Article

Service Assurance Suite

Release number 9.4

How to Maintain IP Manager Settings

January, 2015

- Overview 2
- Requirements 3
- Workflow for maintaining IP Manager settings 4
- Adding an IP Manager to Configuration Manager 5
- Disabling an IP Manager from Configuration Manager control 6
- Modifying IP settings while Configuration Manager transfer is delayed 6
- Removing an IP Manager from Configuration Manager control 7
- Configuring settings for a selected group 7
- Configuring matching criteria for a selected group 8
- Configuring target domains for a selected group 9
- Adding a description for a selected group 9
- Configuring device access for a selected group 10
- Configuring unique identifier tags for a selected group 10
- Configuring discovery settings 11
- Configuring discovery filters 11
- Adding a new group 11
- Deleting a group 12
- Changing the priority of the groups 12
- Copying the configuration of a group 13
- Displaying IP Manager groups 13
- Displaying IP Manager attributes 13
- Configuring EDAA mode for 9.2 and 9.1 IP Managers 14
- Automatically loading settings from a running IP Manager into the Configuration Manager 15
- sm_service install commands for Linux 17
- sm_service install commands for Windows 18

EMC²

Overview

Use the Configuration Manager in the EMC M&R UI to apply a centralized copy of configuration settings to all IP Managers in your deployment. Configuration settings can include: polling intervals, thresholds, device access credentials, unique tagging identifiers for discovered topology, and discovery configuration parameters.

For deployments with multiple IP Managers, Service Assurance Suite provides the Configuration Manager, so you can consistently maintain configuration settings. The Configuration Manager is an optional component.

- Polling settings define the polling intervals. Polling occurs when an IP Manager communicates with a managed device to determine the device's operational status.
- Thresholds are values that define acceptable or unacceptable levels of connectivity or performance. The polled data is compared to the threshold values for monitoring purposes.
- Device access settings define the credentials needed to access the managed devices.
- IP tagging defines a tag that the IP Manager uses to uniquely identify discovered topological objects that have identical names.
- Discovery configuration settings define the discovery process that the IP Manager performs.

The Configuration Manager feature supports the following IP Managers: IP Availability Manager, IP Performance Manager, and the combined IP Availability and Performance Manager.

