SYSKEYOT ASSET DASHBOARD

SyskeyOT
Asset Dashboard

USER GUIDE

WWW.SYSKEYSOFTLABS.COM

Syskey Softlabs

support@syskeysoftlabs.com | sales@syskeysoftlabs.com

Contents

Introduction **1**

Assets Dashboard **1**

Discovery of Assets **1**

How to Run Discovery 1

How to Add Assets Manually 2

Templates **3**

Template Fields 3

How to Create Custom Templates 4

Importing/Exporting Templates 5

Authentication Credentials **5**

How to Store Credentials 5

Assets **6**

How to Run Manual Scan 7

System Configuration **7**

How to Create Active Directory Connection 7

How to Send Audit Logs to Syslog Server 8

How to Configure System Settings 8

How to Configure Default Values for Protocols 8

How to Configure Periodic Scanning 9

User Management **9**

License Management **10**

How to Add the Activation Key 10

Display Customization **10**

How to Add New Display Group 10

How to Add New Display Column 10

Configure Windows Devices for Asset Scanning **11**

How to Configure WMI 11

Admin User 11

Non-Admin User 11

How to Configure WinRM 12
Setup Through Group Policy 12
Setup Manually 16
Configuration of WinRM and IPMI 16
Quick default configuration 16
To configure WinRM with default settings 17

Introduction

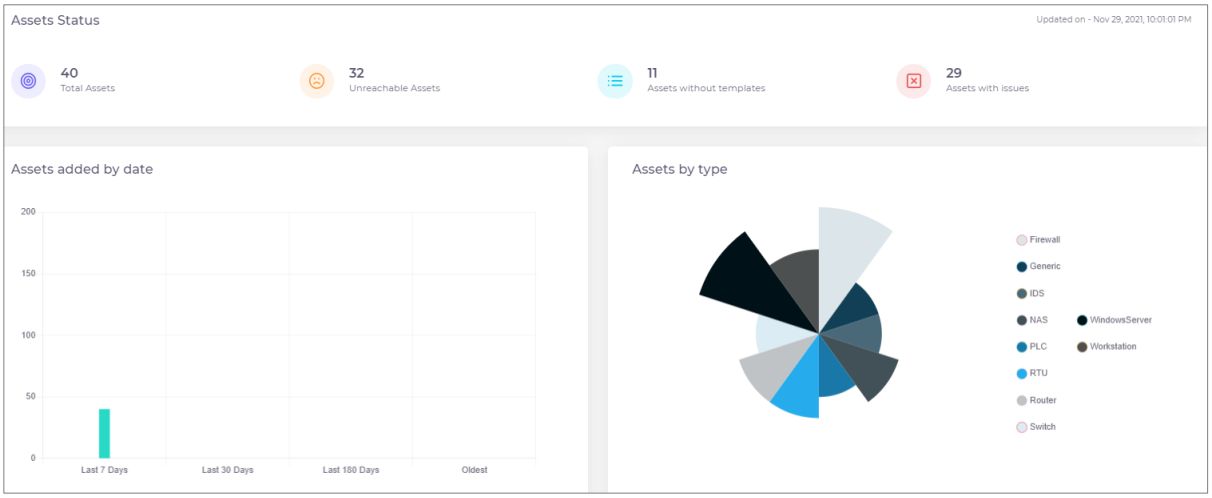
SysKeyOT Asset Dashboard automates asset management by discovering, tracking, and maintaining an inventory of assets in the network. Assets can be a PLC, RTU, IDS, server, router, firewall or any other network enabled device. Asset Manager collects asset data using various industrial standard protocols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



