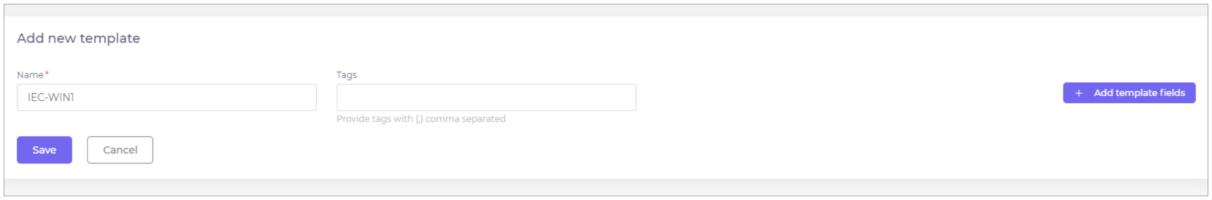
How to Create Custom Templates

You can create new custom templates for different types of assets. You can either create a new template or duplicate an existing template and make the required changes.

You must be an administrator to create or modify templates.

Procedure:

1. Click **Template**.
2. To create a new template, click + Add new template.
3. To make a copy of an existing template, click **Duplicate** against the existing template. Click **Edit** against the copy to make the required changes.



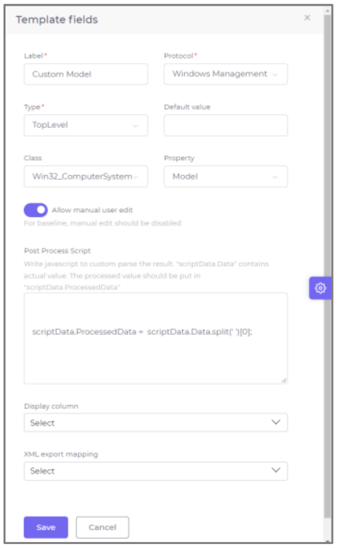
Add new template

Name*: IEC-WIN1

Tags:

Provide tags with (,) comma separated

4. Specify a **Name** for the template.
5. Specify a comma separated list of **Tags**.
6. Click + Add template fields to add new fields.



Template fields

Label*: Custom Model

Protocol*: Windows Management

Type*: TopLevel

Default value:

Class: Win32_ComputerSystem

Property: Model

Allow manual user edit

For baseline, manual edit should be disabled

Post Process Script

Write javascript to custom parse the result. "scriptData.Data" contains actual value. The processed value should be put in "scriptData.ProcessedData"

```
scriptData.ProcessedData = scriptData.Data.split(' ')[0];
```

Display column: Select

XML export mapping: Select

7. Specify a **Label** for the field.

8. Select a suitable **Protocol** for the attribute. The options are:
   - Manual
   - Windows Management
   - IEC61850
   - SNMP
9. Select the **Type** and **Default Value** for the field.
10. Based on the selected protocol, specify the following:
    - If the protocol is Manual, specify the **Command/Address** for the field.
    - If protocol is Windows Management, select a **Class** for the field.
    - If the protocol is IEC61850, specify the **Command/Address** for the field in the format LDN/LN/FC/DO/DA.
    - If the protocol is SNMP, specify the **Command/Address** for the field in the format 1.3.6.1.5.3.21.1.32.12.
11. Optionally, specify a default value, command, display column in the Assets page, and the XML export mapping for the field.
12. You can also specify a script in Post Process Script to perform custom processing of the result data.
    - The script should be a valid java script as per ECMA 2016
    - The scanned data is available in **scriptData.Data** variable.
    - The processed / parsed result should be put into **scriptData.ProcessedData** so that the system will pickup and store the information.
    - Multiline javascripts also supported. Please refer JavaScript | MDN (mozilla.org) on writing javascript .
13. You can allow manual user edits to the field. However, manual edit must be disabled for Baseline type of field.

Importing/Exporting Templates

You can import templates that are in JSON format.

Templates can be exported to JSON file format. Click Export against the individual template or click Export all at the top to export all the available templates.

Authentication Credentials

As an administrator, you can store credentials to access specific devices. The scan operation uses the credentials that are assigned to assets. Same credentials can be assigned to multiple devices. Credentials are protocol specific. Multiple credentials of different protocol can be assigned to a single device.

⚠ Do not assign multiple credentials of same protocol to a single device.

How to Store Credentials

Different protocols require different authentication and connection information.

Procedure:

1. Click **Credential** > **Add new credential**.
2. Select **Protocol** from the list. The options are:
   - Windows Management
   - IEC61850
   - SNMP
3. Enter a suitable **Description**.
4. Enable **Default** if this information should be used as the default authentication for all assets using this protocol in the network.

To provide credentials for **Windows Management** protocol:

1. Select the **Transport Type**. The options are: **Windows remote management** or **Direct WMI**.
2. **Direct WMI**
   a. If you select Direct WMI as the transport type, specify the **Username** and **Password** for the device.
   b. If you select Windows remote management, in addition to the **Username** and **Password**, specify the **Port** number, **Authentication type**, and **Domain**. Indicate if the port is a secured port.
   c. Click **Save**.
3. **Windows remote management**
   a. Provide Port, Secured, Authentication Type, Domain, Username and Password for the asset.
   b. WinRM authentication types has some special considerations
      i. Kerberos – Highly Secured. Password never sent. Uses ticket granting service. Only supports on domain users and domain joined computers.
      ii. NTLM – Secured. Password never sent instead hashes used. Supports both local and domain users.
      iii. Basic – Un Secured should be used over encrypted connection. Password sent in plain text, only local users supported.
   c. NTLM / Kerberos are the preferred authentication types.
   d. Windows computers does not have Basic Auth enabled by default. To enable, Refer Configure WinRM – Basic Auth

To provide credentials for **IEC 61850** protocol:

1. Specify the **Port** number used for IEC 61850.
2. Click **Save**.

To provide credentials for SNMP protocol:

1. Specify the default SNMP **Port** number.
2. Select the SNMP **Version**.
3. If the SNMP version is **V1** or **V2c**, specify the SNMP **Community**.
4. If the SNMP version is **V3**, select the Security type from the options:

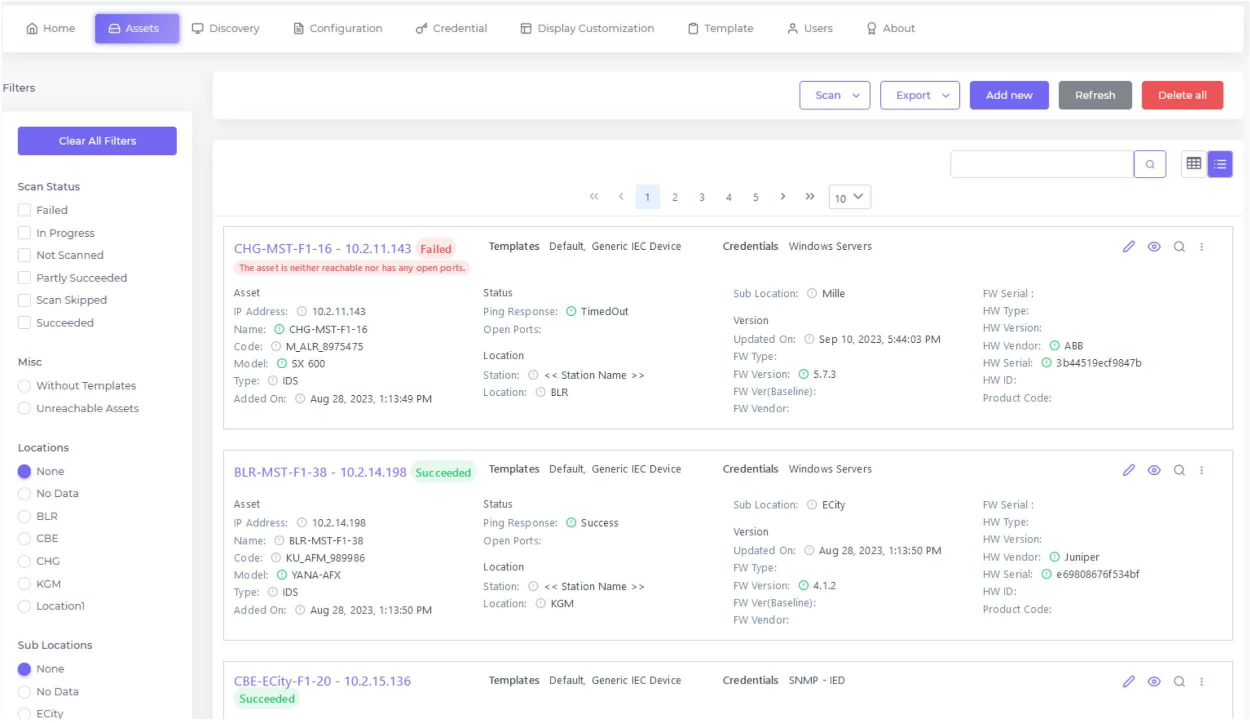
- Authentication privacy – Communication with authentication and privacy. The protocols for authentication are MD5, SHA and HMAC. The protocols for privacy are DES and AES. Provide the privacy password and authentication credentials.
- Authentication no privacy – Communication with authentication and no privacy. The protocols for authentication are MD5, SHA and HMAC. Provide the authentication credentials.
- No authentication no privacy. Communication with no authentication and no privacy.