Figure 1 Example of polling settings

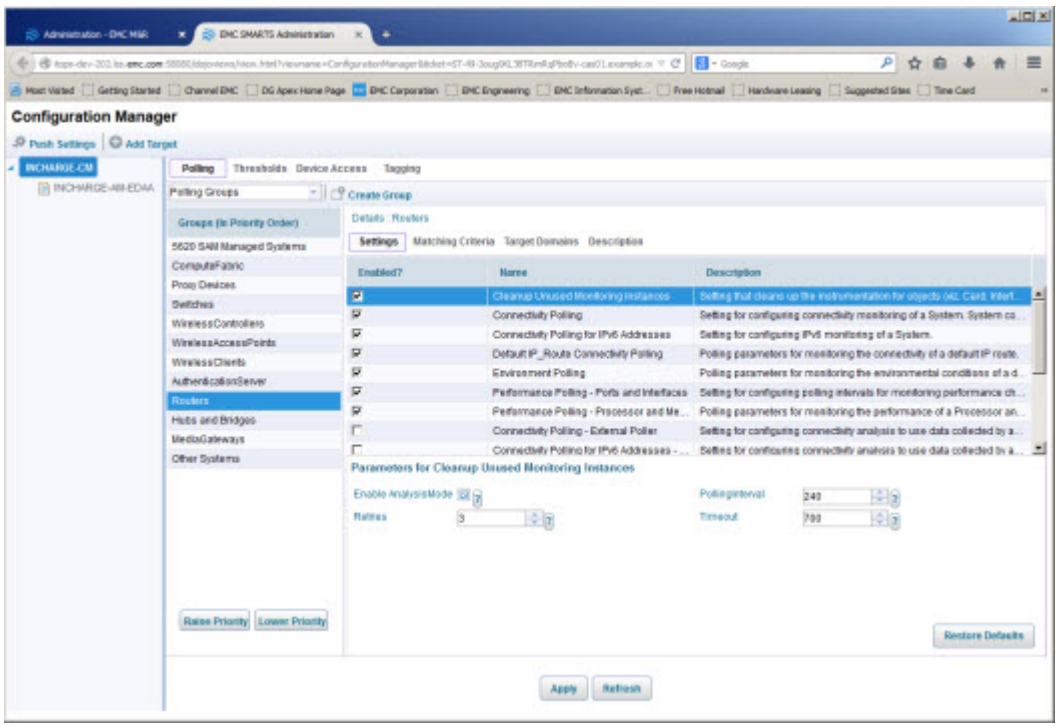
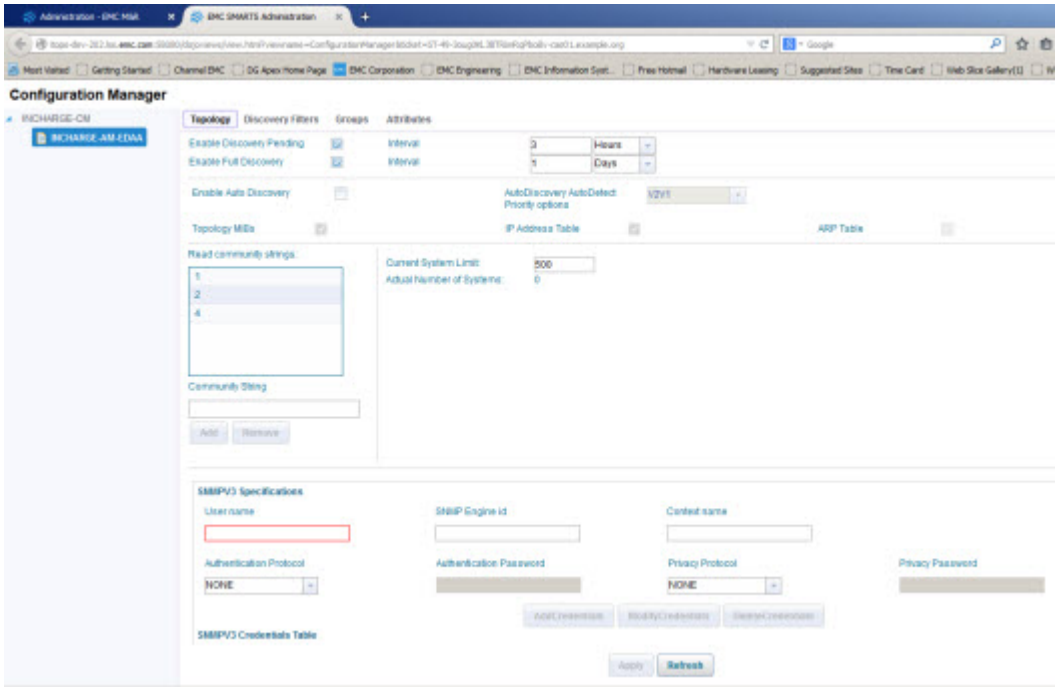


Figure 2 Example of discovery settings



Additional information is described in these documents:

- *EMC M&R Installation and Configuration Guide*
- *SolutionPack for EMC Smarts Summary Sheet*
- *How to Set Up SAM, EMC M&R, and the SolutionPack for EMC Smarts*
- *Troubleshooting the Deployment of SAM, EMC M&R, and the SolutionPack for EMC Smarts*

Requirements

When using the Configuration Manager in the EMC M&R UI to control your configuration settings, ensure that you have the following components set up in your deployment:

- A valid EMC Smarts license, that includes the Configuration Manager, is installed.
- The Configuration Manager is installed and is started with the EMC Data Access API service option (`--edaa=ip/2.0`).
- The SolutionPack for EMC Smarts is installed and configured with the Configuration Manager instance name. In the Report block, under Presentation SAM Configuration Section, select the **Use Smarts Configuration Manager** checkbox and specify the name of the Configuration Manager in the Configuration Manager field if it does not use the default name.
- You planned your configuration carefully:
  - Identified the IP Managers to assign to the Configuration Manager. IP Managers 9.1 and higher are supported but there is limited backward compatibility for 9.1 IP Managers.
  - Modified the `sm_service install` command for the identified 9.4 and 9.3 IP Managers to include the `--edaa=ip/2.0` option (for example: sm_service install commands for Linux on page 17 and sm_service install commands for Windows on page 18).

