# Monitoring IBM MQ

*IBM: MQ* PowerPack version 104

# Table of Contents

# Chapter

# 1

# Introduction

## Overview

This manual describes how to monitor IBM MQ messaging systems in SL1 using the *IBM: MQ* PowerPack.

The following sections provide an overview of IBM MQ and the *IBM: MQ* PowerPack:

This chapter covers the following topics:

**NOTE:** ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

## What is IBM MQ?

The IBM MQ is message-queing middleware that supports messaging between applications, systems, services, and files. An IBM MQ messaging system is made up of one or more queue managers that support asynchronous routing of messages between systems, with producing and consuming applications connected to different queue managers.

# What Does the IBM: MQPowerPack Monitor?

To monitor IBM MQ messaging systems using SL1, you must install the *IBM: MQ* PowerPack. This PowerPack enables you to discover, model, and collect data about IBM MQ messaging systems.

The *IBM: MQ* PowerPack includes:

- Example credentials you can use as a template to create a PowerShell credential, a SOAP/XML credential, or an SSH/Key credential to connect to the IBM MQ messaging system you want to monitor
- Dynamic Applications to discover, model, and monitor performance metrics and collect configuration data for IBM MQ messaging systems
- Device classes for the IBM MQ components that the SL1 monitors
- Event policies and corresponding alerts that are triggered when IBM MQ systems meet certain status criteria

# Installing the IBM: MQ PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *IBM: MQ* PowerPack.

> **TIP:** By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. For more information, see the section on ***Global Settings***.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the ScienceLogic Support Site.
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

# Chapter

# 2

# Configuration and Discovery

## Overview

The following sections describe how to configure and discover IBM MQ messaging systems for monitoring by SL1 using the *IBM: MQ* PowerPack:

This chapter covers the following topics:

## Prerequisites for Monitoring IBM MQ

To configure the SL1 system to monitor IBM MQ messaging systems using the *IBM: MQ* PowerPack, you must first perform the following:

- *Install the IBM MQ PowerShell Snap-in for Monitoring on Windows Servers*
- Give all SSH credential users the "mqm" group permission

# Installing the IBM MQ PowerShell Snap-In for Monitoring on Windows Servers

**NOTE:** Users monitoring MQ on Linux servers do not need to perform these steps.

**NOTE:** On 64-bit versions of Microsoft Windows, both 32-bit and 64-bit versions of Windows PowerShell are installed. SL1's collection processes using Windows PowerShell will default to using the version of powershell.exe whose folder exists first in the PATH environment variable. Because this will vary from system to system, these steps ensure the WebSphereMQ.dll file is registered for both Windows PowerShell environments.

1. Download the Windows PowerShell library package (mo74.zip) for IBM MQ.
2. Extract the contents of the zip file to your Windows server, and find the "manual" subfolder from the extracted files (under the mo74_v2.0.1_x86_x64 folder). Create a new folder on your desktop and move the files in the "manual" subfolder to that folder.
3. Register the IBM WebSphere MQ library for use by both 32-bit and 64-bit Windows PowerShell. To do this:

   - Start a 32-bit Windows PowerShell console window (this will be the Windows PowerShell (x86) application if running on a 64-bit version of Microsoft Windows) using "Run as adminstrator", run the following:

     ```
     %WINDIR%\Microsoft.NET\Framework\v4.0.30319\installutil <Directory
     where WebsphereMQ.dll resides>\WebSphereMQ.dll
     ```

   - Start a 64-bit Windows PowerShell console window (this will be the Windows PowerShell application without (x86) in its program name on a 64-bit version of Microsoft Windows) using "Run as adminstrator" and run the following:

     ```
     %WINDIR%\Microsoft.NET\Framework64\v4.0.30319\installutil <Directory
     where WebsphereMQ.dll resides>\WebSphereMQ.dll
     ```

4. Open your Windows PowerShell console and add the WebSphere MQ for PowerShell snap-in by running the following command:

   ```
   Add-PSSnapin IBM.PowerShell.WebSphereMQ
   ```

# Creating a Credential for IBM: MQ Guided Discovery

To allow SL1 to discover IBM MQ messaging systems with guided discovery, you must first create a IBM: MQ credential. This credential allows the Dynamic Applications in the *IBM: MQ* PowerPack to connect with an IBM MQ system.

**NOTE**: This IBM: MQ credential should only be used with IBM: MQ guided discovery.

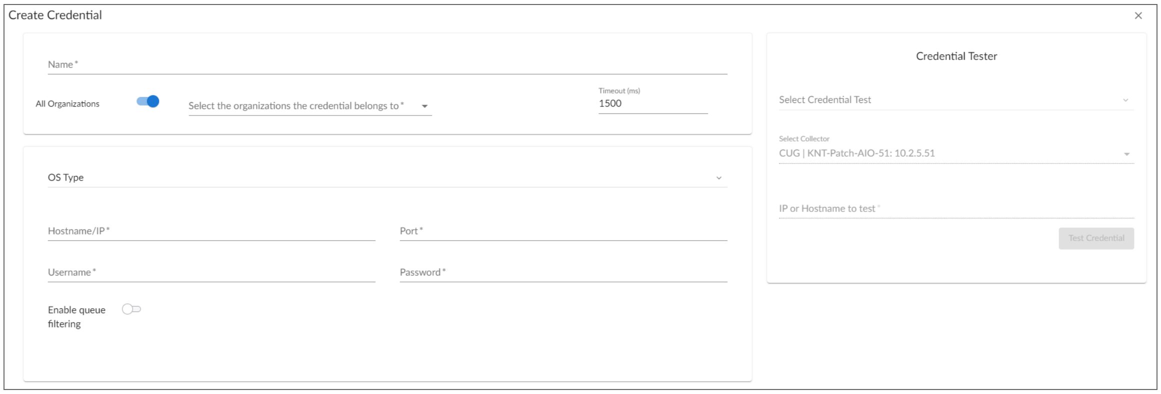
To configure a credential to access an IBM: MQ system for guided discovery:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click the **[Create New]** button and select *Create Ibm mq Credential*. The **Create Credential** modal page appears.
3. Enter values in the following fields:
   - ***Name***. Type a name for the credential.
   - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations. This field is required.
   - ***OS Type***. Select the operating system type (Linux/AIX or Windows) you want to discover in the drop-down field. This field is required.
   - ***Hostname/IP***. Type the IP address where the database resides. This field is required.

     **NOTE**: The Hostname and %D are not supported.

   - ***Port***. Type the Port number associated with the database you want to access with this credential. This field is required.
   - ***Username***. Type the username for a user with administrator access to the IBM: MQ messaging system.
   - ***Password***. Type the password for the IBM: MQ system account username.
   - ***PowerShell Encrypted***. This field is only required for Windows operating systems. Select whether SL1 will communicate with the device using an encrypted connection. Choices are:
     - ***Toggle on (blue)***. When communicating with the Windows server, SL1 will use a local user account with authentication type "Basic Auth". You must then use HTTPS and can choose to use a Microsoft Certificate or a self-signed certificate.
     - ***Toggle off (gray)***. When communicating with the Windows server, SL1 will not encrypt the connection.

