ITSM Automation NG Express

Software release version: 2017.07

Administration Guide

Document release date: July 2017
Product release date: July 2017

Hewlett Packard Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted rights legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/.

This site requires that you register for an HPE Passport and to sign in. To register for an HPE Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HPE Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Support

Visit the HPE Software Support site at: https://softwaresupport.hpe.com.

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE Support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HPE Passport user and to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HPE Passport login page.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

HPE Software Solutions Now accesses the HPESW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.hpe.com/.

Administer

This section describes administration tasks that the IT Administrator and Suite Administer user roles can perform in ITOM Container Deployment Foundation (CDF) and ITSMA NG Express.

Administer CDF

The ITOM Container Deployment Foundation (CDF) Administrator user role can perform administration tasks in the following areas in CDF.

Access ITOM CDF

Logon

To access ITOM Container Deployment Foundation (CDF), follow these steps:

1. Launch the ITOM CDF from your browser:
   https://<*EXTERNAL_ACCESS_HOST* >:5443

   You must use the FQDN instead of its IP address in this URL. That is, the name you specified for EXTERNAL_ACCESS_HOST in the **install.properties** file.

   You access the application using a supported web browser, from any computer with a network connection (intranet or Internet) to the servers. It is recommended to restore your browser settings to default.

   You will be asked to change the password at first logon. See Change your password.

2. Log in to ITOM CDF as the **admin** user.

   Use the out-of-box password **cloud** if this is your first login or use the password that you specified at your initial login after installation.

Logout

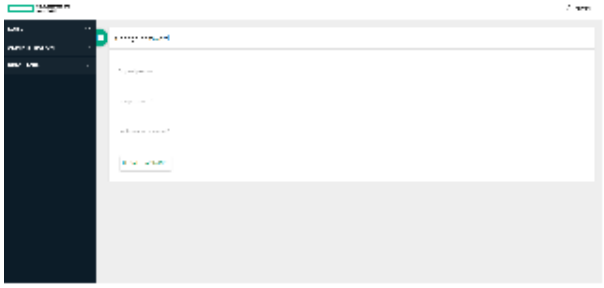
To log out:

1. Click the **[User Name]** button the top right corner of the application and select **Logout**.
2. The application closes and the LOGON screen is displayed again.

When you have completed your session, it is recommended that you log out to prevent unauthorized use.

Change your password

To change your password, follow these steps:

1. Click the **[User Name]** button in the top right corner and select **Change Password**.
   The following page opens:
   
2. Enter the original password, the new password, and verify the new password.
   The password should have minimum 8 characters and must contain characters the following four categories:
   - Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
   - Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
   - Base 10 digits (0 through 9)
   - Nonalphanumeric characters
3. Click **UPDATE PASSWORD**.

Edit the current CDF installation

After ITOM Container Deployment Foundation (CDF) is installed, you can perform the following tasks to edit your existing installation:

- Add more machines to the existing Kubernetes cluster
- Remove machines from the existing Kubernetes cluster
- Edit the hard eviction thresholds of the existing worker nodes

Add more machines to the existing Kubernetes cluster

The administrator can add more worker nodes to the existing Kubernetes cluster.

Remove machines from the existing Kubernetes cluster

The administrator can remove machines from the existing Kubernetes cluster.

Use the following steps:

1. Log on the machine that you want to remove.
2. Go to the installation directory:

   ```
   cd HPESW_ITOM_Suite_Foundation_2017.06.nnnn/
   ```
3. Uninstall the CDF from the node by running the following command: `./uninstall.sh`

Edit the hard eviction thresholds of the existing worker nodes

CDF takes the hard eviction policy for the existing worker nodes. With the eviction service, Kubernetes will end the pod immediately once a hard eviction threshold is met. The eviction can also delete dead pods, dead containers, and unused images when the disk space meets the thresholds. See this Kubernetes article for more details.

To edit the hard eviction threshold, follow these steps:

1. Log on to the worker node for which you want to edit the eviction threshold.
2. Edit the parameter values in the following file: `/usr/lib/systemd/system/kubelet.service`.

   For example, you can change the default thresholds below according to your needs.
   ```
   vim /usr/lib/systemd/system/kubelet.service
   --eviction-hard=memory.available<500Mi,nodefs.available<5Gi,imagefs.available<5Gi
   --system-reserved=memory=1.5Gi
   ```

3. Run the following commands to enable the new thresholds.
   ```
   systemctl daemon-reload
   systemctl restart kubelet
   ```

Logs

This section describes the logs.

Pod logs show the **stderr**/**stdout** of one Kubernetes pod/container.

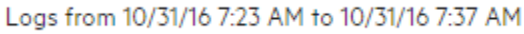
Pod logs

1. Click **RESOURCES > Workloads** > **Pods**.
2. Click the relevant pod.
3. Click **View logs** in the Pod area. The following page is displayed:

You can use the following tools:

- Toggles to change the size of the font used in the log.

- Toggles to change the colors of the log: white characters on black background or black characters on white background.



- Timestamp of the currently displayed log.

- Use the relevant buttons to navigate between logs.

Manage users

ITOM Container Deployment Foundation supports two user roles (or user groups):

IT Administrator

Manages the shared services infrastructure and all suite products, as well as the grow/shrink functions, and adding and removing working nodes (machines). The IT Administrator is a super administrator. This user has ability to request or add resources and has wide access permissions.

Suite Administrator

Manages a specific suite product. The Suite Administrator does not have access to the Admin menu and has the privileges with other operations only under a specific namespace. The Suite Administrator is responsible for the relevant suite deployment, configuration, health, images, and more.

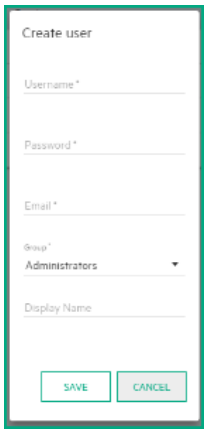
> In ITSMA, the seeded user **sysadmin** has full privileges of the suite and is responsible for suite administration from the ITSMA user interface. We recommends that you configure a Suite Administrator user named **sysadmin** in ITOM CDF so that the same user can administer the ITSMA suite from both the ITOM CDF and ITSMA user interfaces.

This section provides information on how to manage users.

1. Click **ADMIN** > **User Management**. The User page opens.

   For each user, this page displays the user name, password, email, and user group.

   ITOM CDF support two user groups: Administrators and Suite Administrators.
2. To create a user, click **ADD**. The following dialog box opens. Enter the relevant information, and click **SAVE**.



3. To delete a user, click the right-side ACTION icon for the user, select **Delete**, and then click **Delete** again to confirm the deletion.
4. To edit or view a user information, click the ACTION icon for the user, and then select **View/Edit**.

Monitor infrastructure status

The Infrastructure page displays:

- **Namespaces.** The list of the current default namespaces as well as the namespaces for the suites. Every suite on the same Kubernetes cluster is deployed in a different namespace.
- **Nodes.** The composition of the Kubernetes cluster in terms of servers on which the cluster were installed (master and worker nodes, the physical servers or the VMs).
- **Persistent Volumes.** The persistent volume configuration for one or more suites. These volumes contain the data that needs to live outside of the containers.

To access, click **ADMIN** > **Infrastructure**.

Nodes

The Nodes page provides the node CPU and memory usage history, a list of the predefined labels, and a list of nodes.

To access, click **ADMINISTRATION** > **Nodes.**

- View nodes
- Add/delete labels
- Manage node labels
- Add a node
- View the node details

View nodes

To view existing nodes:

1. Click **ADMINISTRATION** > **Nodes**. The following page opens.
2. The window displays the CPU and memory usage of the selected namespace during the past 15 minutes, a list of the node labels, and the status, labels, readiness, and creation timestamps of the corresponding nodes. You can perform the following operations:
    - Define a set of labels you want to use and then assign them to nodes by dragging them to the node.
    - Add a node.
    - Click **REFRESH** to refresh the display.
    - Click a node to see its details.

Add/delete labels

- To add a label in the **Predefined Labels** area, enter the **value** and click **[+]**. The label is added to the list.
- To delete a label: in the **Predefined Labels** area, click **[-]** next to the relevant label.

Manage node labels

- **To assign a label to a node:** drag the label from the **Predefined Labels** area to the node in the **Nodes** area.
- **To unassign a label:** in the **Nodes** area, click **[-]** next to the label and node.
- **To filter the labels:** enter the relevant string or keyword in the Labels box in the table header. The labels with names that include the relevant string are listed.

Add a node

To add a node:

1. Click **+ ADD** in the Nodes area.
2. Enter the following information to add a worker node:
    - the node's host name
    - the name of a user that can remotely execute commands on the host
      For non-root users, run the following command on the remote host you are adding before clicking **ADD**:

      sudo visudo
      Edit the file by adding the following line to the end:

      ```
      <username> ALL=(ALL) NOPASSWD: ALL
      ```

      For example, if the user name is **admin**, add the following line:

      ```
      admin ALL=(ALL) NOPASSWD: ALL
      ```

      Comment out the `Defaults requiretty` setting in the file if it is there:

      ```
      # Defaults requiretty
      ```
    - the password of that user
    - THINPOOL_DEVICE

      The THINPOOL_DEVICE parameter specifies the path to the Docker devicemapper storage driver.
    - FLANNEL_IFACE

      The FLANNEL_IFACE parameter specifies the interface for Docker inter-host communication as a single IPv4 address or interface name. This parameter is used when the nodes have more than one network adapter so that Flannel can set up the correct routing table entries.
3. Click **ADD** to remotely install the extra node.

> You can add multiple nodes simultaneously with **+ ADD**:
>
> - Enter multiple host names or IP addresses separated by a space.
> - Enter the user name and password.
>
> Those added nodes share the same user name and password. The installation of each node runs in parallel.

View the node details

In the Nodes area, select a node name from the list of nodes.

The top of the page displays the CPU and memory usage history of the selected node for the past 15 minutes.

The **Details** area displays details about the selected node, as well as system information.

The **Allocated resources** area displays the minimum CPU requests, CPU limits, memory requests, and memory limits for the container, as well as the used and available percentage ratios of the CPU and memory resources.

The **Conditions** displays the type, status, last heartbeat, last transaction time, reason, and message.

