ScienceLogic

Cherwell SyncPack

Version 1.0.0, rev 1

Table of Contents

Introduction to the Cherwell SyncPack 3
What Can I Do with this SyncPack? 4
Terminology 5
Importing and Installing the Cherwell SyncPack 6
Installing and Configuring Cherwell mApps 8
Installing the Federated CMDB mApp 9
Installing the IS Content mApp 13
Creating the Federation Registration Record 16
Configuring CSM Access for the REST API 19
Creating a New Security Group 19
Creating a New User 26
Verifying the URL for API Access 28
Obtaining a Client Key 29
Configuring CSM Scheduled Tasks 30
Configuring the Back-end Credentials and Endpoints 30
Configuring Credentials and the Federated Registration Record 33
Creating the Cherwell API Credential 34
Creating the PowerFlow Federation Source Credential 35
Configuring the API Credentials 37
Enabling the Federation Registration Record 37
Configuring Incident Creation and Updates 38
Configuring CI Creation and Updates 39
Configuring the Mappings between Source CI Types and CSM CI Types 41
Configuring the Mappings between Source CI Attributes and CSM Fields 41
Configuring Automated Maintenance Windows 42
Configuring Automated CI Retirements 44
Configuring SL1 and SL1 PowerFlow 46
Configuring the Cherwell Integration PowerPack 47
Downloading and Installing the PowerPack in SL1 47
Creating a SOAP/XML Credential for Cherwell Integration 48
Enabling the Run Book Automation Policies 49
Enabling and Customizing the Run Book Action Policy 51
Aligning a Configuration Object with PowerFlow Applications 51
Adding and Editing Credentials in a Configuration Object 52
Aligning a Configuration Object with a PowerFlow Application 53
Sending Additional Metadata for Incident Records 55
Troubleshooting the Cherwell SyncPack 62
Incidents are not being created 63
CIs are not being created 63
No mappings configured for Device Type 64
No field mappings defined 65
Viewing Events Sent from PowerFlow 66
Checking the Automation Process Status 67

Chapter 1

Introduction to the Cherwell SyncPack

Overview

This manual provides an overview of the "Cherwell" SyncPack, which you can use to manage the Federated CMDB integration between Cherwell Service Management (CSM) and ScienceLogic (SL1).

NOTE: This manual assumes that you have already installed CSM, SL1, and SL1 PowerFlow, and that you have a basic level of CSM knowledge and can create and publish CSM Blueprints.

This chapter covers the following topics:

What Can I Do with this SyncPack? 4

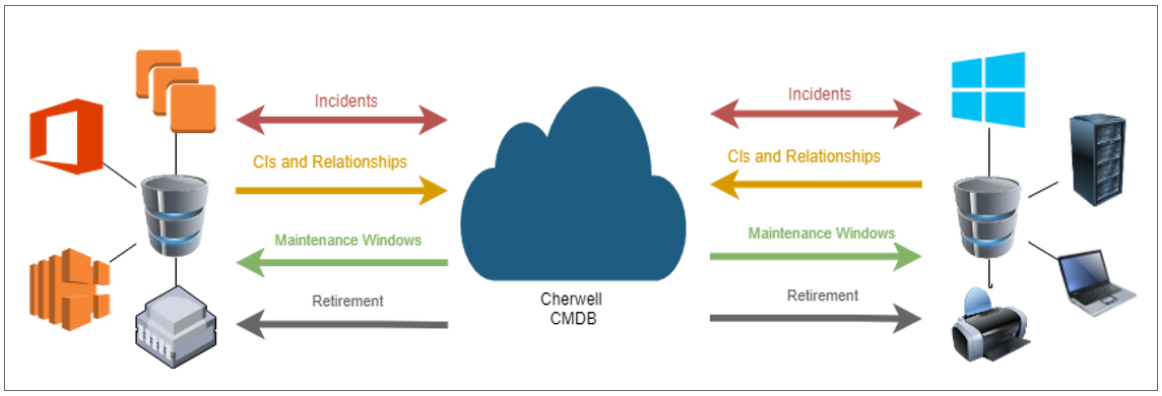
Terminology 5

Importing and Installing the Cherwell SyncPack 6

What Can I Do with this SyncPack?

Cherwell Service Management (CSM) is a low-code, no-code tool where you can manage the CMDB, track the life cycle of assets, manage changes, and manage incidents and requests. You can use the "Cherwell" SyncPack to manage the Federated CMDB integration between CSM and SL1.

The following graphic provides an overview of the various workflows available in the "Cherwell" SyncPack:



The "Cherwell" SyncPack lets you manage the Federated CMDB integration between Cherwell Service Management (CSM) and ScienceLogic (SL1).

Using this SyncPack, you can perform the following integrations between CSM and SL1:

- Incident Creation and Update Sync
- Configuration Item (CI) Creation and Update Sync
- Maintenance Window Sync
- Retirement of CIs from SL1 and CSM

Terminology

The following table lists the names and definitions of the various elements in SL1 and Cherwell:

Name	Definition
Blueprint	An XML file that contains configuration information; these files can be shared between different CSM instances
Business object	Provides a view for the user for objects like CIs, federated relationships, federated field mappings, and federated CI mappings
CI	Configuration Item in CSM, also known as a "Device" in SL1
CR	Change Request
CSM	Cherwell Service Management
CSM Administrator client	The CSM administration application, typically depicted by a round orange icon
CSM User client	The CSM application for CSM users, typically depicted by a round blue icon
Discovery Session (SL1)	Service Catalog Request (CSM)
Incident	A CSM Incident syncs with an SL1 Event.
IS or PF	ScienceLogic SL1 PowerFlow (formerly called the Integration Service)
mApp	CSM Mergeable Application; a combination of Blueprints that contain configuration information
One-Step	A low-code/no-code tool in CSM that allows users to chain a series of actions into a simple or complex workflow
SL1	ScienceLogic SL1 monitoring platform
Topology (SL1)	Dependency (CSM)

Importing and Installing the Cherwell SyncPack

To import a SyncPack in the PowerFlow user interface:

1. On the **SyncPacks** page, click **[Import SyncPack]**. The **Import SyncPack** page appears.
2. Click **[Browse]** and select the **.whl** file for the SyncPack you want to install.

> **TIP:** You can also drag and drop a **.whl** file to the **SyncPacks** page.

3. Click **[Import]**. PowerFlow registers and uploads the SyncPack. The SyncPack is added to the **SyncPacks** page.

> **NOTE:** You cannot edit the content package in a SyncPack published by ScienceLogic. You must make a copy of a ScienceLogic SyncPack and save your changes to the new SyncPack to prevent overwriting any information in the original SyncPack when upgrading.

To activate and install a SyncPack in the PowerFlow user interface:

1. On the **SyncPacks** page of the PowerFlow user interface, click the **[Actions]** button (⋮) for the SyncPack you want to install and select *Activate & Install*. The **Activate & Install SyncPack** modal appears.

> **NOTE:** If you try to activate and install a SyncPack that is already activated and installed, you can choose to "force" installation across all the nodes in the PowerFlow system.

> **TIP:** If you do not see the PowerPack that you want to install, click the Filter icon (⧩) on the **SyncPacks** page and select *Toggle Inactive SyncPacks* to see a list of the imported PowerPacks.

2. Click **[Yes]** to confirm the activation and installation. When the SyncPack is activated, the **SyncPacks** page displays a green check mark icon (✔) for that SyncPack. If the activation or installation failed, then a red exclamation mark icon (❗) appears.
3. For more information about the activation and installation process, click the check mark icon (✔) or the exclamation mark icon (❗) in the **Activated** column for that SyncPack. For a successful installation, the "Activate & Install SyncPack" application appears, and you can view the Step Log for the steps. For a failed installation, the **Error Logs** window appears.
4. If you have other versions of the same SyncPack on your PowerFlow system, you can click the **[Actions]** button (⋮) for that SyncPack and select *Change active version* to activate a different version other than the version that is currently running.

The "Cherwell" SyncPack requires you to install and configure the "Federated CMDB" mApp and the "IS Content" mApp. For more information, see *Installing and Configuring Cherwell mApps*.

After installing and configuring the Cherwell mApps, you will need to perform additional configurations before running the SyncPack. For more information, see the following chapters:

- *Configuring Credentials and the Federated Registration Record*
- *Configuring SL1 and PowerFlow*

Chapter 2

Installing and Configuring Cherwell mApps

Overview

In Cherwell Service Management (CSM), an ***mApp*** is a set of XML files containing configuration information that can be installed and configured on multiple instances of CSM. You need to install and configure the following mApps to before you can use the *Cherwell* SyncPack:

- The "Federated CMDB" mApp
- The "IS Content" mApp

This chapter describes how to install and configure these mApps onto an existing CSM instance, and how to configure the **Federation Registration** record in CSM to use the automation processes and One-Steps in the mApps.

This chapter covers the following topics:

Installing the Federated CMDB mApp *9*

Installing the IS Content mApp *13*

Creating the Federation Registration Record *16*

Configuring CSM Access for the REST API *19*

Configuring CSM Scheduled Tasks *30*

Installing the Federated CMDB mApp

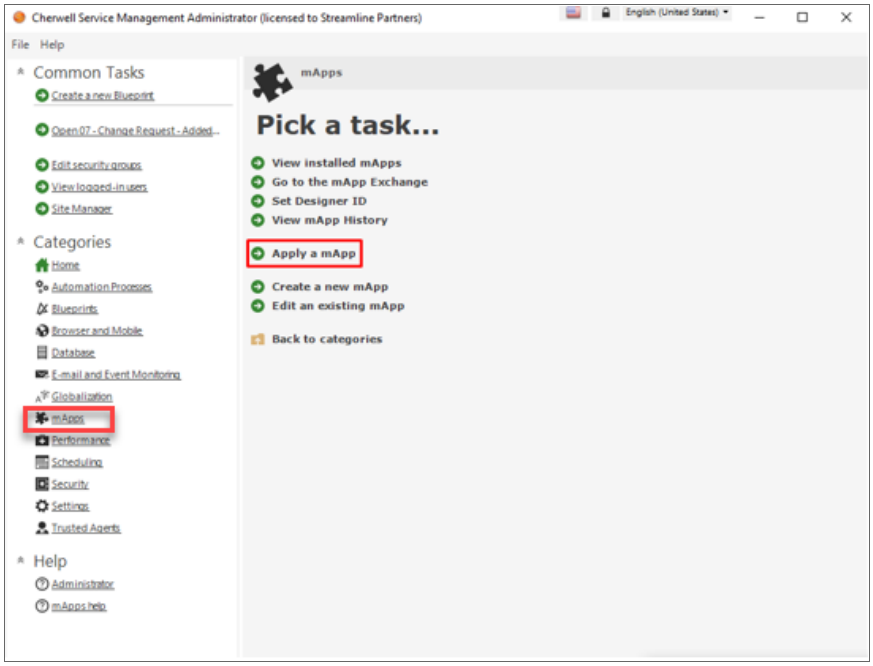
The "Federated CMDB" mApp provides a Federated CMDB solution where you can add and map Federated CMDB sources for Cherwell Configuration Items (CIs).

WARNING: Applying this mApp might overwrite some of your system definitions. Performing a system backup is highly recommended.

NOTE: You will need to have a local version of the mApp to complete this process; see your Cherwell or ScienceLogic contact for the latest mApp. Also, the name of the mApp might be different from the name used in these steps.

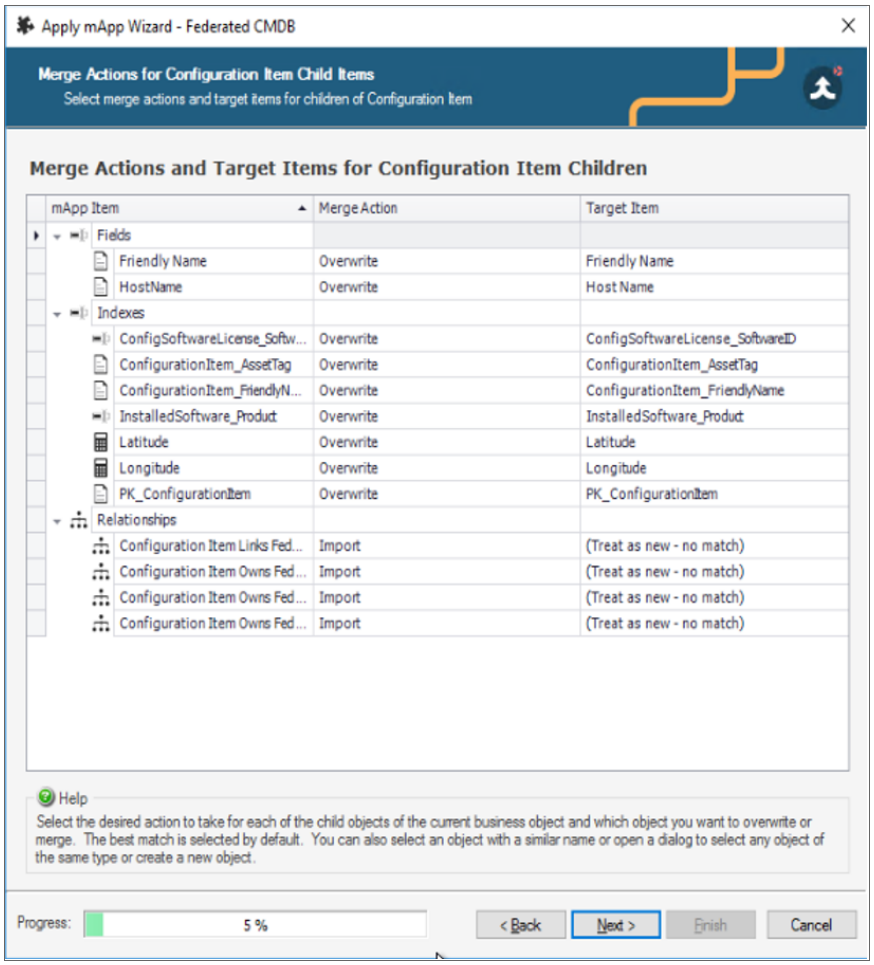
To install the "Federated CMDB" mApp:

1. Open the CSM Administrator client and select **mApps** from the **Categories** sub-menu.



2. From the **Pick a task** section, select **Apply a mApp**. An **Open** dialog appears.
3. Navigate to the mApp on your local drive, select the mApp, and click **[Open]**. The **Apply mApp Wizard** page appears.
4. Click **[Next]**. The **License Information** page appears.
5. Select **Yes, I accept the terms** and click **[Next]**. The **Localization** page appears.
6. Click **[Next]**. The **Amount of User Interaction** page appears.

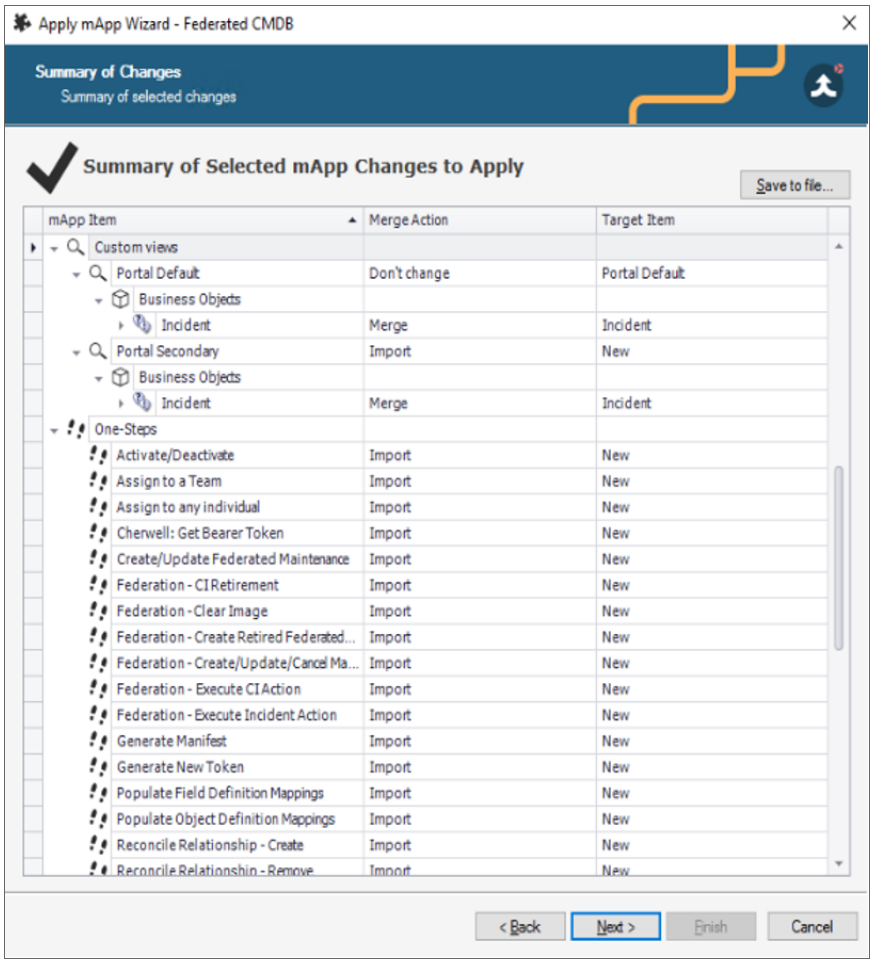
7. Select **Make reasonable decisions, but ask me if unsure** and click **[Next]**. The **Merge Actions for Configuration Item Child Items** page appears:



> **NOTE:** The contents of the windows in this portion of the wizard might vary depending on the system to which you are installing.

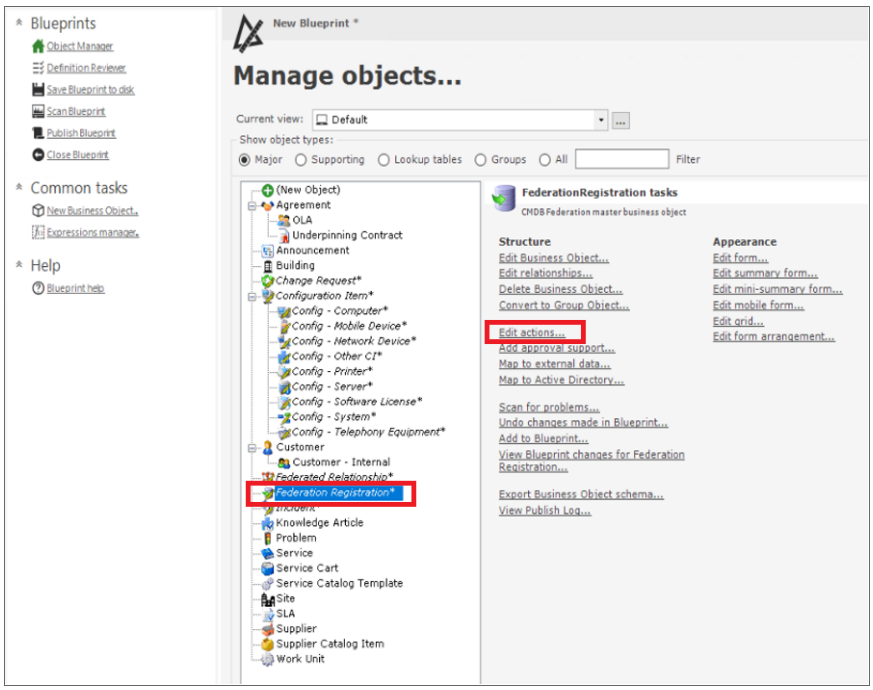
8. Click **[Next]**. The **Merge Actions for Change Request Child Items** page appears.
9. Click **[Next]**. The **Merge Actions for Event Child Items** page appears.
10. Click **[Next]**. The **Merge Actions for Incident Child Items** page appears.
11. Click **[Next]**. A second **Merge Actions for Incident Child Items** page appears.
12. Click **[Next]**. A third **Merge Actions for Incident Child Items** page appears.