- ***PowerShell Proxy Hostname/IP***. Optional.This field is only required for Windows operating systems. If you use a proxy server in front of the Windows devices you want to communicate with, type the fully-qualified domain name or the IP address of the proxy server in this field.
- ***Use Sudo***. This field is only required for Linux/AIX operating systems. Toggle on (blue) to discover a Linux user with `sudo` privileges, otherwise toggle off (gray).
- ***Use Kornshell (AIX)***. This field is only required for Linux/AIX operating systems. Toggle on (blue) to discover AIX, otherwise toggle off (gray).
- ***Private Key***. This field is only required for Linux/AIX operating systems. Paste the SSH private key that you want SL1 to use, in PEM format.
- ***Enable queue filtering***. Toggle on (blue) to select a filter for including or excluding queues, or toggle off (gray) if you do not want to filter queues. See ***Enable Queue Filtering*** for more information.



Timeout (ms): 1500

Select Collector: CUG | KNT-Patch-AIO-51: 10.2.5.51

4. Click **[Save & Close]**.

## Enable Queue Filtering

Queue managers can be included or excluded in the discovery. To filter Queue results with "Include" or "Exclude" filter type, list the Queue Managers separated with comma, percent sign (%), colon, or space; No wildcard is allowed (*). The following Regex are allowed to filter Queues:

### Linux/AIX Operating System

- ***Include filter type***. Include exactly what is provided. If you provide only a Queue manager, only the Queue manager will be discovered without any queues.

  **Queue Names Examples:**

  `QUEUE_MANAGER:{queue_name1,queue_name2}`. Includes the Queue manager along with specified queues.

  `QUEUE_MANAGER1,QUEUE_MANAGER2`. Includes only Queue managers; queues will not be discovered.

- ***Exclude filter type***. Excludes only Queue managers; does not exclude queues.

  **Queue Name Examples:**

  `QUEUE_MANAGER1,QUEUE_MANAGER2,QUEUE_MANAGER3`

  `QUEUE_MANAGER1:QUEUE_MANAGER2:QUEUE_MANAGER3`

  `QUEUE_MANAGER1%QUEUE_MANAGER2%QUEUE_MANAGER3`

  `QUEUE_MANAGER1 QUEUE_MANAGER2 QUEUE_MANAGER3`

**Windows Operating Systems**

- ***Include filter type***. If a Queue manager is provided, the manager will be discovered along with its queues.

  **Queues Name Examples:**

  `QUEUE_MANAGER:{}` . Includes Queue managers and queues.

  `QUEUE_MANAGER:{queue_name1,queue_name2}`. Include the Queue manager along with specified queues.

  `QUEUE_MANAGER1,QUEUE_MANAGER2,QUEUE_MANAGER3`

- ***Exclude filter type***. Excludes only Queue managers; does not exclude queues.

  **QueuesName Examples:**

  `QUEUE_MANAGER1:QUEUE_MANAGER2:QUEUE_MANAGER3`

  `QUEUE_MANAGER1,QUEUE_MANAGER2,QUEUE_MANAGER3`

  `QUEUE_MANAGER1%QUEUE_MANAGER2%QUEUE_MANAGER3`

  `QUEUE_MANAGER1 QUEUE_MANAGER2 QUEUE_MANAGER3`

# Creating a PowerShell Credential for IBM MQ on Windows Systems

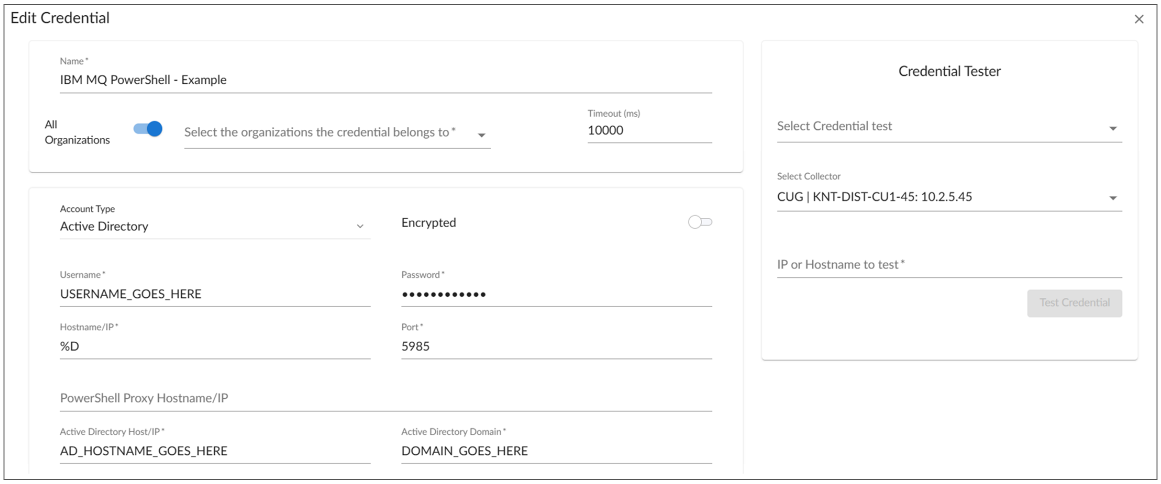
To configure SL1 to monitor IBM MQ messaging systems on Windows systems, you must first create a PowerShell credential. This credential allows the Dynamic Applications in the *IBM: MQ* PowerPack to connect with an IBM MQ system.

The PowerPack includes an example PowerShell credential that you can edit for your own use.

NOTE: If you are using an SL1 system prior to version 11.1.0, the new user interface does not include the ***Duplicate*** option for sample credential(s). ScienceLogic recommends that you use ***the classic user interface and the Save As button*** to create new credentials from sample credential(s). This will prevent you from overwriting the sample credential(s).

To configure a PowerShell credential to access an IBM MQ system:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the **IBM MQ PowerShell - Example** sample credential, click its **[Actions]** icon (⋯) and select ***Duplicate***. A copy of the credential, called **IBM MQ PowerShell - Example copy** appears.
3. Click the **[Actions]** icon (⋯) for the **IBM MQ PowerShell - Example copy** credential and select ***Edit***. The **Edit Credential** modal page appears.



Edit Credential

Name *
IBM MQ PowerShell - Example

All Organizations ●
Select the organizations the credential belongs to *

Timeout (ms)
10000

Account Type
Active Directory

Encrypted ○

Username *
USERNAME_GOES_HERE

Password *
••••••••••••

Hostname/IP *
%D

Port *
5985

PowerShell Proxy Hostname/IP

Active Directory Host/IP *
AD_HOSTNAME_GOES_HERE

Active Directory Domain *
DOMAIN_GOES_HERE

Credential Tester

Select Credential test

Select Collector
CUG | KNT-DIST-CU1-45: 10.2.5.45

IP or Hostname to test *

4. Supply values in the following fields:
   - ***Name***. Type a new name for the credential.
   - ***Hostname/IP***. Keep the default value.
   - ***Username***. Type the username for a user with administrator access to the IBM MQ messaging system.
   - ***Password***. Type the password for the IBM MQ system account username.
   - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the **What organization manages this service?** drop-down field to align the credential with those specific organizations. This field is required.
   - ***Account Type***. Type of authentication for the username and password in this credential. Choices are:
     - *Active Directory*. On the Windows device, Active Directory will authenticate the username and password in this credential.
     - *Local*. Local security on the Windows device will authenticate the username and password in this credential.