5. Click **Save**.

Assets

The data collected for each device are displayed in the Assets page. The asset fields are displayed as per the defined groups and columns. The information can be displayed in either table view or list view.

Assets can be filtered based on the Scan Status, Location, Sub Location, Unreachable state, Type and Model through left side filters.



Scan Status
□ Failed
□ In Progress
□ Not Scanned
□ Partly Succeeded
□ Scan Skipped
□ Succeeded

Misc
○ Without Templates
○ Unreachable Assets

Locations
● None
○ No Data
○ BLR
○ CBE
○ CHG
○ KGM
○ Location1

Sub Locations
● None
○ No Data
○ ECity

CHG-MST-F1-16 - 10.2.11.143 Failed
The asset is neither reachable nor has any open ports.
Templates Default, Generic IEC Device
Credentials Windows Servers

Asset
IP Address: 10.2.11.143
Name: CHG-MST-F1-16
Code: M_ALR_8975475
Model: SX 600
Type: IDS
Added On: Aug 28, 2023, 1:13:49 PM

Status
Ping Response: TimedOut
Open Ports:

Location
Station: << Station Name >>
Location: BLR

Sub Location: Mille

Version
Updated On: Sep 10, 2023, 5:44:03 PM
FW Type:
FW Version: 5.7.3
FW Ver(Baseline):
FW Vendor:

FW Serial :
HW Type:
HW Version:
HW Vendor: ABB
HW Serial: 3b44519ecf9847b
HW ID:
Product Code:

BLR-MST-F1-38 - 10.2.14.198 Succeeded
Templates Default, Generic IEC Device
Credentials Windows Servers

Asset
IP Address: 10.2.14.198
Name: BLR-MST-F1-38
Code: KU_AFM_989986
Model: YANA-AFX
Type: IDS
Added On: Aug 28, 2023, 1:13:50 PM

Status
Ping Response: Success
Open Ports:

Location
Station: << Station Name >>
Location: KGM

Sub Location: ECity

Version
Updated On: Aug 28, 2023, 1:13:50 PM
FW Type:
FW Version: 4.1.2
FW Ver(Baseline):
FW Vendor:

FW Serial :
HW Type:
HW Version:
HW Vendor: Juniper
HW Serial: e69808676f534bf
HW ID:
Product Code:

CBE-ECity-F1-20 - 10.2.15.136 Succeeded
Templates Default, Generic IEC Device
Credentials SNMP - IED

You can download the assets data in either XML or CSV format.

Click 👁 against an asset to view its details such as the asset address, scan status, last scan date and time and last scan message. You can also view the asset attributes, assigned template and credentials. You can also view the history of the asset scan which shows the timeline of the changes detected in the asset in the previous scans.

Click ✎ against the asset to modify the asset attributes and change the assigned templates and credentials. Click ✎ against the attribute you wish to modify.

How to Run Manual Scan

Scan operation can be run manually to collect attributes of all assets or some specific assets.

For information about configuring automatic periodic scan, see How to Configure Periodic Scanning.

Procedure:

1. Go to Assets page.
2. Click **Scan -> All Assets** or **Scan -> All Filtered Assets**
    a. All Filtered Assets -> Scan and update attributes of assets which are currently filtered
    b. All Assets -> Scan and update attributes of all assets in the system.
3. Click ⚙ at the right side of the screen to view details of currently running and completed scans along with the asset details.

System Configuration

As an administrator, you must configure and set up Asset Manager before you can manage assets. The following administrative configurations are required.

How to Create Active Directory Connection

You must set up the connection for Active Directory.

Procedure:

1. Click **Configuration > Active Directory**.
2. Enable Active Directory.
3. Specify the LDAP Server IP or select the server from the list of discovered servers.
4. Modify the LDAP port number, if required. The default LDAP port is 389.
5. Specify if the LDAP connection is secured.
6. Enter the values for the Default Naming Context, Admin Group Name, and User Group Name and verify if the connection is successful.

How to Send Audit Logs to Syslog Server

You can send audit logs to a syslog or audit server for monitoring.

Procedure:

1. Click **Configuration > Audit Log**.
2. Enable audit logging to a syslog server.
3. Enter the syslog server details and protocol details.
4. Enter the audit message format and source host.
5. Click **Save**.

How to Configure System Settings

You can configure certain system settings such as number of attempts before an account is locked, custom banner message, and more.

Procedure:

1. Click **Configuration > General**.
2. Specify how long users are allowed to be inactive in minutes in **Idle timeout session**.
3. Enter a custom text message that will appear in the Login page in **Custom banner Message**.
4. Enter the number of invalid sign-in attempts before a user gets locked out of their account in the **No. of attempts before lockout**.
5. Enter the amount of time in minutes an account will remain locked out after the maximum number of invalid sign-in attempts in **Account lockout time**.
6. Set the password expiration period in **Automatic password expiry**. The default period is 30 days. Users are forced to reset their password after this period.
7. Set the logging levels in **System Log Level**.

How to Configure Default Values for Protocols

The default settings for various protocols such as timeout, ports, and so on can be globally configured. However, some of the default settings can be overridden for a device using the assigned credentials.

Procedure:

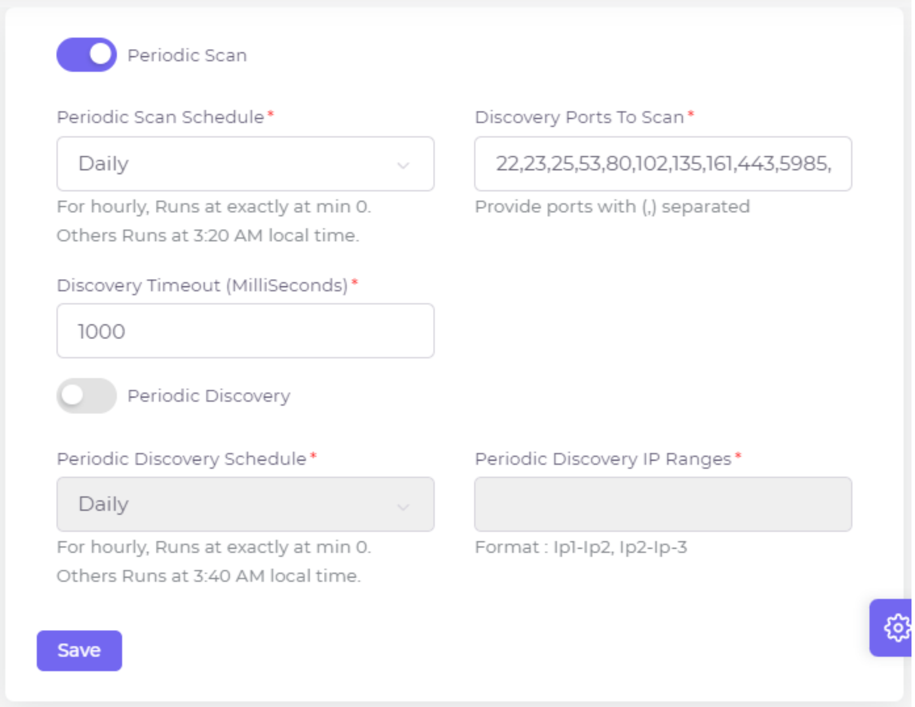
1. Click **Configuration > Protocol**.
2. Enter the network port for the IEC 61850 service. The default port is 102. Specify the number of read attempts to try against the device before failing. The default value is 3. Specify the response timeout in seconds. The default value is 9 seconds.
3. Enter the port for WinRM protocol. The default port is 5985. Specify the operation timeout in seconds. The default value is 100 seconds.
4. Enter the community string and user name for SNMP protocol. The default community name is public. Specify the connection time out. The default value is 10 seconds. Specify the number of read attempts to try against the asset before failing. The default value is 3. Specify the SNMP OID for discovery map tagging. The default value is the system description OID 1.3.6.1.2.1.1.1.0. Specify the SNMP port number. The default value is 161.