The **Pods** area displays the CPU and memory usage history of the pod for the past 15 minutes, the name of the pod, the status, number of restarts in the cycle, the amount of time that has elapsed since the pod was created, the cluster IP, as well as the CPU and memory usage of the pod.

You can do the following:

- Click a Pod name to open the Workloads - Pods page for the pod.
- Click [text subject] icon
  to review the pod log.
- Click [more actions] icon
  and select **Delete** to delete the pod.

The **Events** area displays the message, source, sub-object, count, first seen and last seen information.

Manage licenses

The License page in ITOM Container Deployment Foundation (CDF) enables you to manage your suite licenses.

> By default, there is no license installed. You can view the existing licenses only after you have installed them.

Activate a license

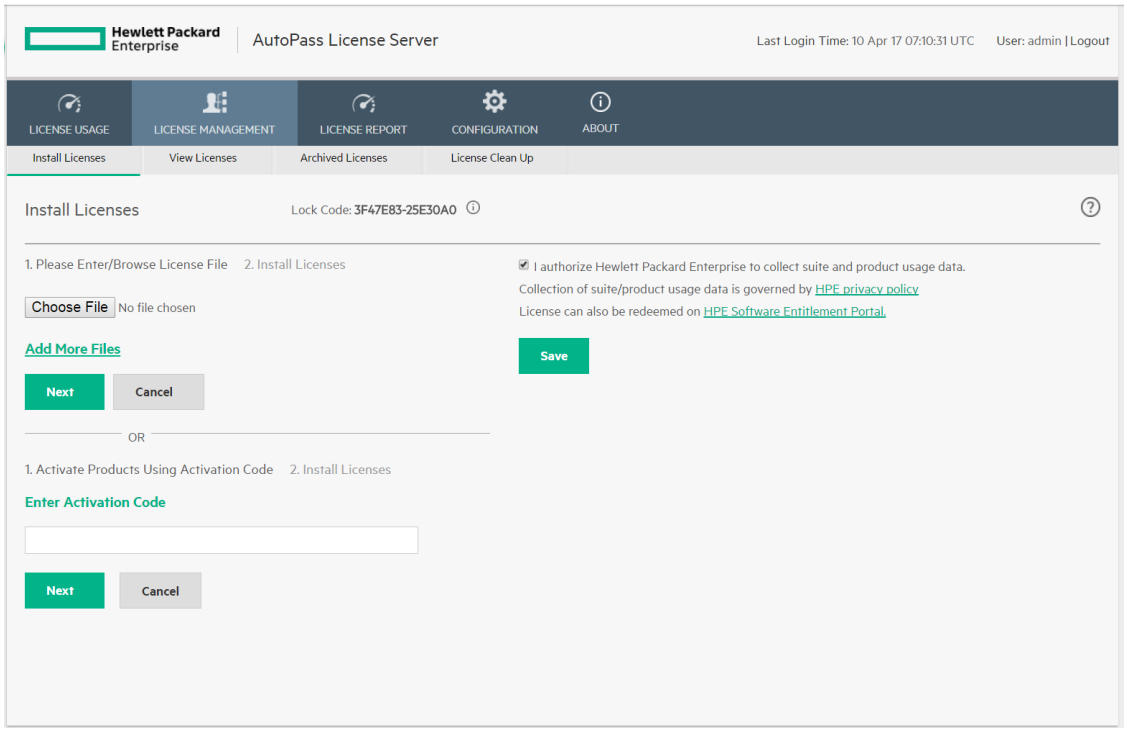
There are two ways to activate a suite license:

Install the license file

1. Log in to ITOM CDF as **admin**.
2. Click **SUITE > Management**.
3. Click the more action icon

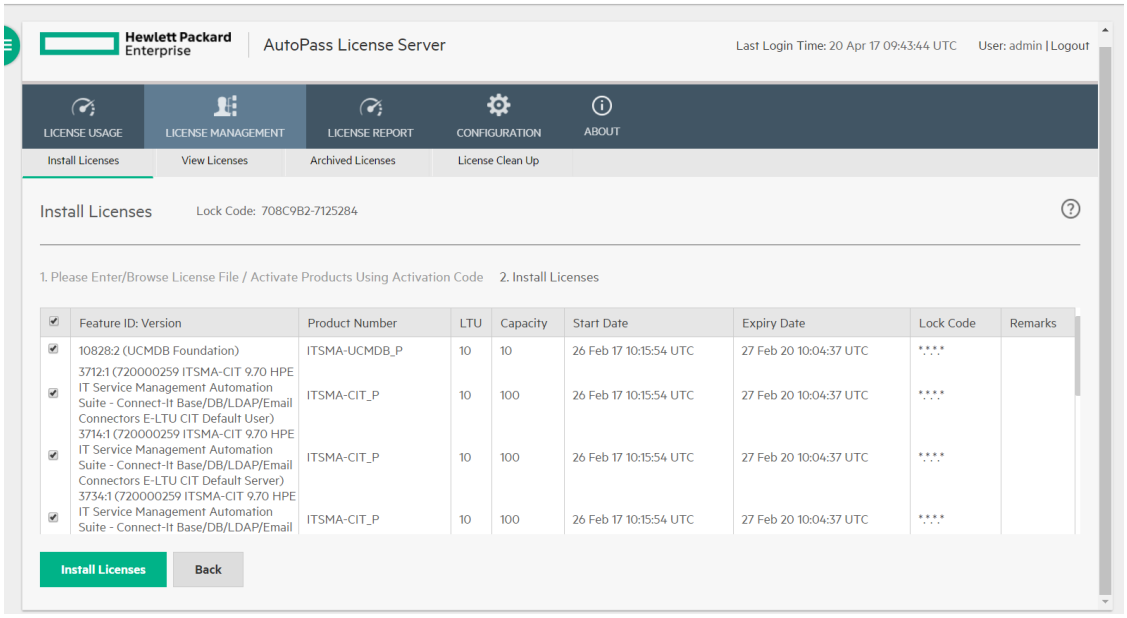
   Unknown Attachment

   for the installed suite instance, and then select **License** > **Install Licenses** to open the following page:



4. Click **Choose file** to select the license file in your local system.
5. Click **Add More Files** to select another license file in your local system.
6. Accept the HPE End User License Agreement and authorize the suite and product usage data collecting.
7. Click **Next**.

   The following page opens:



You can select the appropriate license and click **Install Licenses** to install the license (you can also select to go back to the previous Install Licenses page by clicking the **Back** button).

The table below explains the fields of the license installation.

Fields	Description
Feature ID: Version	A feature ID version is a way of grouping and describing different functionality that makes up a product.
Product Number	Product's number which is given manually (SKU). For example: ITSMA_Expr_30_Fixed_C1
Capacity	Capacity is the field which indicates the actual quantity of a license feature that the customer is entitled to.
Start Date	The start date of the product license.
Expiry Date	The expiry date of the product license.
Lock Code	The lock code is unique for each ITOM Container Deployment Foundation environment, and is used when installing a license.
Remarks	To take notice of the product license details.

8. The page displays the licenses in the selected file. You must select the licenses you want to install out of the displayed licenses. After selecting, click **Install Licenses**. A message displays the number of licenses that were successfully added.

   Once the license is installed successfully, you can view the licenses.

Enter the activation code

The Activation Code is a unique code which is used to redeem licenses against an entitlement from a remote host at HPE.

The Activation Code is used for an automated entitlement process. Once an order is placed, the activation code for the product or suite is provided via email.

> This option is only available for a few products and suites at the moment. Customers who receive an activation code must also redeem the licenses from the Entitlement Portal.

Once the Activation Code is entered in the AutoPass License Server (APLS), the licenses are automatically generated, based on your entitlements.

The APLS must have an internet connection. Once the Activation Code is entered, the APLS establishes a connection to a remote HPE host

to generate and issue licenses.

Follow these steps to install a license:

1. Enter the activation code.
2. Click **Next**. The **License Installation Wizard** page opens.

> There are three activation code types: Full, Partial and Fixed. You can distinguish the activation code from the product number in the License Installation Wizard.

Example:
Full activation code shown in product number: `HPE-ITSMA-PRODUCT-LAT-FULL`

Partial activation code shown in product number: `C4MOOPAEPC_PT_10`

Fixed activation code shown in product number: `HPE-ITSMA-PRODUCT-LAT-Fixed`

3. Check the boxes next to the license you want to install, then click **Next**.
   - Enter the quantity manually for the **Partial** activation code.

> You only need to input the activation quantity for the **Partial** activation code. The entered value should be smaller than the available quantity value. For the **Full/Fixed** activation code, the quantity is disabled.

4. Select the appropriate environment from the drop-down list.

   The table below explains the fields of the **License Installation Wizard**.

Fields	Description
Product Number	Product's number which is given manually (SKU). For example: `ITSMA_Expr_30_Fixed_C1`
Product Name	Product Name is the official name of the product. For example: `HPE-ITSMA_30_Fixed_C1`
Environment	Environment displays a number of elements that differentiate one environment from another. For Example: Production Testing Hot Stand By Cold Stand By, etc.
Total Quantity	The total quantity is quantity of licenses in general, not taking into account how many are still available.
Available Quantity	The license quantity that can be ordered.
Quantity to Activate	Full: Quantity to Activate is equal to the available quantity, so this field is disabled. Partial: Enter the quantity of licenses that you want to activate. This value must be less or equal to the available quantity. Fixed: Quantity to Activate is a fixed quantity, so this field is disabled.
Remarks	To take notice of the product license details.

5. Click **Next**. The requested quantity is activated. You are redirected to the License Management page.

The page displays the licenses in the selected file. You must select the licenses you want to install out of the displayed licenses. After selecting, click **Install Licenses**. A message displays the number of licenses that were successfully added.

View licenses

Click **SUITE > Management** > [more action] icon

>**License** > **View Licenses**.
Select the relevant product in **Select Product**. The page displays the feature ID: version, product number,capacity, start date, expiry Date, the date when it was installed, and who installed it, as well as the Lock Code.

Archive a license

1. In the View Licenses tab, select the unused licenses you want to archive.
2. Click **Archive**.

The licenses are removed from the list of installed licenses in the License Management table and become unavailable.