   - ***Encrypted***. Select whether SL1 will communicate with the device using an encrypted connection. Choices are:
     - Toggle on (blue). When communicating with the Windows server, SL1 will use a local user account with authentication of type "Basic Auth". You must then use HTTPS and can choose to use a Microsoft Certificate or a self-signed certificate.
     - Toggle off (gray). When communicating with the Windows server, SL1 will not encrypt the connection.
   - ***Port***. Type the port name used by the WinRM service on the Windows device. This field is required and is automatically populated with the default port based on the value you selected.
   - ***PowerShell Proxy Hostname/IP***. If you use a proxy server in front of the Windows devices you want to communicate with, type the fully-qualified domain name or the IP address of the proxy server in this field.
   - ***Active Directory Hostname/IP***. If you selected Active Directory in the **Account Type** field, type the hostname or IP address of the Active Directory server that will authenticate the credential.
   - ***Active Directory Domain***. If you selected Active Directory in the **Account Type** field, type the domain where the monitored Windows device resides.

5. Click **[Save & Close]**.

## Creating a PowerShell Credential for IBM MQ on Windows Systems in the Classic SL1 User Interface

To configure SL1 to monitor IBM MQ messaging systems on Windows systems, you must first create a PowerShell credential. This credential allows the Dynamic Applications in the *IBM: MQ* PowerPack to connect with an IBM MQ system.

The PowerPack includes an example PowerShell credential that you can edit for your own use.

To configure a PowerShell credential to access an IBM MQ system:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **IBM MQ PowerShell - Example** credential, then click its wrench icon (🔧). The **Edit PowerShell Credential** modal page appears.
3. Complete the following fields:
   - ***Credential Name***. Type a new name for the credential.
   - ***Hostname/IP***. Keep the default value.
   - ***Username***. Type the username for a user with administrator access to the IBM MQ messaging system.
   - ***Password***. Type the password for the IBM MQ system account username.
   - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the **What organization manages this service?** drop-down field to align the credential with those specific organizations. This field is required.

- ***Account Type***. Type of authentication for the username and password in this credential. Choices are:
    - *Active Directory*. On the Windows device, Active Directory will authenticate the username and password in this credential.
    - *Local*. Local security on the Windows device will authenticate the username and password in this credential.
- ***Encrypted***. Select whether SL1 will communicate with the device using an encrypted connection. Choices are:
    - Toggle on (blue). When communicating with the Windows server, SL1 will use a local user account with authentication of type "Basic Auth". You must then use HTTPS and can choose to use a Microsoft Certificate or a self-signed certificate.
    - Toggle off (gray). When communicating with the Windows server, SL1 will not encrypt the connection.
- ***Port***. Type the port name used by the WinRM service on the Windows device. This field is required and is automatically populated with the default port based on the value you selected.
- ***PowerShell Proxy Hostname/IP***. If you use a proxy server in front of the Windows devices you want to communicate with, type the fully-qualified domain name or the IP address of the proxy server in this field.
- ***Active Directory Hostname/IP***. If you selected Active Directory in the **Account Type** field, type the hostname or IP address of the Active Directory server that will authenticate the credential.
- ***Active Directory Domain***. If you selected Active Directory in the **Account Type** field, type the domain where the monitored Windows device resides.

4. Click the **[Save As]** button.

# Creating an SSH/Key Credential for IBM MQ on Linux Systems

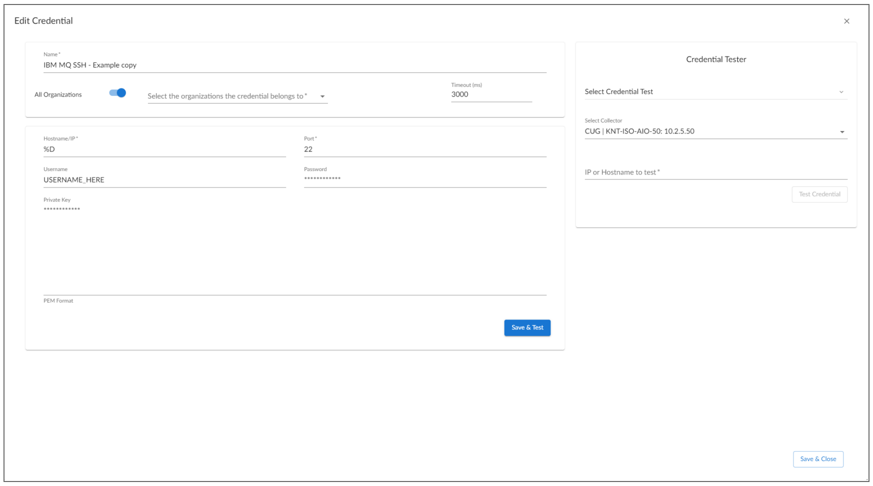
To configure SL1 to monitor IBM MQ messaging systems on Linux systems, you must first create an SSH/Key credential. This credential allows the Dynamic Applications in the *IBM: MQ* PowerPack to connect with an IBM MQ system.

The PowerPack includes an example SSH/Key credential that you can edit for your own use.

**NOTE**: If you are using an SL1 system prior to version 11.1.0, the new user interface does not include the ***Duplicate*** option for sample credential(s). ScienceLogic recommends that you use ***the classic user interface and the Save As button*** to create new credentials from sample credential(s). This will prevent you from overwriting the sample credential(s).

To configure an SSH/Key credential to access an IBM MQ system:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the **IBM MQ SSH - Example** sample credential, click its **[Actions]** icon ( … ) and select ***Duplicate***. A copy of the credential, called **IBM MQ SSH - Example copy** appears.
3. Click the **[Actions]** icon ( … ) for the **IBM MQ SSH - Example copy** credential and select ***Edit***. The **Edit Credential** modal page appears.



Name *: IBM MQ SSH - Example copy

All Organizations: Select the organizations the credential belongs to *

Timeout (ms): 3000

Hostname/IP *: %D

Port *: 22

Username: USERNAME_HERE

Password: ************

Private Key: ************

PEM Format

Select Credential Test

Select Collector: CUG | KNT-ISO-AIO-50: 10.2.5.50

IP or Hostname to test *

4. Supply values in the following fields:
    - ***Name***. Type a new name for the credential.
    - ***Hostname/IP***. Keep the default value.
    - ***Username***. Type the username for a user with administrator access, and who is a member of the "mgm" group, to the IBM MQ messaging system.
    - ***Password***. Type the password for the IBM MQ system account username.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the **What organization manages this service?** drop-down field to align the credential with those specific organizations. This field is required.
    - ***Port***. Type the port number associated with the data you want to retrieve.

**NOTE:** The default TCP port for SSH servers is 22.

- ***Private key***. Paste the SSH private key that you want SL1 to use, in PEM format.

**NOTE:** The private key can have a maximum of 64 characters per line. Therefore, you cannot use keys in the OpenSSH format, because that format uses 70 characters per line. When you attempt to save the credential, SL1 will validate that the private key entered is in the correct format. You will be able to save the credential only if the private key is correctly formatted.

5. Click **[Save & Close]**.

## Creating an SSH/Key Credential for IBM MQ on Linux Systems in the SL1 Classic User Interface

To configure SL1 to monitor IBM MQ messaging systems on Linux systems, you must first create an SSH/Key credential. This credential allows the Dynamic Applications in the *IBM: MQ* PowerPack to connect with an IBM MQ system.