9.2 and 9.1 IP Managers do not support the service command `--edaa=ip/2.0` option. For 9.1 IP Managers, the Configuration Manager does not support discovery configuration settings, but other configuration settings are supported. Use: Configuring EDAA mode for 9.2 and 9.1 IP Managers on page 14

- Be aware that when the Configuration Manager is connected to running IP Managers, it by default transfers the settings and may overwrite unique settings in the IP Managers.
  If you do not want Configuration Manager to transfer the settings to the IP Managers on the initial connection, uncheck the **Config Enabled** checkbox when you add the IP Manager as a target as described in Adding an IP Manager to Configuration Manager on page 5.
- Once you use the Configuration Manager to control configuration settings in the IP Managers, you are no longer able to modify polling and thresholds group settings locally in the IP Managers.
  - The Configuration Manager overwrites all configuration settings in the IP Managers.
  - You can only view the polling and thresholds settings and not modify them in the Domain Manager Administration Console.

  The Topology and Discovery Filters settings remain locally defined for each IP Manager. You can continue to modify the Topology and Discovery Filters settings from the Domain Manager Administration Console and the EMC M&R UI.

- EMC M&R is installed and you have valid administrator credentials.

Workflow for maintaining IP Manager settings

Use the Configuration Manager to apply a centralized copy of configuration settings to all IP Managers in your deployment.

1. Log in to the EMC M&R platform with your administrator username and password.
2. Select **Administration** › **Modules** › **Smarts**.
3. Select the Configuration Manager (Default: INCHARGE-CM).
   - Ensure that the IP Managers are assigned.
   - If not, add the IP Managers: Adding an IP Manager to Configuration Manager on page 5
   - To keep IP Managers assigned but disabled: Disabling an IP Manager from Configuration Manager control on page 6
   - To remove IP Managers: Removing an IP Manager from Configuration Manager control on page 7
4. Click one of the following: **Polling**, **Thresholds**, **Device Access**, **Tagging**, or an IP Manager for discovery configuration and make your configurations accordingly:
   - To configure settings for a selected group: Configuring settings for a selected group on page 7
   - To configuring matching criteria: Configuring matching criteria for a selected group on page 8
   - To configure target domains: Configuring target domains for a selected group on page 9
   - To add a description: Adding a description for a selected group on page 9

- To configure device access: Configuring device access for a selected group on page 10
- To configure tagging: Configuring unique identifier tags for a selected group on page 10
- To configure the discovery process: Configuring discovery settings on page 11
- To configure discovery filters: Configuring discovery filters on page 11
- To create more groups: Adding a new group on page 11
- To delete groups: Deleting a group on page 12
- To change the priority order of the groups: Changing the priority of the groups on page 12
- To copy the configuration of a group to make a new group: Copying the configuration of a group on page 13

5. Start the services for one or more IP Managers.
   Linux: Issue the command:

   ```
   /opt/InCharge/IP/smarts/bin/sm_service start <service_name>
   ```

   Windows: From the application server's desktop, select **Start** › **Administrative Tools** › **Services** and start the service.

IP Manager	Service name
IP Availability Manager	ic-am-server
IP Performance Manager	ic-pm-server
IP Availability and Performance Manager	ic-am-pm-server

   Before you start the service, if you have not already done so, you need to issue the `sm_service install` command to register the product: sm_service install commands for Linux on page 17 and sm_service install commands for Windows on page 18

6. Click **Push Settings**:
   - If you changed configuration settings for one of the target IP Managers.
   - After you enabled the Config Enabled attribute for a target IP Manager.

   The Configuration Manager transfers the settings whenever the IP Managers connect or are reconnected, or when you click Push Settings.

Adding an IP Manager to Configuration Manager

Add one or more IP Managers to the Configuration Manager list if they are not included.

Procedure

1. For the selected Configuration Manager, click **Add Target**.
2. Type the IP Manager instance name in the **Element Name** field (for example, INCHARGE-AM).
3. Decide if you want to keep the following checkboxes selected:

Checkbox	Description
Config enable	By default, this checkbox is selected so that the Configuration Manager automatically transfers the configuration settings to the IP Manager if the IP Manager is started. If you clear the checkbox, the IP Manager is added to the Configuration Manager list but the Configuration Manager does not transfer the settings. Use this option if you want to control when the Configuration Manager transfers the settings. Modifying IP settings while Configuration Manager transfer is delayed on page 6
Reconfigure after push	By default, this checkbox is selected so that the Configuration Manager initiates a reconfigure action on the modified or newly-added configuration settings in the IP Manager. If you clear the checkbox, then you have to manually reconfigure the IP Manager.

4. Click **OK**.

Disabling an IP Manager from Configuration Manager control

You can temporarily stop the Configuration Manager from sending the centralized settings to an IP Manager without removing it from the Configuration Manager list. For example, you can disable the transfer of settings for a specific IP Manager while you create new groups or change settings.