How to Configure Periodic Scanning & Discovery

Scanning operation can be configured to run periodically to collect the inventoried assets attributes.

Procedure:

1. Click **Configuration > Scan**.



Periodic Scan

Periodic Scan Schedule*
Daily
For hourly, Runs at exactly at min 0.
Others Runs at 3:20 AM local time.

Discovery Ports To Scan*
22,23,25,53,80,102,135,161,443,5985,
Provide ports with (,) separated

Discovery Timeout (MilliSeconds)*
1000

Periodic Discovery

Periodic Discovery Schedule*
Daily
For hourly, Runs at exactly at min 0.
Others Runs at 3:40 AM local time.

Periodic Discovery IP Ranges*
Format : Ip1-Ip2, Ip2-Ip-3

2.
3. Enable **Periodic Scan**.
4. Specify the **Periodic Scan Schedule**. The options are: Monthly, Weekly, Daily and Hourly. The default value is daily.
5. Enter the ports to scan during discovery. You can enter multiple ports separated by comma.
6. Specify the **Discovery Timeout** in milliseconds.
7. Enable **Periodic Discovery** and provide IP ranges.
8. Click **Save**.

How to Configure Periodic Export

You can set up periodic export of scanned data.

Procedure:

1. Click **Configuration > Storage**.
2. Enable **Periodic Export**.
3. Specify the **Periodic Export Schedule**. The options are: Monthly, Weekly, Daily, and Hourly. The default value is Daily.
4. Specify the folder to save the asset data. Enter the number of days to store the scan history in the database. The default value is 800 days.
5. Select the export file format. The options are XML or CSV. Indicate whether asset history must be included in the export files.

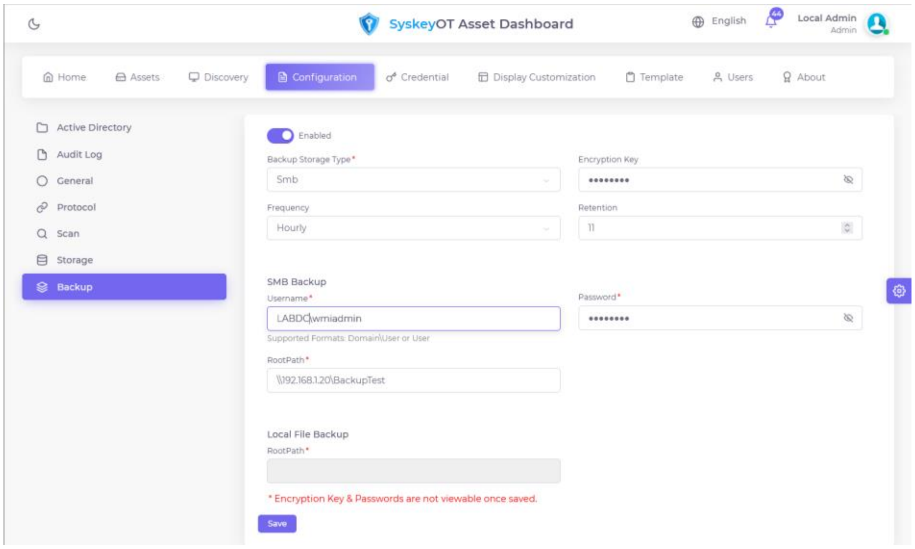
6. Click **Save**.

How to Configure Database Backups

The asset dashboard supports periodic backup of its entire database to local folder or network share for compliance purposes. By default, this option is disabled.

Procedure:

1. Go to **Configuration > Backup**.



Enabled

Backup Storage Type* Smb

Encryption Key ••••••••

Frequency Hourly

Retention 11

SMB Backup

Username* LABDC\wmiadmin

Supported Formats: Domain\User or User

Password* ••••••••

RootPath* \\192.168.1.20\BackupTest

Local File Backup

RootPath*

* Encryption Key & Passwords are not viewable once saved.

2. Enable the backup option.
3. Provide Encryption Key, Frequency and Retention
4. For Network Backups
    a. Choose **Smb** as Backup Storage
    b. Provide Username. E.g. domain\username or username@domain.local
    c. Provide Password
    d. Provide Shared folder path in RootPath.
5. For Local Folder Backups
    a. Provide local folder path to store backups.
6. Click **Save.**

How to Restore Database Backups

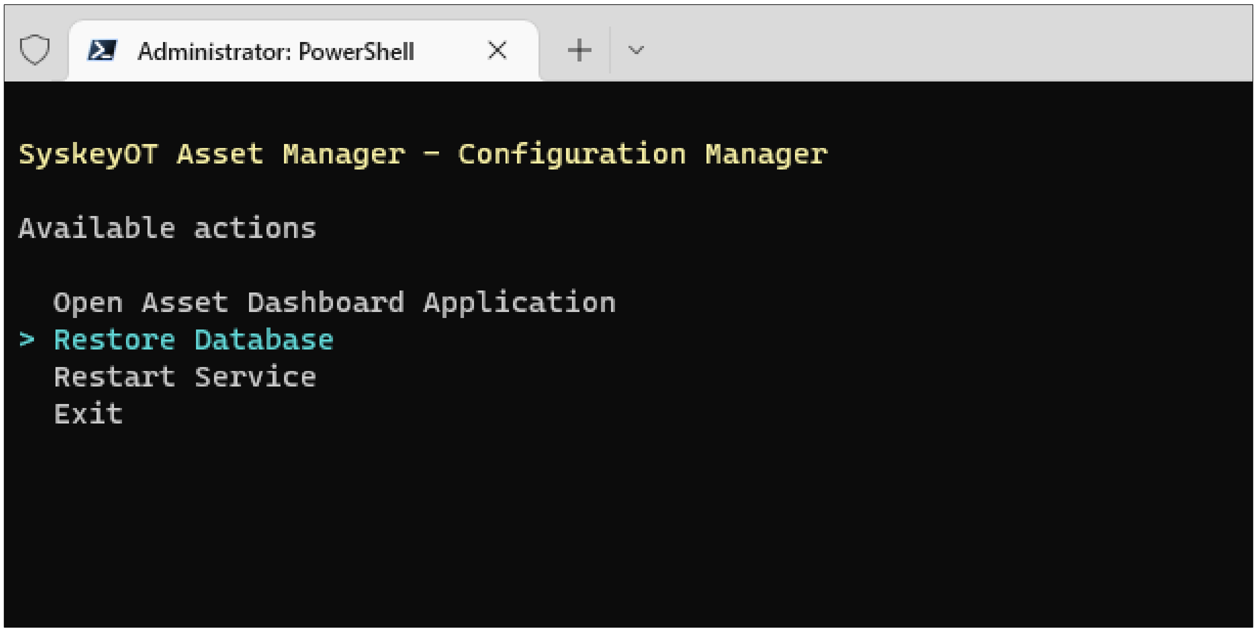
The asset dashboard web interface does not support restoring the database from backup. That should be performed from command line user interface.

Note:

- The restore operation will stop the application service until restore is completed.
- Upon success, The system transitions to the older state as per the backup restored.