Restore an archived license

1. In the **Archived License** tab, select the product whose archived licenses you want to restore.
2. Select the relevant licenses that you want to restore.
3. Click **Restore**.

The licenses are again displayed in the License Management pane and customers can check them out.

> If ID locked licenses are auto archived, they cannot be restored unless all the licenses locked to a lock value belonging to same feature are either deleted or archived.

Delete a license from the License Manager

1. In the **Archived Licenses** tab, select the product whose licenses you want to delete.
2. Select the license to delete.
3. Click **Delete** and confirm the deletion.

View the Licenses Report

Click **SUITE > Management** > [more action] icon

>**License** > **LICENSE REPORT**.

LICENSE REPORT. The license report page tracks and displays the licenses currently installed and used on the License Manager. It also displays specific check out information about a feature license including the product name and version, the requester ID, and the timestamp of when it was accessed last.

You can export the license report details to Excel. You can also search a license with the product name, product version or requester IP address.

View the existing images

To view the existing images, click **ADMINISTRATION > Local Registry**. The following page is displayed.

This section lists the images that are in the local registry.

Manage Resourses

The RESOURCES menu enables you to deploy containerized applications to a Kubernetes cluster, troubleshoot them, and manage the cluster

and its resources itself. You can use it for getting an overview of applications running on the cluster, as well as for creating or modifying individual Kubernetes resources and workloads, such as Daemon sets, Pet sets, Replica sets, Jobs, Replication controllers and corresponding Services, or Pods.

It also provides information on the state of Pods, Replication controllers, etc. and on any errors that might have occurred. You can inspect and manage the Kubernetes resources, as well as your deployed containerized applications. You can also change the number of replicated Pods, delete Pods, and deploy new applications using a deploy wizard.

Namespace

This section provides details about the selected Namespace.

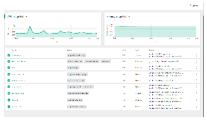
Kubernetes supports multiple virtual clusters backed by the same physical cluster. These virtual clusters are called namespaces.

Select the namespace

You select a namespace to filter the information in the pages of the UI and display only the items related to the namespace.

1. Click **RESOURCES** > **Namespace** and select the relevant namespace.

   The following page opens:

   The page shows the CPU and memory usage history for the selected namespace, for the past 15 minutes, the name of the namespace, its labels, pods, the timestamp of the creation of the namespace and its images.
2. Click the relevant namespace to display more details. See View the namespace details.

View the namespace details

Click **RESOURCES** > **Namespaces** and select the relevant namespace. You can also click **RESOURCES** > **Namespaces**, and click the relevant namespace.

The page shows details about the namespace and details about the events occurring in the namespace.

Workloads

This section displays information about Namespaces, Deployments, Replica Sets, Replication Controllers, Daemon Sets, Jobs, Pods, filtered by the selected namespace.

Click **RESOURCES** > **Workloads**.

The page displays all the resources filtered by the selected namespace.

Pods

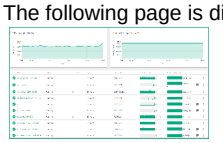
The Pods page provides information about the pods that are currently running or that have been running for the past 15 minutes. You can also access details about a specific pod as well as its log.

By default, pods run with unbounded CPU and memory limits. This means that any pod in the system will be able to consume as much CPU and memory on the node that executes the pod.

You may want to impose restrictions on the amount of resources a single pod in the system may consume for a variety of reasons.

See Glossary.

View the Pods

1. Click **RESOURCES** > **Workloads** > **Pods**.
   The following page is displayed.
   

   The page displays the CPU and memory usage history of the namespace the pod belongs to, namespace the pod belongs to, the name, status, number of restarts during the lifecycle of the pod, the amount of time passed since the creation of the pod, the IP address of the pod, the CPU and memory usage of the pod itself in the last 15 minutes.
   You can:

   - Click
     
     to display the log of a pod. See View log.
   - Click

     and select to delete the pod or to view and edit its YAML. See Pods.
   - Click a pod itself to display its details. See View pod details.

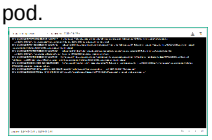
View pod details

1. Click **RESOURCES** > **Workloads** > **Pods**, and then click the relevant Pod.
   

   The page displays the CPU and memory usage history of the pod in the last 15 minutes, the pod details, and the network details. To display the log of the pod. See View log.
   The page also displays information about the pod containers such as the name, image, environment variables, commands, arguments, and more. To display the log of the container. See View log.

View log

1. Click **RESOURCES** > **Workloads** > **Pods**.
2. Click the relevant pod.
3. Click
   in the Pod page or **View logs** in the Pod Details page or click **View logs** in the Container area. The page displays the information for the pod.
   

   You can use the following tools:

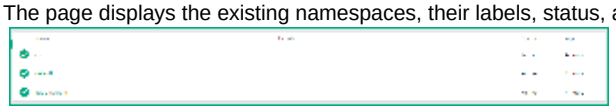
- Toggles to change the size of the font used in the log.
  
- Toggles to change the colors of the log: white characters on black background or black characters on white background.
  Logs from 10/31/16 7:23 AM to 10/31/16 7:37 AM
- The timestamp of the currently displayed log.
  

- Use the relevant buttons to navigate between logs.

Namespaces

The Namespaces page displays information about the existing namespaces, their labels, status, and age.

1. Click **RESOURCES** > **Workloads** > **Namespaces**.
2. The page displays the existing namespaces, their labels, status, and age.



3. Click the relevant namespace to view more details:

The page shows details about the namespace and details about the events occurring in the core such as messages, source, count, first seen and last seen.

Deployments

You create and manage sets of replicated containers (actually, replicated Pods) using Deployments.

A Deployment provides declarative updates for Pods and Replica Sets (the next-generation Replication Controller).

A Deployment simply ensures that a specified number of pod “replicas” are running at any one time. If there are too many, it will kill some. If there are too few, it will start more.

You can select another namespace.

View the deployments

1. Click **RESOURCES** > **Workloads** > **Deployments**.
   The following page is displayed:

The page displays the CPU and memory usage history of the selected namespace during the past 15 minutes, the name of the available deployments, their labels, the number of pods, the creation timestamp of the deployment, and its images.

You can:

- Click a deployment to display its details. See View a deployment details.
- Click

and **Delete**, to delete the deployment.
- Click

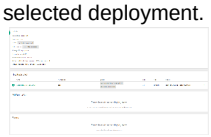
and **View/edit YAML**, to view or edit a deployment.

View a deployment details

1. Click **RESOURCES** > **Workloads > Deployments**, and then click the relevant deployment.

   The following page is displayed:

The page displays the CPU and memory usage history of the selected deployment during the past 15 minutes, and details about the selected deployment.



The page displays details about the new replica set, the old replica sets, and the events that took place.

Daemon Sets

The Daemon Sets page provides information about the Daemon Sets for the selected Namespace. See Glossary.

Replica Sets

Replica Set is the next-generation Replication Controller. The only difference between a ReplicaSet and a Replication Controller right now is the selector support. ReplicaSet supports the new set-based selector requirements as described in the labels user guide whereas a Replication Controller only supports equality-based selector requirements.

This section displays information about replica sets of the selected namespace. See Glossary.

View replica sets

1. Click **RESOURCES** > **Workloads** > **Replica Sets**.
   The following page opens:
   

   The page shows the CPU and memory usage history of the selected namespace during the past 15 minutes, the name of the available replica sets for the selected namespace, its labels, pods, images and creation timestamp.

   You can:

   - Click a replica set to display its details. See View a replica set details.
   - Click

     and **Delete**, to delete the replica set.
   - Click

     and **View/edit YAML**, to edit the replica set.

View a replica set details

1. Click **RESOURCES** > **Workloads > Replica Sets**.
2. Click the relevant replica set.
   

   The details page shows details about the selected replica set, the services (see Services), pods (see Pods), and events related to the replica set.

Replication controllers

The Replication Controllers page provides details about the Replication Controllers.

See Glossary.

View the Replication Controllers

1. Click **RESOURCES** > **Workloads** > **Replication Controllers** to display the current Replication Controllers.
   The following page is displayed.
   

The page displays the CPU and memory usage of the selected namespace during the past 15 minutes, and the list of replication controllers with their name, labels, pods, age, and images of the replication controllers associated with the selected namespace. You can:

- Click the relevant replication controller to view its details. See View the replication controller details.
- Click

  and select:
  View details. You can also click the relevant replication controller. See Scale the number of pods linked to the replication controller.
  Scale. See View the replication controller details.
  View/edit YAML You can edit a Replication Controller.
  Delete. The replication controller is deleted.

Scale the number of pods linked to the replication controller

1. Click **RESOURCES** > **Workloads** > **Replication Controllers** , click and then select **Scale**. Enter the relevant number of pods and click **OK**.

View the replication controller details

1. Click **RESOURCES** > **Workloads** > **Replication Controllers**.
2. Click

   and select **View details**, or click the relevant Replication Controllers.

   The following page opens.

   It displays the CPU and memory usage history of the selected replication controller for the past 15 minutes, the details of the selected replication controller, and the services provided by the selected replication controller.

Pet Sets

The Pet Sets page provides information about pet sets. See Glossary.

Jobs

The Jobs page provides information about jobs. See Glossary.

Services and discovery

Click **Services and discovery** to display information about:

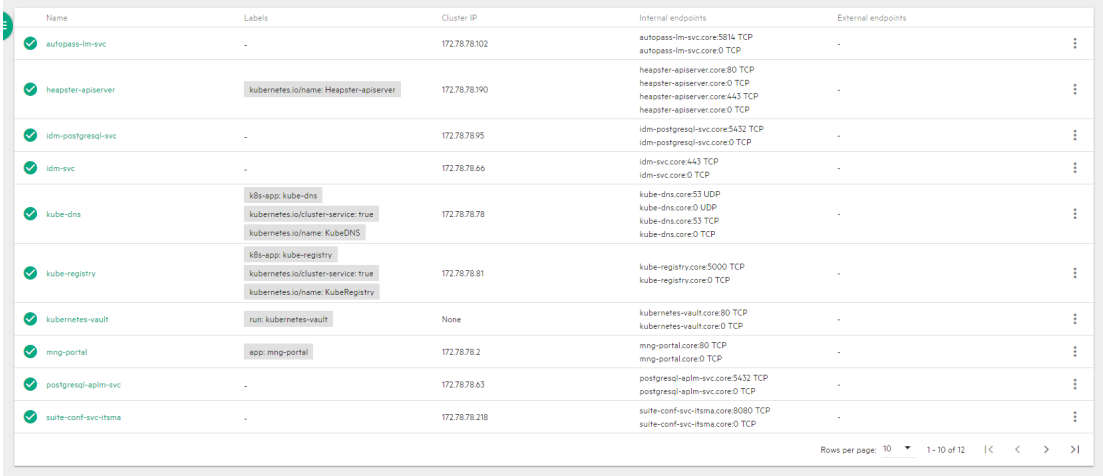
- Services
- Ingress

Services

The Services page provides information about services.