Procedure

1. In the Configuration Manager list, right-click the IP Manager and select **Modify Attributes**.
2. Select the **Config enable** checkbox to remove the checkmark.
3. Select the **Reconfigure after push** checkbox to remove the checkmark.
4. Click **OK**.

Modifying IP settings while Configuration Manager transfer is delayed

Use this alternate approach if you want to configure groups and settings while delaying the transfer of the settings.

Before you begin

The IP Manager is added to the Configuration Manager list but you temporarily disabled it from the Configuration Manager.

Procedure

1. Review which groups are assigned to the IP Manager and their settings.
2. Modify the groups and their settings if necessary.
3. Right-click the IP Manager and select **Modify Attributes**.
4. Select the **Config enable** checkbox.
5. Select the **Reconfigure after push** checkbox.
6. Click **Push Settings** to transfer the settings.

Removing an IP Manager from Configuration Manager control

One method to stop the Configuration Manager from sending the centralized settings to an IP Manager is to permanently remove it from the Configuration Manager list. Or, if you accidently added the incorrect IP Manager to the Configuration Manager list, you can remove it.

Procedure

1. Clear the value for the Service Name attribute.
   a. Attach the Domain Manager Administration Console to the IP Manager.
   b. Press **Ctrl + ALT + M**.
   c. Go to **ICIM_Manager->ICIM-Manager.**
   d. Clear the value in the Service Name attribute.
   e. Click **Apply**.
2. In the EMC M&R UI, in the Configuration Manager list, right-click the IP Manager and select **Delete**.
3. Reinstall the service for the IP Manager without the `--edaa` option.
   a. Stop the IP Manager service.

      Linux: Issue the command:

      ```
      /opt/InCharge/IP/smarts/bin/sm_service stop <service_name>
      ```

      Windows: From the application server's desktop, select **Start** › **Administrative Tools** › **Services** and stop the service.
   b. Issue the `sm_service install` command for the IP Manager minus the `--edaa` option.
   c. Start the IP Manager service.

Configuring settings for a selected group

You can accept the default settings or change the settings and their parameters for a selected group.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following choices:
   - Polling
   - Thresholds
   - Device Access
   - Tagging

2. Select a group category from the dropdown box.
3. Select a group from the list that appears for the group category.
4. Click **Settings**.

   The default settings are already enabled.
5. To add more settings to the group,

   a. Scroll and click the **Enabled** checkbox for each setting that you want to apply.

   b. Click **Apply** and **Refresh**.

   The Configuration Manager transfers only the enabled settings.
6. To examine the parameters of each setting, click the setting.
7. To modify the setting parameters, click the setting, and modify the values as necessary.

   To restore the parameters to their default values, click **Restore Defaults**.
8. Click **Apply** to save your changes.

Configuring matching criteria for a selected group

You can configure matching criteria for a selected group. The matching criteria determines group membership. A managed object becomes a member of the group, when the managed object matches a group's target class and matches all of the attributes defined for the target class.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following choices:

   - Polling
   - Thresholds
   - Device Access
   - Tagging
2. Select a group category from the dropdown box.
3. Select a group from the list that appears for the group category.
4. Click **Matching criteria** to create matching criteria which determines the members of the group.

   a. Select a class attribute from the dropdown box.

   b. Specify a value for the class attribute.

   Value can be: Boolean, text, integers, and wildcard characters. The Value field is not case-sensitive.
5. Click **Add** to add more pairs of class attributes and values.

   To remove a class attribute and its value, click the **Delete icon**.
6. Click **Apply** to save your changes.

Configuring target domains for a selected group

You can specify IP Managers for a selected group and assign the setting to specific IP Managers. For example, you have a group of routers with a specific threshold setting and three IP Managers monitor the routers.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following choices:
   - Polling
   - Thresholds
   - Device Access
   - Tagging
2. Select a group category from the dropdown box.
3. Select a group from the list that appears for the group category.
4. Click **Target Domains** to assign the setting to specific IP Managers.
5. Specify a filter in the group that you want to assign to the target IP Managers.
   a. Type wildcard characters, integers, regular expressions, or an IP Manager name in the `Search By` field and click **Search** to search for particular IP Managers or a group of IP Managers.
   b. Select one or more IP Managers from the list.

   The IP Managers that you select can be a subset of the IP Managers listed under the IP Configuration Manager. Previously enabled or disabled IP Managers (other than the search criteria) will not be modified.
6. Click **Apply** to save your changes.