The PowerPack includes an example SSH/Key credential that you can edit for your own use.

To configure an SSH/Key credential to access an IBM MQ system:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **IBM MQ SSH - Example** credential, then click its wrench icon (🔧). The **Edit SSH/Key Credential** modal page appears:
3. Complete the following fields:

    - ***Credential Name***. Type a new name for the credential.
    - ***Hostname/IP***. Keep the default value.
    - ***Username***. Type the username for a user with administrator access, and who is a member of the "mgm" group, to the IBM MQ messaging system.
    - ***Password***. Type the password for the IBM MQ system account username.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the **What organization manages this service?** drop-down field to align the credential with those specific organizations. This field is required.
    - ***Port***. Type the port number associated with the data you want to retrieve.

**NOTE:** The default TCP port for SSH servers is 22.

- ***Private key***. Paste the SSH private key that you want SL1 to use, in PEM format.

**NOTE:** The private key can have a maximum of 64 characters per line. Therefore, you cannot use keys in the OpenSSH format, because that format uses 70 characters per line. When you attempt to save the credential, SL1 will validate that the private key entered is in the correct format. You will be able to save the credential only if the private key is correctly formatted.

4. Click the **[Save As]** button.

## Creating a SOAP/XML Credential for IBM MQ on AIX and Linux Systems

To configure SL1 to monitor IBM MQ messaging systems on your AIX and Linux systems, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *IBM: MQ* PowerPack to connect with an IBM MQ system.

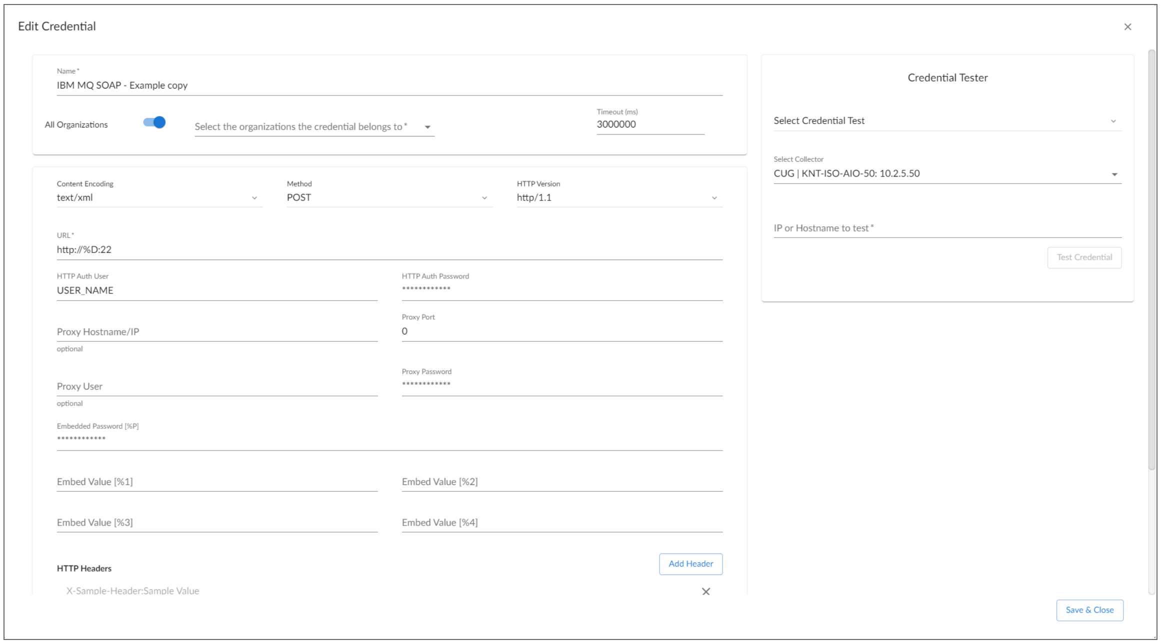
**NOTE**: You are only required to create SOAP/XML credential for your Linux system if you want to utilize the Kornshell. If you want to use the sudo commands for your Linux systems, ScienceLogic recommends you use the Universal Credential.

The PowerPack includes an example SOAP/XML credential that you can edit for your own use.

**NOTE**: If you are using an SL1 system prior to version 11.1.0, the new user interface does not include the ***Duplicate*** option for sample credential(s). ScienceLogic recommends that you use ***the classic user interface and the Save As button*** to create new credentials from sample credential(s). This will prevent you from overwriting the sample credential(s).

To configure a SOAP/XML credential to access an IBM MQ system:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the **IBM MQ SOAP - Example** sample credential, click its **[Actions]** icon (⋯) and select ***Duplicate***. A copy of the credential, called **IBM MQ SOAP - Example copy** appears.
3. Click the **[Actions]** icon (⋯) for the **IBM MQ SOAP - Example copy** credential and select ***Edit***. The **Edit Credential** modal page appears.



Edit Credential

Name *: IBM MQ SOAP - Example copy

All Organizations: ●

Select the organizations the credential belongs to *

Timeout (ms): 3000000

Content Encoding: text/xml

Method: POST

HTTP Version: http/1.1

URL *: http://%D:22

HTTP Auth User: USER_NAME

HTTP Auth Password: ************

Proxy Hostname/IP (optional)

Proxy Port: 0

Proxy User (optional)

Proxy Password: ************

Embedded Password [%P]: ************

Embed Value [%1]

Embed Value [%2]

Embed Value [%3]

Embed Value [%4]

HTTP Headers

X-Sample-Header:Sample Value

Credential Tester

Select Credential Test

Select Collector: CUG | KNT-ISO-AIO-50: 10.2.5.50

IP or Hostname to test *

4. Supply values in the following fields:

    - ***Name***. Type a new name for the credential.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the **What organization manages this service?** drop-down field to align the credential with those specific organizations.
    - ***URL***. Keep the default value.
    - ***HTTP Auth User***. Type the username for a user with administrator access to the IBM MQ messaging system.
    - ***HTTP Auth Password***. Type the password for the IBM MQ system account username.

### HTTP Headers

- ***HTTP Headers***. The following headers can be entered to use KornShell and sudo. Create a separate header for each feature:
    - KORNSHELL
    - SUDO

5. For all remaining fields, use the default values.
6. Click **[Save & Close]** .

## Creating a SOAP/XML Credential for IBM MQ on AIX and Linux Systems in the Classic SL1 User Interface

To configure SL1 to monitor IBM MQ messaging systems on your AIX and Linux systems, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *IBM: MQ* PowerPack to connect with an IBM MQ system.

The PowerPack includes an example SOAP/XML credential that you can edit for your own use.

To configure a SOAP/XML credential to access an IBM MQ system:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **IBM MQ SOAP - Example** credential, then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears:
3. Complete the following fields:

   **Basic Settings**

   - ***Profile Name***. Type a new name for the credential.
   - ***URL***. Keep the default value.
   - ***HTTP Auth User***. Type the username for a user with administrator access to the IBM MQ messaging system.
   - ***HTTP Auth Password***. Type the password for the IBM MQ system account username.