View services

1. Click **RESOURCES** > **Services and Discovery** > **Services** .
   The following page is displayed.

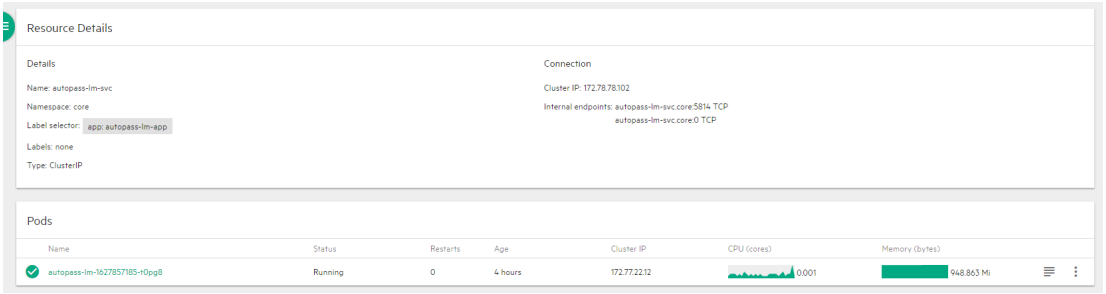


The page displays the name of the services attached to the selected namespace, the labels assigned to the service, the IP address of the related cluster, and the internal and external endpoints.
You can:

- Click
  and select **Delete** to delete the service.
- Click
  and select **View/edit YAML** to edit the service.
- Click the relevant service to display its details. See View a Service Details.

View service details

1. Click **RESOURCES** > **Services and Discovery** > **Services** , and then click the relevant Service.
   The following page is displayed:



The page displays details about the service and the connection as well as information about the related pods.

Ingress

The Ingress page provides details about the ingresses. See Glossary.

View ingresses

1. Click **RESOURCES** > **Services and Discovery** > **Ingress**.
   The following page is displayed.
   Broken image

   The page displays the names of the ingresses attached to the selected namespace, the labels assigned to the ingress, the IP of the related cluster, and the internal and external endpoints.
   You can click the relevant ingress to display its details. See View an Ingress Details.

View an Ingress Details

Click **RESOURCES** > **Services and discovery > Ingress**, and then click the relevant Ingress.
The following page is displayed:
Broken image

The page displays details of the selected ingress and its related pods.

Persistent Volume Claims

The Persistent Volume Claims page displays information about the currently running persistent volumes.

A persistent volume claim is bound to a persistent volume. The claim is subsequently used inside a container volume specification. This provides volume technology abstraction for the suite deployment as suites request size and access type rather than a certain specific storage provider.

A volume is a directory, possibly with some data in it, which is accessible to the containers in a pod.

See Glossary.

View the Persistent Volume Claims

1. Click **RESOURCES** > **Persistent Volume Claims**. The following page opens:

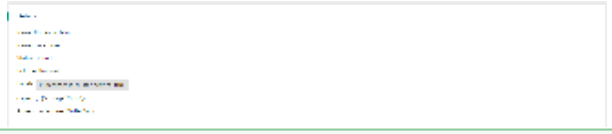
The page displays the name of the persistent volume, the volume it belongs to, the labels, and the timestamp of the creation of the persistent volume.

Each suite will have at least one persistent volume but may have more depending on the suite.

You can click the relevant volume to display its details. See View a persistent volume claim details.

View a persistent volume claim details

1. Click **RESOURCES** > **Persistent Volume Claims**, and then click the relevant Persistent Volume Claims. The page that opens displays detailed information about the persistent volume claim.



To see the contents of **itom-vol**, go to the master node (the NFS server) and enter **cd /var/vols/itom/**. It contains the **baseinfra-<version-number>** and the **suite-install** subdirectories.

Enter **ls -R baseinfra-<version-number>**; this shows the **PrivateRegistry**.

Enter **ls -R suite-install/**; this shows information about the containers that includes the configuration information to deploy the supported suites.

Configuration

Click **RESOURCES > Configuration** to display information about:

- Secrets. See Secrets.
- Config Maps. See Config Maps.

Secrets

The Secrets page provides information about Secrets that are currently running.

See Glossary.

View the Secrets

Click **RESOURCES** > **Configuration > Secrets**.
The following page opens:

The page displays the list of secrets and their age. You can click the relevant secret to display its details. See View a Secret details.

View a Secret details

Click **RESOURCES** > **Configuration >Secrets**. In the page that opens, click the relevant secret.

The page displays the details of the selected secret and its data.

Config Maps

The Config Maps page provides information about the config maps that are currently running.

See Glossary.

View the Config Maps

1. Click **RESOURCES** > **Configuration** > **Config Maps**.The following page opens:

   The page opened displays the names of the configuration map and its labels, and the amount of time passed since the configuration map was created.
   You can:

   - Click

     and select **Delete** to delete the config map.
   - Click

     and select **View/edit YAML** to edit the config map.
   - Click the relevant config map to display its details. See View a Config Map details.

View a Config Map details

1. Click **RESOURCES** > **Configuration > Config Maps** to display the currently running Config Maps.
2. In the page that opens, click the relevant name.
   The following page opens:

   The page opened displays the selected config map details, and its related data.

Security

This section is intended for ITOM Container Deployment Foundation (CDF) implementers and system administrators who need to implement their ITOM CDF environment in a secure manner.

Secure implementation and deployment

This section provides information on implementing and deploying the ITOM Container Deployment Foundation (CDF) in a secure manner.

Technical system landscape

ITOM CDF is a container that integrates with other Suites. ITOM CDF is written in Java and JavaScript and Go.

For more information about typical deployment schemes and options, see Overview of HPE ITOM CDF.

Security in ITOM CDF configurations

ITOM CDF configurations may be deployed in the following three implementations. See Overview of HPE ITOM CDF.

- Single mode.

- Distributed mode 1 (one master node and multiple worker nodes)
- Distributed mode 2 (multiple master nodes and multiple worker nodes)

All of these implementations share the same basic out-of-the-box security configuration options.

1. In an out-of-the-box default installation, the Transport Layer Security/Secure Socket Layer (TLS/SSL) security is enabled between the browser and the ITOM CDF server by default.
2. In an out-of-the-box default installation, ITOM CDF requires users to enter username and password credentials to gain access to the application.

External Authentication

With additional configuration, it is possible to supplement or replace the default authentication & authorization provider for ITOM CDF by using a variety of industry-standard protocols and tools such as LDAP and Single Sign-On.

Common security considerations

ITOM CDF can only be deployed on supported operating systems.

It is recommended to follow vendor-provided best practices and security hardening guides for each of the third-party components used in support of your ITOM CDF deployment, which includes Docker, Kubernetes, Vault and Nginx, NFS. Below are some resources that can serve as a starting point for researching these recommended security considerations:

Docker Security Tips

https://www.docker.com/docker-security

Kubernetes Security Tips

http://kubernetes.io/docs/troubleshooting/

Vault Security Tips

https://www.hashicorp.com/security.html

Nginx Security Tips

http://nginx.org/en/security_advisories.html

NFS Security Tips

http://www.cert.org/historical/advisories/

ITOM CDF security parameters

This section contains reference to some of ITOM Container Deployment Foundation (CDF) parameters that are relevant to security.

Secure file storage

ITOM CDF allows users to upload files (suite installation binary) to the ITOM CDF Server. All files uploaded to the server must be validated, since they can contain viruses, malicious code, or Trojans.

As a result, it is strongly recommended to implement proper antivirus protection for the file storage.

Installation security

This section provides information on aspects of installation security.

Supported operating systems

See Support matrix.

Harden SSH on OS

On each node, the SSH server is configured with weak cipher and weak KexAlgorithms by default.

Set the values of **KexAlgorithms**, **Ciphers** and **MACs** in file: /etc/ssh/sshd_config as follows:

- **KexAlgorithms** ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256
- **Ciphers** aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
- **MACs** hmac-sha2-256

Database security recommendations

For PostgreSQL, see http://www.openscg.com/postgresql-security-guidelines/ for information about PostgreSQL database security solutions.

Application server security recommendations

Always change default passwords.

Always use the minimal possible permissions when installing and running ITOM Container Deployment Foundation (CDF).

Action	Permissions needed for user
Installing or running the HPE ITOM CDF	You must install and run root permissions using the sudo command.

Network and communication

Secure topology

ITOM Container Deployment Foundation (CDF) is designed to be part of a secure architecture and to deal with the security threats to which it could potentially be exposed.

To securely deploy the CDF, we recommends that you use the TLS/SSL communication protocol.

Replace the ingress service certificate with a custom certificate

To replace the certificate and private key of Ingress Service with a custom certificate and private key, follow these steps:

1. Generate a certificate and private key for the host on which the ingress service is running. Save the certificate and key on the master node.
2. On the master node, run the following command to delete a secret:
   kubectl delete secret nginx-default-secret -n core
3. On the master node, run the following commands to recreate the secret with the new certificate and private key:

   > You must keep the format of the following commands as it is, especially the indented spaces.