13. Click **[Next]**. The **Summary of Changes** page appears:

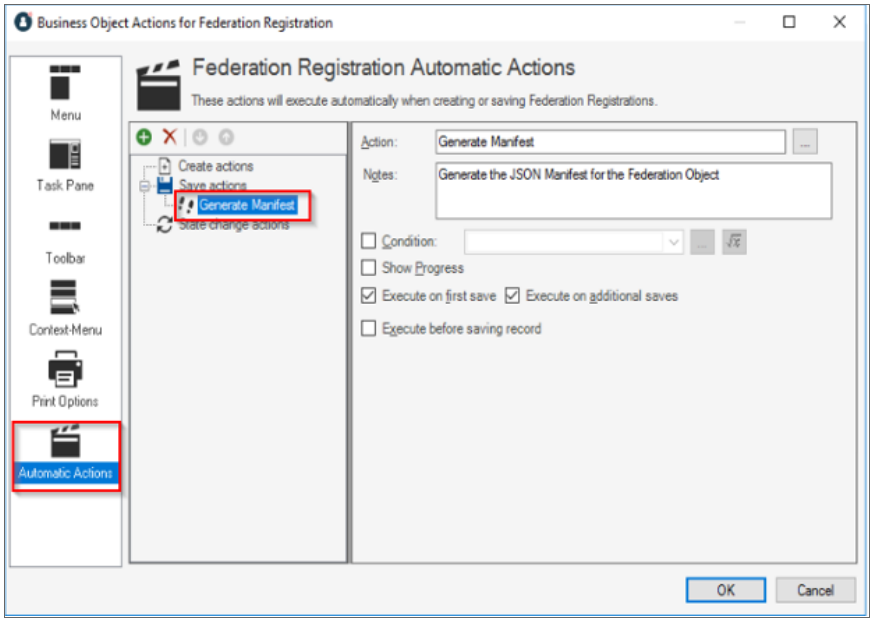


14. Review your list of selected mApp changes and click **[Next]**. The **Final Options** page appears.

15. Select **Open a Blueprint so that I can preview the changes** and click **[Finish]**. CSM will create a *Blueprint*, which is an XML definition of changes being made to the underlying system. When the Blueprint is created, the **Manage objects** page appears:



16. From the list of objects, select the "Federation Registration" object and then click **Edit Actions**. The **Business Object Actions for Federation Registration** window appears:



17. From the **Blueprints** sub-menu, select **Save Blueprint to disk** and provide a name and location for the Blueprint when prompted.

18. From the **Blueprints** sub-menu, select **Publish Blueprint** to apply the Blueprint changes to the current CSM system. A **Publish Options** page appears.
19. Leave the options set to the defaults and click **[Publish]**. The Blueprint is scanned for changes against the current CSM system. When the scan completes, a **Scan successful** dialog appears.
20. Click **[OK]**. The publishing process for the Blueprint begins. When the Blueprint is published, a **Blueprint has been published** dialog appears.

> **NOTE:** During the publishing process, a rollback Blueprint is created. This rollback Blueprint is in the same file system location as the saved Blueprint, but it has **_rollback** added to the name. You can use this Blueprint to roll back the published changes if needed.

21. Click **[Close]**. The "Federated CMDB" mApp is now published.

Installing the IS Content mApp

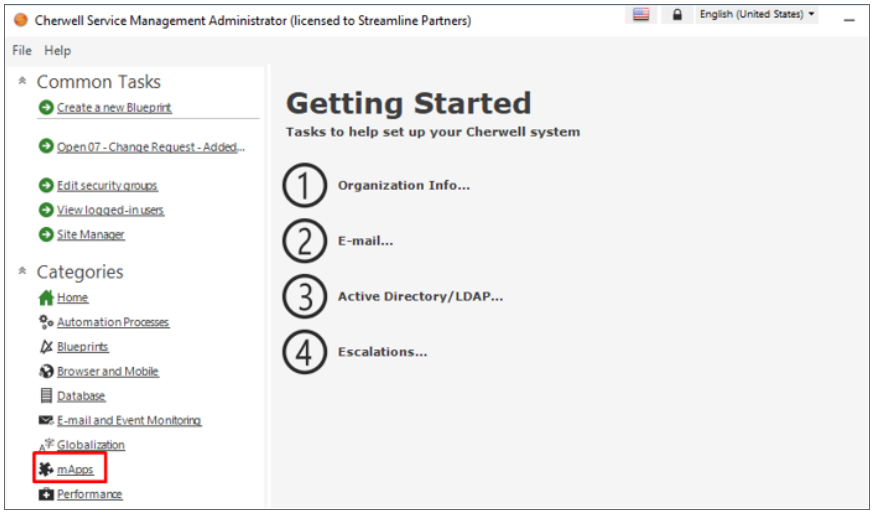
Integration with a Federated source such as PowerFlow is typically accomplished using automation processes and One-Steps that have been specifically configured for this purpose. These features are known as *Content*, and they are contained in the "IS Content" mApp.

> **WARNING:** Applying this mApp might overwrite some of your system definitions. Performing a system backup is highly recommended.

> **NOTE:** You will need to have a local version of the mApp to complete this process; see your Cherwell or ScienceLogic contact for the latest mApp. Also, the name of the mApp might be different from the name used in these steps.

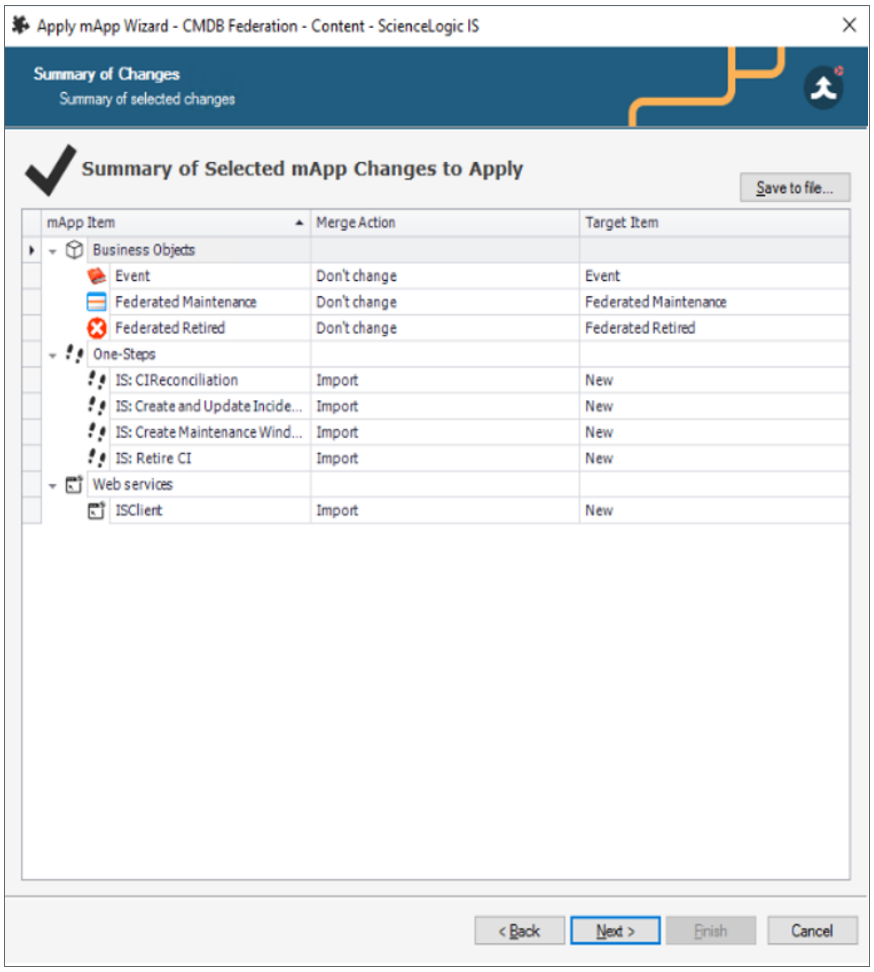
To install the "IS Content" mApp:

1. Open the CSM Administrator client and select **mApps** from the **Categories** sub-menu:



2. From the **Pick a task** section, select **Apply a mApp**. An **Open** dialog appears.
3. Navigate to the mApp on your local drive, select the mApp, and click **[Open]**. The **Apply mApp Wizard** page appears.
4. Click **[Next]**. The **License Information** page appears.
5. Select **Yes, I accept the terms** and click **[Next]**. The **Localization** page appears.
6. Click **[Next]**. The **Amount of User Interaction** page appears.

7. Select **Make reasonable decisions, but ask me if unsure** and click **[Next]**. The **Summary of Changes** page appears:



8. Review your list of selected mApp changes and click **[Next]**. The **Final Options** page appears.
9. Select **Open a Blueprint so that I can preview the changes** and click **[Finish]**. When the Blueprint is created, the **Manage objects** page appears.
10. From the **Blueprints** sub-menu on the left, select **Save Blueprint to disk** and provide a name and location for the Blueprint when prompted.
11. From the **Blueprints** sub-menu, select **Publish Blueprint** to apply the Blueprint changes to the current CSM system. A **Publish Options** page appears.
12. Leave the options set to the defaults and click **[Publish]**. The Blueprint is scanned for changes against the current CSM system. When the scan completes, a **Scan successful** dialog appears.

13. Click **[OK]**. The publishing process for the Blueprint begins. When the Blueprint is published, a **Blueprint has been published** dialog appears.

> **NOTE:** During the publishing process, a rollback Blueprint is created. This rollback Blueprint is in the same file system location as the saved Blueprint, but it has **_rollback** added to the name. You can use this Blueprint to roll back the published changes if needed.

14. Click **[Close]**. The "IS Content" mApp is now published.

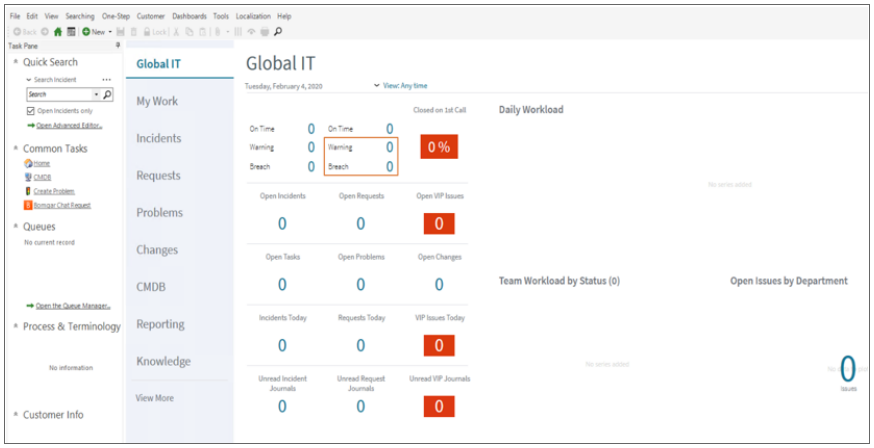
Creating the Federation Registration Record

The main component of the Federated CMDB system is the ***Federation Registration record***. Before any further configuration can occur, you must create at least one Federation Registration record.

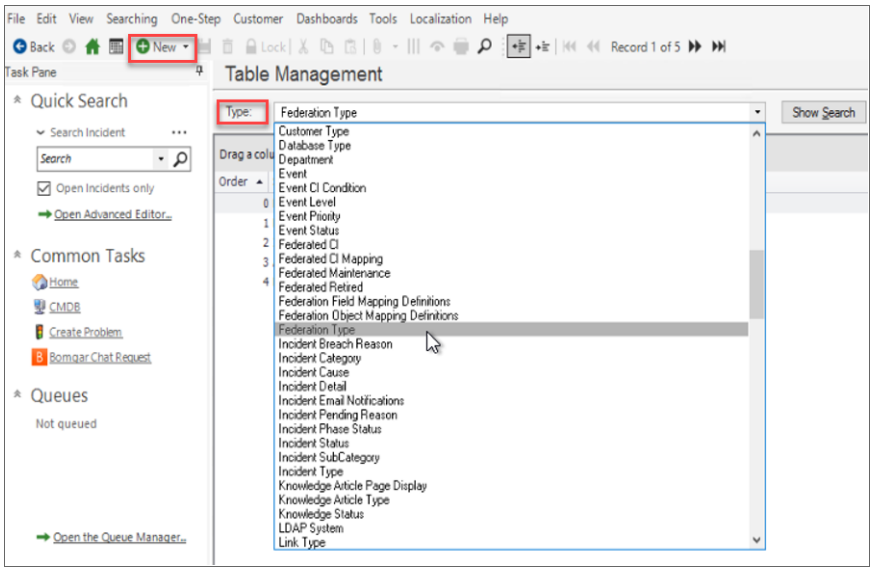
After you create the Federation Registration record, you can configure that record to use the various automation processes and One-Steps in the two mApps you just installed.

To create a new Federation Registration record:

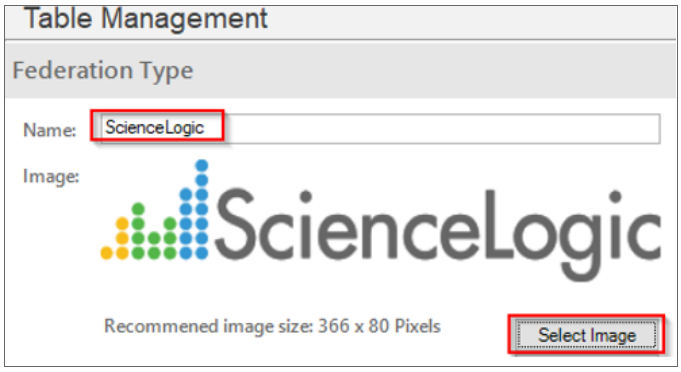
1. Open the CSM User client (not the Administrator client) and log in to CSM using your credentials, preferably with administrator rights:



2. Open the **Tools** menu and select *Table Management*. The **Table Management** page appears:



3. In the ***Type*** drop-down, select *Federation Type*.
4. Click **[New]** to create a new Federation Type. A new **Federation Type** record appears:

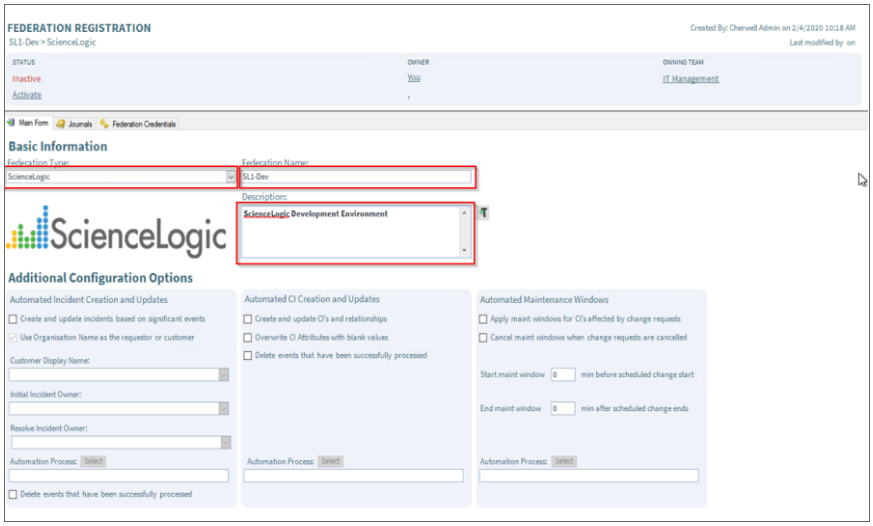


5. Type a name in the ***Federation Type*** field, such as "ScienceLogic", and click **[Select Image]** to select an appropriate image for this type.

> **NOTE:** You select images from the Cherwell Image Manager. If the image you need is not available, you can import it by right-clicking in the Explorer view of the Image Manager screen and selecting *New*.

6. Click the **[Save]** button ( ).

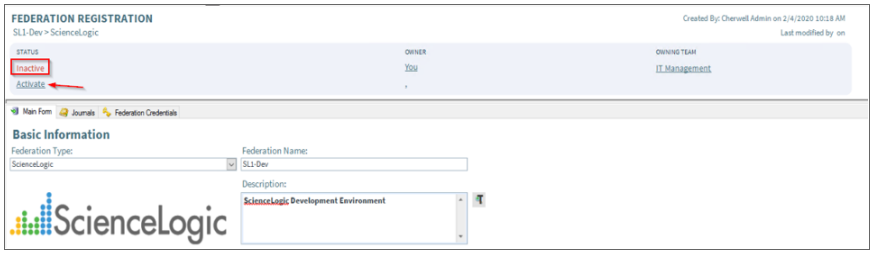
7. Click the **[New]** button ( ) and select *New Federation Registration* from the menu. A new **Federation Registration** record appears:



8. From the ***Federation Type*** drop-down, select the Federation Type that you created in steps 3-6.
9. Type a name for the ***Federation Name*** field, such as "SL1-Dev", and add a description to the ***Description*** field for the new record.

> **NOTE:** ***Federation Name*** is a system-unique value and cannot be duplicated. You will use this value when PowerFlow applications interact with the Federated CMDB. The PowerFlow applications need to be configured to pass this unique name in all interactions.

10. Click **[Save]**.
11. Click **Activate** if you wish to progress this record to the "Active" state. The **Federation Registration** record is initially created in an "Inactive" state:



> **NOTE:** PowerFlow applications and any custom applications should check for this state before passing integration data to CSM. Only "Active" records should be allowed to process data. This allows the CSM administrator to turn off poorly behaving applications.

12. The **Federation Registration** record is now "Active", but it is not properly configured to support integrations. Go to the following topic to continue the configuration process.

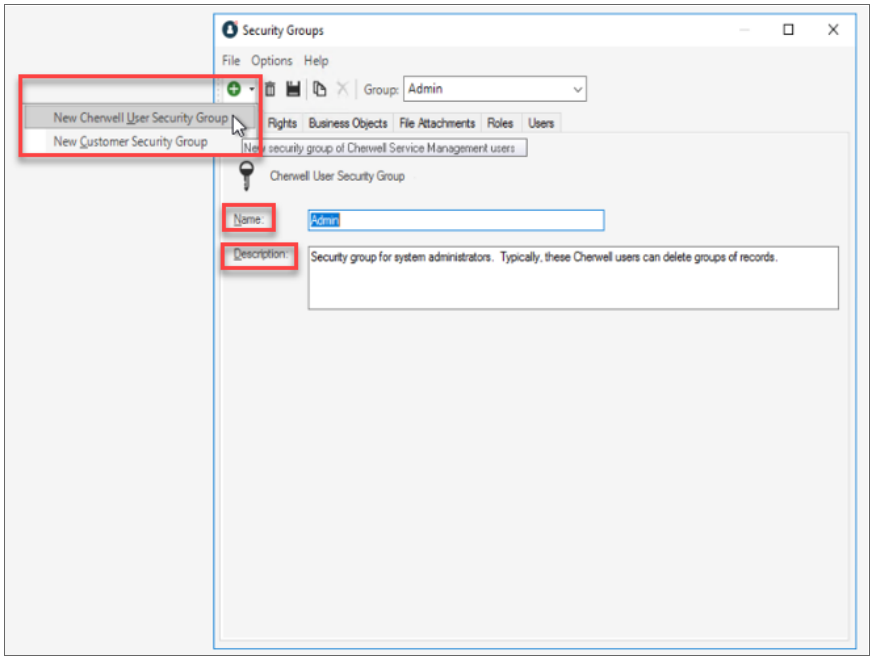
Configuring CSM Access for the REST API

The Federation Registration One-Steps use the CSM REST API to create and update CI records. You need to create a new CSM Security Group and a CSM user account that has Create, Read, and Write access to all Federation business objects and all Configuration Item business objects. This account must be able to access the CSM REST API remotely.