Discovery of Assets

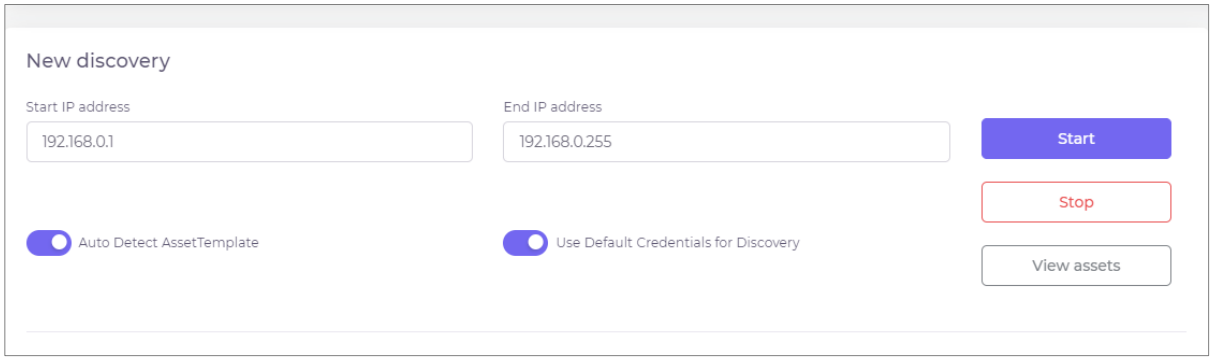
Assets can be added automatically by running a discovery probe over a network range or individual assets can be manually added.

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**.



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 AssetTemplate** 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.

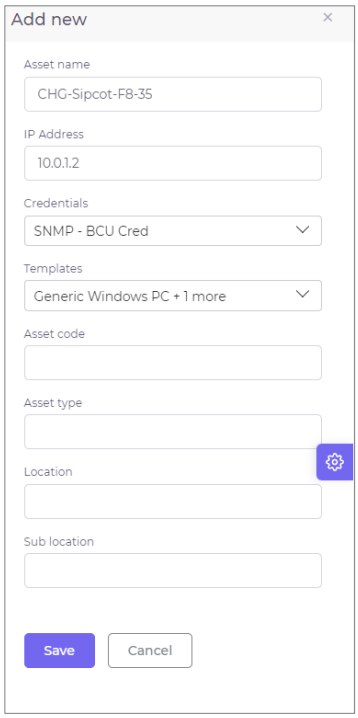
   The discovery progress and status are displayed along with details of the discovered assets. You can also view the list of skipped assets along with the reason for skipping.

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**.



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

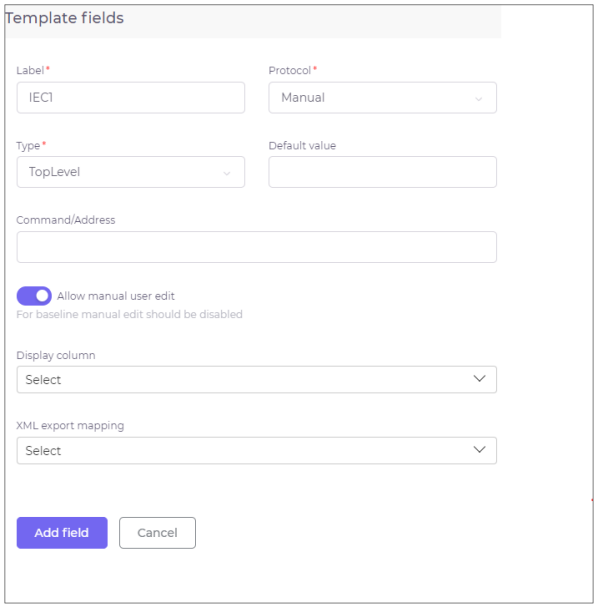
You can create new custom templates for different types of assets. You can either create a new template or duplicate an existing template and make the required changes.

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.

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



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 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. If you select Direct WMI as the transport type, specify the **Username** and **Password** for the device.
3. 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.
4. Click **Save**.

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

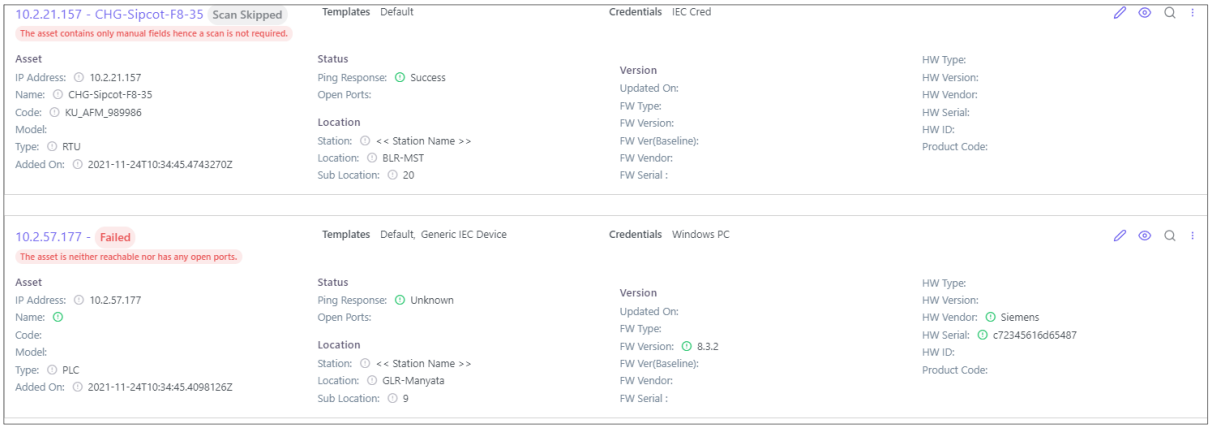
1. Specify the **Port** number used for IEC 61850.
2. Click **Save**.