   **HTTP Headers**

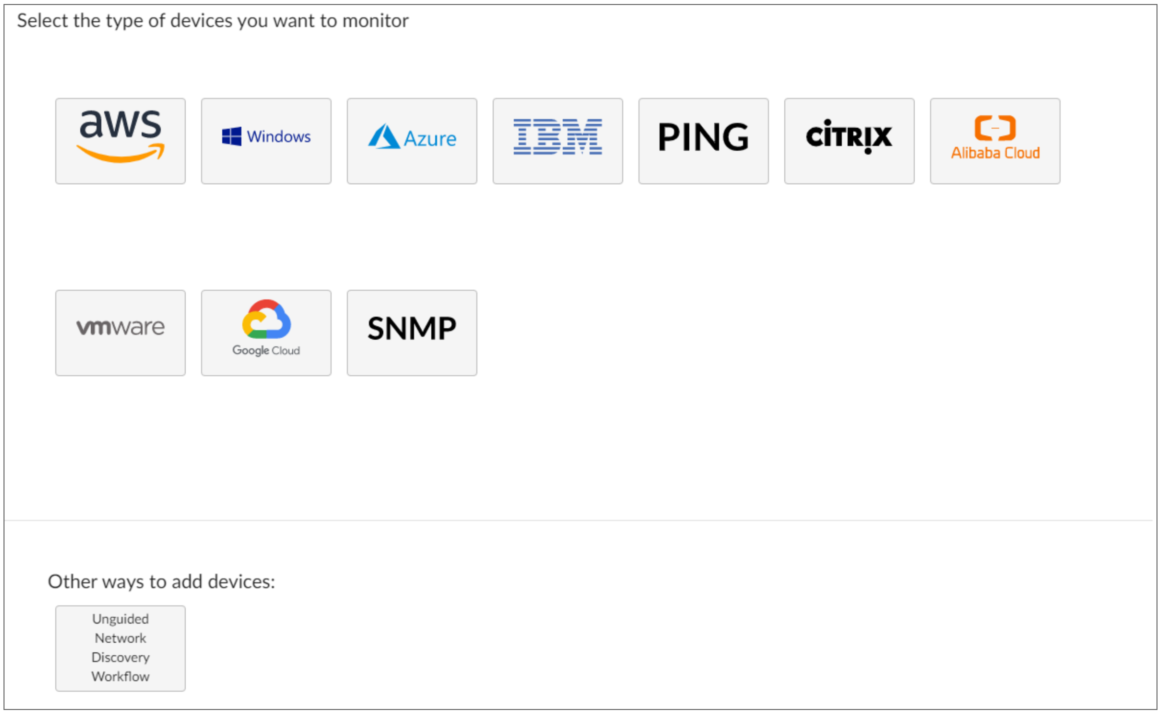
   - ***HTTP Headers***. The following headers can be entered to use KornShell and sudo. Create a separate header for each feature:
     - KORNSHELL
     - SUDO
4. Click the **[Save As]** button.

# IBM: MQ Guided Discovery

You can use the Guided Discovery Framework process in SL1to guide you through a variety of existing discovery types in addition to traditional SNMP discovery. This process, which is also called "guided discovery", lets you choose a discovery type based on the type of devices you want to monitor. The Guided Discovery workflow includes a button for IBM: MQ.

To run a Guided Discovery:

1. On the **Devices** page (🖥) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears.



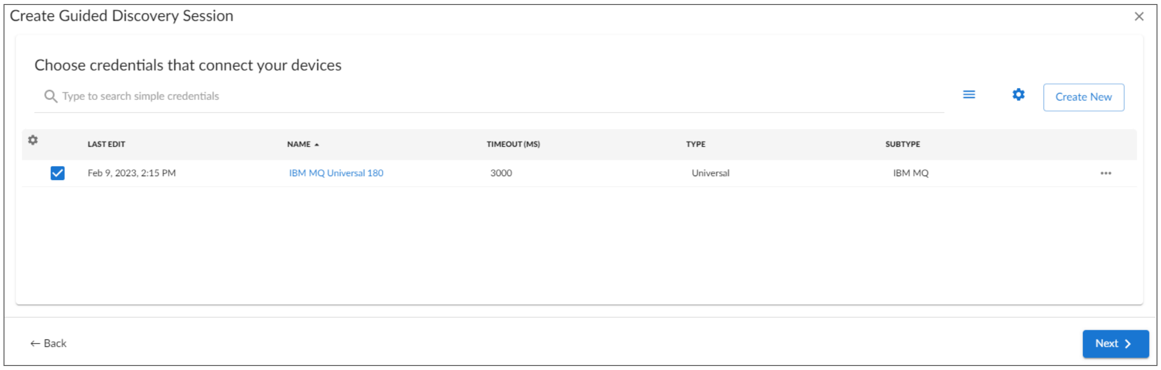
Select the type of devices you want to monitor

Other ways to add devices:

2. Select the **[IBM]** button. Then select the *IBM: MQ* radio button. Additional information about the requirements for device discovery appears in the **General Information** pane to the right.

3. Click **[Select]**. The **Credential Selection** page appears.

> NOTE: Only credentials created for guided discovery will display on the **Credential Selection** page, and you can only use those credentials for guided discovery.



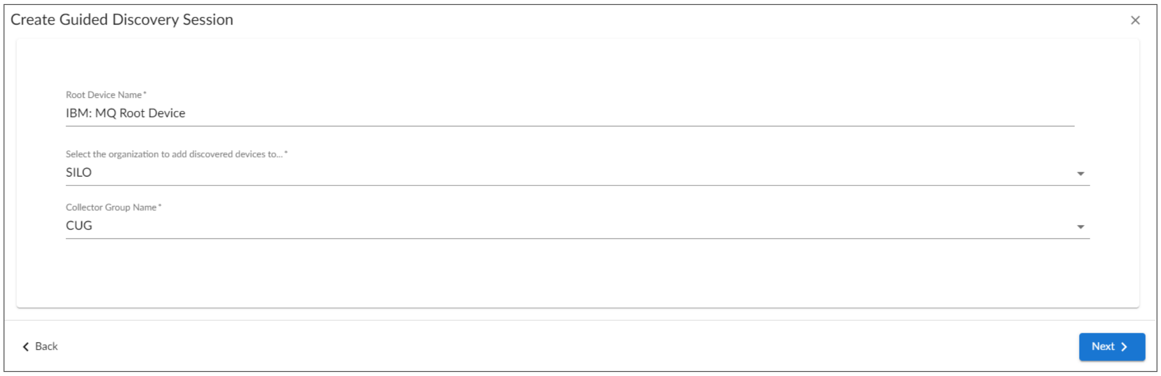
Create Guided Discovery Session

Choose credentials that connect your devices

| | LAST EDIT | NAME ▲ | TIMEOUT (MS) | TYPE | SUBTYPE | |
|---|---|---|---|---|---|---|
| ☑ | Feb 9, 2023, 2:15 PM | IBM MQ Universal 180 | 3000 | Universal | IBM MQ | ••• |

NOTE: During the guided discovery process, you cannot click **[Next]** until the required fields are filled on the page, nor can you skip to future steps. However, you can revisit previous steps that you have already completed.

4. On the **Credential Selection** page of the guided discovery process, select the IBM: MQ credential that you configured, and then click **[Next]**. The **Root Device Details** page appears.