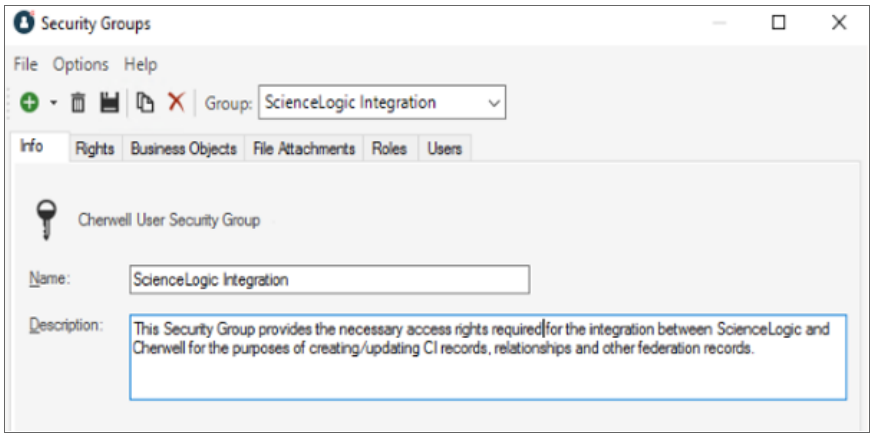
Creating a New Security Group

To create a new Security Group with CSM access:

1. Open the CSM Administrator client and select **Security** from the **Categories** sub-menu on the left.
2. From the **Pick a task** section, select **Edit security groups**. A **Security Groups** window appears:



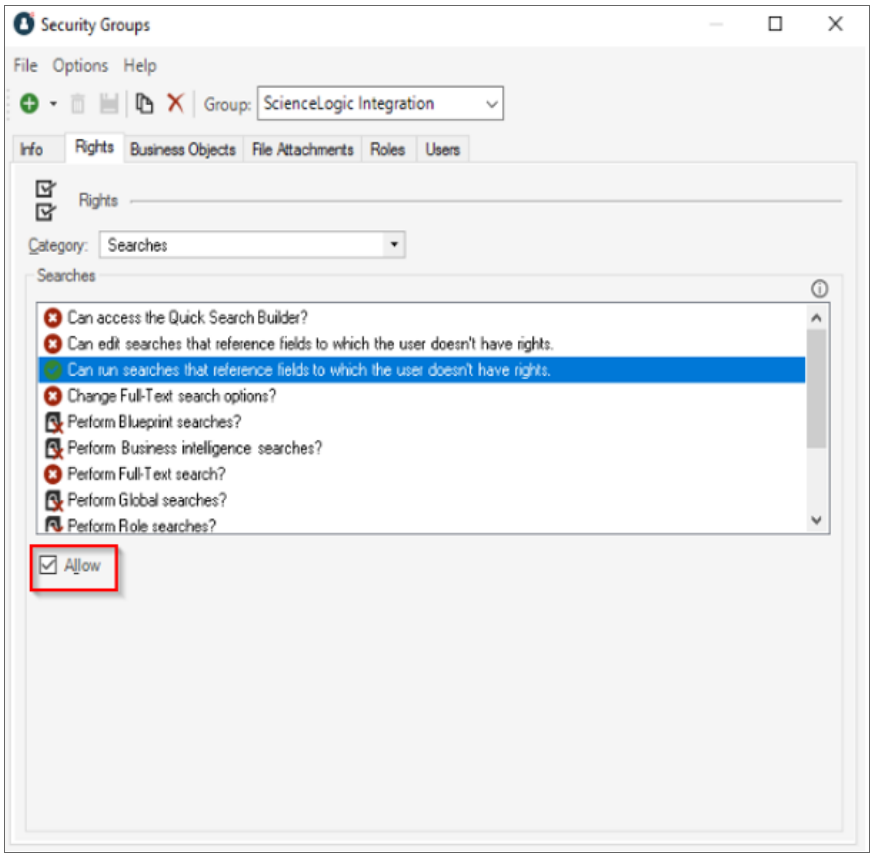
3. Click **[New]** and select *New Cherwell User Security Group*. A new **Security Groups** dialog appears.



4. In the ***Name*** field, type a name for the new Security Group, and type a description of the group in the ***Description*** field.

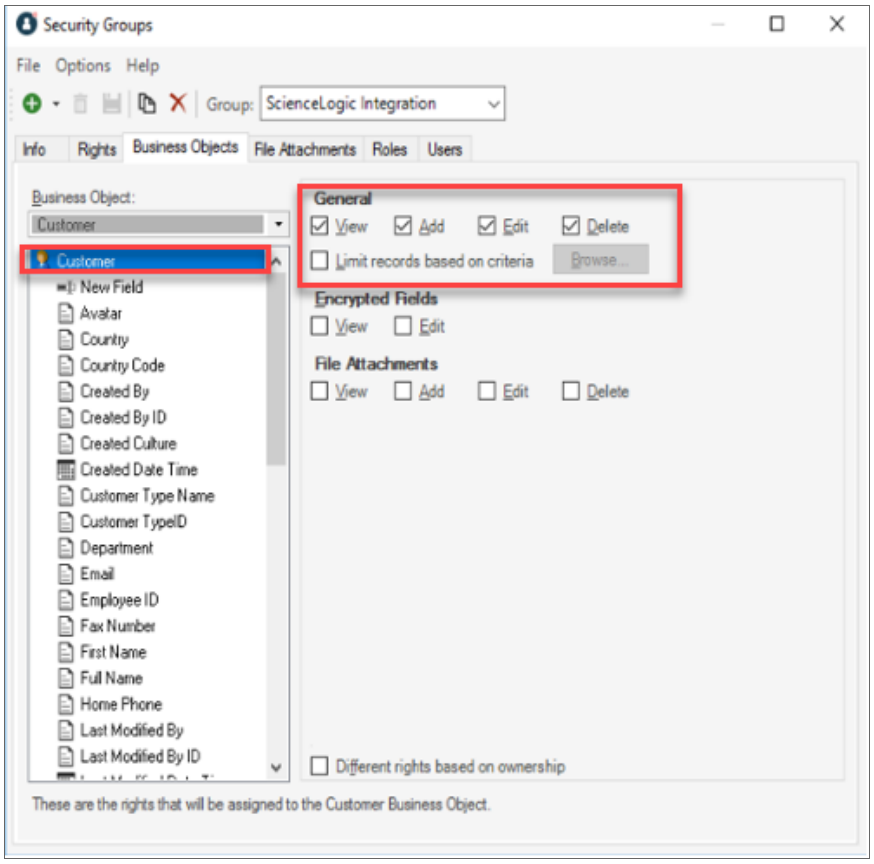
> **NOTE:** The name you create for the group is not important, as the CSM This Security Group user will later be linked to this Security Group. The name can abide by other naming standards if needed.

5. Click the **[Rights]** tab and make sure that the *Can run searches that reference fields to which the user doesn't have rights* option is configured for "Allow":

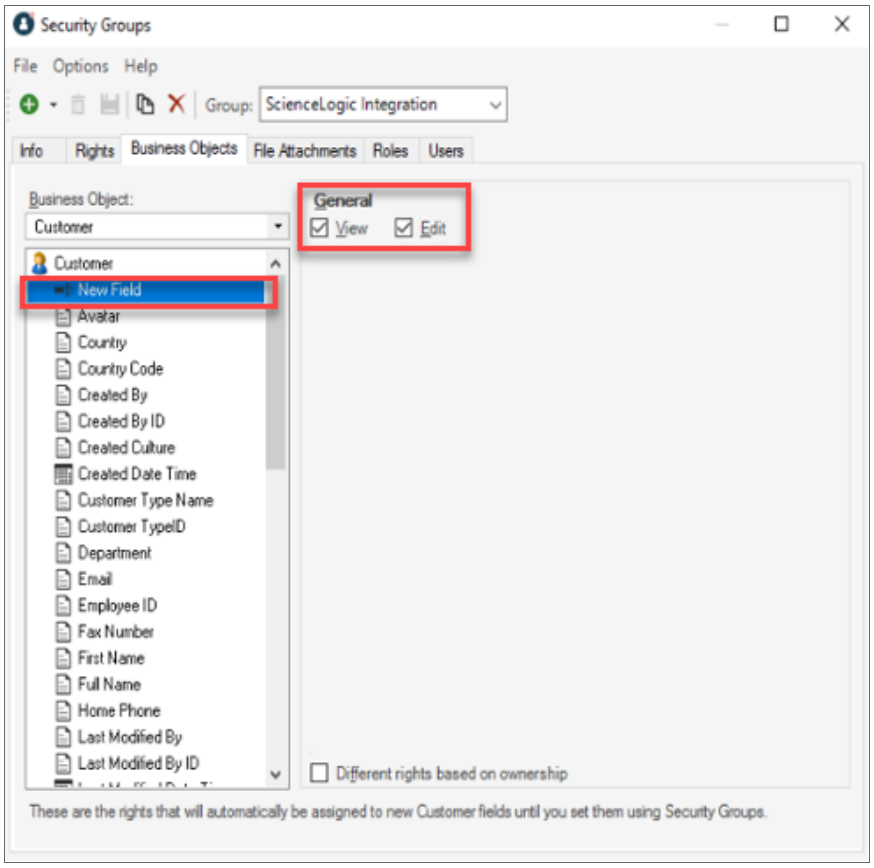


6. Click the **[Business Objects]** tab.

7. Select the *Customer* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*:



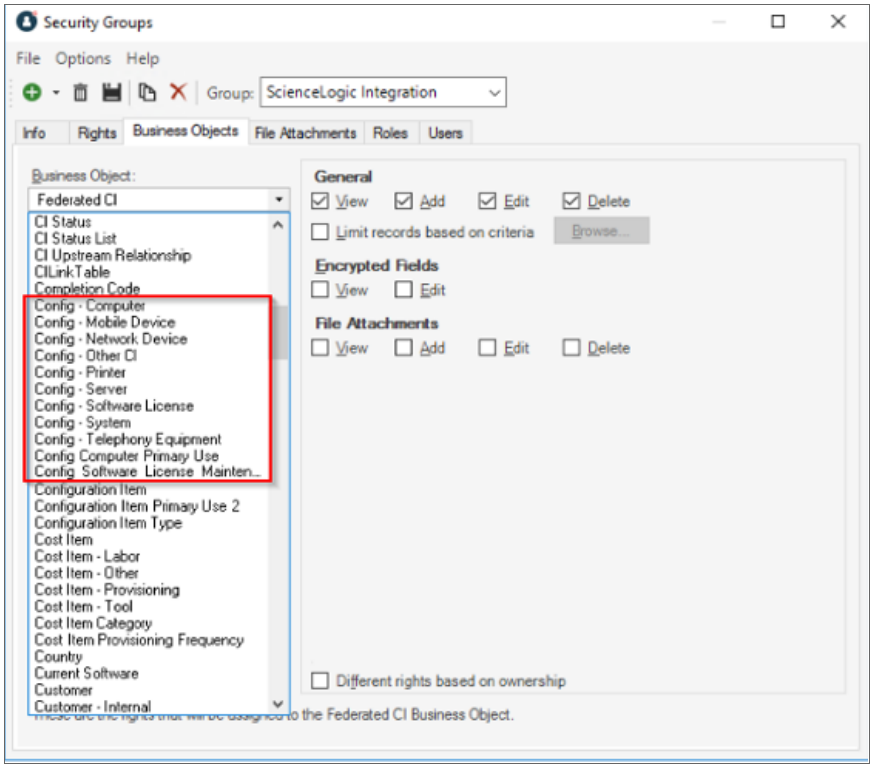
8. Select *New Field* under the *Customer* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*:



9. Select the *Customer - Internal* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
10. Select *New Field* under the *Customer - Internal* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
11. Select the *Event* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
12. Select *New Field* under the *Event* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
13. Select the *Federated CI* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
14. Select *New Field* under the *Federated CI* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.

15. Select the *Federated CI Mapping* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
16. Select *New Field* under the *Federated CI Mapping* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
17. Select the *Federated Field Mapping* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
18. Select *New Field* under the *Federated Field Mapping* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
19. Select the *Federated Maintenance* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
20. Select *New Field* under the *Federated Maintenance* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
21. Select the *Federated Relationship* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
22. Select *New Field* under the *Federated Relationship* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
23. Select the *Federated Retired* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
24. Select *New Field* under the *Federated Retired* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
25. Select the *Federated Credential* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
26. Select *New Field* under the *Federated Credential* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
27. Select the *Federated Field Mapping Definitions* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
28. Select *New Field* under the *Federated Field Mapping Definitions* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
29. Select the *Federated Registration* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
30. Select *New Field* under the *Federated Registration* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.

31. Select the *Federated Type* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
32. Select *New Field* under the *Federated Type* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
33. Select the *Federation_joins_CI* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
34. Select *New Field* under the *Federation_joins_CI* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
35. Select the *Configuration Item* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
36. Select *New Field* under the *Configuration Item* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
37. Make sure that the following rights are selected in the **General** section for all *Configuration Item* types remaining in the drop-down: *View*, *Add*, *Edit*, and *Delete* (or just *View* and *Edit* where relevant):



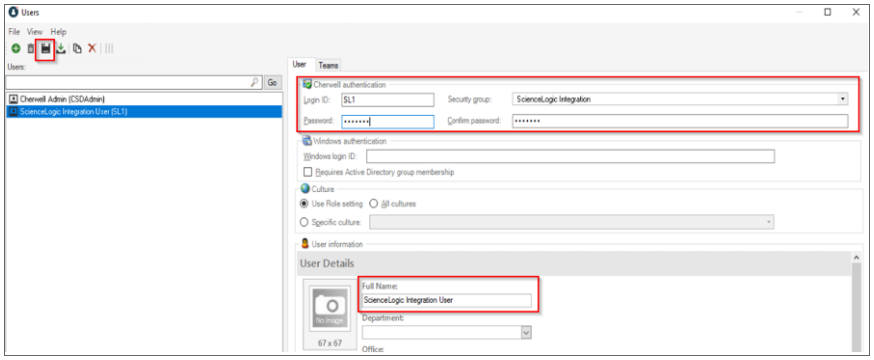
TIP: The *Configuration Item* types all have "Config" at the start of their names.

38. Select the *CILink Table* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
39. Select *New Field* under the *CILink Table* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
40. Select the *Manufacturer* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
41. Select *New Field* under the *Manufacturer* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
42. Select the *CI Upstream Relationship* business object from the ***Business Object*** drop-down and make sure that the following rights are selected in the **General** section for that business object: *View*, *Add*, *Edit*, and *Delete*. No other options should be selected.
43. Select *New Field* under the *CI Upstream Relationship* business object and make sure that the following rights are selected in the **General** section for that business object: *View* and *Edit*.
44. Click the **[Save]** button ( ) to save the new Security Group, and then close the **Security Groups** window.

Creating a New User

To create a user for the new Security Group:

1. From the **Pick a task** section of the CSM Administrator client, select **Edit users**. The **Users** window appears:

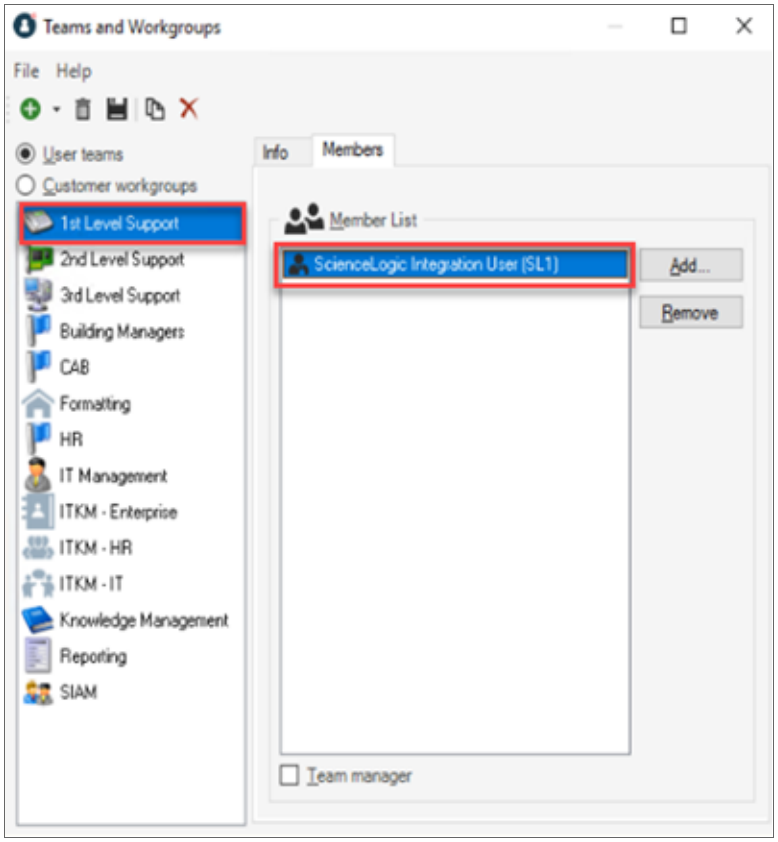


2. Click the **[New]** button ( ).
3. On the **[User]** tab, complete the following fields:
    - ***Login ID***. Type a unique login for the user, such as "SL1".
    - ***Security Group***. Select the Security Group that you created in the previous procedure.
    - ***Password***. Type a password for the user, and confirm the password in the corresponding field.

- ***Full Name***. Type a unique name for the user, such as "ScienceLogic Integration User".

> **NOTE:** Make a note of the **Login ID** and **Password** values, as you will use these in additional configuration steps.

4. Click the **[Save]** button ( ).
5. From the **Pick a task** section, select **Edit teams and workgroups**. The **Teams and Workgroups** dialog appears:



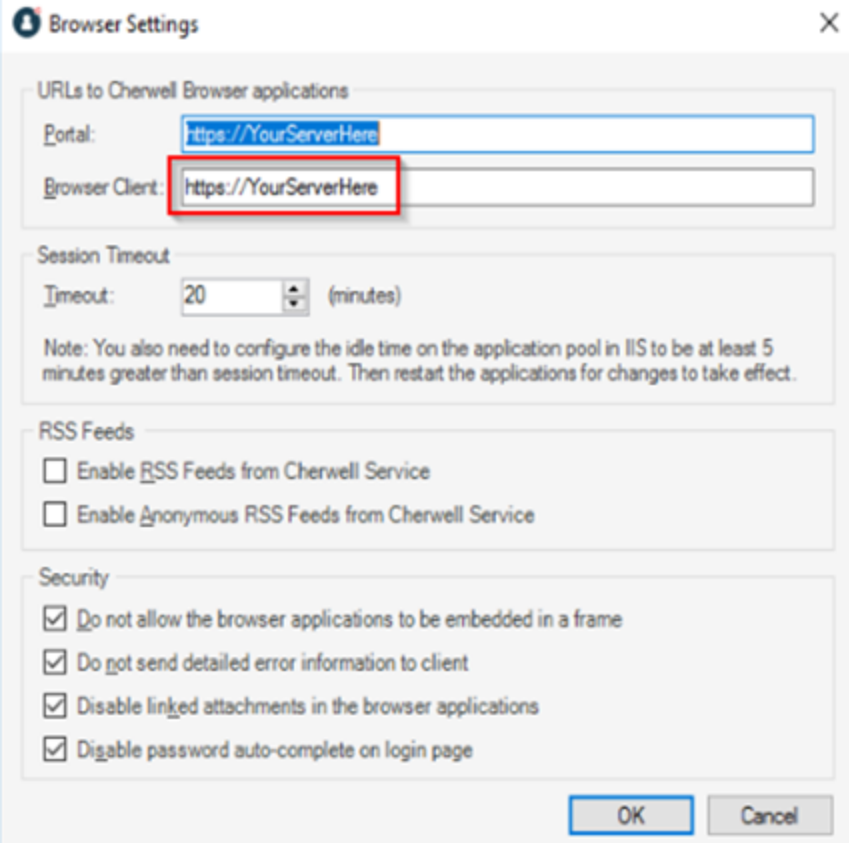
6. In the **User teams** section, select **1st Level Support**.
7. Click the **[Members]** tab and make sure that the new user is listed as a member of this team.

Verifying the URL for API Access

By default, the URL used by the Federated CMDB integration is the same URL used by the web-based client. This section describes how to find this URL and how to make sure that the API is functioning using this URL.