Procedure:

1. Run the **SyskeyOT Asset Manager - Configurator** application. The following options will be displayed.



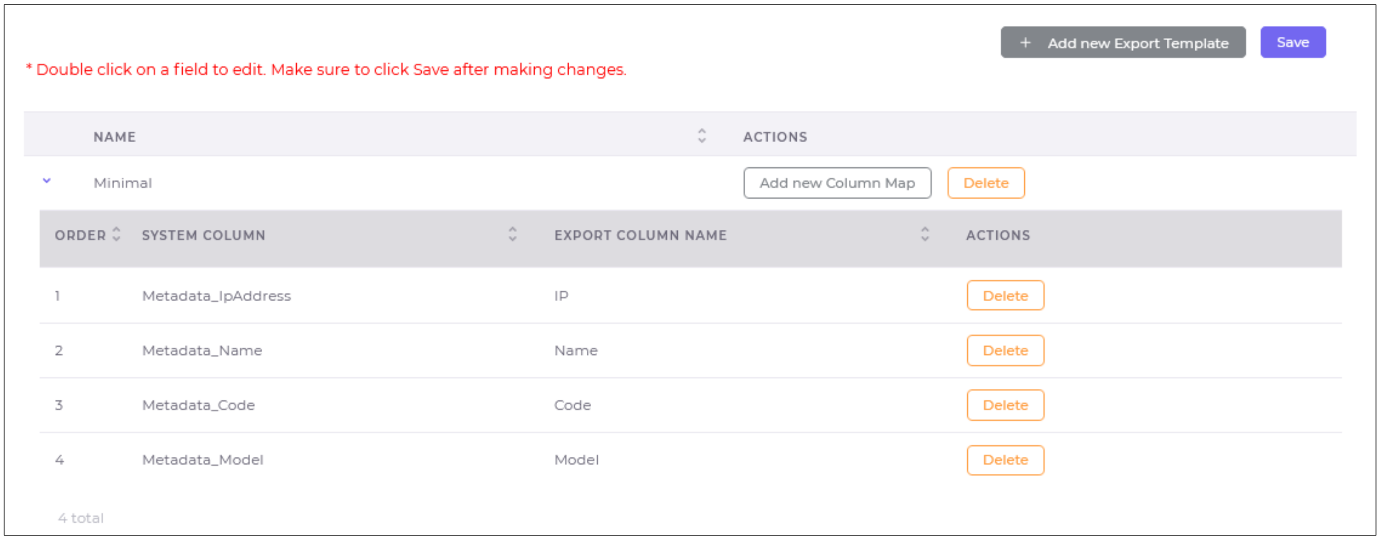
```
SyskeyOT Asset Manager - Configuration Manager

Available actions

  Open Asset Dashboard Application
> Restore Database
  Restart Service
  Exit
```

2. Choose **Restore Database**
3. Provide the full path of the backup. If the backup is on the network drive, Download it to a local folder and provide the full path of the backup in the command line.
    a. E.g. *C:\Shared\asset-dashboard_20230827_193720\asset-dashboard_20230827_193720*
    b. Make sure to wrap the path with double quotes if there is a space in path.
4. Provide the backup encryption key to decrypt and restore the backup.
5. Follow the on-screen instructions to restore the backup.
6. Once completed the services will be automatically started and system will transition to the state of the restored database.

How to Export custom asset attributes as CSV

The system supports a concept of export templates where the fields to export can be defined and used for export.

1. Goto Configuration -> Export Templates
2. Click + Add new Export Template. That will add a export template named “NEW TEMPLATE” at the bottom of the page.
3. Double click the name to changed it.
4. Click Add new Column Map button next to the template name. That will add a new column map under the template.
5. Expand the template and double click the column map attributes to provide custom values.
6. Click Save .
7. A sample export template is shown below.



+ Add new Export Template | Save

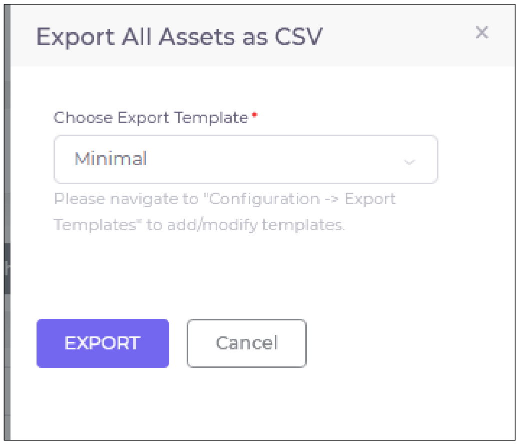
* Double click on a field to edit. Make sure to click Save after making changes.

NAME	ACTIONS
Minimal	Add new Column Map / Delete

ORDER	SYSTEM COLUMN	EXPORT COLUMN NAME	ACTIONS
1	Metadata_IpAddress	IP	Delete
2	Metadata_Name	Name	Delete
3	Metadata_Code	Code	Delete
4	Metadata_Model	Model	Delete

4 total

8. Go to the assets page and select “Export” -> “All Assets as CSV”



Export All Assets as CSV

Choose Export Template *

Minimal

Please navigate to "Configuration -> Export Templates" to add/modify templates.

EXPORT | Cancel

9.
10. Choose the template created previously. And click the export.

User Management

As an administrator, you can view the list of administrators and users in the Users page. An administrator can create new users, reset passwords, and modify user details. A new user can either be assigned the administrator role or the user role.

Click + New User to add a new user. Enter the user details such as first and last name of the user, username, password, role assigned to the user, email, and status of the user profile.

License Management

By default, Asset Manager is installed in fully functional trial mode for a limited number of days. It is important to activate the application within the trial period. After the trial period has passed, you will be unable to use the application unless you activate it.

How to Add the Activation Key

Procedure:

1. Click **About**.
2. Add the license in the **Activation Key** field.
3. Click **Apply** to unlock the full mode of Asset Manager.

Display Customization

The Assets page can be customized with custom attributes of order, group, and colors.

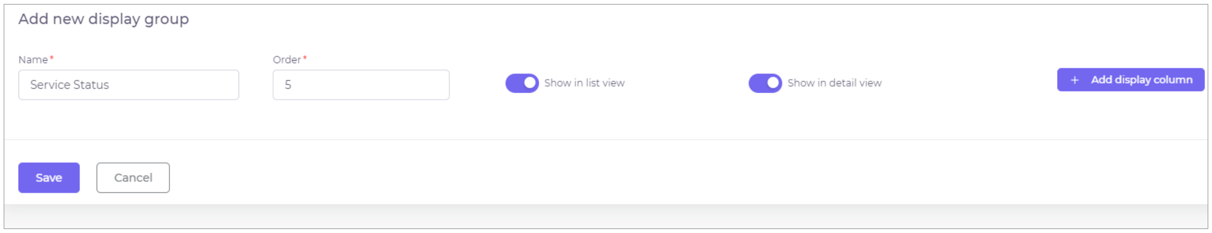
The display groups and their child columns can be defined and the columns are mapped to the device attribute through template fields.

How to Add New Display Group

You can add new groups to be displayed in the Assets page.

To add a new display column

1. Click **Display Customization > Add new display group**.



Add new display group

Name* Service Status

Order* 5

Show in list view

Show in detail view

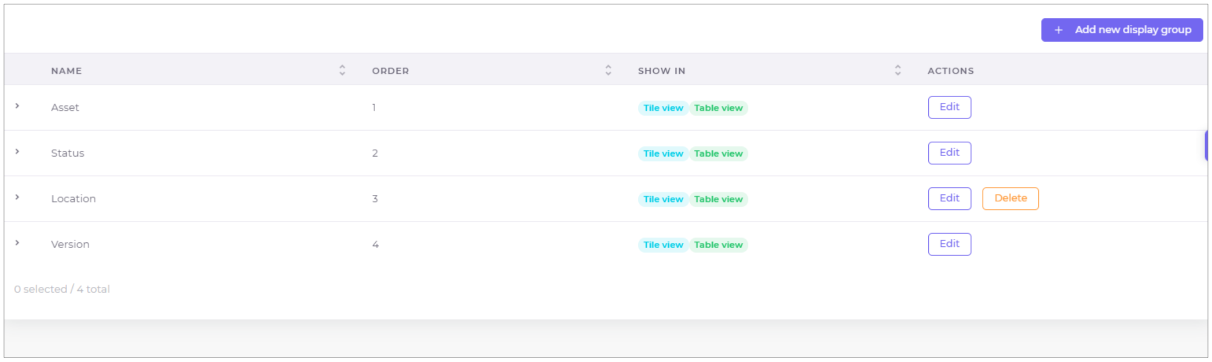
2. Specify a suitable **Name** for the group.
3. Specify the **Order** in which the group will be displayed on the Asset page.
4. Enable **list view** and **detail view** as required.
5. Click **Save**.