Adding a description for a selected group

You can create a description to identify a group.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following choices:
   - Polling
   - Thresholds
   - Device Access

- Tagging

2. Select a group category from the dropdown box.
3. Select a group from the list that appears for the group category.
4. Click **Description** and type information about the group.
5. Click **Apply** to save your changes.

Configuring device access for a selected group

You can configure the device access setting for a selected group. Device credentials, for example login credentials, are used for command line interface (CLI) discovery, CLI polling, and XML discovery.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).
- Assign IP Managers.

Procedure

1. Click **Device Access**.
2. Select the group category **Device Access Configurations** from the dropdown box.
3. Select a group (for example, **CLI Access Group** or **XML Access Group**) from the list that appears for the group category.
4. Click **Settings**.

   The default settings are already enabled.

   The Configuration Manager transfers only the enabled settings.
5. To examine the parameters of each setting, click the setting.
6. To modify the credentials, click the setting, and modify the values as necessary.
7. Click **Apply** to save your changes.

Configuring unique identifier tags for a selected group

You can configure an IP tag naming convention that the IP Manager uses to uniquely identify discovered topological objects that have identical names.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).
- Assign IP Managers.

Procedure

1. Click **Tagging**.
2. Select the group category **System IP Tag Groups** from the dropdown box.
3. Select a group (for example, **IP Tag**) from the list that appears for the group category.
4. Click **Settings**.

   The default settings are already enabled.

   The Configuration Manager transfers only the enabled settings.

5. To create the tagging convention, click the setting, and modify the values as necessary.
6. Click **Apply** to save your changes.

Configuring discovery settings

You can configure the discovery process for the IP Manager. You can specify whether the IP Manager performs a full discovery or autodiscovery, the time intervals for discovery, whether pending discovery is performed for candidate systems, user-defined community strings, and SNMPV3 specifications.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the IP Managers in the Configuration Manager list.
2. Click **Topology**.
3. Click the checkboxes and modify the values as necessary.
4. Click **Apply** to save your changes.

Configuring discovery filters

You can configure discovery filters for candidate systems that the IP Manager uses during the discovery process. The filters can include IP address ranges, System OIDs, and so on.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the IP Managers in the Configuration Manager list.
2. Click **Discovery Filters**.
3. Click the checkboxes and modify the values as necessary.

   Use the **View Extended Filter** checkbox for SNMP fields and SNMPV3 specifications.
4. Click **Apply** to save your changes.

Adding a new group

When you are using the Configuration Manager to maintain settings for IP Managers, you can add a new group to the group category for Polling, Thresholds, Device Access, or Tagging.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).

- Assign IP Managers.

Procedure

1. Click one of the following: **Polling**, **Thresholds**, **Device Access**, or **Tagging**.
2. Select a group category from the dropdown box.

   The choices vary accordingly for Polling, Thresholds, Device Access, or Tagging.
3. Click **Create Group**.
4. Type the name of the new group and a description. Click **OK**.

   The new group appears in the group list.

Deleting a group

When you are using the Configuration Manager to maintain settings for IP Managers, you can delete a user-defined group or a default group from the group category for Polling, Thresholds, Device Access, or Tagging.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following: **Polling**, **Thresholds**, **Device Access**, or **Tagging**.
2. Select a group category from the dropdown box.

   The choices vary accordingly for Polling, Thresholds, Device Access, or Tagging.
3. In the group list, right-click the group and select **Delete**.

Changing the priority of the groups

In any group category, you can arrange the groups in a high-to-low priority. During the matching criteria process which determines the members of a group, a candidate member object is compared against the highest priority group first. The candidate becomes a member of the first group for which there is a criteria match.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following: **Polling**, **Thresholds**, **Device Access**, or **Tagging**.
2. Select a group category from the dropdown box.

   The choices vary accordingly for Polling, Thresholds, Device Access, or Tagging.
3. In the group list, select the group and click either **Raise Priority** or **Lower Priority** to move the group to the appropriate position in the list.
4. Click **Apply** to save your changes.

Copying the configuration of a group

When you are using the Configuration Manager to maintain settings for IP Managers, you can create a new group by copying an existing group with its configurations, making minimal changes, and reassigning IP Managers to it.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following: **Polling**, **Thresholds**, **Device Access**, or **Tagging**.
2. Select a group category from the dropdown box.