Create Guided Discovery Session

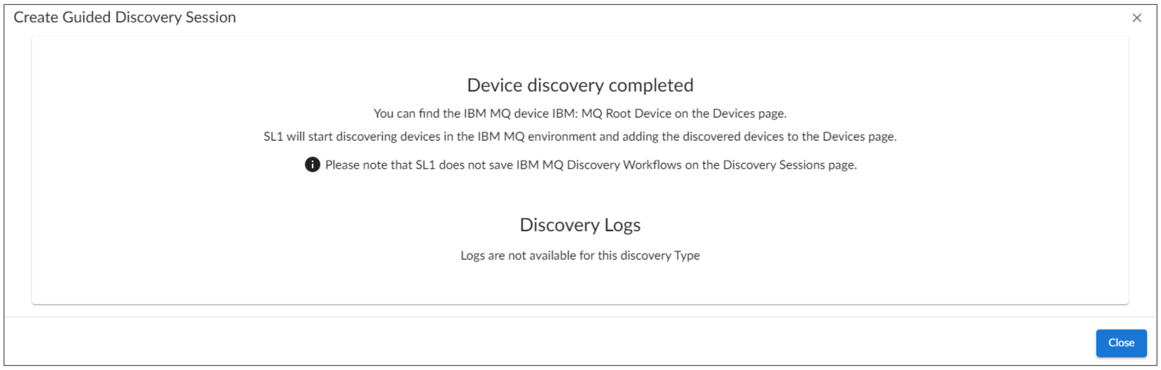
Root Device Name*
IBM: MQ Root Device

Select the organization to add discovered devices to...*
SILO

Collector Group Name*
CUG

5. Complete the following fields:
   - ***Root Device Name***. Type the name of the root device for the IBM: MQ root device you want to monitor.
   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered device.
   - ***Collector Group Name***. Select an existing collector group to communicate with the discovered device. This field is required.

6. Click **[Next]**. SL1 creates the IBM: MQ root device with the appropriate Device Class assigned to it and aligns the relevant Dynamic Applications. The **Final Summary** page appears.



Create Guided Discovery Session

Device discovery completed

You can find the IBM MQ device IBM: MQ Root Device on the Devices page.

SL1 will start discovering devices in the IBM MQ environment and adding the discovered devices to the Devices page.

Please note that SL1 does not save IBM MQ Discovery Workflows on the Discovery Sessions page.

Discovery Logs

Logs are not available for this discovery Type

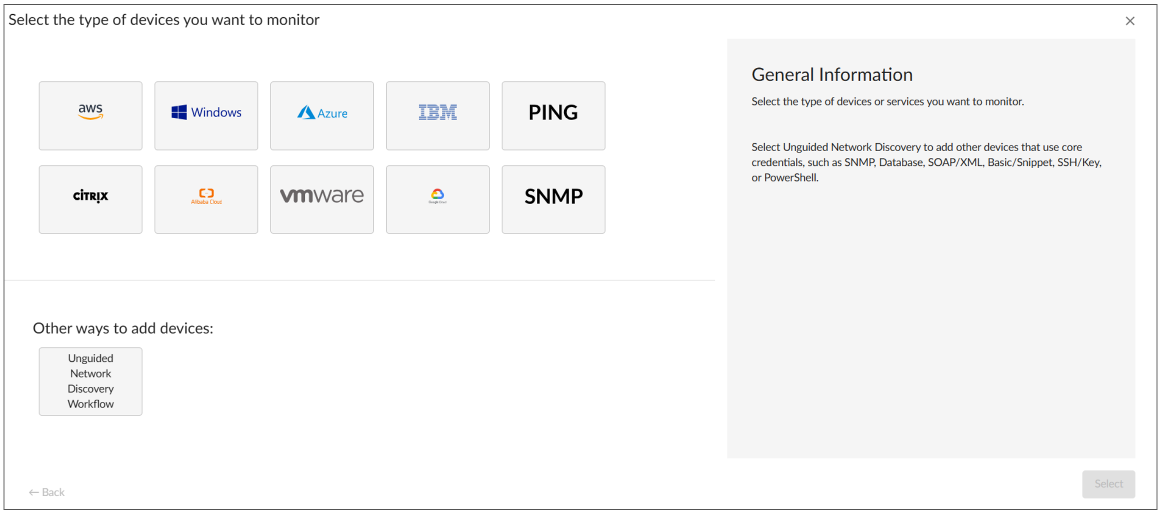
7. Click **[Close]**.

**NOTE:** The results of a guided discovery do not display on the **Discovery Sessions** page (Devices > Discovery Sessions).

# Discovering IBM MQ Component Devices

To discover an IBM MQ messaging system:

1. On the **Devices** page (🖥) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



Select the type of devices you want to monitor

General Information

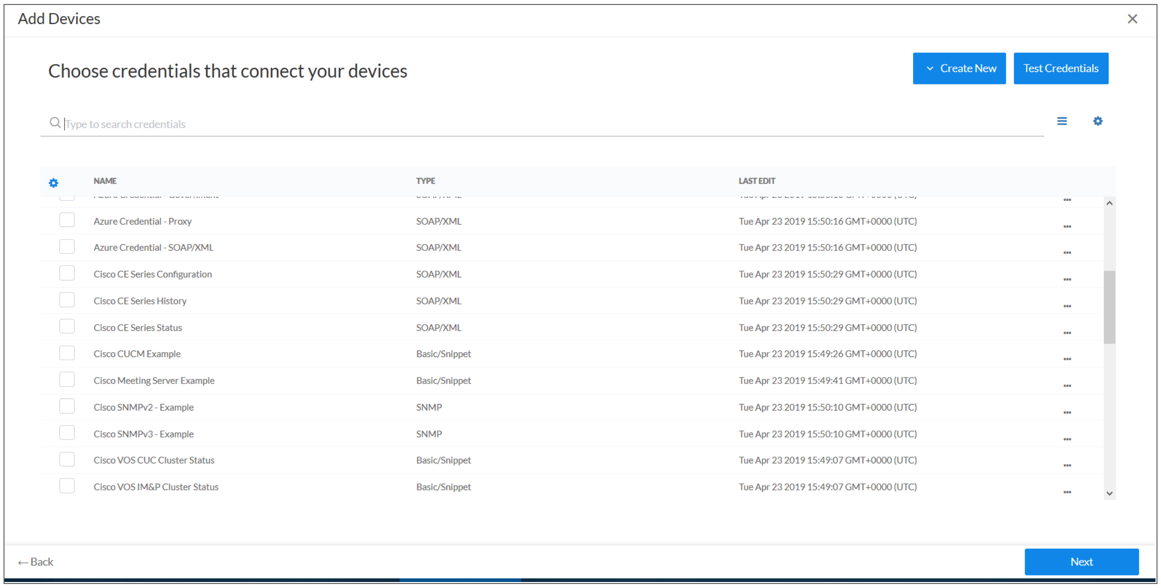
Select the type of devices or services you want to monitor.

Select Unguided Network Discovery to add other devices that use core credentials, such as SNMP, Database, SOAP/XML, Basic/Snippet, SSH/Key, or PowerShell.

2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** page appears.
4. Complete the following fields:

   - ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
   - ***Description***. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.
   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices.