   ```
   echo "
   apiVersion: v1
   kind: Secret
   metadata:
   name: nginx-default-secret
   namespace: core
   data:
     tls.crt: `base64 -w 0 $K8S_HOME/ssl/${hostName}.crt`
     tls.key: `base64 -w 0 $K8S_HOME/ssl/${hostName}.key`
   "| kubectl create -f -
   ```

4. On the master node, run the following commands to delete and recreate the ingress service.
   kubectl delete -f ${K8S_HOME}/objectdefs/nginx-ingress.yaml
   kubectl create -f ${K8S_HOME}/objectdefs/nginx-ingress.yaml

Renew the client.crt, client.key, server.crt, and server.key certificates

You cannot replace these certificate files with your own. When these certificates expire, you must renew them.

To renew the certificates, follow these steps:

1. Generate new server certificates or client certificates with the following commands:

cd $<*K8S_HOME*>/scripts

./renewCert.sh

2. Copy the new server certificates or client certificates to other nodes.
    a. Copy the server certificates (server.crt, server.key, client.crt, and client.key) to other master nodes.
    b. Copy the client certificates (client.crt and client.key) to the worker nodes.
3. Restart the kubelete service with the following commands:
4. **cd $<*K8S_HOME*>/bin**

   ./ kube-restart.sh
5. Run the following commands to delete three default tokens in the core, default, and suite namespaces:

   kubectl get secrets --all-namespaces

   kubectl get delete secret xxxx -n default-token-xxxx
6. Run the following commands to recreate the yaml files:

   cd $<*K8S_HOME*>/objectives

   kubectl delete -f kube-vault.yaml

   kubectl delete -f mng-portal.yaml

   kubectl delete -f nginx-ingress.yaml

   kubectl create -f kube-vault.yaml

   kubectl create -f mng-portal.yaml

   kubectl create -f nginx-ingress.yaml

   kubectl delete -f ingress yaml
7. Run the following commands to recreate the suite ingress yaml file:

   cd /var/vols/itom/core/suite-install/<*suite_ingress _yaml_directory*>/objectives

   kubectl delete -f xxxx-nginx-ingress.yaml

   kubectl create -f xxxx-nginx-ingress.yaml

Security recommendations

We recommend that you add the following iptables rules.

> Apart from the listed ports, all other ports should be blocked at the localhost level.

Target server to configure the rules	Required ports	Service	Direction	Short description
NFS server	111	NFS	Nodes -> NFS Server	NFS server port access by all nodes
NFS server	2049	NFS	Nodes -> NFS Server	NFS server port access by all nodes
Master Node	2380	Etcd	Master <-> Master	Etcd service port for etcd cluster communication
Master Node	4001	Etcd	Nodes -> Master	Etcd service port for connection from client
Ingress Node	5443	MngPortal	All -> Ingress Node	The port exposed on ingress node. All clients could access this port
Master Node	8200	Vault	Nodes->Master	Vault port for client connection
Master Node	8201	Vault	Nodes->Master	Vault port for peer member connection
Master Node	8443	Kubernetes	Nodes -> Master	API server port for client connection
All Nodes in Cluster	10250	Kubernetes	Nodes -> Nodes	Kubernete port for internal communication

All Nodes in Cluster	10251	Kubernetes	Nodes -> Nodes	Kubernete port for internal communication
All Nodes in Cluster	10252	Kubernetes	Nodes -> Nodes	Kubernete port for internal communication
All Nodes in Cluster	10255	Kubernetes	Nodes -> Nodes	Kubernete port for internal communication
NFS server	20048	NFS	Nodes -> NFS Server	NFS server port access by all nodes

Example:

Assume that the cluster is installed on 10.10.10.10, 10.10.10.11, 10.10.10.12, and the master node is installed on: 10.10.10.10. In this example. t o add iptable rules to port 8443 on the master node, you run the following commands:

iptables -I INPUT 1 -p tcp -m tcp -s 0.0.0.0/0 --dport 8443 -j DROP

iptables -I INPUT 1 -p tcp -s 127.0.0.1 --dport 8443 -j ACCEPT

iptables -I INPUT 1 -p tcp -s 10.10.10.10 --dport 8443 -j ACCEPT

iptables -I INPUT 1 -p tcp -s 10.10.10.11 --dport 8443 -j ACCEPT

iptables -I INPUT 1 -p tcp -s 10.10.10.12 --dport 8443 -j ACCEPT

Authorization

This section provides information related to user authorization in ITOM Container Deployment Foundation (CDF).

Authorization model

Access to ITOM CDF resources is authorized based on the user's following settings:

- User name
- Session and inactivity timer timeouts

FAQ

Question

Can ITOM CDF inherit users' information and authorization profiles from an external repository, such as LDAP?

Answer

No.

Data integrity

The database server is used as a simple data store and is responsible for all persistent storage. While the database contains definitions describing business logic, no processing is actually performed in this tier, other than create, read, update, and delete (CRUD) operations in response to requests from ITOM Container Deployment Foundation (CDF). Referential integrity is enforced by the application, thereby protecting transactions. In addition, the database captures a complete audit log of all changes to data.

The data backup procedure is also an integral part of data integrity and while ITOM CDF does not provide native backup capabilities, the following guidelines should be considered:

- Database backup is especially important before critical actions such as upgrades.
- Backup files should be stored properly according to the industry best practices to avoid unauthorized access.
- Since database backup can be a resource intensive process, it is strongly recommended to avoid running backups during peak demand times.

Enable firewall on a running node

Follow the steps below on each running node to enable firewall.

On the NFS server

Run the following commands to enable firewall on the NFS server.

systemctl start firewalld;systemctl enable firewalld
firewall-cmd --permanent --add-port=111/udp
firewall-cmd --permanent --add-port=111/tcp
firewall-cmd --permanent --add-port=2049/tcp
firewall-cmd --permanent --add-port=20048/tcp
firewall-cmd --reload

On the running master nodes

Run the following commands to enable firewall on each running master node.

systemctl start firewalld; systemctl enable firewalld
firewall-cmd --permanent --add-port=4001/tcp
firewall-cmd --permanent --add-port=2380/tcp
firewall-cmd --permanent --add-port=8200/tcp
firewall-cmd --permanent --add-port=8201/tcp
firewall-cmd --permanent --add-port=8443/tcp
firewall-cmd --permanent --add-port=10250/tcp
firewall-cmd --permanent--direct --add-rule ipv4 filter FORWARD 1 -o docker0 -j ACCEPT -m comment --comment "docker subnet"
firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 1 -i docker0 -j ACCEPT -m comment --comment 'kube-proxy redirects'
firewall-cmd --reload

On the running worker nodes

Run the following commands to enable firewall on each running worker node.

systemctl start firewalld; systemctl enable firewalld
firewall-cmd --permanent --add-port=10250/tcp
firewall-cmd --permanent--direct --add-rule ipv4 filter FORWARD 1 -o docker0 -j ACCEPT -m comment --comment "docker subnet"
firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 1 -i docker0 -j ACCEPT -m comment --comment 'kube-proxy redirects'
firewall-cmd --reload

Data backup for the single-master cluster

To back up the data in the `data` directory for the single-master cluster, use the `etcdctl backup` command.

For example:

```
etcdctl backup \

--data-dir %data_dir% \

--backup-dir %backup_data_dir%
```

You can also use the `etcdctl backup` command to back up all the exported folders in the NFS server too.

The `etcdctl backup` command will rewrite some of metadata contained in the backup (specifically, the node ID and cluster ID), which means that the node will lose its former identity.

> In order to recreate a cluster from the backup, you will need to start a new, single-node cluster. The metadata is rewritten to prevent the new node from inadvertently being joined onto an existing cluster.

Encryption

This section provides information on data encryption in ITOM Container Deployment Foundation (CDF).

TLS/SSL Data Transmission

ITOM CDF was configured to use TLS/SSL to transmit data between the server and browsers.

Customers can change the default value of SSL CIPHER through the following steps:

1. On the master node, change the **ssl-ciphers** value in file **$K8S_HOME/objectdefs/nginx-ingress.yaml**.
2. Recreate the ingress container with the commands below:
   kubectl delete -f **$K8S_HOME/objectdefs/nginx-ingress.yaml**

kubectl create -f **$K8S_HOME/objectdefs/nginx-ingress.yaml**

Encryption of stored database fields

ITOM CDF uses proprietary algorithms when encrypting data stored in the database and uses HPE Identity Manager (IDM) to manage user passwords.

Docker logs

This section provides information related to docker logs.

Log and Trace Model

Recommendations:

- Pay attention to the log level and do not leave tracing or debug parameters enabled unnecessarily.
- Pay attention to log rotation/switching.

Log rotation

The CDF supports the log rotation. By default, the maximum log file size is 10 MB, and the maximum number of the log file is 5. You can also change the maximum log file size and maximum log file number with the following steps.

1. Open the `docker` file with the following commands.

   ```
   cd /opt/kubernetes/cfg
   ```

   ```
   vim docker
   ```
2. Change the value of `max-size` and `max-file` in the parameter `DOCKER_LOG_OPTS`.

   For example:

   ```
   DOCKER_LOG_OPTS="--log-driver=json-file --log-opt
   labels=io.kubernetes.container.name,io.kubernetes.pod.uid --log-opt max-size=12m --log-opt
   max-file=6"
   ```

3. Restart Docker to enable the changes with the following command:
   `systemctl restart docker`

> The default maximum log size number and maximum log file number is recommended. Do not set a large number for the `max-size` and `max-file`. Too large maximum size and maximum file number may affect the free disk size.

Network and Communication Security

HPE recommends that you add iptables rules listed below.

> The ports in this topic are the pods for CDF. For the ports specific to ITSMA suite, see ITSMA node ports.

> Apart from the listed ports, all other ports should be blocked at the localhost level.