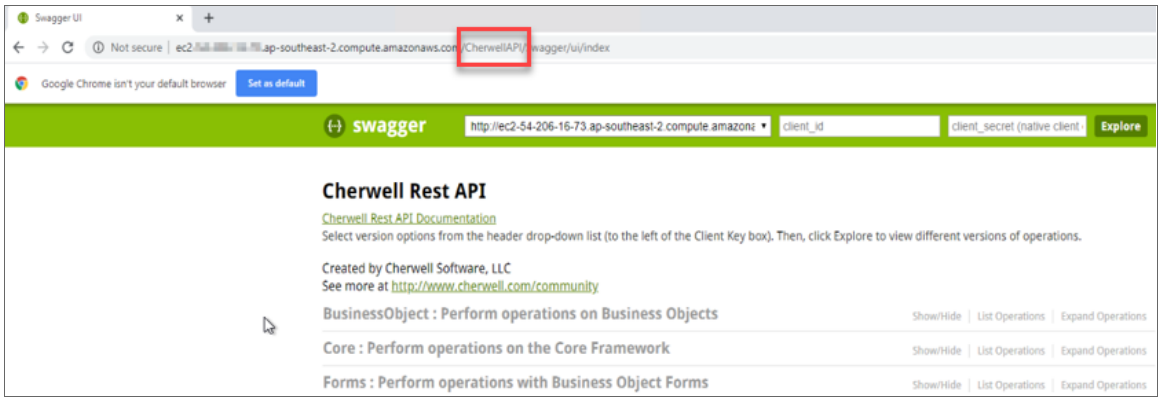
To verify the URL for API access:

1. From the **Categories** sub-menu of the CSM Administrator client, select **Browser and Mobile**:
2. From the **Pick a task** section, select **Browser Application Settings**. A **Browser Settings** window appears:



3. Review the URL in the ***Browser Client*** field. If the field displays **https://YourServerHere**, then this value has not been set yet.
4. If the value has not been set, specify the URL in the ***Browser Client*** field and then click **[OK]**.

5. If you add a suffix of **/CherwellAPI** to that URL in a web browser, the browser opens a Swagger window similar to the following:



6. Make a note of that URL for later configuration steps.

> **NOTE:** If a DNS name is used in the URL, then that DNS name must be able to be resolved on the server itself, as that is where all API calls are made.

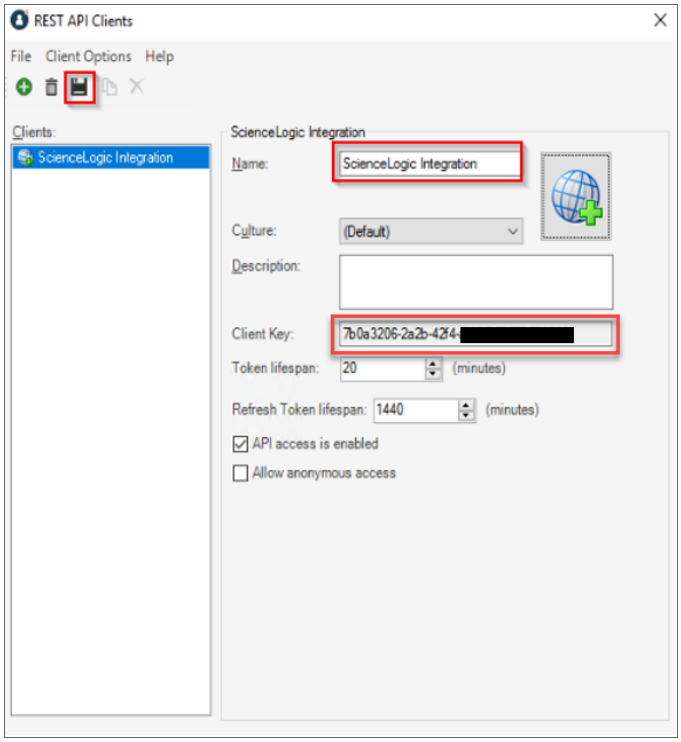
Obtaining a Client Key

Access to the CSM REST API is controlled with the username and password as well as what is known as a Client Key.

To create the Client Key:

1. Open the CSM Administrator client and select **Security** from the **Categories** sub-menu on the left.
2. From the **Pick a task** section, select **Edit REST API Client settings**. A **REST API Clients** window appears.

3. Click the **[New]** button ( ) to create a new Client Key. A new record appears:



4. In the ***Name*** field, type a name for the Client Key, such as "ScienceLogic Integration".
5. Copy the value in the ***Client Key*** field for later configuration steps.
6. Click the **[Save]** button ( ).

Configuring CSM Scheduled Tasks

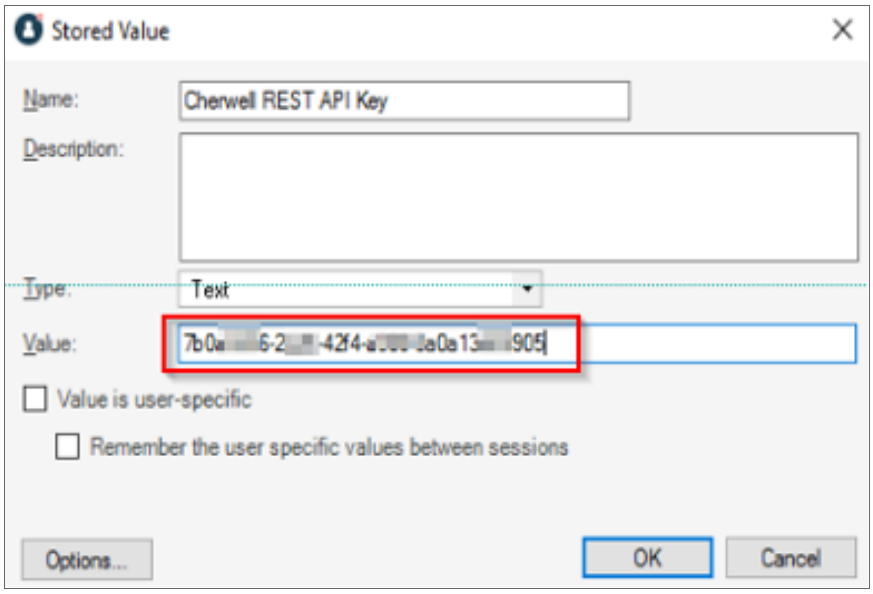
Various back-end configuration processes, including scheduled tasks, are needed to cache configuration data for the Federation to occur in an automated fashion. This back-end configuration uses web services, and you will use the CSM user account that you just created for these configurations.

Configuring the Back-end Credentials and Endpoints

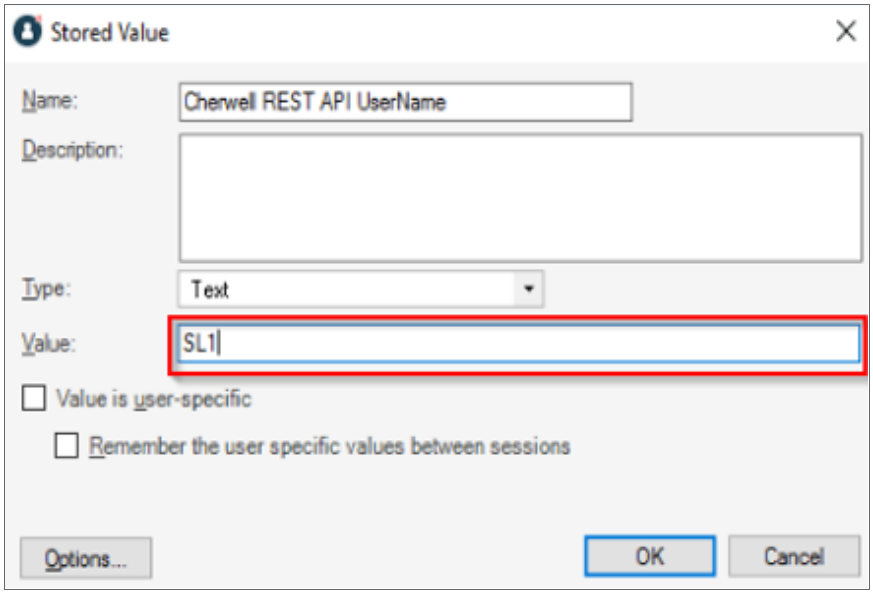
To configure the back-end credentials and endpoints:

1. Log in to the CSM Administrator client as an administrator and select **Create a new Blueprint** in the **Common Tasks** sub-menu on the left.
2. From the **[Managers]** menu, select *Stored Values*. The **Stored Values Manager** window appears.
3. Select the Blueprint scope so you can edit the stored values.

4. Right-click the ***Cherwell REST API Key*** and select *Edit*. The **Stored Value** dialog appears:

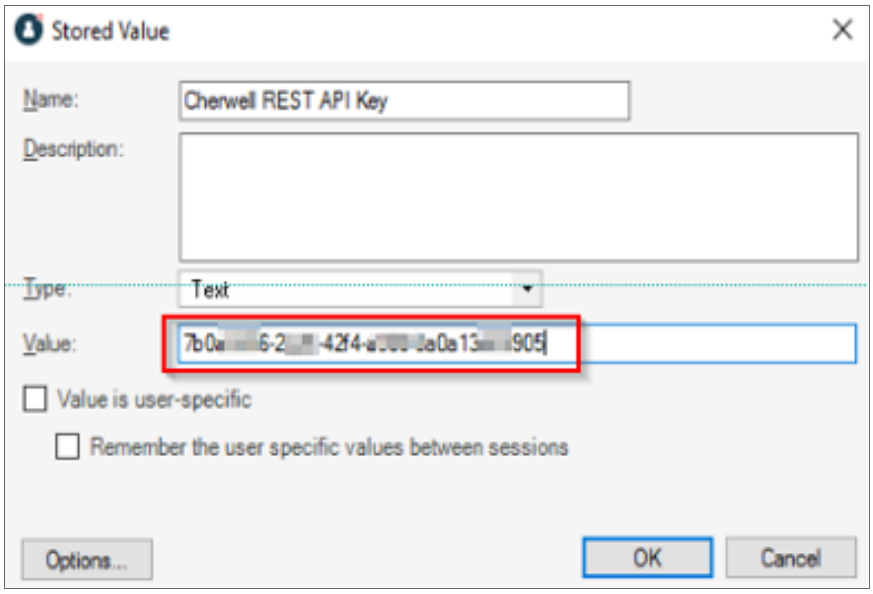


5. In the ***Value*** field, add the REST API Client Key that you configured in *Obtaining a Client Key* and click **[OK]**. This value authenticates against the CSM REST API.
6. Right-click the ***Cherwell REST API Username*** and select *Edit*. The **Stored Value** dialog appears:



7. In the ***Value*** field, type the unique login, such as "SL1", for the user you created in *Creating a New User* and click **[OK]**.

8. Right-click the ***Cherwell REST API Password*** and select *Edit*. The **Stored Value** dialog appears:



9. In the ***Value*** field, type the password for the user you created in *Creating a New User* and click **[OK]**.
10. Close the **Stored Value Manager** window and then click **Save Blueprint to disk** from the **Blueprints** sub-menu.
11. Click **Publish Blueprint**. The Publish Options dialog appears.
12. Accept all defaults and click **[Publish]**.
13. After the changes have been published, go to the following section to add the scheduled tasks.

Chapter 3

Configuring Credentials and the Federated Registration Record

Overview

Before you can enable and use the "Cherwell" SyncPack, you must create credentials to enable communication between PowerFlow, CSM, and SL1. You also need to configure a number of settings on the **Federated Registration** record to enable integrations between CSM and SL1.

> **NOTE:** You should perform these configurations with the Cherwell Service Management (CSM) User client, not the CSM Administrator client.

This chapter covers the following topics:

Creating the Cherwell API Credential *34*
Creating the PowerFlow Federation Source Credential *35*
Configuring the API Credentials *37*
Enabling the Federation Registration Record *37*
Configuring Incident Creation and Updates *38*
Configuring CI Creation and Updates *39*
Configuring Automated Maintenance Windows *42*
Configuring Automated CI Retirements *44*

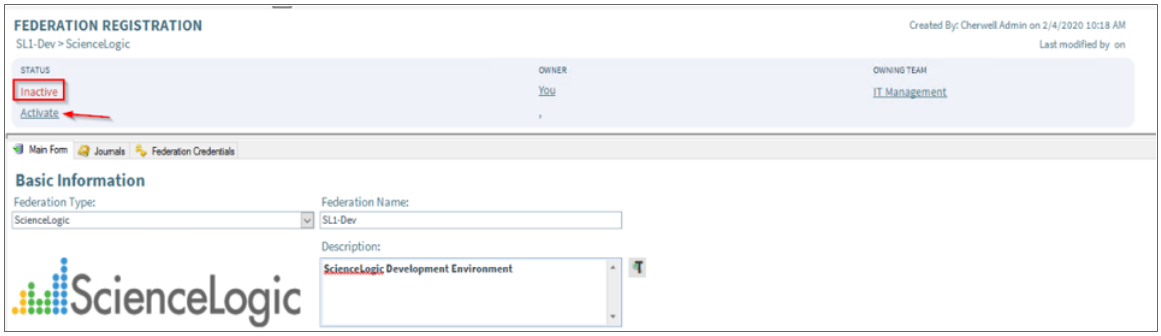
Creating the Cherwell API Credential

Federation Registration records use the Cherwell API to create, update, and search for CIs, and these processes require a Cherwell API credential. Each **Federation Registration** record can use a different credential that tracks which Federation source changed an attribute.

You can use the same CSM username, password, and REST Client Key credentials that you created in *Configuring the Back-end Credentials and Endpoints*.

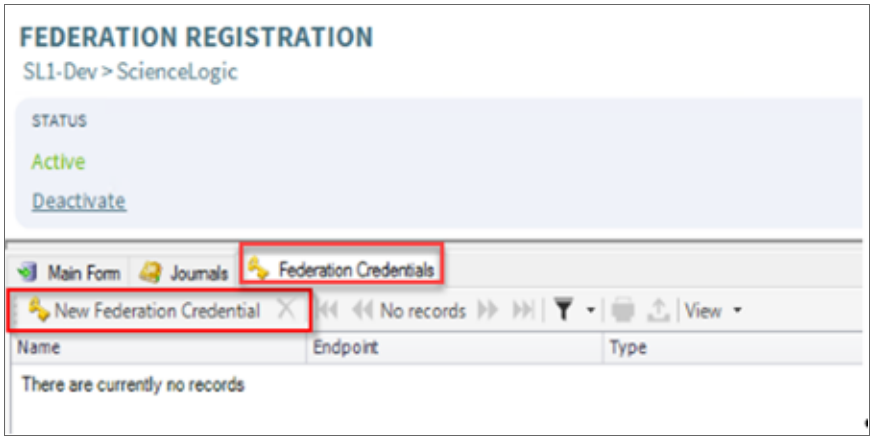
To create the Cherwell API credential:

1. Log in to the CSM User client and go to the **Federation Registration** record you created in *Creating the Federation Registration Record:*

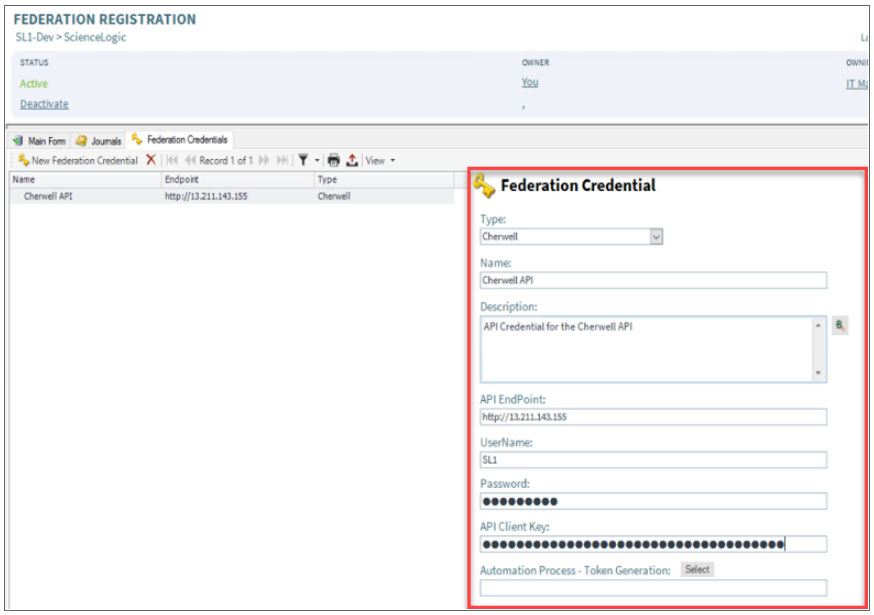


> **TIP:** To quickly find this record, go to **Searching** > **Search Manager** and use the search queries provided. For example, select the **Global** folder under the **Team** folder in the **Search** folder on the left, select *Federation Registration* from the ***Association*** drop-down, and search through the different sources in the bottom pane. The sample Federation Name for this record was "SL1-Dev".

2. On the **Federation Registration** record, go to the **[Federation Credentials]** tab:



3. Click **[New Federation Credential]**. A new **Federation Credential** pane appears:



4. Update the following fields:
   - ***Type***. Select *Cherwell*.
   - ***Name***. Type a unique name, such as "Cherwell API Credential".
   - ***Description***. Type a short explanation of the credential.
   - ***API Endpoint***. Type the URL for the Cherwell API.
   - ***User Name***. Type the username for the user you created in *Creating a New User.*
   - ***Password***. Type the password for the user you created in *Creating a New User.*
   - ***API Client Key***. Add the REST API Client Key you configured in *Obtaining a Client Key.*
5. Click the **[Select]** button to avoid repeated CSM REST API authentication requests by enabling this credential and associated One-Steps to cache the Cherwell Bearer token for re-use. A **Choose Action** dialog appears.
6. On the **[One-Steps]** tab, select **Blueprint > Federation > Cherwell** in the **Action** section.
7. In the ***Association*** drop-down, select *Federation Credential*.
8. In the right-hand pane, double-click **Cherwell: Get Bearer Token**.
9. Click **[OK]**. On the **Federation Registration** record, click the **[Save]** button (💾) to save the new credential.

Creating the PowerFlow Federation Source Credential

You need an API credential for **Federation Registration** records that update a Federation source, such as PowerFlow, with incident reference numbers, maintenance windows, and CI retirement information. You can use this API credential to authenticate with the PowerFlow API and provide updates with that API.

To create the PowerFlow Federation source credential:

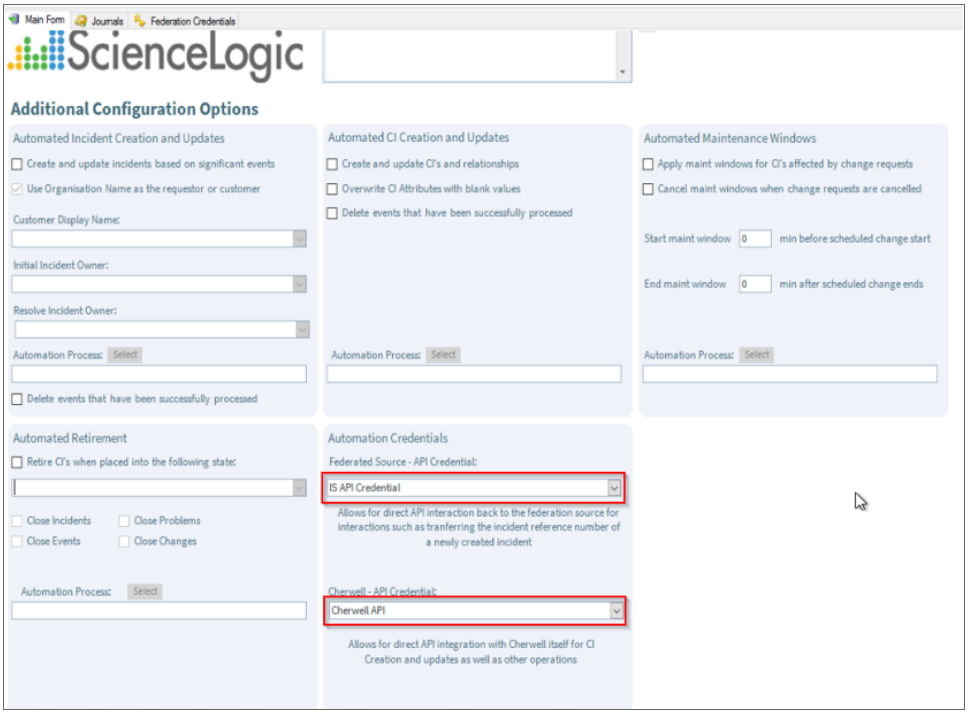
1. Log in to the CSM User client and go to the **Federation Registration** record you created in *Creating the Federation Registration Record.*
2. On the **Federation Registration** record, go to the **[Federation Credentials]** tab.
3. Click **[New Federation Credential]**. A new **Federation Credential** pane appears.
4. Update the following fields:
   - ***Type***. Select *Other*.
   - ***Name***. Type a unique name, such as "IS API Credential".
   - ***Description***. Type a short explanation of the credential.
   - ***API Endpoint***. Type the URL for the PowerFlow API.
   - ***User Name***. Type the username for PowerFlow, such as "isadmin".
   - ***Password***. Type the admin password for PowerFlow.
   - ***API Client Key***. Add the API Client Key for PowerFlow. The API Client Key for PowerFlow credentials is a string encoded in Base64:
     `'IS_username+'':"+IS_password'`

   NOTE: Unless a One-Step author requests you to add a Token Generation process, you do not need to click **[Select]** to add a token. If you need to add a token, see steps 5-8 in *Creating the Cherwell API Credential*.