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 scanned device are displayed in the Assets page. The parameters are displayed as per the defined groups and columns. The information can be displayed in either table view or list view.



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 newly discovered assets.

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

Procedure:

1. Go to Assets page.
2. Click Scan all.
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

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

Procedure:

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

How to Configure Periodic Export

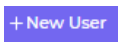
You can set up periodic export of scanned data.

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**.

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 

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.

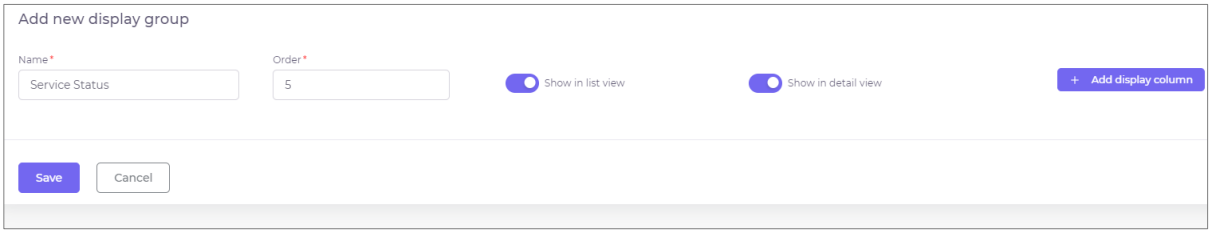
The display groups and their child columns can be defined and the columns are mapped to the device attribute through template fields.

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**.



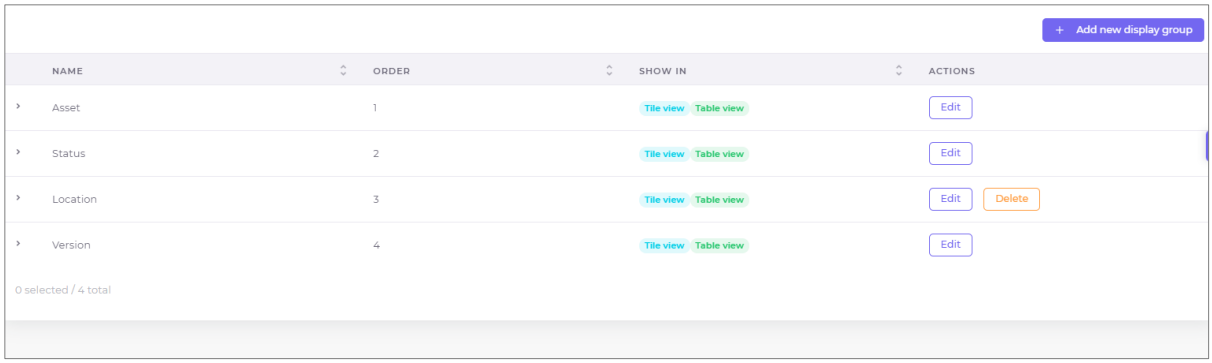
2. Specify a suitable **Name** for the group.
3. Specify the **Order** in which the group will be displayed on the Asset page.
4. Enable **list view** and **detail view** as required.
5. Click **Save**.

How to Add New Display Column

You can add new columns to existing groups.

To add new column:

1. Click Display Customization.



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

The WMI can be configured for remote access in the following ways.

Admin User

By default, remote WMI is enabled for users of local administrator group. No special configuration is required.