Target server to configure the rules	Required ports	Service	Direction	Short description
NFS server	111	NFS	Nodes -> NFS Server	NFS server port access by all nodes
NFS server	2049	NFS	Nodes -> NFS Server	NFS server port access by all nodes
Master Node	2380	Etcd	Master <-> Master	Etcd service port for etcd cluster communication
Master Node	4001	Etcd	Nodes -> Master	Etcd service port for connection from client

Ingress Node	5443	MngPortal	All -> Ingress Node	The port exposed on ingress node. All clients could access this port
Master Node	8200	Vault	Nodes->Master	Vault port for client connection
Master Node	8201	Vault	Nodes->Master	Vault port for peer member connection
Master Node	8443	Kubernetes	Nodes -> Master	API server port for client connection
All Nodes in Cluster	10250	Kubernetes	Nodes -> Nodes	Kubernete port for internal communication
All Nodes in Cluster	10251	Kubernetes	Nodes -> Nodes	Kubernete port for internal communication
All Nodes in Cluster	10252	Kubernetes	Nodes -> Nodes	Kubernete port for internal communication
All Nodes in Cluster	10255	Kubernetes	Nodes -> Nodes	Kubernete port for internal communication
NFS server	20048	NFS	Nodes -> NFS Server	NFS server port access by all nodes

Example:

The cluster is installed on 10.10.10.10, 10.10.10.11, 10.10.10.12, and the master node is on: 10.10.10.10 .

To add iptable rules to port 8443 on the master node, do the following:

```
iptables -I INPUT 1 -p tcp -m tcp -s 0.0.0.0/0 --dport 8443 -j DROP

iptables -I INPUT 1 -p tcp -s 127.0.0.1 --dport 8443 -j ACCEPT

iptables -I INPUT 1 -p tcp -s 10.10.10.10 --dport 8443 -j ACCEPT

iptables -I INPUT 1 -p tcp -s 10.10.10.11 --dport 8443 -j ACCEPT

iptables -I INPUT 1 -p tcp -s 10.10.10.12 --dport 8443 -j ACCEPT
```

Restart ITOM CDF

To restart ITOM Container Deployment Foundation (CDF), stop and then start it.

Follow the steps below to stop ITOM

1. On the master node:

   ```
   cd $K8S_HOME/bin

   ./kube-stop.sh
   ```
2. On each worker node:

   ```
   cd $K8S_HOME/bin

   ./kube-stop.sh
   ```

Follow the steps below to start ITOM CDF:

1. On the master node:
   ```
   cd $K8S_HOME/bin

   ./kube-start.sh
   ```
2. On each worker node:

   ```
   cd $K8S_HOME/bin

   ./kube-start.sh
   ```

Download and upload suite images

You can download suite images from Docker Hub and then upload the images to ITOM Container Deployment Foundation (CDF). For details, see Download ITSMA images from Docker Hub to CDF.

Customize the parameters for kubelet

You can modify the default values of the kubelet parameters and add some customized parameters for kubelet. Follow the steps below to customize the parameters.

Follow these steps:

1. Log on to any of the cluster node.
2. Edit or add the parameters in the `kubelet.service` under the `/usr/lib/systemd/system`directory.
3. Run the following commands to restart the kubelet:
   systemctl daemon-reload
   systemctl restart kubelet

Modify the external database configuration

You can modify the external database configuration with the following command: `$K8S_HOME/bin/updateExternalDbInfo`
Example Usage:

```
Usage: $updateExternalDbInfo <-t|--dbtype <DB type>> <-u|--user <username>> <-H|--host <DB host>>
<-p|--port <DB port>> <-d|--dbname <DB name>>

or updateExternalDbInfo <-t|--dbtype <DB type>> <-u|--user <username>> <-U|--url <DB connection URL>>

-u|--user External database username.

-H|--host External database host.

-p|--port External database port.

-d|--dbname External database name.

-U|--url External database connection URL.

-t|--dbtype External database type, optional choices are ("EMBEDDED","EXTERNAL_PG","EXTERNAL_ORA") . The
database type must be capitalized.

-h|--help Show help.
```

When you modified any external default database configuration, you must recreate the IDM pod with the following commands:

```
kubectl delete -f $K8S_HOME/objectdefs/idm.yaml

kubectl create -f $K8S_HOME/objectdefs/idm.yaml
```

Create or modify security groups in AWS

If you deploy ITSMA in a cloud-based environment, three security groups will be configured for the Virtual Private Cloud (VPC) after ITSMA is successfully deployed on Amazon Web Services (AWS). These security groups provide access to the instances in the VPC. They act as a firewall for the associated instances to control both inbound and outbound traffic at the instance level.

Group Name Pattern	Target
${aws_resource_prefix}-master-sg	master nodes
${aws_resource_prefix}-worker-sg	worker nodes
${aws_resource_prefix}-efs-sg	EFS

For example, if you use "itom-itsma1" as the deployment name prefix, you will find security groups "itom-itsma1-master-sg", "itom-itsma1-worker-sg", and "itom-itsma1-efs_sg".

Usually, you do not need to modify these security groups, as they allow access to ITSMA by default. However, if you do need to modify the security group settings, follow these steps:

1. Log in to the AWS console.
2. Click **VPC**.
3. On the left-hand menu, click **Security Group**.
4. Create a new security group or modify the existing security group as required.

For more information about AWS security groups, refer to the following Amazon website:

Administer the ITSMA suite

The Suite Administrator user role can perform the following administration tasks.

- Install an ITSMA suite license
- Configure LDAP
- Import master data
- Configure Email
- Replace the certificate for ITSMA
- Configure SAML SSO
- Configure the Service Portal mobile app
- Configure log level for debugging
- Change the ITSMA suite administrator password
- Service Portal administration
- Smart Analytics administration

Install an ITSMA suite license

A license for ITOM Container Deployment Foundation (CDF) is included in each suite license. Each ITSMA suite license includes a license key for each of the suite components. When ITSMA is running in fully containerized mode, a suite license is required; when running in mixed mode, a suite license may or may not be required depending on the actual situation.

Deployment mode based licensing

The following licensing rules apply for ITSMA NG Express 2017.07.

For more information about the deployment modes, see Deployment modes.

Fully containerized mode

When running in fully containerized mode, ITSMA requires an ITSMA suite license. ITSMA comes with a 21-day trial license. After the trail period, you must purchase and activate a perpetual license.

Mixed mode

For mixed mode scenario 2, an ITSMA suite license is required and UCMDB requires a license of its own. For mixed mode scenario 1, no suite license is required.

Additionally, you can optionally purchase a Smart Analytics license according to your business needs:

- If without a Smart Analytics license: IDOL-based search is enabled for Service Portal users; however, the following features are disabled in Service Management: Smart Ticketing, Hot Topic Analytics (HTA), OCR, Smart Search, and Smart Analytics related features in Virtual Agent and Smart Email (that is, automatically proposing knowledge articles or service catalog offerings).
- If with a Smart Analytics license: all Smart Analytics related features listed above are enabled.

> The Virtual Agent feature in Service Portal is enabled regardless of whether the system has a Smart Analytics license installed.

Activate an ITSMA suite license

> **License menu option**
> Once ITSMA is installed, you can locate the installed ITSMA instance from the ITOM CDF user interface (**Suite** > **Management**) and then access the **License** menu option from its more action icon. You must use the **License** menu option to install and manage suite licenses.

To activate an ITSMA license, follow these steps:

1. Install your ITSMA license. For details, see the license installation section in Manage licenses.
2. Restart the Service Management RTE deployments:
    a. Click **RESOURCES,** and then select your <namespace>. For example, **itsma1**.
    b. Click **Workloads** > **Deployments**, and then locate one of the following deployments:

        sm-rte
        sm-rte-integration
        sm-rte-irque

sm-rte-scheduler
sm-rte-emailout
sm-rte-integration-cit
sm-rte-report-export
sm-rte-gossip

> The **sm-rte-gossip** deployment must be the last one to stop. No sequence is required for the rest of the deployments.

c. Click the more action icon (

), and then click **View/edit YAML**.
d. Locate "replicas" under "spec", and then do the following:
   i. Make a note of the current value. You will need to use the value when you start the pod again later in step g.
   ii. Set the value to 0.
   iii. Click the **UPDATE** button.
e. Repeat the steps above to stop all the deployments listed in step **b**. The **sm-rte-gossip** deployment must be the last one to stop.
f. Wait until the **Pods** field for each deployment is changed to 0/0.
g. Change the value of "replicas" in the YAML from 0 to the original number for all the deployments listed in step b.

> You must start the **sm-rte-gossip** deployment first. No sequence is required for the rest of the deployments.

Configure LDAP

See the following topics for LDAP related configurations for ITSMA NG Express:

- Configure an external LDAP server
- Configure LDAP for CMDB
- Configure LDAP for Service Portal
- Configure users in the internal LDAP server

Configure an external LDAP server

User role: Suite Administrator

The ITSMA suite must be integrated with an LDAP server for user authentication. All LDAP servers are supported, including OpenLDAP and Microsoft Active Directory.

The ITSMA LDAP settings fall into these categories: LDAP Server Settings, LDAP User Attributes, LDAP Group Attributes, and Group Mappings. You have the option to configure LDAP either during installation or after installation (by using the Suite Configuration utility). The LDAP settings that you see during installation and after installation are basically the same. However, Group Mappings available during installation are not available in the Suite Configuration user interface.

Additionally, ITSMA supports SAML 2.0 based single sign-on (SAML SSO), which relies on correct LDAP configuration to work, and therefore the LDAP configuration page in the Suite Configuration user interface also contains a **SAML 2.0 Configuration** section. If you do not want to enable SAML, ignore SAML configuration fields on this page.

> The ITSMA suite has a seeded user account named **sysadmin,** which is stored in ITSMA's IdM database. This user has super administrator privileges for the suite. For this reason, make sure that your external LDAP server does NOT contain a **sysadmin** user account.

This topic describes the steps to configure an external LDAP server after installation by using the Suite Configuration utility. For information about how to configure LDAP during installation, see Run the Suite Installer.

To configure an external LDAP server, follow these steps:

1. Open the **Suite Configuration** utility. For details, see Access ITSMA capabilities.
2. Navigate to **Configuration** > **Accounts** > **LDAP & SAML**.
3. Optional. Select one of the following options according to your own LDAP server: **OpenLDAP**, **Active Directory**, or **Other LDAP**.

   A default value is provided for certain LDAP fields if **OpenLDAP** or **Active Directory** is selected.
4. Configure your external LDAP server settings as described in the following tables. All fields are mandatory unless otherwise specified.