5. Click **[OK]**. On the **Federation Registration** record, click the **[Save]** button ( ) to save the new credential.

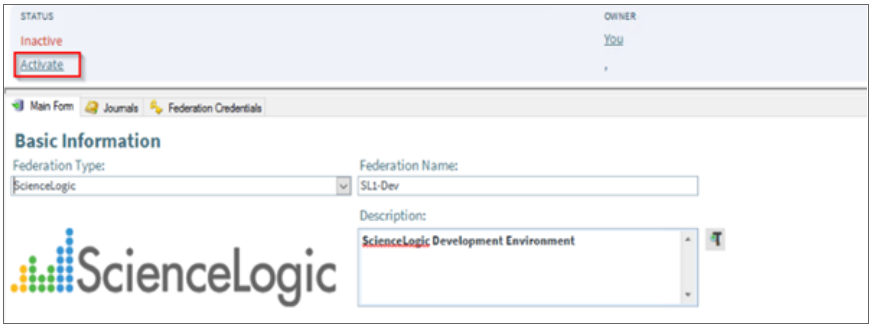
Configuring the API Credentials

After you have created the Cherwell API credential and the PowerFlow (Federation source) credential, align the credentials on the **[Main Form]** tab of the **Federation Registration** record:



Enabling the Federation Registration Record

To enable processing, the **Federation Registration** record must be active and integration must be enabled. If necessary, click **Activate** to activate the record:

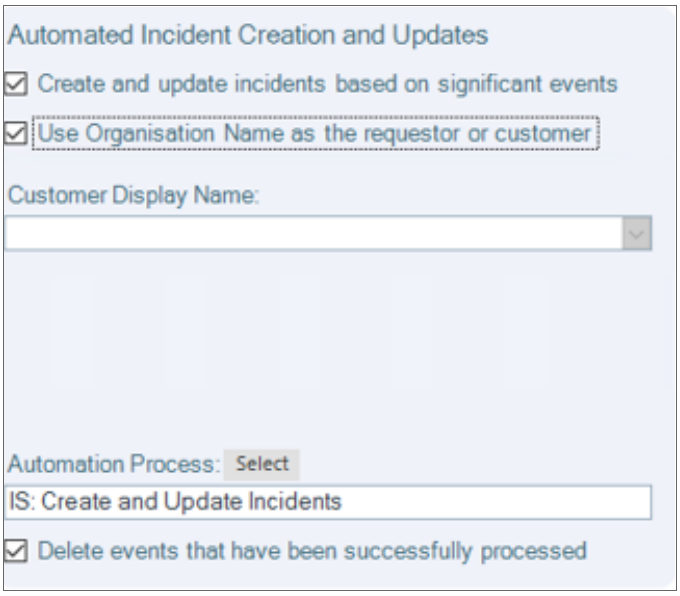


Configuring Incident Creation and Updates

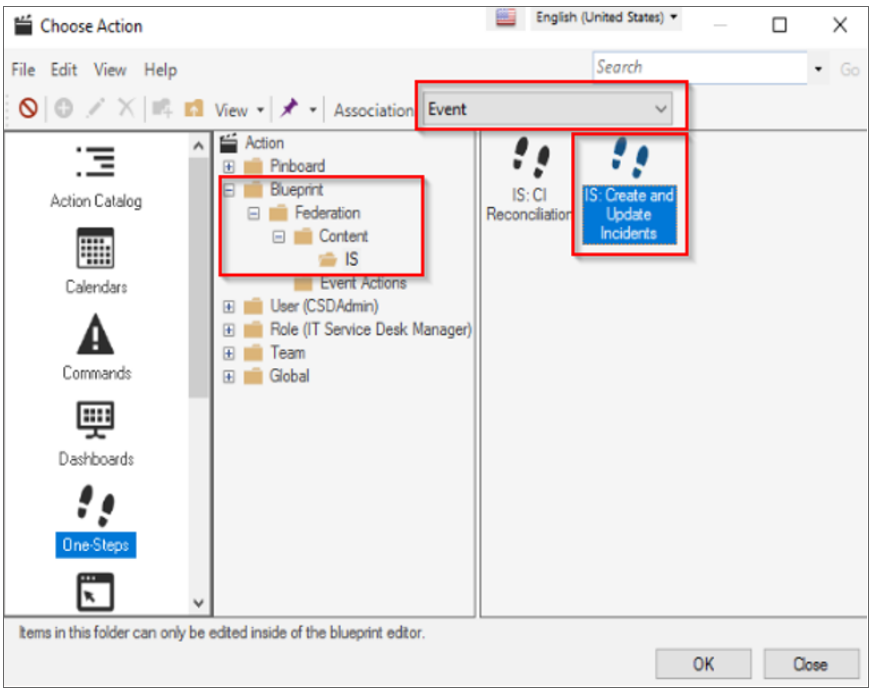
The following settings on the **[Main Form]** tab of the **Federation Registration** record affect how Incident creation and updates work:

- ***Create and update Incidents based on significant events***. Select this option to enable Incident creation and updates .
- ***Use Organization Name as the requester or customer***. All Federated sources are required to send an Organization name as part of the Incident payload. This setting allows the Organization name to be used as the "Customer" name on a newly created Incident record. If the Organization name does not exist as a Customer, it will be created.
- ***Customer Display Name***. If the ***Use Organization Name as the requester or customer*** checkbox is not selected, you can use this drop-down to select a customer record that will be populated as the "Customer" name on each newly created Incident record.
- ***Automation Process***. Regarded as Content, use the **[Select]** button to select the automation process or One-Step that will be executed when a new Incident is needed. You can create different automation processes or One-Steps for different Federation sources, and they can be one-way or, like the PowerFlow integration, two-way where the automations pass back the newly created Incident reference number to PowerFlow through its REST API.
- ***Delete events that have been successfully processed***. This setting helps reduce the storage space used by incoming Incident events by deleting event records that have been successfully processed into Incident records. You can create different automation processes or One-Steps for different Federation sources.

Configure these settings as needed. The following image shows an example configuration:



You can find custom automation processes and One-Steps for Content in the following location after you click the **[Select]** button next to the ***Automation Process*** field:

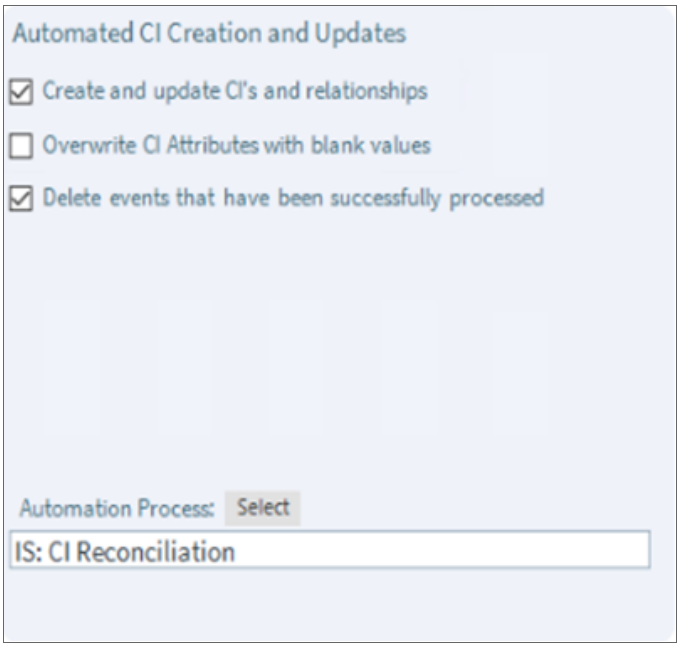


Configuring CI Creation and Updates

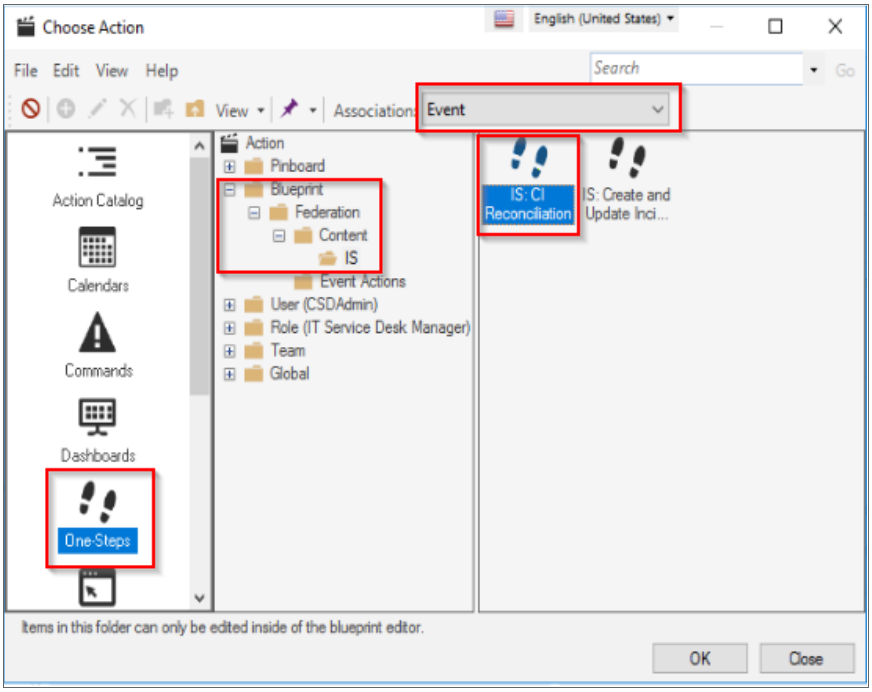
The following settings on the **[Main Form]** tab of the **Federation Registration** record affect how incident creation and updates work:

- ***Create and update CIs and relationships***. Select this option to enable CI creation and updates.
- ***Overwrite CI attributes with blank values***. This setting determines whether CSM CI fields will be overwritten with blank values from a Federation source, even if that CSM CI attribute has data. If you check this option, a CSM CI field that has valid data will be overwritten with blank data from a Federated source if that CSM Field is mapped.
- ***Delete events that have been successfully processed***. This setting helps reduce the storage space used by incoming CI events by deleting event records that have been successfully processed into CI records. These event records are not recoverable except from a backup if this option is selected.
- ***Automation Process***. Regarded as Content, use the **[Select]** button to select the automation process or One-Step that will be executed when a new CI event is received. You can create different automation processes or One-Steps for different Federation sources.

Configure the settings as needed. The following image shows an example configuration:



You can find custom automation processes and One-Steps for Content in the following location after you click the **[Select]** button next to the ***Automation Process*** field:



Configuring the Mappings between Source CI Types and CSM CI Types

To map incoming CI or Device Types from Federated sources like PowerFlow, you must configure the mapping between source CI Types and CSM CI Types.

To map source CI Types and CSM CI Types:

1. While on **Federation Registration** record, select the **[Federated CI Type Mapping]** tab.
2. Click the **[New Federated CI Mapping]** button. A new Federated CI Mapping record appears.
3. Complete the following fields:

    - ***Federated CI Type***. Type the name that identifies the device or CI in the Federated source.
    - ***Target CI Type Name***. Select the name that identifies what CSM CI Type will be created when a new CI is required and the "Federated CI Type" for that new CI matches the value in the ***Federated CI Type*** field.

    > **NOTE:** If this drop-down is blank, refer to *Creating and Testing the Populate Field Definition Mappings*, as this process must be working for this drop-down to work.

    - ***Target CI Type***. Select the target CSM CI Type, which is related to the CSM CI Type Name. This value can be regarded as a further CI Type classification, and in most CSM instances this is not a required field.

4. Click the **[Save]** button ( ) to save the mapping. Repeat this process for any other CI Type mappings.

> **NOTE:** This process can sometimes involve a large number of configurations, but the process can be automated to create a large number of these configurations automatically.

Configuring the Mappings between Source CI Attributes and CSM Fields

To map incoming Device attributes from a Federated source to CI attributes, you must configure the mapping between Federated source CI attributes and CSM fields.

To map Federated source CI attributes and CSM fields:

1. While on **Federation Registration** record, select the **[Federated Field Mappings]** tab.
2. Click the **[New Federated Field Mapping]** button. A new record appears.
3. Complete the following fields:

- ***Federated Field Name Type***. Type the name of the CI attribute or field name that will be passed in from the Federated source.
- ***Cherwell Business Object Name*** drop-down, select the CSM CI Type Name to which the CI attribute will be mapped. Different CSM CI Types have different fields, and this drop-down drives the values in the ***Cherwell Field Name*** drop-down.

> **NOTE:** If this drop-down is blank, refer to *Creating and Testing the Populate Field Definition Mappings*, as this process must be working for this drop-down to work. Additionally, if you need to map the same Federated source CI attribute or field name to multiple CSM CI Types, you must create multiple records for each CSM CI Type.

- ***Cherwell Field Name***. Select the CI field name to which the Federated source attribute or field will be mapped.
- ***This field is used for reconciliation...*** Select this option if this attribute or field name is to be used for CI reconciliation, such as finding an existing CI to update rather than creating a new one. As a best practice, you should select at least one or more CI Field mappings for CI reconciliation for each CI Type. Otherwise, new CIs will be created for every sync to the Federated source.

4. Click the **[Save]** button ( ) to save the mapping. Repeat this process for subsequent CI Type mappings.

> **NOTE:** If more than one CI attribute or field is selected for CI reconciliation per CSM CI Type Name, an AND operation is performed to find a CI. For example, if you used "FriendlyName" and "IPAddress" for reconciliation, then a match must be found on "FriendlyName" AND "IPAddress" to find a CI. If not, a new CI is created.

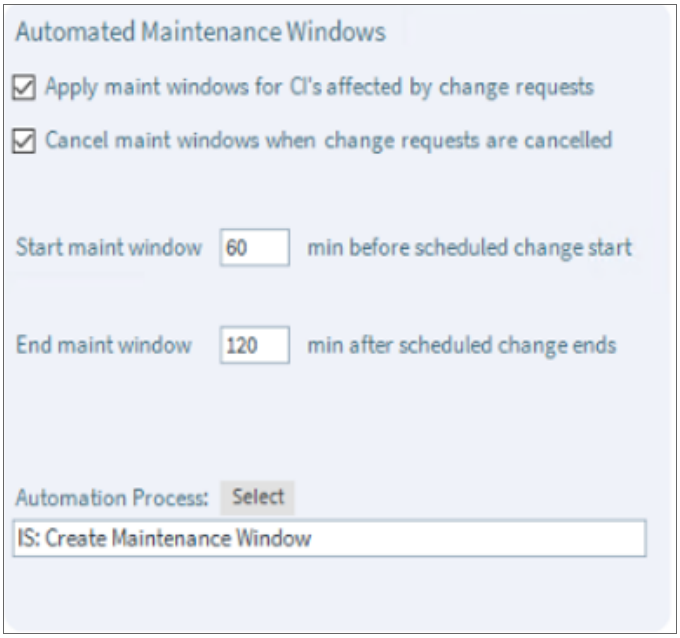
Configuring Automated Maintenance Windows

The following settings on the **[Main Form]** tab of the **Federation Registration** record affect how Automated Maintenance Windows work:

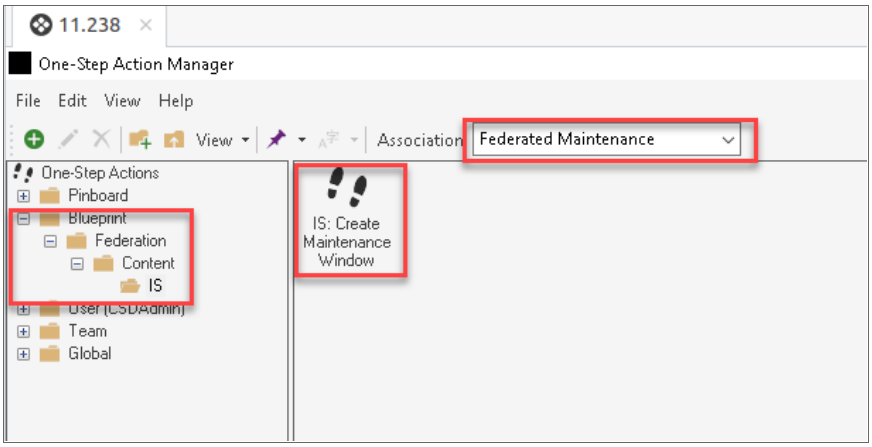
- ***Apply maintenance windows for CIs affected by change requests***. Select this option to enable automated Maintenance Windows.
- ***Cancel maintenance windows when change requests are canceled***. Select this option to cancel Maintenance Windows when a corresponding CSM Change Request record is canceled.
- ***Start maintenance window N minutes before scheduled change starts***. If it is required that the Maintenance Window on the Federated source is started *before* the CSM Change Window starts, specify the number of minutes that should be subtracted from the start time of the CSM Change Window. For example, specifying a value of 60 in this field ensures that the Maintenance Window on a Federated device will start one hour before the CSM Change Window.

- ***Start maintenance window N minutes before scheduled change starts***. If it is required that the Maintenance Window on the Federated source device is completed *after* the CSM change window ends, specify the number of minutes that should be added after the scheduled CSM Change Window ends. For example, specifying a value of 60 in this field ensures that the Maintenance Window on a Federated device ends one hour after the CSM Change Window.
- ***Automation Process***. Regarded as Content, use the **[Select]** button to select the automation process or One-Step that will be executed for new or updated Maintenance Windows. You can create different automation processes or One-Steps for different Federation sources.