How to Add New Display Column

You can add new columns to existing groups.

To add new column:

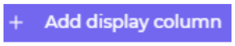
1. Click Display Customization.



NAME	ORDER	SHOW IN	ACTIONS
Asset	1	Tile view Table view	Edit
Status	2	Tile view Table view	Edit
Location	3	Tile view Table view	Edit Delete
Version	4	Tile view Table view	Edit

0 selected / 4 total

2. Click **Edit** against the group to which you want to add new columns.

3. Click  + Add display column to add a display column.
4. In the New display column page, specify a **Name** for the column.
5. Enter a suitable **Description**.
6. Select a color for the text from the color palette.
7. Specify the order in which the column will appear in the group.
8. Enable **list view** and **details view** for the column as required.
9. Click **Add column**.

Configure Windows Devices for Asset Scanning

Windows devices require some special configuration to expose its information through WMI and WinRM. The following sections describe the procedures to configure WMI and WinRM.

How to Configure WMI

WMI has the following requirements to access it's data remotely

- WMI Traffic to be allowed in firewall
- The user should have necessary rights to access WMI Hives
- The user should have Remote DCOM activation rights
- To remotely gather the installed patches,
    - The user should be the "local administrator (**administrator**)". Requirement from Microsoft Windows
    - A user member of local admin group does not work if UAC turned on. This is not applicable to domain users who are part of local admin group.

Recommended User Setup

- To Get WMI data & Installed Programs List
    - For domain joined computers,
        - Create a domain user.
        - Make the user part of the **Distributed COM Users or Administrators** group of the domain joined PCs
        - Give explicit access to the WMI registry Hives. Refer To give access to WMI Hives for a user
    - For non domain joined computers,
        - Create a local user
        - Make the user part of the **Distributed COM Users or Administrators** group
        - Give explicit access to the WMI registry Hives. Refer To give access to WMI Hives for a user
- For WMI, Installed Programs & Windows Patches to get work
    - For domain joined computers,
        - Create a domain user.
        - Make the user part of the local Administrators groups of all of the domain joined PCs
    - For non domain joined computers,
        - Use the **default** local administrator account.

Allow WMI Traffic in Firewall

- Open **Control Panel**, click **Security** and then click **Windows Firewall**.
- Click **Change Settings** and then click the **Exceptions** tab.
- In the Exceptions window, select the check box for **Windows Management Instrumentation (WMI)** to enable WMI traffic through the firewall. To disable WMI traffic, clear the check box.
- **Or** Run the following command in Administrative Command Prompt
  - *netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes*

To give access to WMI Hives for a user

1. Create a new local user / Identify an existing local user
2. Open Computer Management and Under **Services and Applications**, open the properties dialog of WMI Control (or run *wmimgmt.msc*).
   a. In the **Security** tab, select **Root/CIMV2.**
   b. Click **Security**
   c. Add the user**.**
   d. Select ***Enable Account*** and ***Remote Enable*** only and recurse the permissions to the sub-namespaces using the Advanced window in Security.
3. Open Computer Management and Under **Services and Applications**, open the properties dialog of WMI Control (or run *wmimgmt.msc*).
   a. In the **Security** tab, select **Root/Default.**
   b. Click **Security**
   c. Add the user**.**
   d. Select ***Enable Account*** and ***Remote Enable*** only and recurse the permissions to the sub-namespaces using the Advanced window in Security.

Explicit DCOM Permissions for WMI

If there is a requirement to provide explicit permissions for WMI user instead of adding him to Administrator / Distributed COM Users

4. Run *dcomcnfg*. Click **Component Services** > **Computers** > **My Computer**. In the COM Security tab of the Properties dialog click **Edit Limits** for both Access Permissions and Launch and Activation Permissions. Add the user and allow Remote Access, Remote Launch, and Remote Activation.
5. Select **Windows Management Instrumentation** under **Component Services** > **Computers** > **My Computer** > **DCOM Config** and give Remote Launch and Remote Activation privileges to the user Group.

References

- https://docs.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-on-a-remote-computer
- https://docs.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-remotely-starting-with-vista
- https://docs.microsoft.com/en-us/windows/win32/wmisdk/troubleshooting-a-remote-wmi-connection
- https://learn.microsoft.com/en-us/windows/win32/wmisdk/user-account-control-and-wmi

How to Configure WinRM

WinRM is modern protocol in Windows for remote management and data querying, which has better integration with domain group policy.

WinRM requires WMF (Windows Management Framework) 5.1. Which is bundled in Windows 10 +, and Windows Server 2016+ .

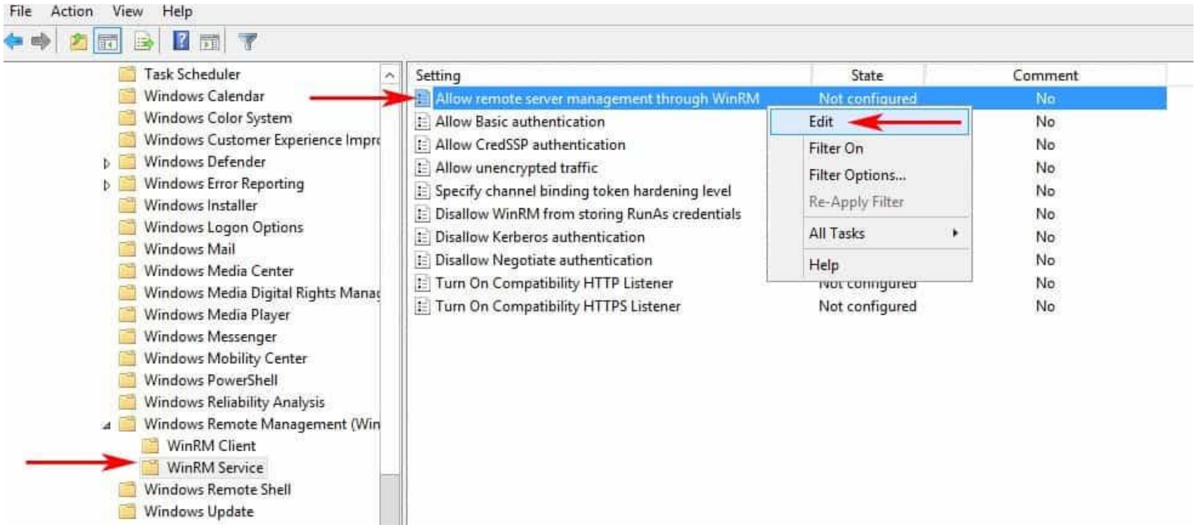
For older operating system please download and install WMF 5.1 from the following location.