   LDAP Server Settings

Field	Description	OpenLDAP default value
Host	The fully-qualified domain name (server.domain.com) or IP address of the LDAP server.	
Port	The port used to connect to the LDAP server (by default, 389).	389
Base DN	Base distinguished name. The Base DN is the top level of the LDAP directory that is used as the basis of a search.	dc=itsma,dc=com
User ID (Full DN)	The fully distinguished name of any user with authentication rights to the LDAP server.	cn=admin,dc=itsma,dc=com
Password	Password of the User ID. If the LDAP server does not require a User ID or password for authentication, this value can be omitted.	
Enable SSL	If your LDAP server is configured to require ldaps (LDAP over SSL), select the **Enable SSL** checkbox.	
Search Subtree	When a user logs in, the LDAP directory is queried to find the user's account. The **Search Subtree** setting controls the depth of the search under User Searchbase. If you want to search for a matching user in the User Searchbase and all subtrees under the User Searchbase, make sure the **Search Subtree** checkbox is selected. If you want to restrict the search for a matching user to only the User Searchbase, excluding any subtrees, unselect the **Search Subtree** checkbox.	

LDAP User Attributes

Field	Description	OpenLDAP example value
User Base DN	Base distinguished name for the User object. The User Base DN is the top level of the LDAP directory that is used as the basis of a search for the User object.	ou=people,dc=itsma,dc=com
User Class	Value of objectClass that is used to identify the user.	inetOrgPerson
User Filter	Specifies the general form of the LDAP query used to identify users during login. It must include the pattern {0}, which represents the user name entered by the user when logging in. The filter must use the following format: (&(objectclass=*)(cn=falcon))	(objectclass=inetOrgPerson)

First Name	**Optional field.** First name of the user.	givenName
Last Name	**Optional field.** Last name of the user.	sn
User Display Name	The display name of the user.	cn
User Name Attributes	The name of the attribute of a user object that contains the username that will be used to log in. The value for this field can be determined by looking at one or more user objects in the LDAP directory to determine which attribute consistently contains a unique user name. Often, you will want a User Name Attribute whose value in a user object is an email address.	uid
User Email	The email address of the user.	mail
Phone Number	**Optional field.** Business phone number of the user.	telephoneNumber
User Avatar	**Optional field.** The LDAP attribute whose value is the URL to a user avatar image that is displayed for the logged-in user. If no avatar is specified, a default avatar image is used.	jpegPhoto
Manager Identifier	**Optional field.** The name of the attribute of a user object that identifies the manager of the user.	manager
Manager Identifier Value	**Optional field.** The name of the attribute of a user object that describes the value of the Manager Identifier's attribute. For example, if the value of the Manager Identifier attribute is a distinguished name (such as cn=John Smith, ou=People, o=xyz.com) then the value of this field could be dn (distinguished name). Or, if the Manager Identifier is an email address (such as **admin@xyz.com**) then the value of this field could be email.	dn

Last Modified	**Optional field.** The LDAP attribute that stores the timestamp when an object was last updated.	modifyTimestamp (for OpenLDAP) whenChanged (for Active Directory)

LDAP Group Attributes

Field	Description	OpenLDAP example value
Group Base DN	Base distinguished name for the Group object. The Group Base DN is the top level of the LDAP directory that is used as the basis of a search for the Group object.	ou=groups,dc=itsma,dc=com
Group Class	Value of objectClass that is used to identify the Group object.	groupOfUniqueNames
Group Filter	Specifies the general form of the LDAP query used to identify user groups during login. It must use a standard search filter syntax for your LDAP server.	(objectclass=groupOfUniqueNames)
Group Display Name	The display name of the user group.	cn
Group Membership	The name of the attribute(s) of a group object that identifies a user as belonging to the group. If multiple attributes convey group membership, the attribute names should be separated by a comma.	uniqueMember

> Skip SAML configuration at this point. Configure SAML SSO after you complete the LDAP configuration. For details, see Configure SAML SSO.

5. If you selected the **Enable SSL** option, before you apply the LDAP configuration, copy the LDAP CA certificate file to the **{itsma_global_volume}/certificate/ca-trust/** folder, where **{itsma_global_volume}** is the ITSMA global NFS volume (see Set up three NFS shares for ITSMA). For example: /var/vols/itom/itsma/itsma-itsma-global/certificate/ca-trust/. Note that UCMDB only supports importing a certificate file whose extension is ".crt", which means you need to convert or rename the certificate file to that format.
6. Click **Test** to make sure all settings are correct.
   All LDAP settings are validated, and an error message is displayed if a validation fails.
7. Click **Apply** to save your configuration.

   After you apply the changes, the system restarts the related services.
8. Wait until the background services restart.
   ITSMA automatically updates the LDAP mapping settings in Service Management, Service Portal, and CMDB according to your configuration.
9. Go to Service Management, Service Portal, and CMDB to check the LDAP settings, and perform additional configurations:
   - Configure LDAP for Service Portal
   - Configure LDAP for CMDB
10. Log out of the ITSMA suite, and then log in by using an LDAP account to verify the LDAP server.

Configure LDAP for CMDB

In an out-of-box ITSMA system, only the **sysadmin** user can access CMDB. To enable other users to access CMDB, you need to configure LDAP settings in CMDB. See also Import user data into ITSMA.

Configuring LDAP settings in CMDB is required for both the internal and an external LDAP server.

To configure an external LDAP server for CMDB, make sure that you have configured the global LDAP settings in the Suite Configuration user interface (**CONFIGURATION** > **Accounts** > **LDAP & SAML**) before your perform the steps here. For details, see Configure an external LDAP server.

This document uses screenshots based on the internal LDAP server.

To configure LDAP in CMDB, perform these steps:

Fully containerized mode (CMDB is containerized)

If ITSMA is installed in fully containerized mode, once you have selected the internal LDAP server during the installation or have configured an external LDAP server (see Configure an external LDAP server), ITSMA automatically populates CMDB with the internal or external LDAP settings. You only need to configure LDAP groups in CMDB.

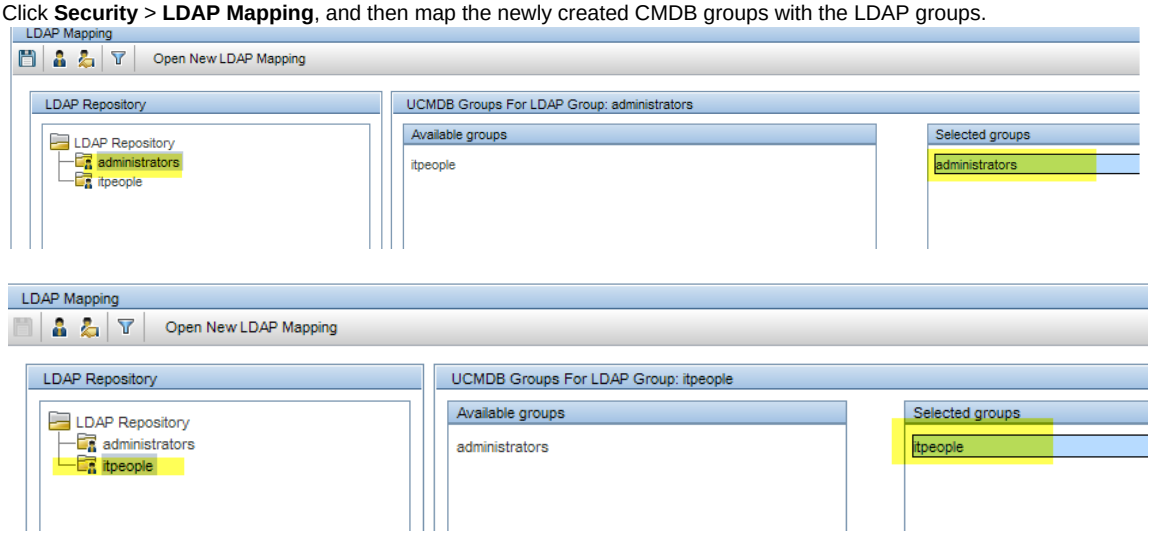
In fully containerized mode, perform the following steps.

Step 1: Create groups in CMDB and map them with LDAP groups

1. Log on to ITSMA suite as **sysadmin**: https://<EXTERNAL_ACCESS_HOST>/main.
2. From the ITSMA landing page, click **CMDB Administrator**.
3. Create two CMDB groups:
   a. Click **Security** > **User and Groups**.
   b. Create a new group "administrators" and assign the "SuperAdmin" role to this group.
   c. Create a new group "itpeople" and assign the "Viewer" role to this group.

   If you use external LDAP, you need to create the groups in CMDB according to the actual groups in your external LDAP server and assign the appropriate right to each group.

4. Click **Security** > **LDAP Mapping**, and then map the newly created CMDB groups with the LDAP groups.

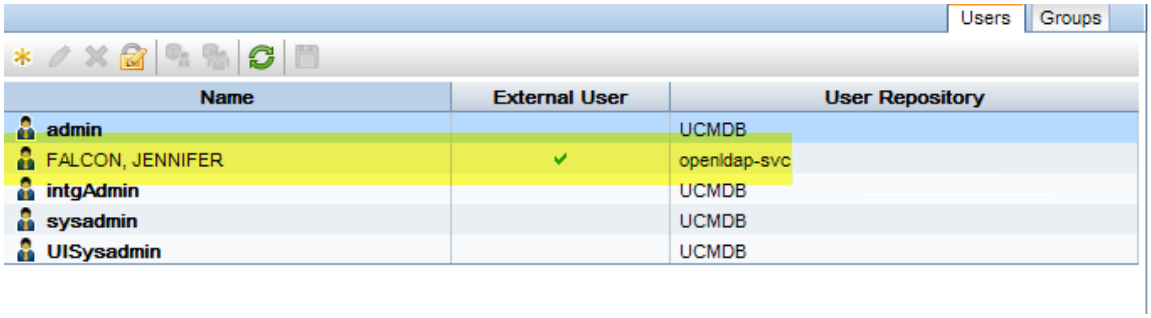


Step 2: Enable LDAP authentication

Select **Administration** > **Infrastructure Settings** > **LDAP General** > **Enable LDAP authentication**, and then set the value to **True**.

Step 3: Verify your LDAP settings

1. Log on to CMDB and CMDB browser as a user from the admin group (the group with the "SuperAdmin" role assigned in CMDB) of your LDAP server.
   For example, if you use internal LDAP, you can use "falcon" to log on to CMDB and CDMB browser.
2. Check that the user information is from LDAP.