   The choices vary accordingly for Polling, Thresholds, Device Access, or Tagging.
3. In the group list, right-click the group to copy and select **Copy Configuration**.
4. Type the new group name, the description, the IP Managers to assign to it, select the **Copy Matching Criteria** checkbox, and click **OK**.

   Helper lists the configuration-enabled IP Managers.

   The new group appears above the source group from which it was copied. This ensures that the custom group settings are applied first to the IP Managers assigned to this group and not overwritten by the default group settings.

Displaying IP Manager groups

You can view all of the groups for a specific IP Manager.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the IP Managers in the Configuration Manager list.
2. Click **Groups**.

Displaying IP Manager attributes

You can view all of the attributes for a specific IP Manager.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** › **Modules** › **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the IP Managers in the Configuration Manager list.

2. Click **Attributes**.

Configuring EDAA mode for 9.2 and 9.1 IP Managers

Configure EDAA mode for the services of the older IP Managers so the IP Managers can interact with the Configuration Manager. Older IP Managers do not support the service command `--edaa=ip/2.0` option.

Procedure

1. Edit the `msa-sources.xml` file located in the SAM installation in `<SAM-BASEDIR>/smarts/tomcat/webapps/smarts-edaa/WEB-INF/classes` to add entries for your IP Managers.

   a. For example, add the entry key information:

   ```
   <entry key="INCHARGE-AM-92"
   value-ref="MsaDMTDataSource__INCHARGE-AM-92" />
   ```

   b. Add the corresponding bean id information.

   ```
   <bean id="MsaDMTDataSource__INCHARGE-AM-92"
    class="com.emc.msa.dmt.dmpool.MSADMTContext">
    <property name="brokerContext"
   ref="MsaDMTDataSource__Broker" />
    <property name="dmtName" value="INCHARGE-AM-92" />
    <property name="dataSourceName" value="INCHARGE-AM-92" />
    <property name="modelName" value="ip" />
    <property name="modelVersion" value="2.0" />
    <property name="useTLS" value="true" />
    <property name="disableKeepalives" value="true" />
    <property name="lockBoxSupport" value="false" />
    <property name="excludeClasses" ref="IP-
   ExcludeClassesDefault"/>
    <property name="excludeAttributes" ref="IP-
   ExcludeAttrsDefault"/>
    </bean>
   ```

   Use the full domain name as it is registered with the Broker (for example, INCHARGE-AM-92 and not AM-92). The entry key parameter value should match the datasource name (the domain name with which the IP Manager is started).

   The value of the bean id parameter must match the value-ref parameter value.

   The dmtName property value and the dataSourceName property value must match the entry key value.

2. Open the `msa-model-defaults.xml` file in the `<SAM-BASEDIR>/smarts/tomcat/webapps/smarts-edaa/WEB-INF/classes/` directory. If not commented, comment the MR_MetaObject value in the xml node with `id="IP-ExcludeClassesDefault"`. For example:

   ```
   <!-- Start of Default Values for Provider Entries -->
    <util:list id="IP-ExcludeClassesDefault">
    <value>GA.*</value>
    <!--<value>MR_MetaObject</value> -->
    <value>ICIM_Test</value>
    <value>NasManager</value>
    <value>Topo.*</value>
    <value>Hierarchical.*</value>
    <value>VOIP.*</value>
    </util:list>
   ```

3. Use sm_edit to open the `<SAM-BASEDIR>/smarts/conf/edaaClientConnect.conf` file.
   a. Add an entry for the IP Manager using the format `*:<DOMAIN-NAME>:admin:changeme`.

      ```
      *:INCHARGE-AM-92:admin:changeme
       ::_edaa:changeme
      ```

      The account `_edaa` is used to log in to IP Managers 9.3 and higher.
   b. Save the file.
4. Stop and start the smarts-tomcat, smarts-rabbit-mq, and smarts-elasticsearch services.

Automatically loading settings from a running IP Manager into the Configuration Manager

Manually transferring settings from a running IP Manager into the Configuration Manager can be time-consuming. You can use an automated alternative, the sm_settings.pl script, to export the settings from the IP Manager and import them into the Configuration Manager.