5. Click **[Next]**. The **Credentials** page of the **Add Devices** wizard appears:

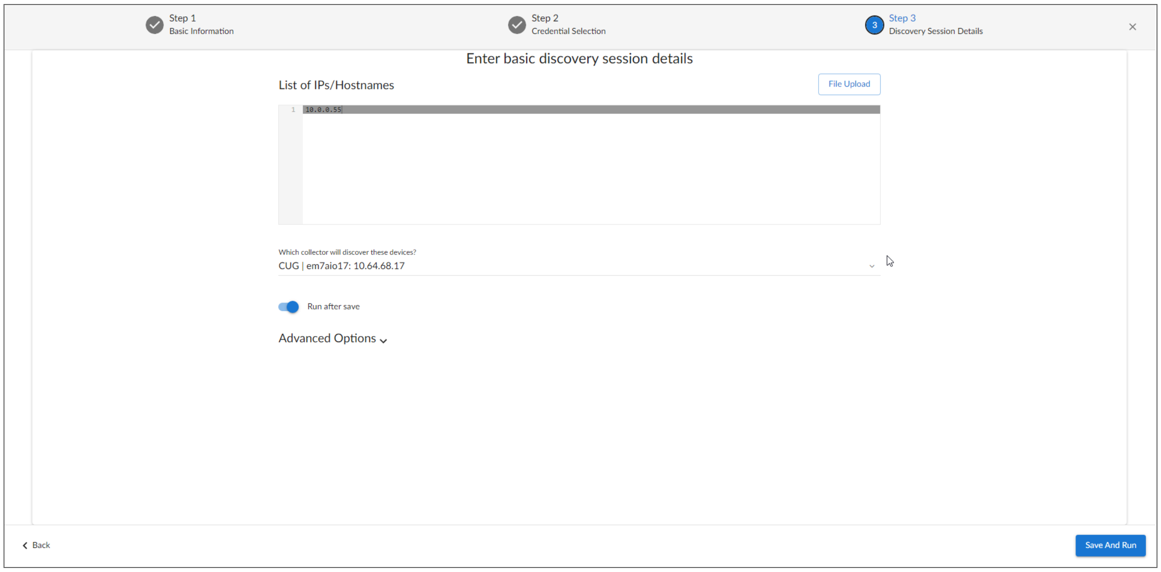


Add Devices

Choose credentials that connect your devices

|  | NAME | TYPE | LAST EDIT |  |
|---|---|---|---|---|
| □ | Azure Credential - Proxy | SOAP/XML | Tue Apr 23 2019 15:50:16 GMT+0000 (UTC) | ... |
| □ | Azure Credential - SOAP/XML | SOAP/XML | Tue Apr 23 2019 15:50:16 GMT+0000 (UTC) | ... |
| □ | Cisco CE Series Configuration | SOAP/XML | Tue Apr 23 2019 15:50:29 GMT+0000 (UTC) | ... |
| □ | Cisco CE Series History | SOAP/XML | Tue Apr 23 2019 15:50:29 GMT+0000 (UTC) | ... |
| □ | Cisco CE Series Status | SOAP/XML | Tue Apr 23 2019 15:50:29 GMT+0000 (UTC) | ... |
| □ | Cisco CUCM Example | Basic/Snippet | Tue Apr 23 2019 15:49:26 GMT+0000 (UTC) | ... |
| □ | Cisco Meeting Server Example | Basic/Snippet | Tue Apr 23 2019 15:49:41 GMT+0000 (UTC) | ... |
| □ | Cisco SNMPv2 - Example | SNMP | Tue Apr 23 2019 15:50:10 GMT+0000 (UTC) | ... |
| □ | Cisco SNMPv3 - Example | SNMP | Tue Apr 23 2019 15:50:10 GMT+0000 (UTC) | ... |
| □ | Cisco VOS CUC Cluster Status | Basic/Snippet | Tue Apr 23 2019 15:49:07 GMT+0000 (UTC) | ... |
| □ | Cisco VOS IM&P Cluster Status | Basic/Snippet | Tue Apr 23 2019 15:49:07 GMT+0000 (UTC) | ... |

6. On the **Credentials** page, locate and select the PowerShell, SOAP/XML, or SSH/Key credential you created for the IBM MQ system.
7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



Enter basic discovery session details

List of IPs/Hostnames

```
10.0.0.55
```

Which collector will discover these devices?
CUG | em7aio17: 10.64.68.17

Run after save

Advanced Options

8. Complete the following fields:

    - ***List of IPs/Hostnames***. Type the IP addresses for the IBM MQ messaging system.
    - ***Which collector will monitor these devices?***. Select an existing collector to monitor the discovered devices. Required.
    - ***Run after save***. Select this option to run this discovery session as soon as you save the session.

    In the **Advanced options** section, click the down arrow icon (⌄) to complete the following fields:

    - ***Discover Non-SNMP***. Enable this setting.
    - ***Model Devices***. Enable this setting.

9. Click **[Save and Run]** if you enabled the Run after save setting, or **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.

## Discovering IBM Component Devices in the SL1 Classic User Interface

To discover an IBM MQ messaging system:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. In the **Discovery Control Panel**, click the **[Create]** button. The **Discovery Session Editor** page appears.
3. In the **Discovery Session Editor** page, complete the following fields:

    - ***Name***. Type a name for the discovery session.
    - ***IP Address/Hostname Discovery List***. Type the IP address for the IBM MQ messaging system.

- ***Other Credentials***. Select the PowerShell or SSH/Key credential you created for the IBM MQ messaging system.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button to save the discovery session and then close the **Discovery Session Editor** window.
6. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon ( ) to run the discovery session.
7. The **Discovery Session** window appears. When the cluster root device(s) are discovered, click the device icon ( ) to view the **Device Properties** page for each device.

# Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, click the device icon for the IBM MQ device ( ). From the **Device Properties** page for the IBM MQ device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the device are automatically aligned during discovery.

**NOTE:** It can take several minutes after the discovery session has completed for Dynamic Applications to appear in the **Dynamic Application Collections** page.

You should see the following Dynamic Applications aligned to the IBM MQ root device:

- IBM: MQ Discovery

**NOTE:** When discovering IBM MQ Component Devices using a discovery session, the Dynamic Applications from the Linux Base Pack and Microsoft: Windows Server PowerPacks may align with Linux and Windows systems, respectively.

You should see the following Dynamic Applications aligned to the IBM MQ server:

- IBM: MQ Queue Manager Discovery
- IBM: MQ Error Log Configuration

You should see the following Dynamic Applications aligned to the IBM MQ queue managers:

- IBM: MQ Cluster Channel Configuration

**NOTE:** For Windows users, in the "IBM: MQ Cluster Channel Configuration" Dynamic Application, when a channel is configured with a cluster and that cluster is deleted, the status for that cluster cannot be returned.

**NOTE:** For Windows users, in the "IBM: MQ Cluster Channel Configuration" Dynamic Application, the "CLUSSDRA" and "CLUSSDRB" are shown as "CLUSSDR".

- IBM: MQ Channel Configuration
- IBM: MQ Queue Discovery
- IBM: MQ Cluster Channel Performance
- IBM: MQ Listener Configuration

**NOTE:** For Windows users, the "IBM: MQ Discovery" Dynamic Application currently does not return "Connections", "Parent Queue Manager", or "Start Date" metrics. On some MQ installations, SL1 may be unable to collect the "Standby Host" property.