Configure the settings as needed. The following image shows an example configuration:



You can find custom automation processes and One-Steps for Content in the following location after you click the **[Select]** button next to the ***Automation Process*** field:



Configuring Automated CI Retirements

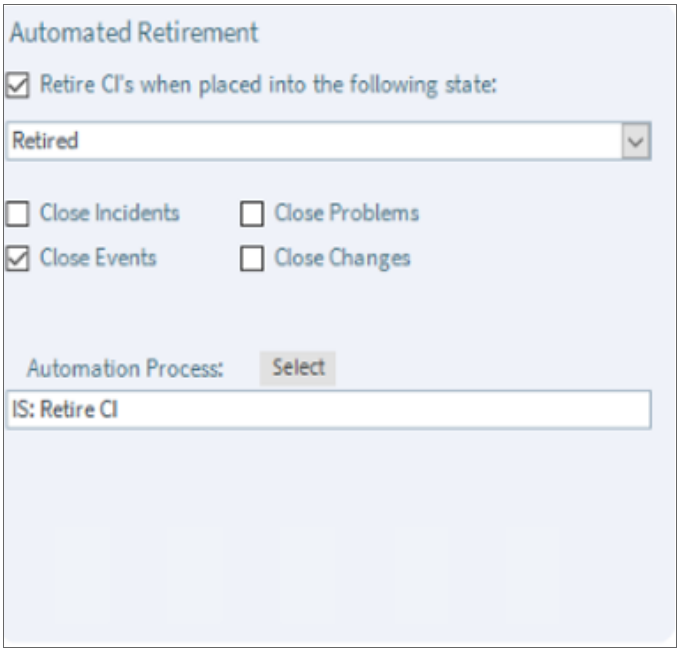
The following settings on the **[Main Form]** tab of the **Federation Registration** record affect how Automated CI retirement works:

1. ***Retire CIs when placed into the following state:*** Select this option to enable automated CI retirement. Use the drop-down to select what CI status will trigger the retirement workflow. Different implementations of CSM – could have different statuses. When a CI is placed into this status, the retirement process will be triggered.
2. ***Close Incidents/Problems/Events/Changes***. Select the relevant checkboxes to control whether CSM records and associated monitoring events in the Federated source will be closed as a result of CI retirement.

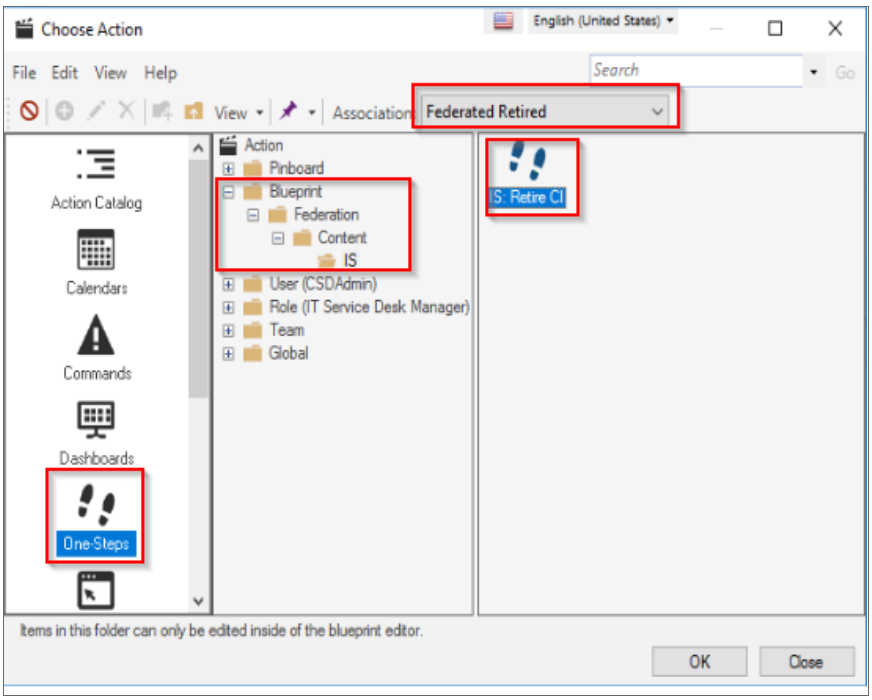
   > **NOTE:** Because of varying closure procedures and ITIL processes, the automation process or One-Step will need to be tuned for each customer environment. For example, some CSM implementations have required fields on closure.

3. ***Automation Process***. Regarded as Content, use the **[Select]** button to select the automation process or One-Step that will be executed when retiring CIs. You can create different automation processes or One-Steps for different Federation sources.

Configure the settings as needed. The following image shows an example configuration:



You can find custom automation processes and One-Steps for Content in the following location after you click the **[Select]** button next to the ***Automation Process*** field:



Chapter 4

Configuring SL1 and SL1 PowerFlow

Overview

This chapter describes how to install and configure the "Cherwell Integration" PowerPack in SL1. This chapter also covers how to configure the applications in the "Cherwell" SyncPack to properly authenticate SL1 PowerFlow with CSM and SL1.

NOTE: Follow the procedures in this chapter only after you have configured the settings in CSM from the previous chapters.

This chapter covers the following topics:

Configuring the Cherwell Integration PowerPack *47*

Creating a SOAP/XML Credential for Cherwell Integration *48*

Enabling the Run Book Automation Policies *49*

Enabling and Customizing the Run Book Action Policy *51*

Aligning a Configuration Object with PowerFlow Applications *51*

Sending Additional Metadata for Incident Records *55*

Configuring the Cherwell Integration PowerPack

The "Cherwell Integration" PowerPack includes:

- A Sample SL1 credential, "SL1 IS4 API Creds"

> **NOTE:** "IS4" is a now-deprecated name for SL1 PowerFlow.

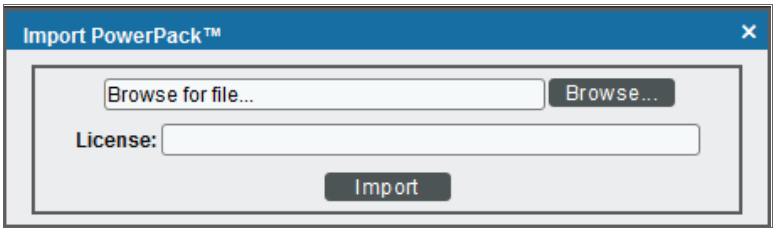
- The "Cherwell Event IS4 Integration" run book action policy, which you can use to automate adding, updating, and clearing SL1 events
- The following run book automation policies to automate adding, updating, and clearing events:
    - Cherwell Create Event IS4
    - Cherwell Update Ticket on Acknowledge
    - Cherwell Clear Event IS4

After you have configured CSM to work with the SyncPack, you will need to install and configure the "Cherwell Integration" PowerPack in SL1.

Downloading and Installing the PowerPack in SL1

To download and install the PowerPack:

1. Download the PowerPack from the ScienceLogic Support Site.
2. In SL1, go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.
4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal appears, click the **[Install]** button to install the PowerPack.

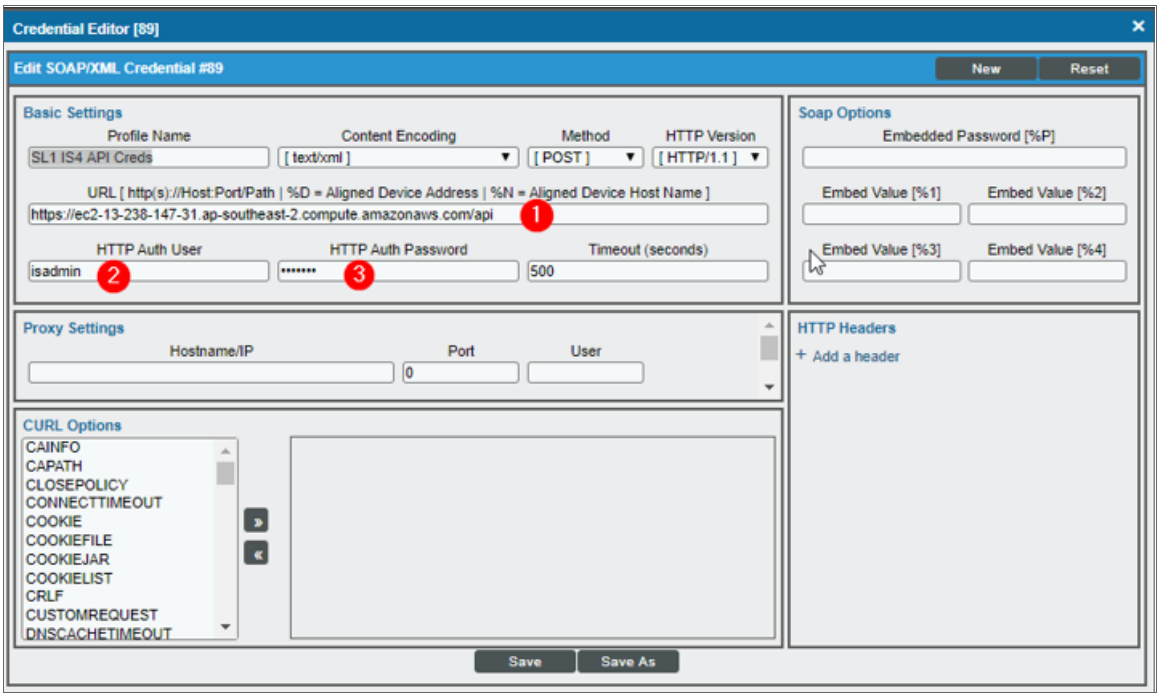
NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]**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

Creating a SOAP/XML Credential for Cherwell Integration

You will need to create a credential in SL1 that allows SL1 to communicate with CSM. The "Cherwell Integration" PowerPack includes the *SL1 IS4 API Creds* credential, which you can use as a template to create this credential.

To create the SL1 credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon ( ) for the *SL1 IS4 API Creds* credential. The **Credential Editor** modal window appears:



3. Supply values in the following fields, and the leave the remaining fields at their default settings:

   - ***URL***. Type the URL for the PowerFlow API, which is the same URL that you used to create the PowerFlow Credential in the Federation Registration record. You will need to add "/api" to the end of this URL.
   - ***HTTP Auth User***. Type the PowerFlow username that will authenticate to the PowerFlow API. This is the same username that you created and configured in the Federation Registration credential.

- ***HTTP Auth Password***. Type the PowerFlow password for the PowerFlow user that will authenticate to the PowerFlow API. This is the same username that you created and configured in the Federation Registration credential.

4. Click the **[Save As]** button and type a new name for this credential.
5. When the confirmation message appears, click **[OK]**.

Enabling the Run Book Automation Policies

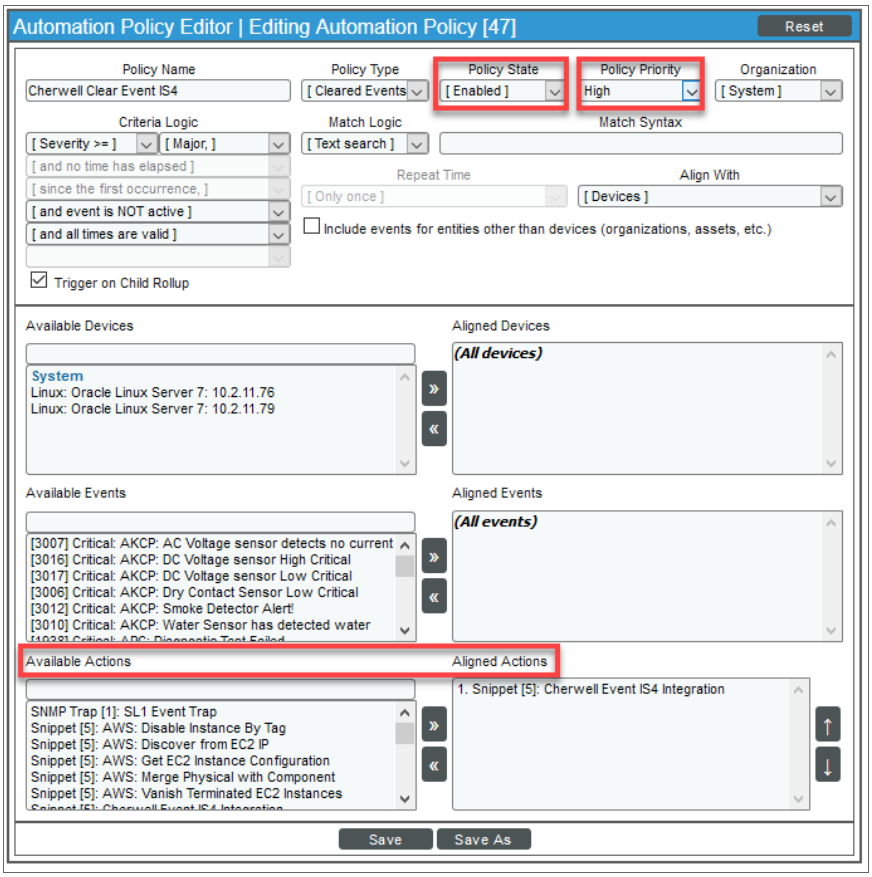
Before you can run the "Cherwell Event IS4 Integration" run book action, you must enable the three related run book automation policies in SL1:

- Cherwell Create Event IS4
- Cherwell Update Ticket on Acknowledged IS4
- Cherwell Clear Event IS4

> **NOTE:** "IS4" is a now-deprecated name for SL1 PowerFlow.

To enable the three Cherwell Run Book Automation policies:

1. In SL1, go to the **Automation Policy Manager** page (Registry > Run Book > Automation).
2. Locate the "Cherwell Create Event IS4" automation policy and click its wrench icon (). The **Automation Policy Editor** page appears:



3. Update the following fields:
   - ***Policy State***. Select *Enabled*.
   - ***Policy Priority***. Select *High* to ensure that this automation policy is added to the top of the queue.
   - ***Available Actions***. If it is not already selected, select the corresponding Cherwell Run Book Action policy.

TIP: By default, the "Cherwell Create Event IS4" automation policy will create Cherwell incidents for ***all*** devices. You can limit the devices affected by making changes to the ***Organization***, ***Severity***, ***Match Logic***, ***Aligned Devices***, and/or ***Aligned Events*** fields.

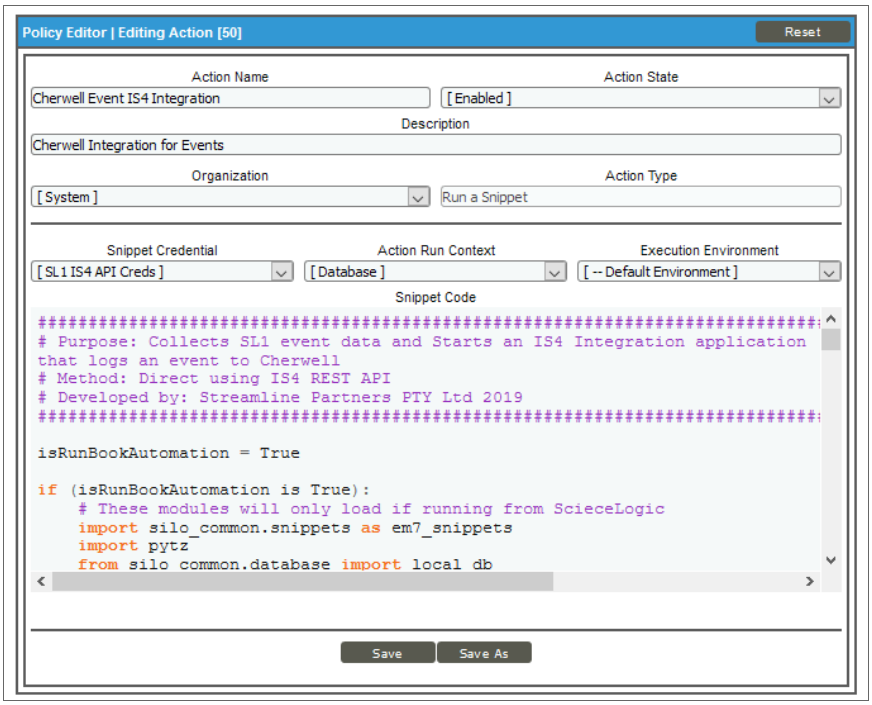
WARNING: ScienceLogic highly recommends that you do not make changes to the ***Policy Type***, ***Repeat Time***, or ***Align With*** fields or the *And event is NOT acknowledged* setting.

4. Click **[Save]**.
5. Repeat steps 2-4 for the "Cherwell Update Ticket on Acknowledge" and "Cherwell Clear Event IS4" run book automation policies.

Enabling and Customizing the Run Book Action Policy

To enable the run book action:

1. In SL1, go to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. Locate the **Cherwell Event IS4 Integration** policy and click its wrench icon (). The **Action Policy Editor** page appears:



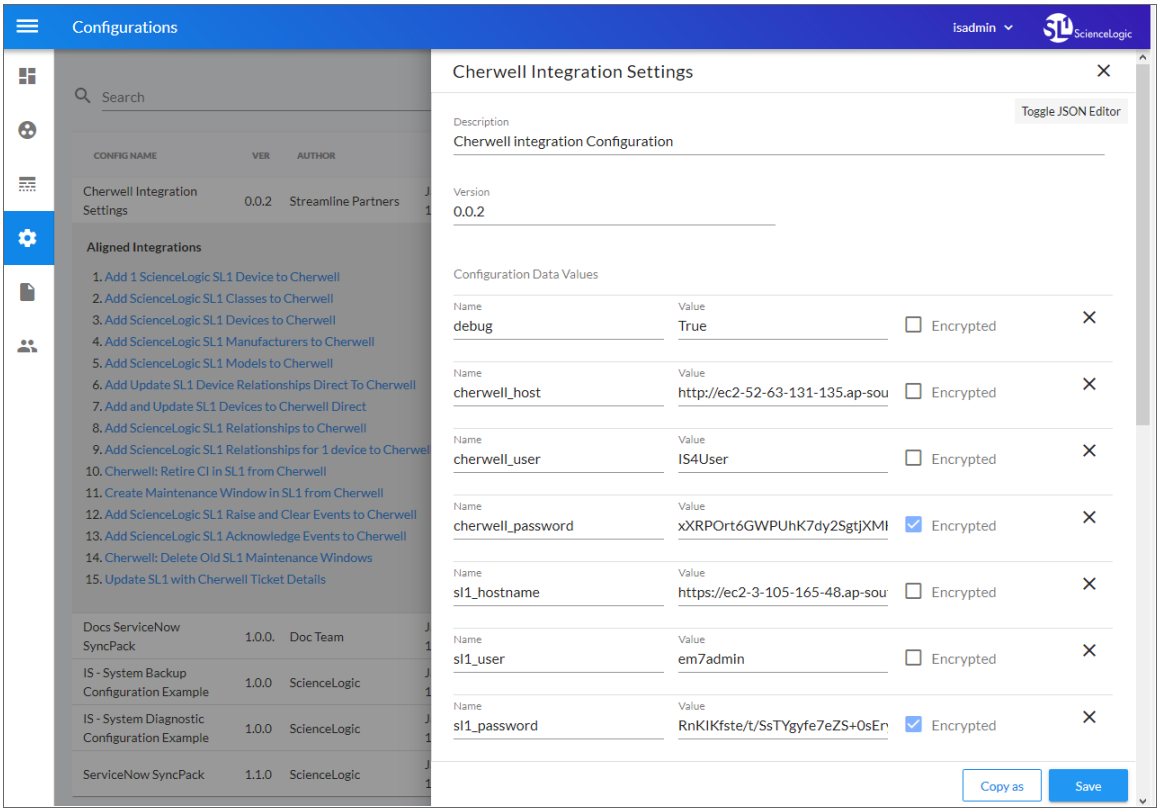
3. For the ***Action State*** filed select *Enabled*.
4. Click **[Save]**. SL1 events are now synced with CSM incidents.

Aligning a Configuration Object with PowerFlow Applications

The "Cherwell" SyncPack includes the "Cherwell Integration Settings" (cherwell_config) configuration object, which you can access in the PowerFlow user interface.

This configuration file contains default name-value pairs for the CSM and SL1 hosts, the CSM and SL1 users and passwords, the PowerFlow host, user, and password, and other keys and values. You can use this configuration file as a template for the configuration objects you need to create and align with the relevant Cherwell applications.