Non-Admin User

1. Create a new user in Windows
2. Add the user to the **Performance Monitor Users** group.
3. Under **Services and Applications**, open the properties dialog of WMI Control (or run *wmimgmt.msc*). In the **Security** tab, select **Root/CIMV2.** Click **Security** add **Performance Monitor Users. E**nable the options: *Enable Account* and *Remote Enable* and recurse the permissions to the sub-namespaces using the Advanced window in Security.
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 Performance Monitor Users 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 **Performance Monitor Users** Group.

As an alternative to steps 4 and 5, you can assign the user to the **Distributed COM Users** 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

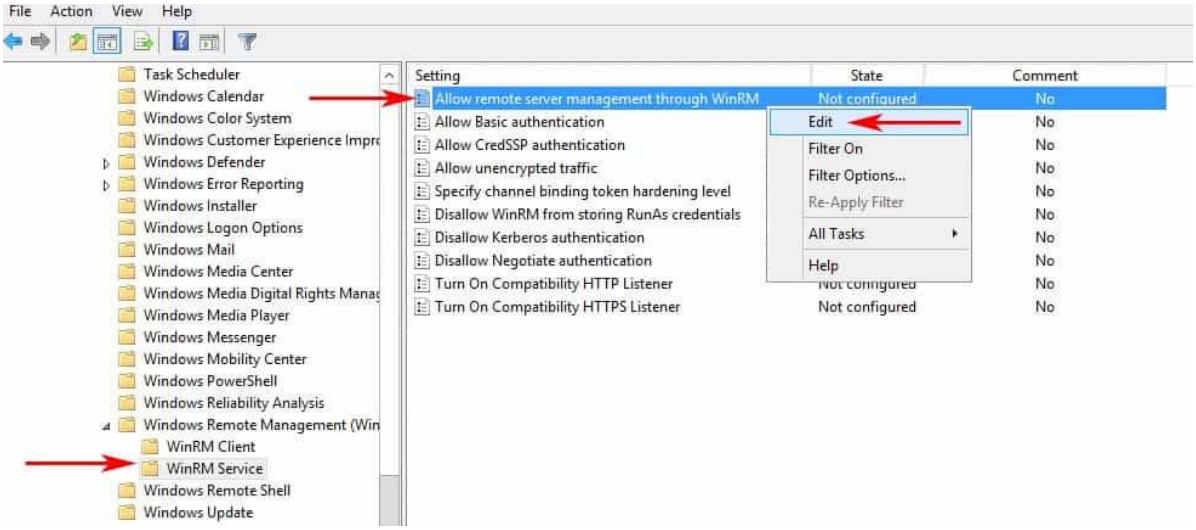
How to Configure WinRM

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

Setup Through Group Policy

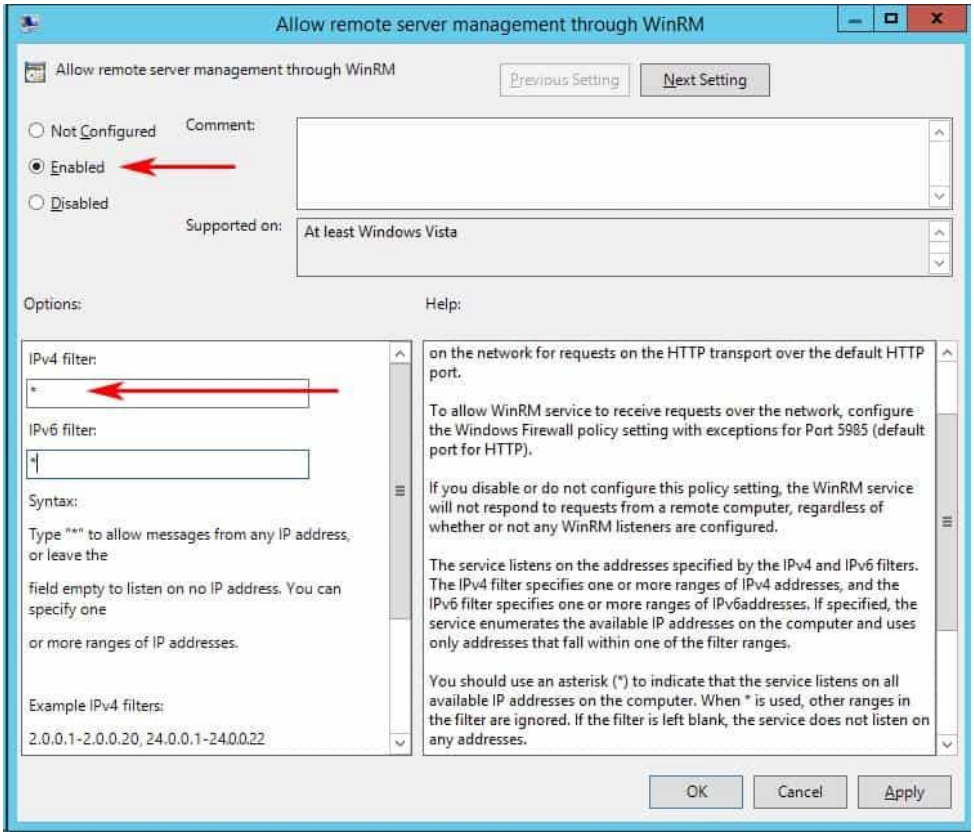
Procedure

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.

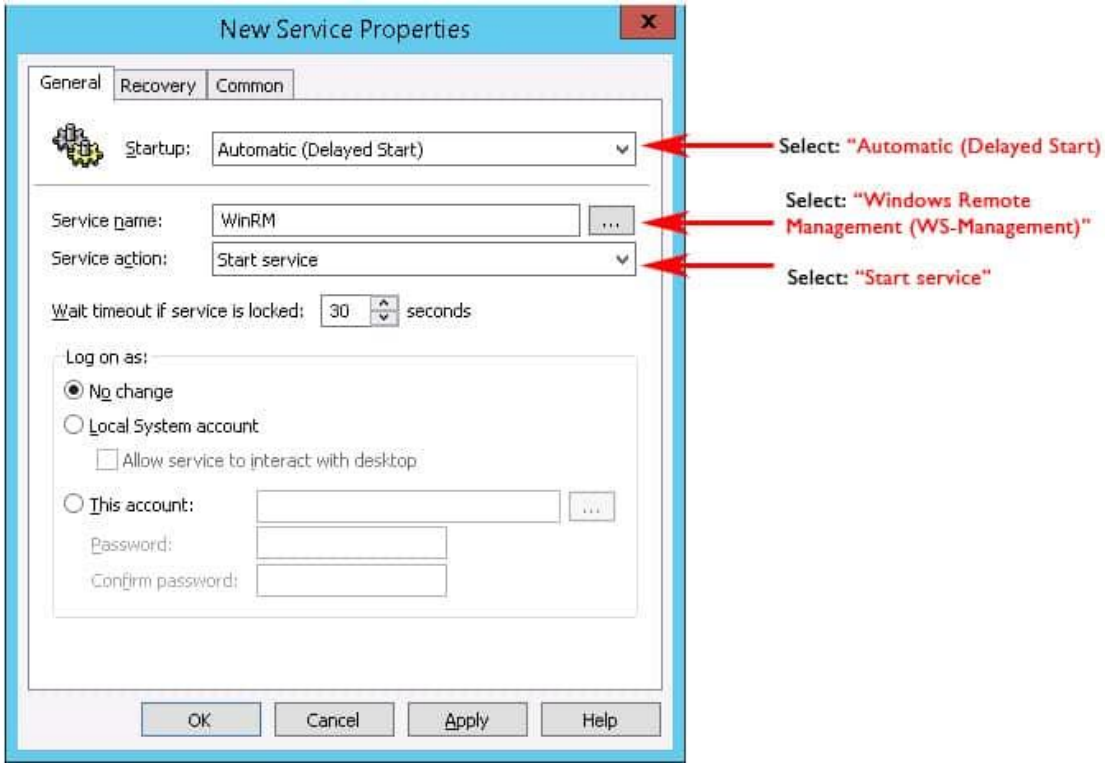


7. In the Allow remote server management through WinRM window, select **Enabled** and in the Options section, either specify an IP Address range or enter an Asterisk "*" to allow all IP