Procedure

1. To export the settings from a running IP domain manager, run the script from `<BASEDIR>/IP/smarts/bin`:

   ```
   ./sm_perl sm_settings.pl --server=<server_name> --export=<filename>
   ```

   For example: `./sm_perl sm_settings.pl -s INCHARGE-AM --export=pt_goups`

   The export output is written as a file to the `<BASEDIR>/IP/smarts/local/logs` directory.
2. Optional, you can modify the script output to include new polling groups: Other modifications to sm_settings.pl output on page 15
3. To import the content into the Configuration Manager, run the script from `<BASEDIR>/IP/smarts/bin`:

   ```
   ./sm_perl sm_settings.pl --server=<CM_server> --import=<filename>
   ```

   For example: `./sm_perl sm_settings.pl -s INCHARGE-CM --import=pt_goups`

Other modifications to sm_settings.pl output

When you use the sm_settings.pl script, you can also modify the script output to include new polling groups, for example, before importing the content into the Configuration Manager.

If you want add another polling group, use sm_edit from the BASEDIR/smarts/bin directory to open the exported output file (for example, type: `sm_edit <BASEDIR>/IP/smarts/local/logs/pt_groups`). Add the new group definition under the polling category ICIM_UnitaryComputerSystem Polling Groups line. Below this line, you see definitions for all polling groups applicable to Unitary Computer systems

(routers, switches, etc). Add the new definition immediately after the category line or between other definitions, as long as it is above the next category line.

- To create a new group definition, you can copy an existing group in the file and modify it.
- Alternatively, you can run the sm_settings.pl script against an IP Manager that is not under Configuration Manager control and that contains the desired group definition. Then, copy and paste the group definition into the file.

In addition, after you add the group definition, type the IP Manager or multiple IP Managers for the group. The general syntax is: `config <Group Name>: DM1|DM2`

Then, save the file and import it into the Configuration Manager.

If a domain name specified in a group definition is not configured as a target IP Manager for the Configuration Manager, the IP Manager will be added as part of the import.

The settings for the newly-added Domain Managers need to be verified and then pushed manually.

Note

Export can be run on any of the installations of IP Manager. However, to import the settings, the file needs to be placed at SM_HOME/local/logs or SM_WRITEABLE/logs of the server's installation folder and then import needs to be invoked from the bin folder of the same install.

Note

Even though the Device Access groups can be imported into the IP Configuration Manager, passwords still need to be added manually because passwords are not exported due to security reasons. However, once the Configuration Manager pushes the settings to the target domains, it is done through secure connection, so it can push the credentials.

The output file contains configuration of all polling and threshold groups and settings. Each group definition starts with `config <group name>` line. Group definitions are separated from each other by blank lines. They are also organized by category. When you add a new group, make sure that the new group definition is added under the correct category.

```
Polling Group Categories
polling category CIM_FileSystem Managed FileSystems
polling category RedundancyGroup Unmanaged RedundancyGroups
polling category Interface Unmanaged Interfaces
polling category RedundancyGroup Managed RedundancyGroups
polling category Interface Managed Interfaces
polling category CIM_FileSystem Unmanaged FileSystems
polling category ICIM_ServiceAccessPoint Managed STPNodes
polling category ICIM_UnitaryComputerSystem Polling Groups
polling category CIM_LogicalDevice Unmanaged Logical Devices
polling category Port Managed Port
polling category CIM_LogicalDevice Managed Logical Devices
polling category ICIM_ServiceAccessPoint Unmanaged STPNodes
polling category Port Unmanaged Ports

Threshold Group Categories
threshold category Port Port Groups - Trunk Ports
threshold category FileSystem File Systems
threshold category ICIM_UnitaryComputerSystem System Resource Groups
threshold category WirelessControllerRedundancyGroup
WirelessControllerRedundancyGroups
```

```
threshold category ICIM_UnitaryComputerSystem System VLAN Tag Groups
threshold category Port Port Groups - Access Ports
threshold category TemperatureSensor TemperatureSensor
threshold category Interface Interface Groups
threshold category WirelessRadioInterface WirelessRadioInterfaceGroup
threshold category AggregatePort AggregatePortsGroup
threshold category VoltageSensor VoltageSensor

Tagging
tagging category ICIM_UnitaryComputerSystem System IP Tag Groups

CLI groups
security category ICIM_UnitaryComputerSystem Device Access
Configurations
```

sm_service install commands for Linux

The `sm_service install` command for products that interoperate with the EMC M&R User Interface includes additional options. Before you start the service, if you have not already done so, you need to issue the `sm_service install` command from the `/opt/InCharge/IP/smarts/bin` directory to register the product with the EMC Smarts Broker.