To view the contents of the "Cherwell Integration Settings" (cherwell_config) configuration object, go to the **Configurations** page of the PowerFlow user interface and click the **[Actions]** button (⋮) next to the "Cherwell Integration Settings" configuration. The **Configuration** pane appears:



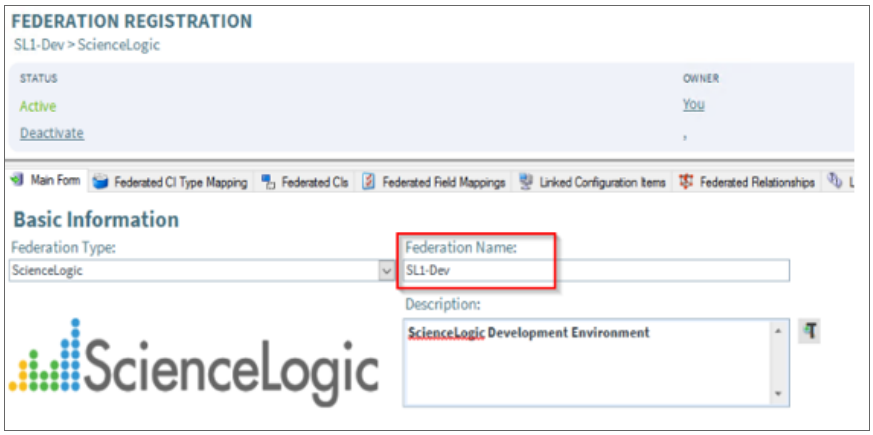
Adding and Editing Credentials in a Configuration Object

From the **Configurations** page of the PowerFlow user interface, you can edit an existing configuration object or create a new configuration object.

For example, you can edit the variables in the "Cherwell Integration Settings" configuration object that came with the SyncPack and then align that configuration object with one or more CSM-related applications. You can also use the **[Copy As]** button to make a copy of that configuration object so you can align it with other applications.

The following configuration object variables are required for the "Cherwell" SyncPack:

- ***cherwell_host***. Type the URL you use to access the Cherwell host. This is the same URL that you used in *Creating the Cherwell API Credential*.
- ***cherwell_user***. Type the CSM Login ID that will be used to authenticate to the CSM API. This is the same username that you created in *Creating a New User.*
- ***cherwell_password***. Type the CSM password for the Cherwell User that will be used to authenticate to the CSM API. This is the same password that you created in *Creating a New User.*
- ***cherwell_api_key***. Add the REST API Client Key that you configured in *Obtaining a Client Key*.
- ***federation_source***. Type the Federation Name that you used in *Creating the Federation Registration Record*:



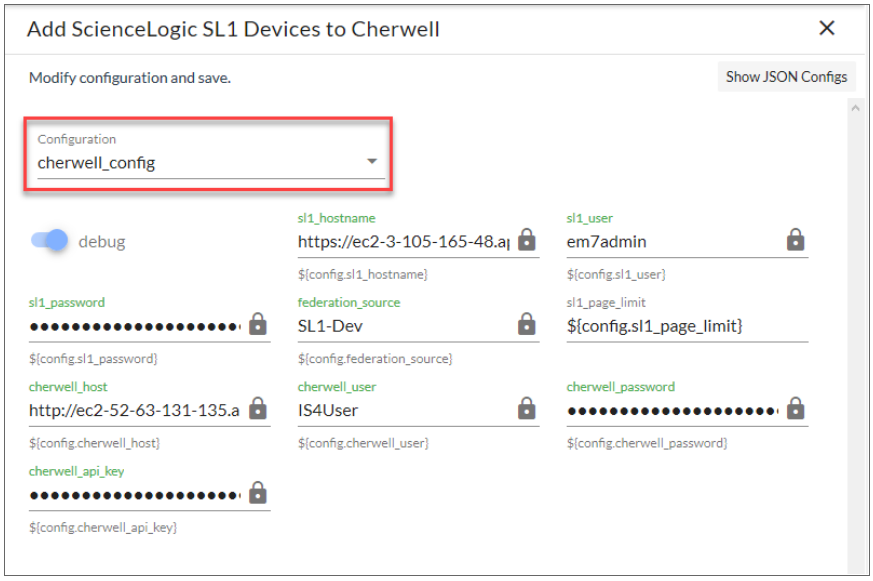
Aligning a Configuration Object with a PowerFlow Application

For every application in PowerFlow, you will need to "align" a configuration object to that application to ensure that the application can properly authenticate to CSM. You can align the same configuration object with multiple applications.

To align a configuration object with an application:

1. In the PowerFlow user interface, go to the **Applications** page ( ).
2. Select the application that you want to align with the configuration object, such as "Add ScienceLogic SL1 Devices to Cherwell". The **Application** page for that application appears.

3. Click **[Configure]** ( ). The **Configuration** pane opens on the right side of the **Application** page:



> **TIP:** To view a pop-up description of a field on the **Configuration** pane for an application, hover over the label name for that field.

4. Select a configuration from the ***Configuration*** drop-down to "align" to this application. This step is required for all applications.

> **TIP:** Click **[Show JSON Configs]** to view the JSON configuration data for the configuration object. Click **[Hide JSON Editor]** again to view the fields instead.

5. As needed, edit the other configuration values for the application. Press **[Enter]** after editing an item to make sure your changes are saved.

> **NOTE:** To prevent potential issues with security and configuration, any fields that are encrypted and any configuration-specific fields containing a padlock icon ( ) on the **Configuration** pane cannot be edited.

6. When you are finished, click **[Save]** at the bottom of the **Configuration** pane.

Sending Additional Metadata for Incident Records

You can pass additional information from SL1 to PowerFlow and populate any additional field on the Incident record. This process uses the "Cherwell Event IS4 Integration" run book action from the "Cherwell Integration" PowerPack.

The "Cherwell Event IS4 Integration" run book action collects information about the event and sends it to PowerFlow to create an incident.

To pass additional information from SL1 to PowerFlow:

1. In SL1, navigate to the **Action Policy Manager** page (Registry > Run Book > Action) and edit the "Cherwell Event IS4 Integration" run book action to enable it to collect the data from SL1 using the API or some other source.
2. In the snippet section, update the **em7_data** dictionary with the key you want the value to be addressed by and the value. For example: `"ClassName": EM7_VALUES[%_class_name]`:

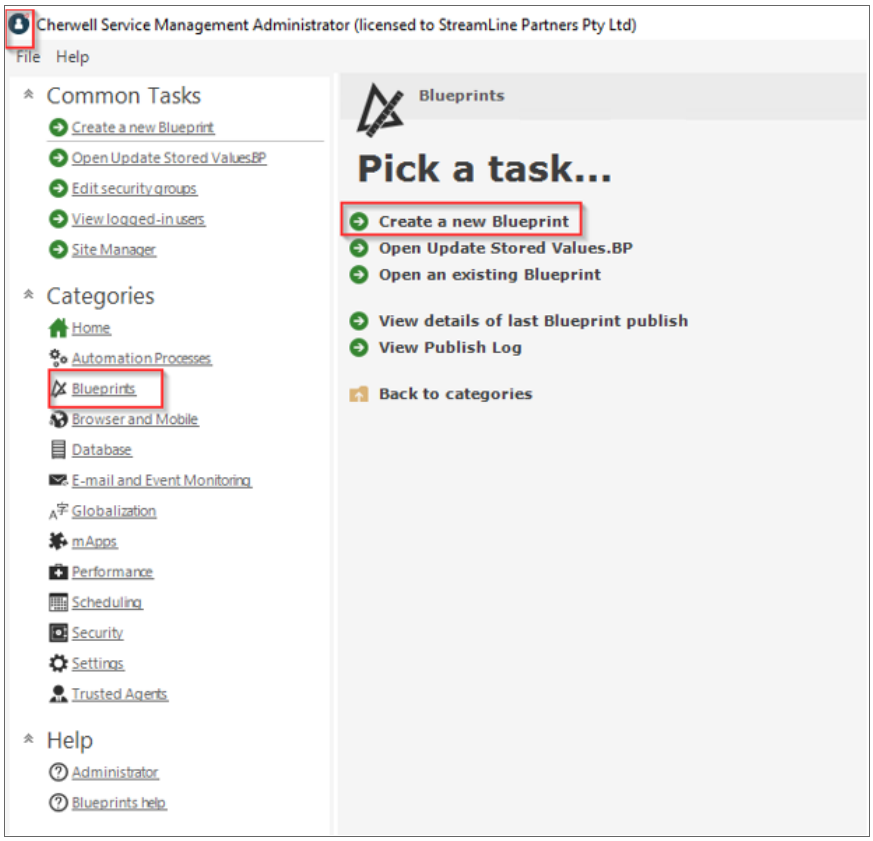
```
em7_data = {
    "EventClearedBy": TicketValues["EventClearedBy"],
    "EventSeverity": TicketValues["EventSeverity"],
    "EventCount": TicketValues["EventCount"],
    "EventSource": TicketValues["EventSource"],
    "ScienceLogicOrganisation": TicketValues["ScienceLogicOrganisation"],
    "Device": TicketValues["Device"],
    "DeviceID": TicketValues["DeviceID"],
    "DeviceIPAddress": TicketValues["DeviceIPAddress"],
    "DeviceCategory": TicketValues["DeviceCategory"],
    "DeviceClass": TicketValues["DeviceClass"],
    "EventMessage": TicketValues["EventMessage"],
    "AutomationActionName": TicketValues["AutomationActionName"],
    "EventURL": TicketValues["EventURL"],
    "EventNote": TicketValues["EventNote"],
    "ExternalTicketNumber": TicketValues["ExternalTicketNumber"],
    "EventCleared": TicketValues["EventCleared"],
    "Priority": TicketValues["Priority"],
    "EventFirstOccurred": TicketValues["EventFirstOccurred"],
    "EventTime": TicketValues["EventTime"],
    "EventSummaryOccured": TicketValues["EventSummaryOccured"],
    "EventLastOccurred": TicketValues["EventLastOccurred"],
    "ClearedTimeStamp": TicketValues["ClearedTimeStamp"],
    "EventID": EM7_VALUES['%e']
}
```

3. In the PowerFlow user interface, navigate to the **SyncPacks** page (⚙), select *Cherwell SyncPack*, and on the **[Steps]** tab select the "Collect and Transform SL1 RBA Data" step. This step collects the data sent by the run book action and passes it to the "Cherwell: Create Event" step, which processes the SL1 Event into a Cherwell Event.
4. Update the payload dictionary in the step with the key and value you added. For example: `"ClassName": event_details["ClassName"]`

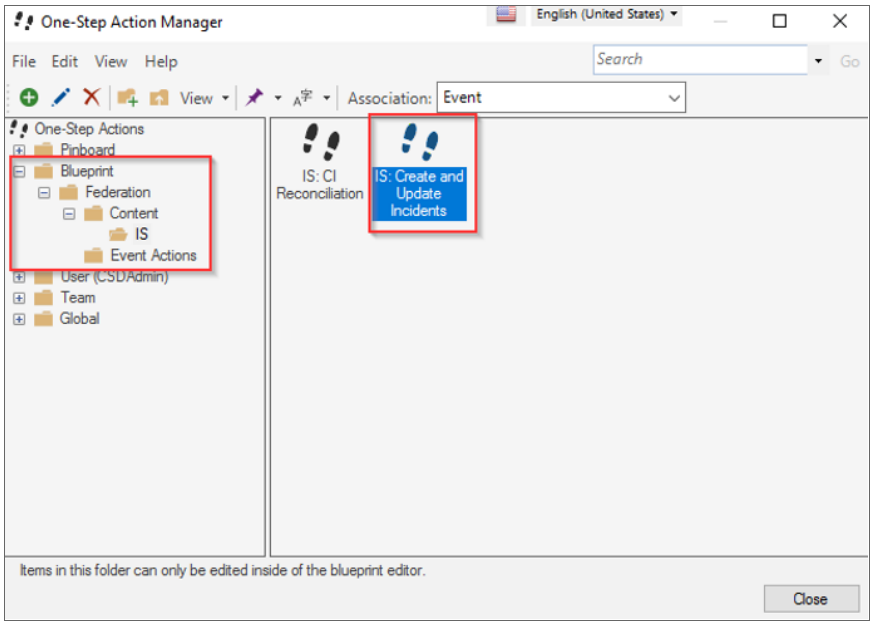
```
event_details = self.get_parameter("eventDetails")

payload = {
    "em7_data": {
        "EventClearedBy": event_details["EventClearedBy"],
        "EventSeverity": event_details["EventSeverity"],
        "EventCount": event_details["EventCount"],
        "EventSource": event_details["EventSource"],
        "ScienceLogicOrganisation": event_details["ScienceLogicOrganisation"],
        "Device": event_details["Device"],
        "DeviceID": event_details["DeviceID"],
        "DeviceIPAddress": event_details["DeviceIPAddress"],
        "DeviceCategory": event_details["DeviceCategory"],
        "DeviceClass": event_details["DeviceClass"],
        "EventMessage": event_details["EventMessage"],
        "AutomationActionName": event_details["AutomationActionName"],
        "EventURL": event_details["EventURL"],
        "EventNote": event_details["EventNote"],
        "ExternalTicketNumber": event_details["ExternalTicketNumber"],
        "EventCleared": event_details["EventCleared"],
        "Priority": event_details["Priority"],
        "EventFirstOccurred": event_details["EventFirstOccurred"],
        "EventTime": event_details["EventTime"],
        "EventSummaryOccured": event_details["EventSummaryOccured"],
        "EventLastOccurred": event_details["EventLastOccurred"],
        "ClearedTimeStamp": event_details["ClearedTimeStamp"],
        "EventID": event_details["EventID"]
    }
}
```

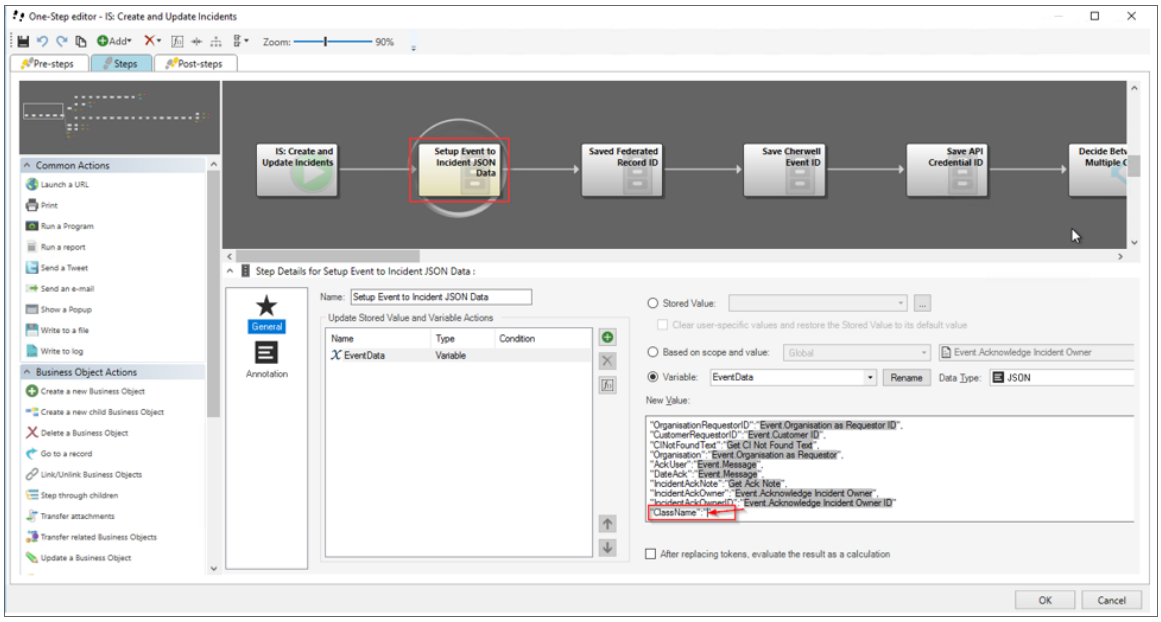
5. Log in to the CSM Administrator client as an administrator, select **Blueprints** in the **Categories** sub-menu on the left, and select **Create a new Blueprint**:



6. In the **New Blueprint** window, select the **Managers > One-Step** . The **One-Step Action Manager** window appears:

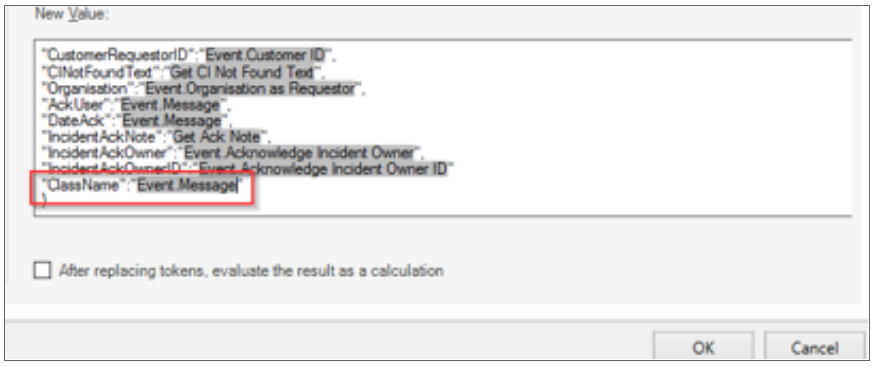


7. In the **Association** drop-down, select *Event*.
8. Navigate to the "Blueprint/Federation/Content/IS" folder, right-click the "IS: Create and Update Incidents" One-Step file, and select *Edit*. The **One-Step Editor** page appears:



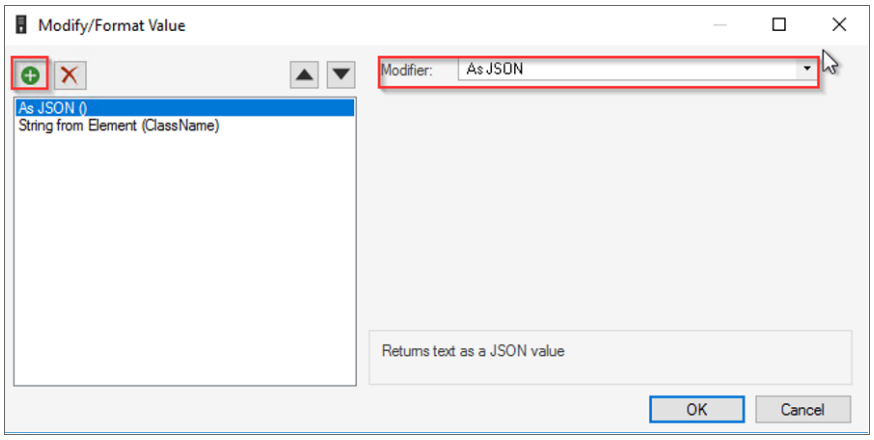
9. Select the "Setup Event to Incident JSON Data" step so you can append the value you added to the dictionary in step 4 as a key-value pair at the end of the dictionary on this step. For example: `"ClassName": event_details["ClassName"]`
10. To append the value, type the key for the new value in the ***New Value*** field, such as `"ClassName"`.

11. To add a value to associate with the new key, right-click between the two quotation marks in the entry you made in step 10 in the ***New Value*** field and select *Message* from the pop-up dialog.
12. Type the value after the new key, such as `"ClassName":"Event.Message"`:



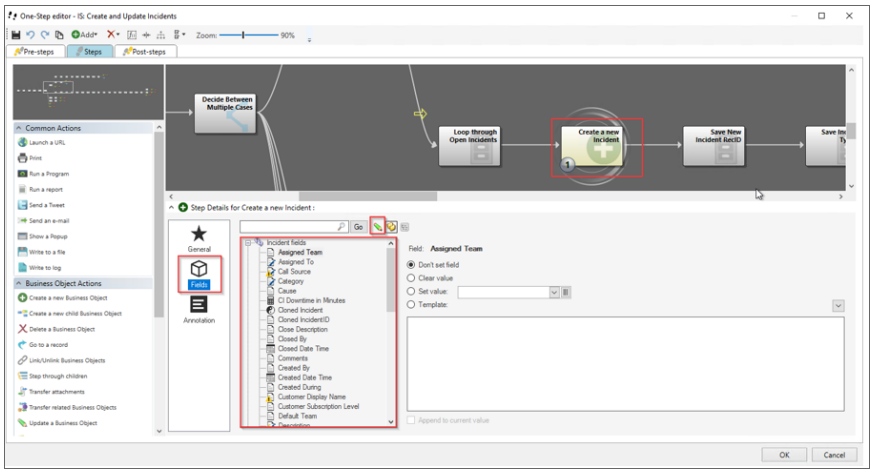
> **NOTE:** `Event.Message` is a reference to the Cherwell ***Message*** field in the event. The ***Message*** field holds all the information about the SL1 event in it via the payload you modified in step 4.