- IBM: MQ Queue Manager Configuration

**NOTE:** For Windows users, the "IBM: MQ Queue Manager Configuration" Dynamic Application currently does not return "Connections", "Parent Queue Manager", or "Start Date" metrics.

You should see the following Dynamic Applications aligned to the IBM MQ queues:

- IBM: MQ Queue Configuration
- IBM: MQ Queue Performance

If the listed Dynamic Applications have not been automatically aligned during discovery, you can align them manually. To do so, perform the following steps:

1. Click the **[Action]** button and then select *Add Dynamic Application*. The **Dynamic Application Alignment** page appears:
2. In the ***Dynamic Applications*** field, select the Dynamic Application you want to align.
3. In the ***Credentials*** field, select the appropriate IBM: MQ credential.
4. Click the **[Save]** button.
5. Repeat steps 1-4 for the other unaligned Dynamic Applications.

## Configuring the IBM: MQ Queue Discovery Snippet

The "IBM: MQ Queue Discovery" Dynamic Application snippet allows you to customize the list of queue names and types of queues that SL1 will discover. Up to 20 queue names can be specified, and those names will be discovered under each queue manager where they are found.

For specifying queue types, an integer can be specified as one item in the list, and the allowed values for type are:

1 : Dead letter queue will be discovered

2 : Transmission queues will be discovered

To edit the snippet:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Find the "IBM: MQ Queue Discovery" Dynamic Application and click its wrench icon (🔧).
3. In the **Dynamic Applications Properties Editor**, click the **[Snippets]** tab.
4. In the **Dynamic Applications Snippet Editor & Registry** page, click the wrench icon (🔧) of the "Discover-Queues" snippet.
5. The content of the snippet will appear. Add the following text to the snippet to customize the list of queue names and queue types that can be discovered:

   ```
   QUEUES_TO_DISCOVER = ['<queue name>','<queue name>','<queue type>']
   ```

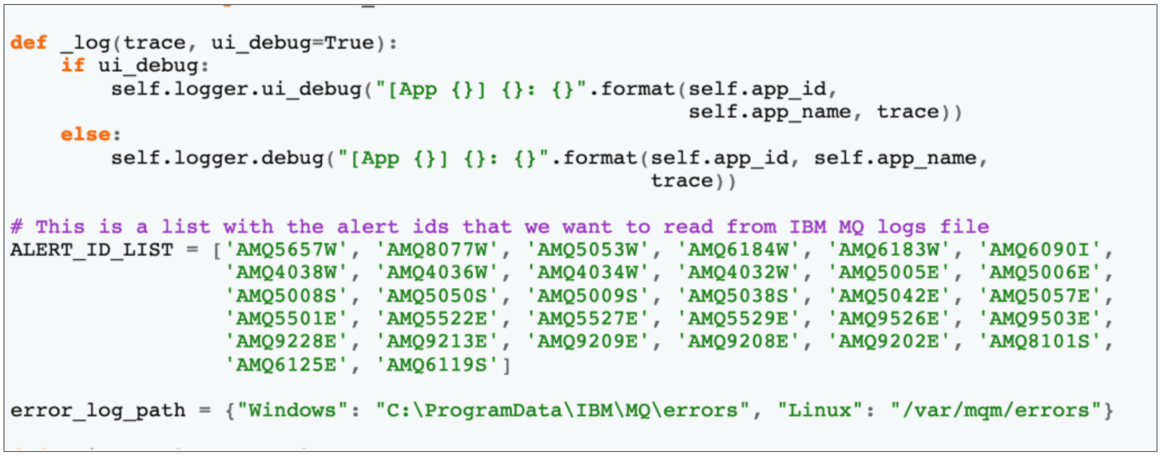
   Use commas to separate queue names and queue types.

## Configuring the IBM: MQ Error Log Configuration Snippet

By default, only some errors are monitored and alerted in SL1. The IDs of the errors supported can be found in the snippet of the "IBM: MQ Error Log Configuration" Dynamic Application. You can add other error messages by adding the alert ID to the ALERT_ID_LIST list in the snippet.

To edit the snippet:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Find the "IBM: MQ Error Log Configuration" Dynamic Application and click its wrench icon (🔧).
3. In the **Dynamic Applications Properties Editor**, click the **[Snippets]** tab.
4. In the **Dynamic Applications Snippet Editor & Registry** page, click the wrench icon (🔧) of the "Get-ErrorLogRecords" snippet.
5. The content of the snippet will appear. Add the alert IDs you want added to the `ALERT_ID_LIST` in the snippet:



```
def _log(trace, ui_debug=True):
    if ui_debug:
        self.logger.ui_debug("[App {}] {}: {}".format(self.app_id,
                                                      self.app_name, trace))
    else:
        self.logger.debug("[App {}] {}: {}".format(self.app_id, self.app_name,
                                                   trace))

# This is a list with the alert ids that we want to read from IBM MQ logs file
ALERT_ID_LIST = ['AMQ5657W', 'AMQ8077W', 'AMQ5053W', 'AMQ6184W', 'AMQ6183W', 'AMQ6090I',
                 'AMQ4038W', 'AMQ4036W', 'AMQ4034W', 'AMQ4032W', 'AMQ5005E', 'AMQ5006E',
                 'AMQ5008S', 'AMQ5050S', 'AMQ5009S', 'AMQ5038S', 'AMQ5042E', 'AMQ5057E',
                 'AMQ5501E', 'AMQ5522E', 'AMQ5527E', 'AMQ5529E', 'AMQ9526E', 'AMQ9503E',
                 'AMQ9228E', 'AMQ9213E', 'AMQ9209E', 'AMQ9208E', 'AMQ9202E', 'AMQ8101S',
                 'AMQ6125E', 'AMQ6119S']

error_log_path = {"Windows": "C:\ProgramData\IBM\MQ\errors", "Linux": "/var/mqm/errors"}
```

## Viewing IBM MQ Component Devices

In addition to the **Devices** page, you can view the IBM MQ system and all associated component devices in the following places in the user interface:

- The **Device Investigator** Map page (click **Map** in the **Device Investigator** page) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the listed devices reloads the page to make the selected device the primary device

- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1 in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with a Kubernetes cluster, find the cluster device and click its plus icon (**+**).

- The **Component Map** page (Classic Maps > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the **Component Map** as new component devices are discovered. SL1 also updates each map with the latest status and event information. To view the map for a Kubernetes cluster, go to Classic Maps > Device Maps > Components, and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.

# Chapter 3

# Dashboards

## Overview

The *IBM: MQ* PowerPack contains device dashboards that present data related to your message queues and queue managers.

The following section provides a description of each dashboard:

This chapter covers the following topics:

## IBM MQ Device Dashboards

### IBM MQ: Queue

The IBM MQ: Queue device dashboard displays the following information:

- A line graph that displays message depth
- A line graph that displays input and output handles
- A list of device logs displaying events

### IBM MQ: Queue Manager

The IBM MQ: Queue Manager device dashboard displays the following information:

- A line graph that displays XMITQ message depths
- A list of device logs displaying events

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

## Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

## Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com. For more information, see https://sciencelogic.com/company/legal.

ScienceLogic

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010