https://www.microsoft.com/en-us/download/details.aspx?id=54616

Setup Through Group Policy

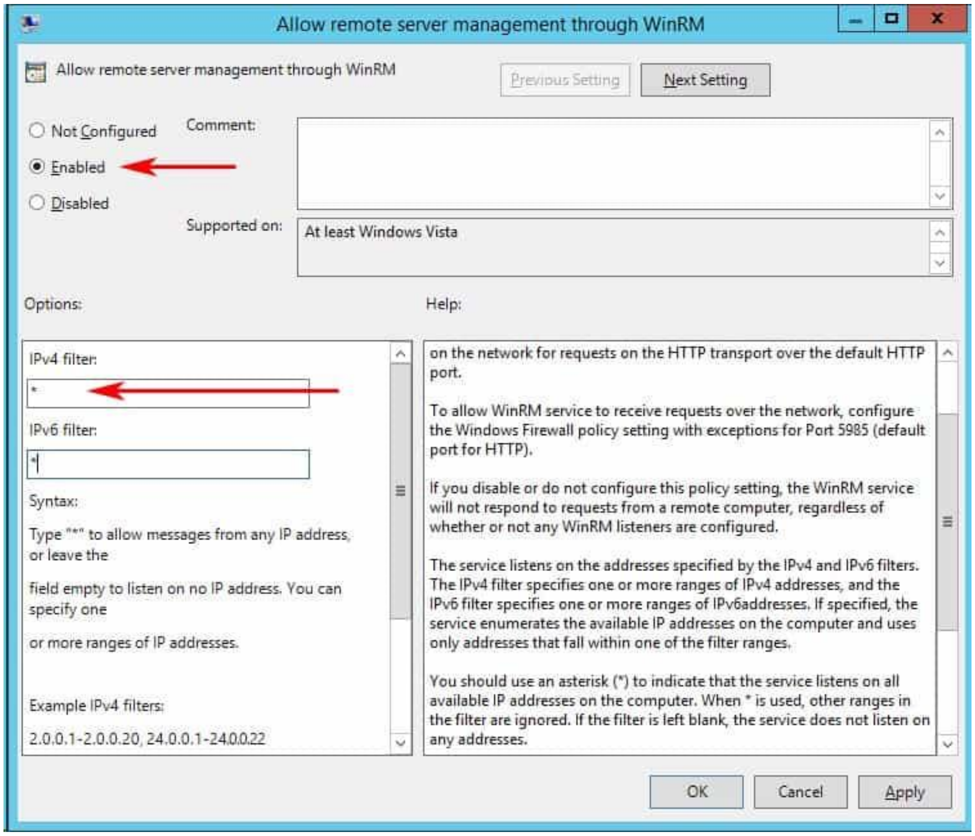
Procedure

1. Open **Group Policy Management** in the Administrative Tools folder.
2. Right-click on the desired OU that you want to create a Group Policy Object for and click **Create a GPO in this Domain, and Link it here**…"
3. Rename the GPO with a suitable name, for example, "Enable WinRM via GPO" and click **OK**.
4. After the new GPO has been created, right-click on the newly created GPO and click **Edit**.
5. Expand the Menu tree as follows: **Computer Configuration > Policies > Administrative Templates: Policy definitions > Windows Components > Windows Remote Management (WinRM) > WinRM Service**.
6. Find the setting that says "Allow remote server management through WinRM" and right-click and click **Edit** to configure the settings as shown in the following image.



Setting	State	Comment
Allow remote server management through WinRM	Not configured	No
Allow Basic authentication		No
Allow CredSSP authentication		No
Allow unencrypted traffic		No
Specify channel binding token hardening level		No
Disallow WinRM from storing RunAs credentials		No
Disallow Kerberos authentication		No
Disallow Negotiate authentication		No
Turn On Compatibility HTTP Listener	Not configured	No
Turn On Compatibility HTTPS Listener	Not configured	No

7. In the Allow remote server management through WinRM window, select **Enabled** and in the Options section, either specify an IP Address range or enter an Asterisk "*" to allow all IP addresses to remotely manage the PC. (We recommend specifying an IP Address to reduce any risk of a security compromise of your systems/network).



Allow remote server management through WinRM

Allow remote server management through WinRM

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

IPv4 filter: *

IPv6 filter: *

Syntax:

Type "*" to allow messages from any IP address, or leave the

field empty to listen on no IP address. You can specify one

or more ranges of IP addresses.

Example IPv4 filters:

2.0.0.1-2.0.0.20, 24.0.0.1-24.0.0.22

Help:

on the network for requests on the HTTP transport over the default HTTP port.

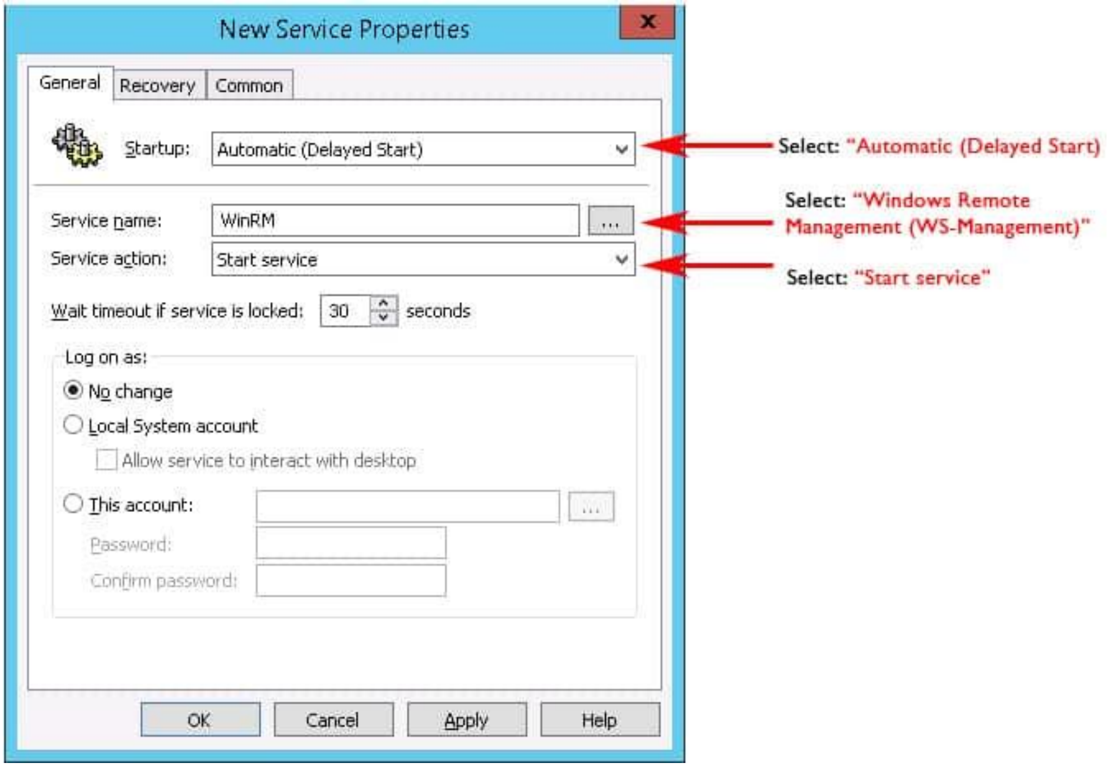
To allow WinRM service to receive requests over the network, configure the Windows Firewall policy setting with exceptions for Port 5985 (default port for HTTP).

If you disable or do not configure this policy setting, the WinRM service will not respond to requests from a remote computer, regardless of whether or not any WinRM listeners are configured.

The service listens on the addresses specified by the IPv4 and IPv6 filters. The IPv4 filter specifies one or more ranges of IPv4 addresses, and the IPv6 filter specifies one or more ranges of IPv6addresses. If specified, the service enumerates the available IP addresses on the computer and uses only addresses that fall within one of the filter ranges.

You should use an asterisk (*) to indicate that the service listens on all available IP addresses on the computer. When * is used, other ranges in the filter are ignored. If the filter is left blank, the service does not listen on any addresses.