13. To get the field you want in the payload for `ClassName`, you need to apply a filter by right-clicking `Event.Message` and selecting *Modifiers*. The **Modify/Format Value** window appears, where you can apply filters to assign a value for `ClassName`:

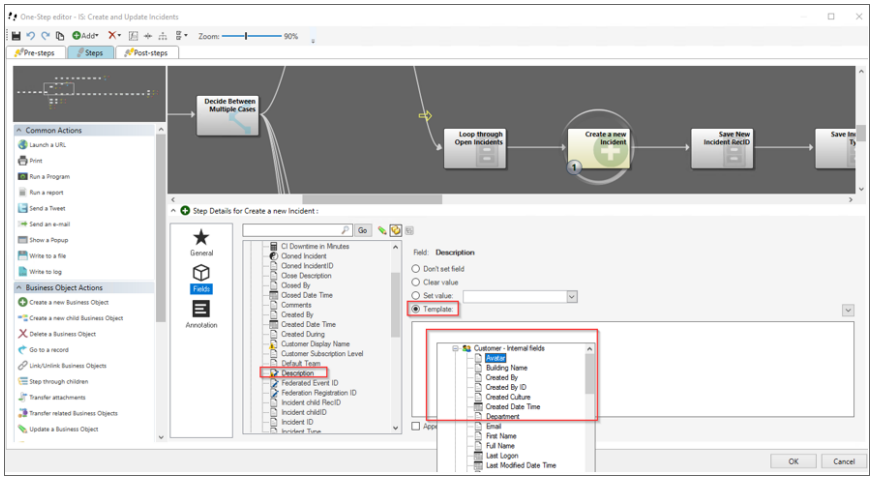


14. Click **[+]** at top left and select *As JSON* from the ***Modifier*** drop-down.
15. Click **[+]** again, select *String from Element* from the ***Modifier*** drop-down, and type the name of the key for the new value you put in the dictionary in step 4, such as `ClassName`.
16. Click **[OK]**. The relevant value in the dictionary contains the variable next to *ClassName*.

17. On the **One-Step Editor** page, select the "Create a new Incident" step and click the **Fields** tab:

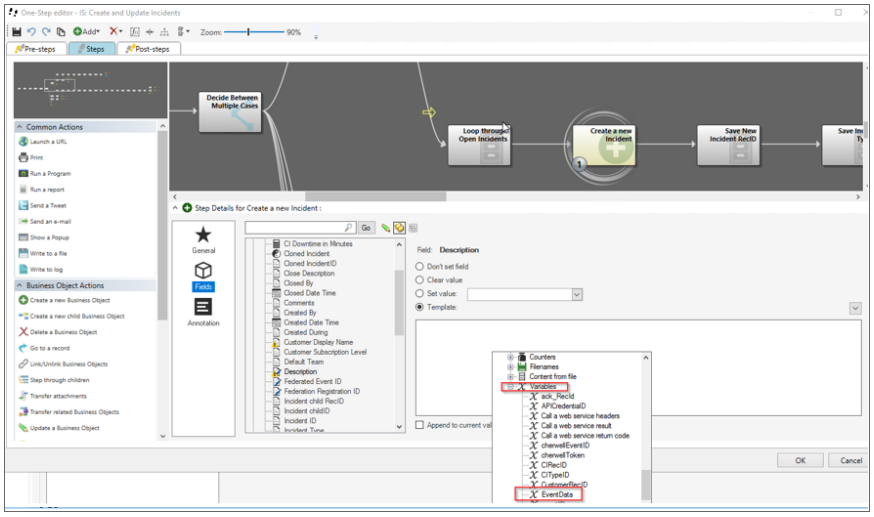


18. Make sure that the pencil icon is unchecked so you can assign the `ClassName` variable to any of the fields available in the incident:



19. For example, if you wanted to add `ClassName` to the ***Description*** field, select *Description* in the list of fields, select *Template*, and right-click on the empty text area below to bring up the variable selector.

20. From the variable selector, scroll down to the ***Variables*** drop-down and select *EventData* as this is the variable we assigned to the payload in the "Setup Event to Incident JSON Data" step:



21. Apply filters to the "`EventData`" variable to assign the relevant value to it from the payload by right-clicking **EventData** and selecting *Modifiers*. The **Modify/Format Value** window appears.
22. Click **[+]**, select *String from Element* from the ***Modifier*** drop-down, and type the name of the key for the new value you appended in the dictionary in the step "Setup Event to Incident JSON Data".
23. Click **[OK]**. The **Manage objects** page appears.
24. Accept the changes you made to the One-Step and save the Blueprint by clicking **Save Blueprint to disk**.
25. Publish the Blueprint by clicking **Publish Blueprint**. The **Publish Options** dialog appears.
26. Use the default settings and click **[Publish]**. When the publish process is complete, the next time an event occurs, you will see the enriched data in the field you selected on the form.

Chapter 5

Troubleshooting the Cherwell SyncPack

Overview

This chapter describes how to troubleshoot certain aspects of the SL1 and CSM integration for the "Cherwell" SyncPack.

This chapter covers the following topics:

Incidents are not being created *63*

CIs are not being created *63*

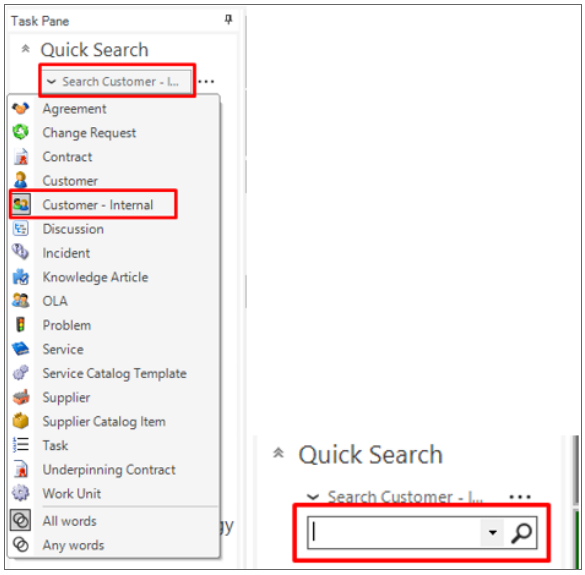
Viewing Events Sent from PowerFlow *66*

Checking the Automation Process Status *67*

Incidents are not being created

If Incident Creation is set up to use the SL1 Organization as a Customer for the Incident, and Incidents are not being created, check to see if a record for the SL1 Organization has not been created multiple times:

1. In the CSM User client, search all "Customer – Internals" Records by going to the following menu:



2. Click in the empty ***Search*** field and press **[Enter]** to search all records.
3. If you find a duplicate record for the SL1 Organization, select the duplicate, and go to **File > Delete.**
4. After you delete all duplicates, when events come in for that Organization in SL1, the tickets should be created without any issues.

TIP: Another option for fixing this issue is to manually create all SL1 Organizations in CSM before enabling Automated Incident Creation.

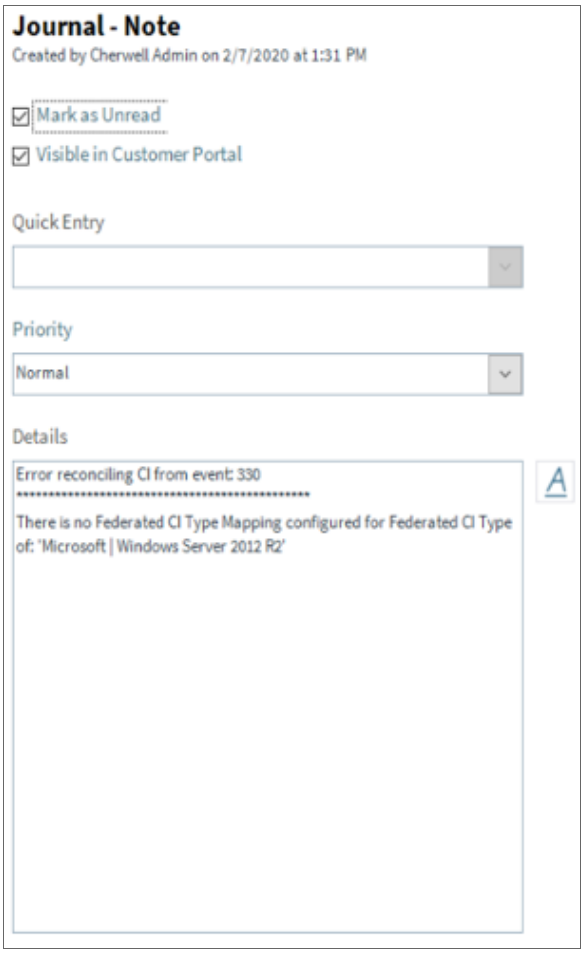
CIs are not being created

During the CI creation process, various issues might occur. You can find more information about these issues on the **[Journal]** tab of the **Federation Registration** record.

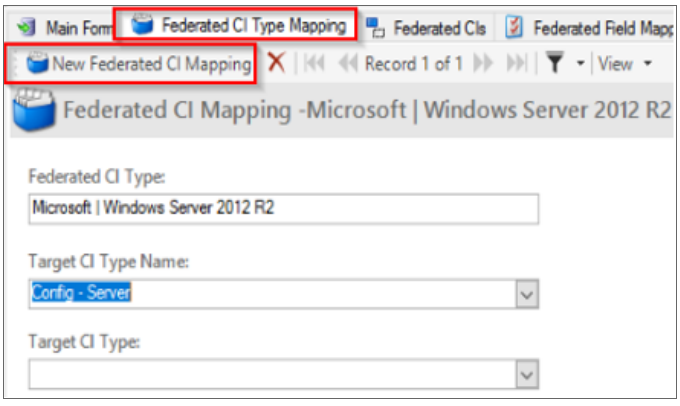
Some examples and possible solutions to those issues are listed below.

No mappings configured for Device Type

The following Journal entry indicates that a Device Type of "Microsoft | Windows Server 2012 R2" was sent from PowerFlow (Federation source), but CSM does not know what type of CI to create or update for this device type:



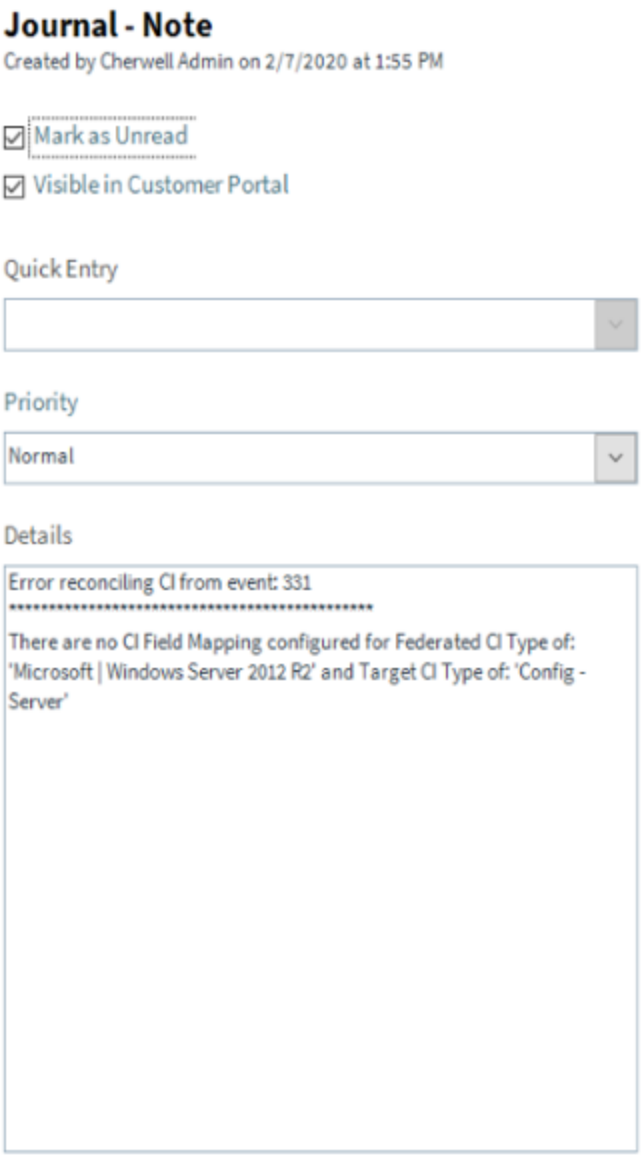
To address this issue, create a Federated CI Type Mapping for this device type:



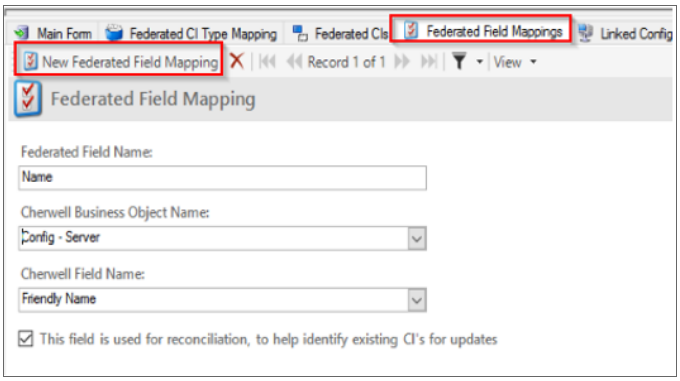
For more information, see *Configuring the Mappings between Source CI Types and CSM CI Types*.

No field mappings defined

The following Journal entry indicates that a Device Type of "Microsoft | Windows Server 2012 R2" was sent from PowerFlow (Federation source), and CSM knows that this Device Type is mapped to a CSM CI Type of "Config – Server". However, there are no fields that have been mapped from the source data to CSM CI Attributes in the "Config – Server" CI type:



To address this issue, create a Federated CI Field Mapping for this CSM CI Type:



For more information, see *Configuring the Mappings between Source CI Attributes and CSM Fields*.

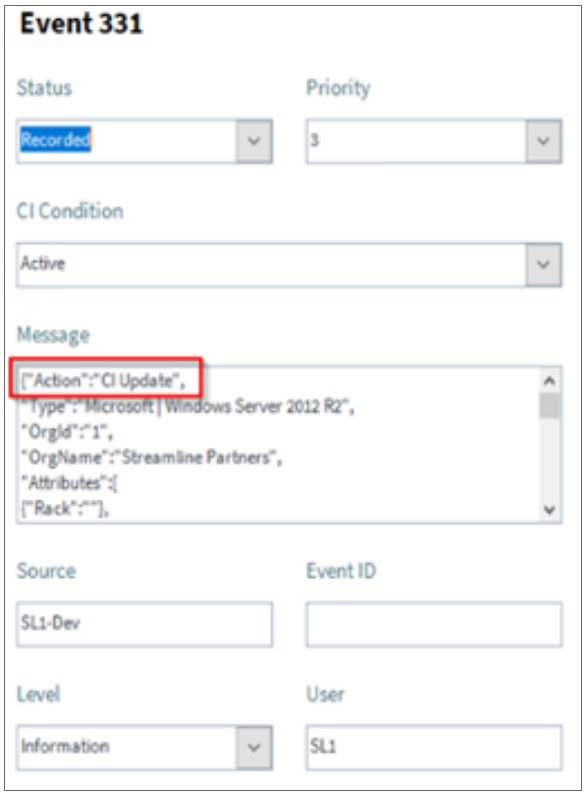
Viewing Events Sent from PowerFlow

Viewing the data from PowerFlow (Federated source) might help you with troubleshooting issues with the "Cherwell" SyncPack.

To view data from PowerFlow:

1. Log in to the CSM User client and go to **Searching**> **Search Manager**. The **Search Manager** dialog appears.
2. From the **Association** drop-down, select *Event*.

3. Double-click All Events to run the search. A list of current events appears. The events sent from PowerFlow are typically tagged with an *Action* attribute in the ***Message*** field that signifies a CI Creation or Update:



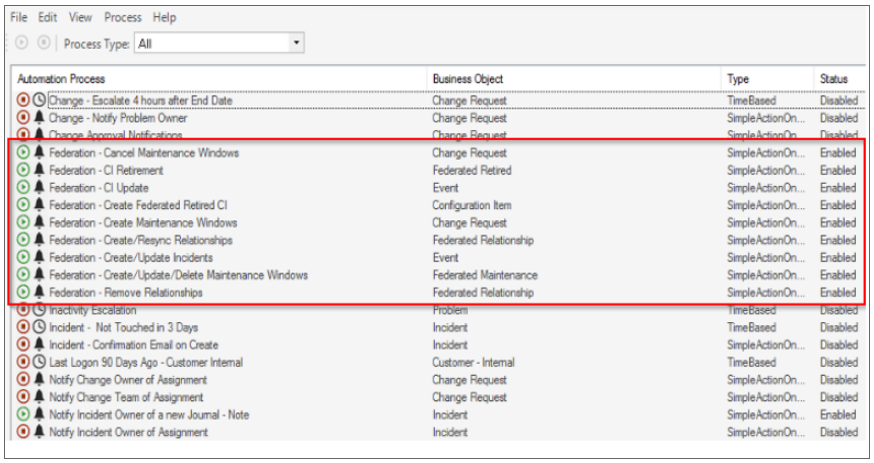
The following Action attributes are currently configured :

- ***CIUpdate***. This attribute is sent or received when a CI needs to be created or updated.
- ***Event Raised***. A new Event in PowerFlow (Federation source) has been registered, which usually results in a new Incident.
- ***Event Cleared***. An existing Event in PowerFlow (Federation source) has been cleared and sent through, which usually results in an existing Incident in CSM being resolved.
- ***Event Acknowledged***. An existing Event in PowerFlow (Federation source) has been acknowledged and sent through, which usually results in an existing CSM incident being acknowledged and notes attached.

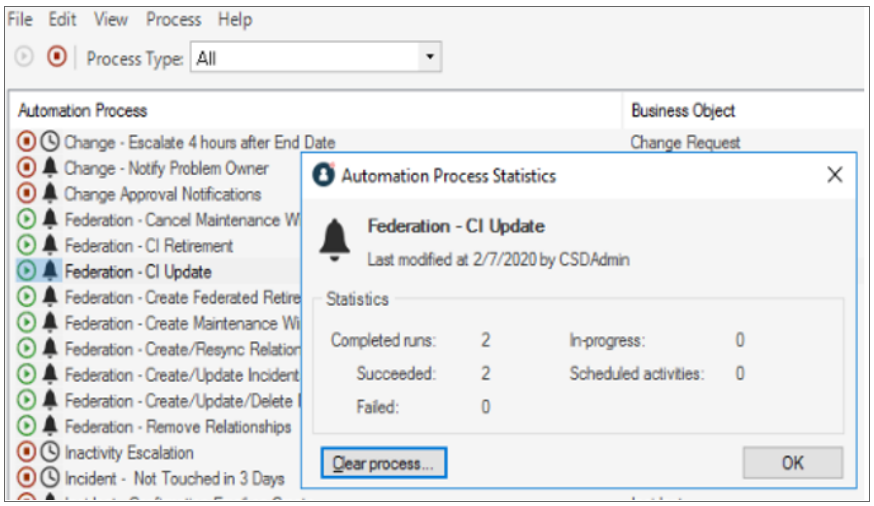
Checking the Automation Process Status

Federation processing such as creation of Incidents, CI, Relationships, Maintenance windows etc relies on a lot of CSM backend processes which is typically accomplished with what's called CSM "Automation Processes". These processes should always be enabled and can be confirmed using the following process.

1. Open the CSM Administrator client and select **Automation Processes** from the **Categories** sub-menu.
2. From the **Pick a task** section, select **Individual Automation Process Status**. A list of automation processes appears. The processes used by the Federation system are highlighted below, and all processes should have a ***Status*** of *Enabled*:



3. Additionally, you can right-click an automation process and select *Statistics* to view more information about runs that succeeded, failed, or were in progress:



© 2003 - 2024, ScienceLogic, Inc.

All rights reserved.

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.

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

International: +1-703-354-1010