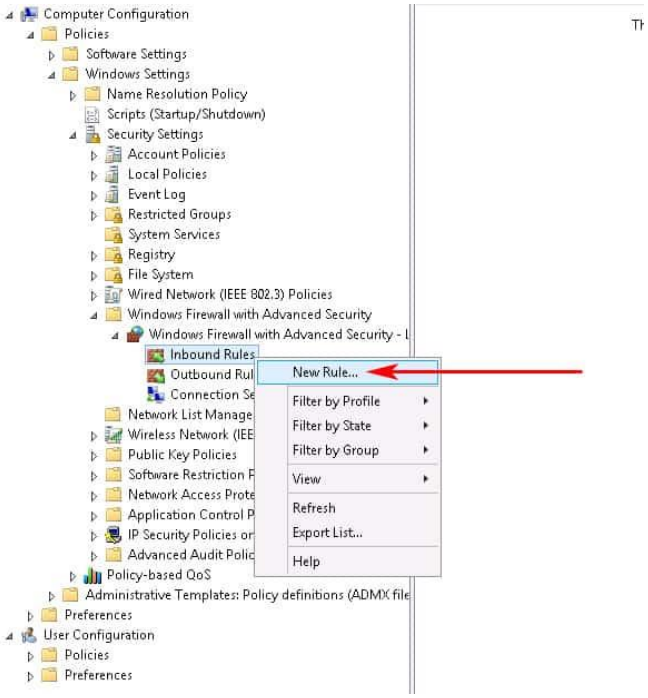
addresses to remotely manage the PC. (We recommend specifying an IP Address to reduce any risk of a security compromise of your systems/network).



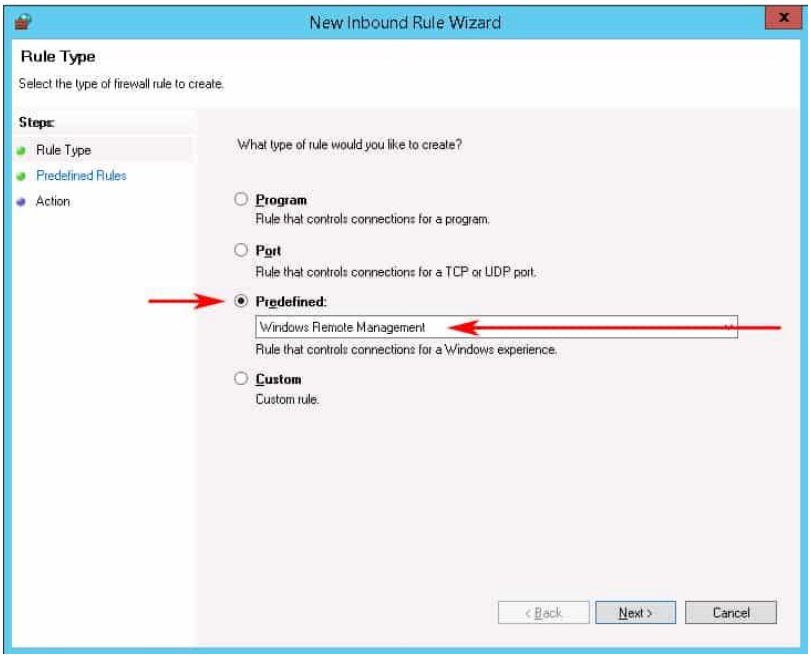
8. To enable the Windows Remote Management (WS-sManagement) Service to start automatically, go to **Computer Configuration > Preferences > Control Panel Settings > Services** and right-click and select **New** and **Service**.
9. In the New Service Properties window, change Startup to **Automatic (Delayed 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**.
10. After you've selected the Service, under the **Service action** menu, click **Start service.**



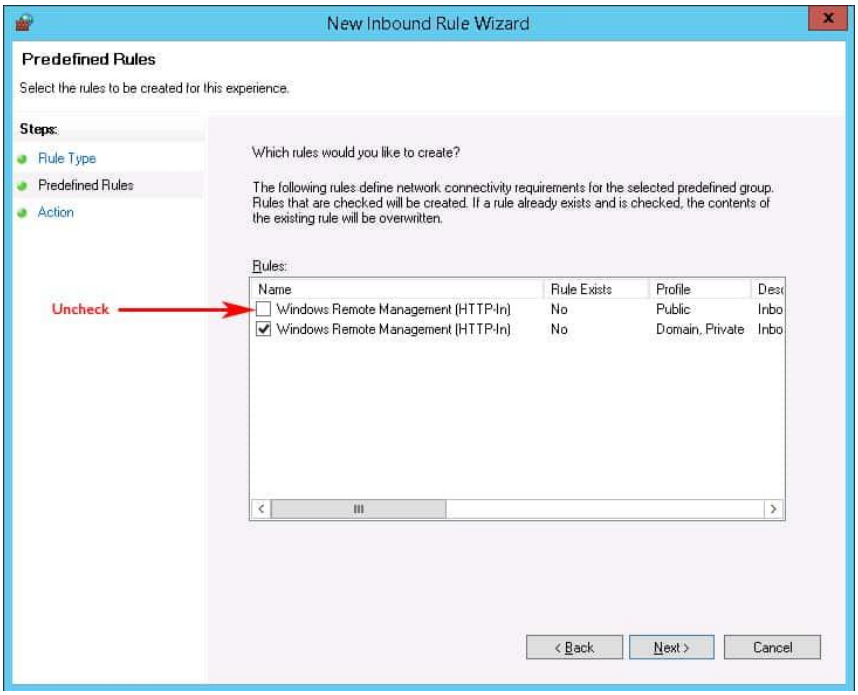
11. To configure the Windows Firewall to allow the proper ports inbound, go to Computer Configuration > expand Policies > expand Windows Settings > expand Security Settings > expand Windows Firewall with Advanced Security > expand Windows Firewall with Advanced Security > expand Inbound Rules. Right-click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