8. To Enable Basic Authentication. (This is typically not required when authentication is performed over NTLM / Kerberos)
   a. Set Allow Basic authentication -> Enabled
9. To Allow Un Encrypted Communication [Required if https certificates not available]
   a. Allow Unencrypted traffic -> Enabled
10. To enable the Windows Remote Management (WS-sManagement) Service to start automatically, go to **Computer Configuration > Preferences > Control Panel Settings > Services** and right-click and select **New** and **Service**.
11. In the New Service Properties window, change Startup to **Automatic (Delayed Start)** and then in the Service Name dialog box, click the box with the 3 dots in it to the right of the Service name box and select **Windows Remote Management (WS-Management)** and click **Select**.
12. After you've selected the Service, under the **Service action** menu, click **Start service.**



New Service Properties

Startup: Automatic (Delayed Start)

Service name: WinRM

Service action: Start service

Wait timeout if service is locked: 30 seconds

Log on as:

● No change

○ Local System account

□ Allow service to interact with desktop

○ This account:

Password:

Confirm password:

Select: "Automatic (Delayed Start)

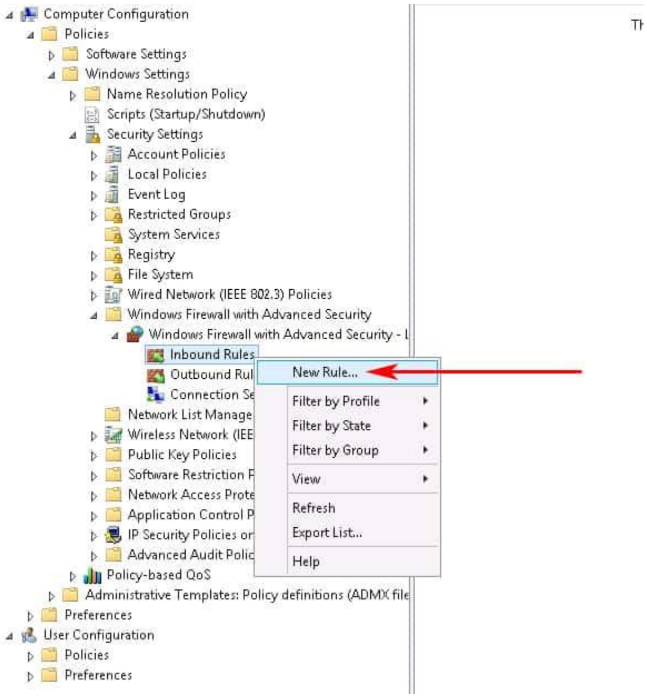
Select: "Windows Remote Management (WS-Management)"

Select: "Start service"

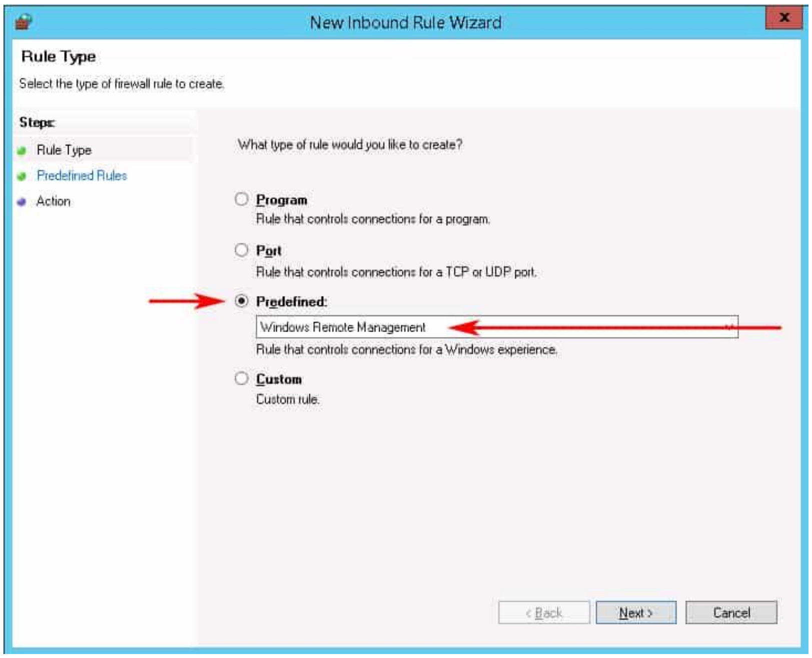
13. The group policy does not have a direct support to enable winrm over https. Do the following to enable WinRM over https
    a. Setup AD CA (Active Directory Certificate Services) in the domain environment.
    b. Setup auto enrollable certificate template with Server Authentication.
        i. Open the **Certificate Authority** management console, Right-Clicking on **Certificate Templates** and selecting **Manage**
        ii. It will open a template management console. Scroll down and select **WebServer** template and Right-Click on it selecting **Duplicate Template**
        iii. In the certificate property window for the new template navigate to the **General** Tab and set a **Display Name** to WinRM Machine Cert and **Template Name** to WinRM Machine Cert**.**
        iv. In the **Subject Name** tab select in **Subject name format** select **Common Name** and click on the checkbox of **DNS name**.
        v. In the Security tab, Add the group **Domain Computers** and provide **Read, Enrolll** and **Autoenroll** permission**.**
        vi. To auto enroll the computer on the domain or OUs Create a GPO and link it.
        vii. In the Group Policy Object Select **Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Public Key Policies** and select and enter in to the properties of **Certificate Services Client - Auto-Enrollment**
        viii. In the Policy Configuration, choose **Configuration Model** to **Enable** and select the options to auto renew and to update the certificate if changes as it fits your policies.
        ix. Link the gpo and wait for it to sync.
    c. Enable WinRM over HTTPS

   i. Microsoft does not provide a direct way to enable WinRM HTTPS using GPO. As a workaround, Place put the following command in a logon script on a new GPO and link it.
   ii. winrm quickconfig -transport:https

14. To configure the Windows Firewall to allow the proper ports inbound, go to Computer Configuration > expand Policies > expand Windows Settings > expand Security Settings > expand Windows Firewall with Advanced Security > expand Windows Firewall with Advanced Security > expand Inbound Rules. Right-click the Inbound Rules node and choose New Rule as shows in the following image.



15. In the New Inbound Rule wizard, select **Predefined** and scroll down to “Windows Remote Management” and click on it as shown in the following image.



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Predefined Rules
- Action

What type of rule would you like to create?

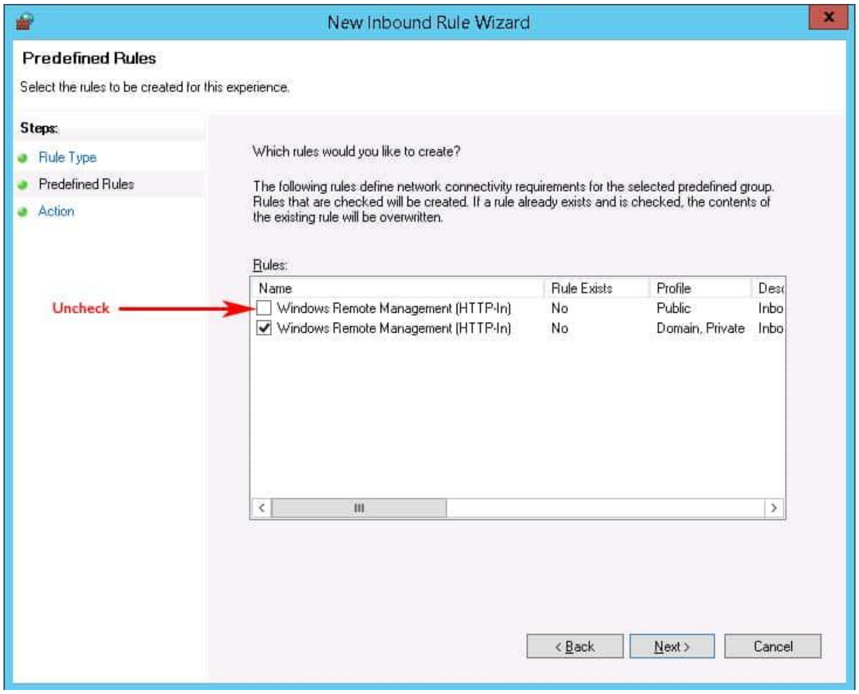
○ **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

● **Predefined:**
Windows Remote Management
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

16. To block the firewall from opening this port to the public network, click **Predefined Rules** in the left sidebar menu**.** Uncheck the Public profile option. This ensures that we only allow WinRM access to the Private and Domain networks. Then Click the Next button.



New Inbound Rule Wizard

Predefined Rules

Select the rules to be created for this experience.