sm_service install command for Configuration Manager

As a prerequisite, the Configuration Manager is already running.

```
/opt/InCharge/IP/smarts/bin/sm_service install --force
--unmanaged
--startmode=runonce
--name=ic-ip-configuration-edaa
"--description=EMC Smarts IP Configuration Manager for EDAA"
/opt/InCharge/IP/smarts/bin/sm_server
--name=INCHARGE-CM
--config=icf-c
--bootstrap=bootstrap.conf
--port=0
--edaa=ip/2.0
--ignore-restore-errors
--nodx
--output
```

sm_service install command for IP Availability Manager

```
/opt/InCharge/IP/smarts/bin/sm_service install
--force
--name=ic-am-server
"--description= EMC Smarts IP Availability Manager Server"
--startmode=runonce
/opt/InCharge/IP/smarts/bin/sm_server
--name=INCHARGE-AM
--config=icf
--bootstrap=bootstrap-am.conf
--port=0
--edaa=ip/2.0
--ignore-restore-errors
--output
```

sm_service install command for IP Performance Manager

```
/opt/InCharge/IP/smarts/bin/sm_service install
--force
--name=ic-pm-server
```

```
"--description= EMC Smarts IP Performance Manager Server"
--startmode=runonce
/opt/InCharge/IP/smarts/bin/sm_server
--name=INCHARGE-PM
--config=icf
--bootstrap=bootstrap-pm.conf
--port=0
--edaa=ip/2.0
--ignore-restore-errors
--output
```

sm_service install command for IP Availability-Performance Manager

```
/opt/InCharge/IP/smarts/bin/sm_service install
--force
--name=ic-am-pm-server
"--description= EMC Smarts IP Availability Manager and Performance
Manager Server"
--startmode=runonce
/opt/InCharge/IP/smarts/bin/sm_server
--name=INCHARGE-AM-PM
--config=icf
--bootstrap=bootstrap-am-pm.conf
--port=0
--edaa=ip/2.0
--ignore-restore-errors
--output
```

sm_service install commands for Windows

The `sm_service install` command for products that interoperate with the EMC M&R User Interface includes additional options. Before you start the service, if you have not already done so, you need to issue the `sm_service install` command from the `/opt/InCharge/IP/smarts/bin` directory to register the product with the EMC Smarts Broker.

sm_service install command for Configuration Manager
As a prerequisite, the Configuration Manager is already running.

```
C:\InCharge\IP\smarts\bin\sm_service install --force
--unmanaged
--startmode=runonce
--name=ic-ip-configuration-edaa
"--description=EMC Smarts IP Configuration Manager for EDAA"
C:\InCharge\IP\smarts\bin\sm_server.exe
"--name=INCHARGE-CM"
"--config=icf-c"
"--bootstrap=bootstrap.conf"
"--port=0"
"--edaa=ip\2.0"
"--ignore-restore-errors "
"--nodx "
"--output"
```

sm_service install command for IP Availability Manager

```
C:\InCharge\IP\smarts\bin\sm_service install
--force
--name=ic-am-server
"--description= EMC Smarts IP Availability Manager Server"
--startmode=runonce
C:\InCharge\IP\smarts\bin\sm_server.exe
```

```
"--name=INCHARGE-AM"
"--config=icf"
"--bootstrap=bootstrap-am.conf"
"--port=0"
"--edaa=ip\2.0"
"--ignore-restore-errors"
"--output"
```

sm_service install command for IP Performance Manager

```
C:\InCharge\IP\smarts\bin\sm_service install
--force
--name=ic-pm-server
"--description= EMC Smarts IP Performance Manager Server"
--startmode=runonce
C:\InCharge\IP\smarts\bin\sm_server.exe
"--name=INCHARGE-PM"
"--config=icf"
"--bootstrap=bootstrap-pm.conf"
"--port=0"
"--edaa=ip\2.0"
"--ignore-restore-errors"
"--output"
```

sm_service install command for IP Availability-Performance Manager

```
C:\InCharge\IP\smarts\bin\sm_service install
--force
--name=ic-am-pm-server
"--description= EMC Smarts IP Availability Manager and Performance
Manager Server"
--startmode=runonce
C:\InCharge\IP\smarts\bin\sm_server.exe
"--name=INCHARGE-AM-PM"
"--config=icf"
"--bootstrap=bootstrap-am-pm.conf"
"--port=0"
"--edaa=ip\2.0"
"--ignore-restore-errors"
"--output"
```

Copyright © 2015 EMC Corporation. All rights reserved. Published in USA.

Published January, 2015

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (https://support.emc.com).