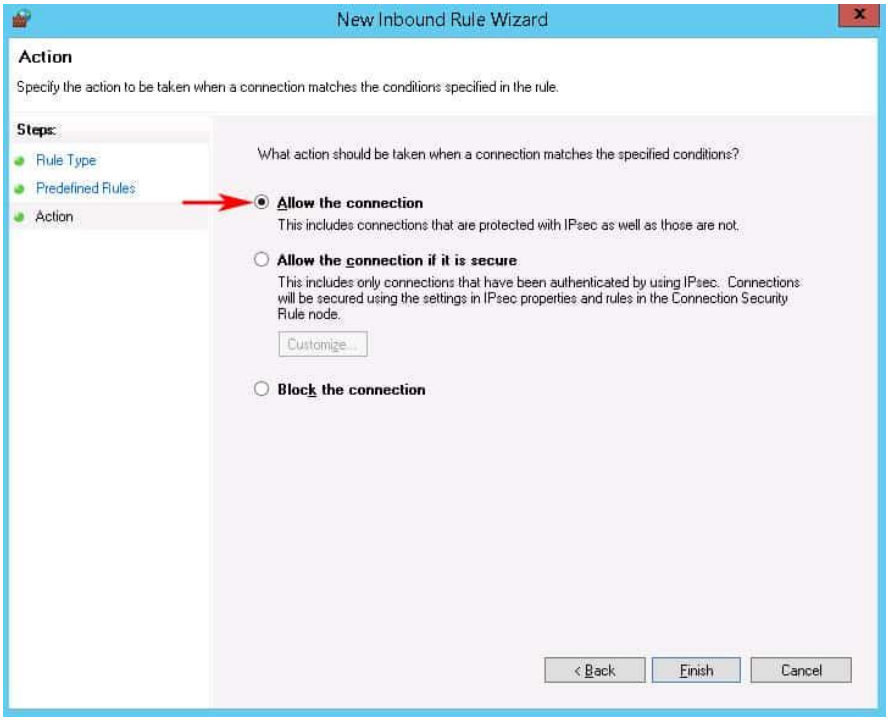
12. In the New Inbound Rule wizard, select **Predefined** and scroll down to “Windows Remote Management” and click on it as shown in the following image.



13. 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.



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



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.

To configure WinRM with default settings

1. Type `winrm quickconfig` at a command prompt.

   If you're not running under the local computer Administrator account, then you must either select **Run as Administrator** from the **Start** menu, or use the **Runas** command at a command prompt.

2. When the tool displays **Make these changes [y/n]?,** type **y**.

   If configuration is successful, then the following output is displayed.

   ```
   WinRM has been updated for remote management.

   WinRM service type changed to delayed auto start.

   WinRM service started.

   Created a WinRM listener on https://* to accept WS-Man requests
   to any IP on this machine
   ```

3. Keep the default settings for client and server components of WinRM, or customize them. For example, you might need to add certain remote computers to the client configuration TrustedHosts list.

   You should set up a trusted hosts list when mutual authentication can't be established. Kerberos allows mutual authentication, but it can't be used in workgroups—only domains. A best practice when setting up trusted hosts for a workgroup is to make the list as restricted as possible.

   Create an HTTPS listener by typing the command `winrm quickconfig -transport:https`. Be aware that you must open port 5986 for HTTPS transport to work.