Steps:
- Rule Type
- Predefined Rules
- Action

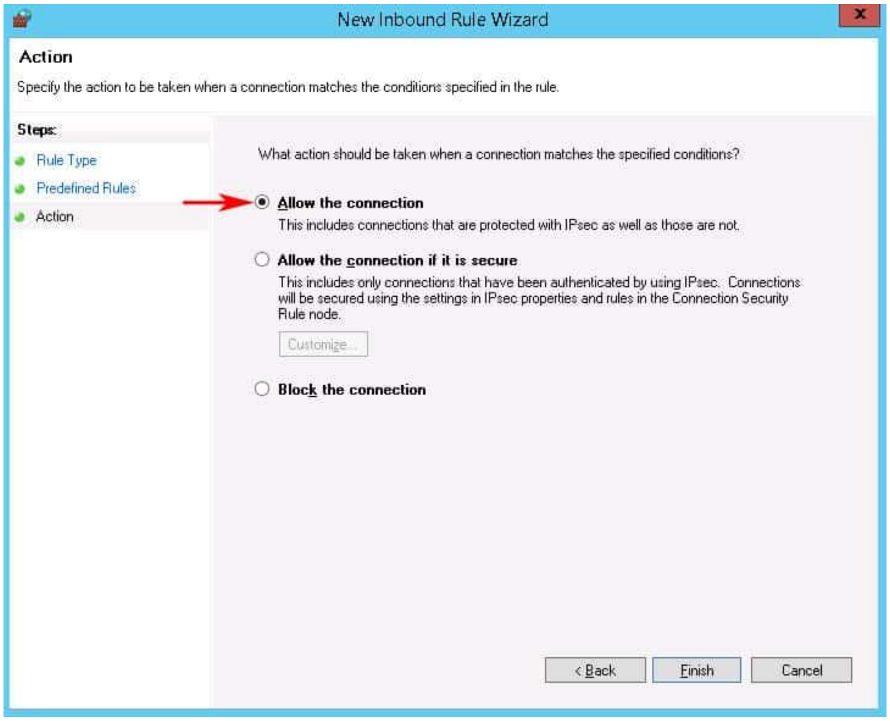
Which rules would you like to create?

The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of the existing rule will be overwritten.

Rules:

Name	Rule Exists	Profile	Desc
□ Windows Remote Management (HTTP-In)	No	Public	Inbo
☑ Windows Remote Management (HTTP-In)	No	Domain, Private	Inbo

17. Select the **Allow the connection** option and click **Finish**.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

● Allow the connection
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ Block the connection

The GPO is successfully finished and you'll need to wait for the GPO to propagate throughout your network.

Setup Manually

To setup manually:

Configuration of WinRM and IPMI

The WinRM and Intelligent Platform Management Interface (IPMI) WMI provider components are installed with the operating system.

- The WinRM service starts automatically on Windows Server 2008 and onwards (on Windows Vista, you need to start the service manually).
- By default, no WinRM listener is configured. Even if the WinRM service is running, WS-Management protocol messages that request data can't be received or sent.
- Internet Connection Firewall (ICF) blocks access to ports.

Use the `Winrm` command to locate listeners and the addresses by typing the following command at a command prompt.

```
winrm e winrm/config/listener
```

To check the state of configuration settings, type the following command.

```
winrm get winrm/config
```

Quick default configuration

You can enable the WS-Management protocol on the local computer, and set up the default configuration for remote management with the command `winrm quickconfig`.

The `winrm quickconfig` command (or the abbreviated version `winrm qc`) performs these operations.

- Starts the WinRM service, and sets the service startup type to auto-start.
- Configures a listener for the ports that send and receive WS-Management protocol messages using either HTTP or HTTPS on any IP address.
- Defines ICF exceptions for the WinRM service, and opens the ports for HTTP and HTTPS.

The `winrm quickconfig` command creates a firewall exception only for the current user profile. If the firewall profile is changed for any reason, then you should run `winrm quickconfig` to enable the firewall exception for the new profile; otherwise, the exception might not be enabled.

To retrieve information about customizing a configuration, type `winrm help config` at a command prompt.

Configure WinRM – (HTTP)

1. Open Admin Command Prompt
2. Run `winrm quickconfig`
    a. When the tool displays **Make these changes [y/n]?,** type **y**.
3. Run `winrm set winrm/config/service @{AllowUnencrypted="true"}`
4. That’s All

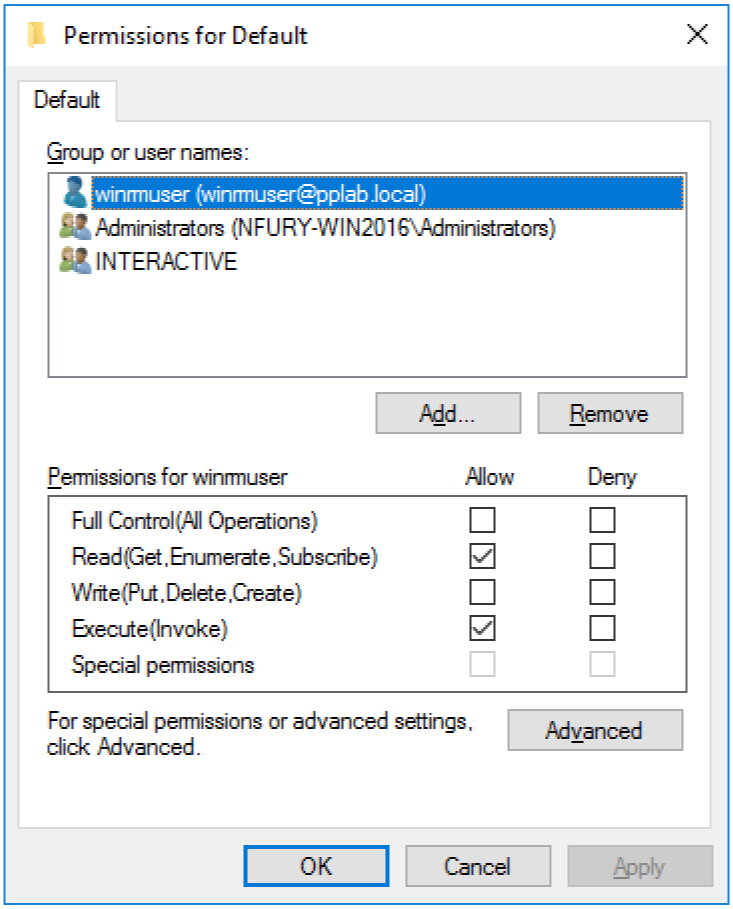
Configure WinRM – (HTTPS)

1. Install Certificate
    a. WinRM HTTPS requires a local computer Server Authentication certificate with a CN matching the hostname to be installed. The certificate mustn't be expired, revoked, or self-signed.
    b. If you don't have a Server Authenticating certificate, consult your certificate administrator. If you have a microsoft Certificate server, you may be able to request a certificate using the web certificate template from HTTPS://<MyDomainCertificateServer>/certsrv.
    c. Install the certificate into local computer’s personal store
2. Open Admin Command Prompt
3. Run `winrm quickconfig -transport:https`
    a. When the tool displays **Make these changes [y/n]?,** type **y**.
4. That’s All
5. Run `winrm enumerate winrm/config/listener` To view whether the https listener is enabled or not.

Configure WinRM – Basic Auth

1. To enable WinRM Basic Authentication run the following command in Admin Command Prompt
2. `winrm set winrm/config/service/auth @{Basic="true"}`
3. Note: Basic Auth does not work for domain users.

Configure WinRM - Users

- Like WMI, The default local administrator account and domain users who are member of local administrator group work out of the box for WinRM without any configuration.
- For Other users, Please follow the below steps
    - Add the user as a member of the local **Distributed COM Users, Remote Management Users** groups.
    - Edit WinRM default SDDL. Run the following command in Admin command prompt
        - `winrm configSDDL default`
        - Give Read and Execute permission for that user as shown below
        - 

Group or user names:

winrmuser (winrmuser@pplab.local)
Administrators (NFURY-WIN2016\Administrators)
INTERACTIVE

Permissions for winrmuser	Allow	Deny
Full Control(All Operations)	□	□
Read(Get,Enumerate,Subscribe)	☑	□
Write(Put,Delete,Create)	□	□
Execute(Invoke)	☑	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

    - Give WMI hives permission for that user Refer To give access to WMI Hives for a user
    - That's it.