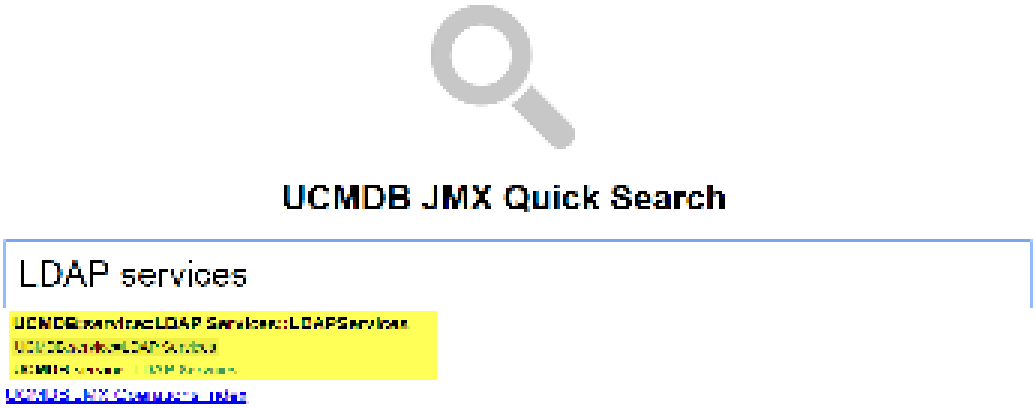
Mixed mode (CMDB is non-containerized)

In mixed mode, CMDB is an external UCMDB system. For this reason, UCMDB is not automatically populated with the global LDAP settings that you have configured (see Configure an external LDAP server), and you have to manually configure the required settings by using the UCMDB JMX console.

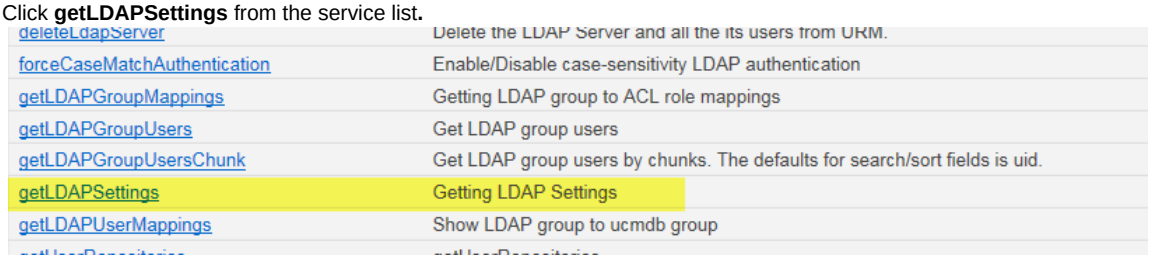
In mixed mode, perform the following steps.

Step 1: Configure "LDAP Services" in the UCMDB JMX console

1. On the UCMDB server, launch the Web browser and enter the following address: https://localhost:8443/jmx-console.
2. Log in as **sysadmin**.
3. Search for "LDAP Services" and then click the corresponding service.



4. Get the LDAP URL:
   a. Click **getLDAPSettings** from the service list**.**



   b. Click the **Invoke button.**

Mbean: UCMDB:service=LDAP Services. Method: getLDAPSettings

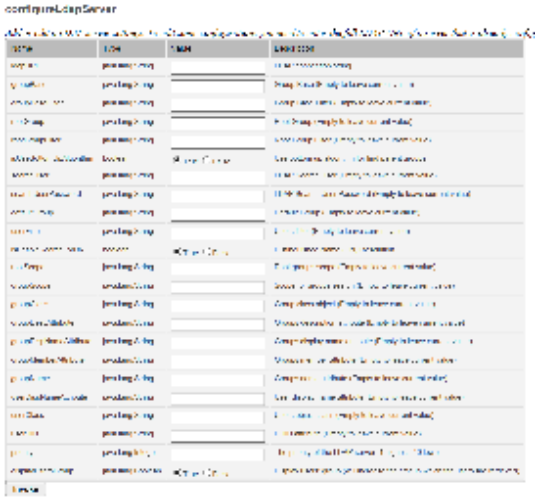
```
Is LDAP synchronization enabled : true

Is case-sensitivity enforced in LDAP authentication enabled : false
```

openldap-svc.itsma1.svc.cluster.local

Setting	Value
Connection	
URL	ldap://openldap-svc.itsma1.svc.cluster.local:389/dc=itsma,dc=com
Host	openldap-svc.itsma1.svc.cluster.local
Port	389

c. Get the LDAP URL. For example, the out-of-box internal LDAP URL is: **ldap:openldap-svc.itsma1.svc.cluster.local:389/dc=itsma,dc=com**

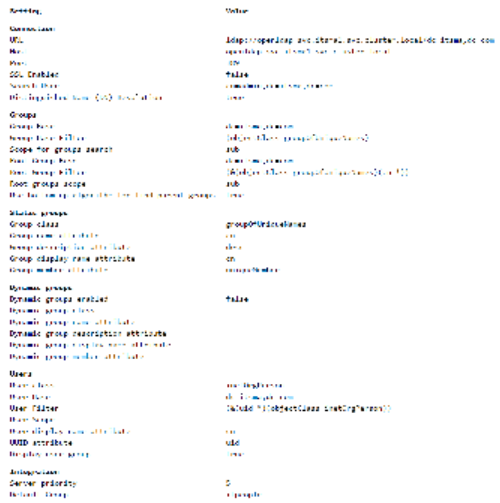
5. Configure the LDAP settings for UCMDB.
   a. From the LDAP Services list, click **configureLdapServer**. The following screen is displayed.



   b. In the **ldapURL** field, enter the LDAP URL you obtained previously, and then enter the correct values for all the required fields as indicated in the following example.

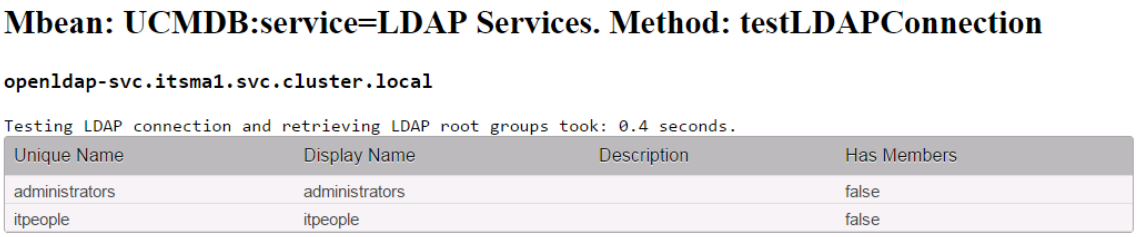
> The following example describes the required values for configuring internal LDAP server. For external LDAP, you must change the values accordingly based on your external LDAP server setting. For example the LDAP URL must be your external LDAP server URL.

> Be sure to also configure "searchUserPassword" for the system to log on to the LDAP server. The default value is "secret" for the internal LDAP server.



c. After you configure the LDAP settings, click **Invoke**.

6. Test the LDAP connection after your configuration:
   a. From the LDAP Services list, click **testLDAPConnection.**
   b. Click the **Invoke** button. Make sure that you can see your LDAP groups. For internal LDAP, you can see the following two groups in the test result.



Mbean: UCMDB:service=LDAP Services. Method: testLDAPConnection

openldap-svc.itsma1.svc.cluster.local

Testing LDAP connection and retrieving LDAP root groups took: 0.4 seconds.

Unique Name	Display Name	Description	Has Members
administrators	administrators		false
itpeople	itpeople		false

*Step 2: **Create groups in CMDB and map them with LDAP groups***

Log on to the external UCMDB system and then follow the instructions provided in step 1 for fully containerized mode.

Step 3: Enable LDAP authentication

Log on to the external UCMDB system and then follow the instructions provided in step 2 for fully containerized mode.

Step 4: Verify your LDAP settings

For details, see step 3 for fully containerized mode.

Configure LDAP for Service Portal

Service Portal uses HPE Identity Manager (IdM) for user authentication. Once you have configured an external LDAP server (see Configure an external LDAP server), you still need to manually configure LDAP groups in Service Portal to synchronize users from the LDAP server to IdM so that LDAP users can log in to Service Portal. For more information, see Import user data into ITSMA.

> If you configure LDAP during installation, a self-service user group is automatically created in Service Portal and mapped to the Consumer group. If you skip LDAP configuration during installation and configure LDAP after installation, no group is automatically created.

To manually configure groups, follow these steps:

1. Log on to ITSMA as **sysadmin**.
2. Click **Suite Configuration** > **Operation** > **Service Portal Administration**.
3. Click the **Identity** application in the Launchpad.
4. In the Organization List view, click **ITSMA**.
5. Follow these steps to add a group to which you can assign roles:
   a. In the Organization Details view, click **Groups**.

b. In the Groups view, click **Add Group**.
c. In the **Add Group** dialog, provide the following required information:
    i. Type a descriptive Group Name.
    ii. In the **Group Representation Type** field, select **LDAP Representation**.
    iii. In the Distinguished Name field, enter a value according to your LDAP data hierarchy. For example: **cn=<Group Name in LDAP>.ou=Groups**.
    iv. In the Authentication field, select the LDAP server that you configured.
d. Click **Save** to save your new group.

6. Follow these steps to add the groups created above to the corresponding roles. By default, Consumer and Organization Administrator roles are available.
    a. In the Organization Details view, click **Permissions**.
    b. In the Permissions view, click **Add Group** for the role that you want to associate with a group
    c. In the Add Group dialog, select the group, and then click **Save**. The specified group is associated with the role and listed under the role.

For more information on Service Portal LDAP related tasks, see the "Configure LDAP" topic from the Service Manager Help Center.

Configure users in the internal LDAP server

ITSMA has bundled an internal OpenLDAP server for demonstration purposes only. This internal LDAP server has only a very limited number of sample users configured. You can configure more users if needed.

The ITSMA suite uses the following port and user to connect Service Management and CMDB to the internal LDAP server:

- Port: 31389
- LDAP DN: cn=falcon,ou=people,dc=itsma,dc=com (password: 123456)

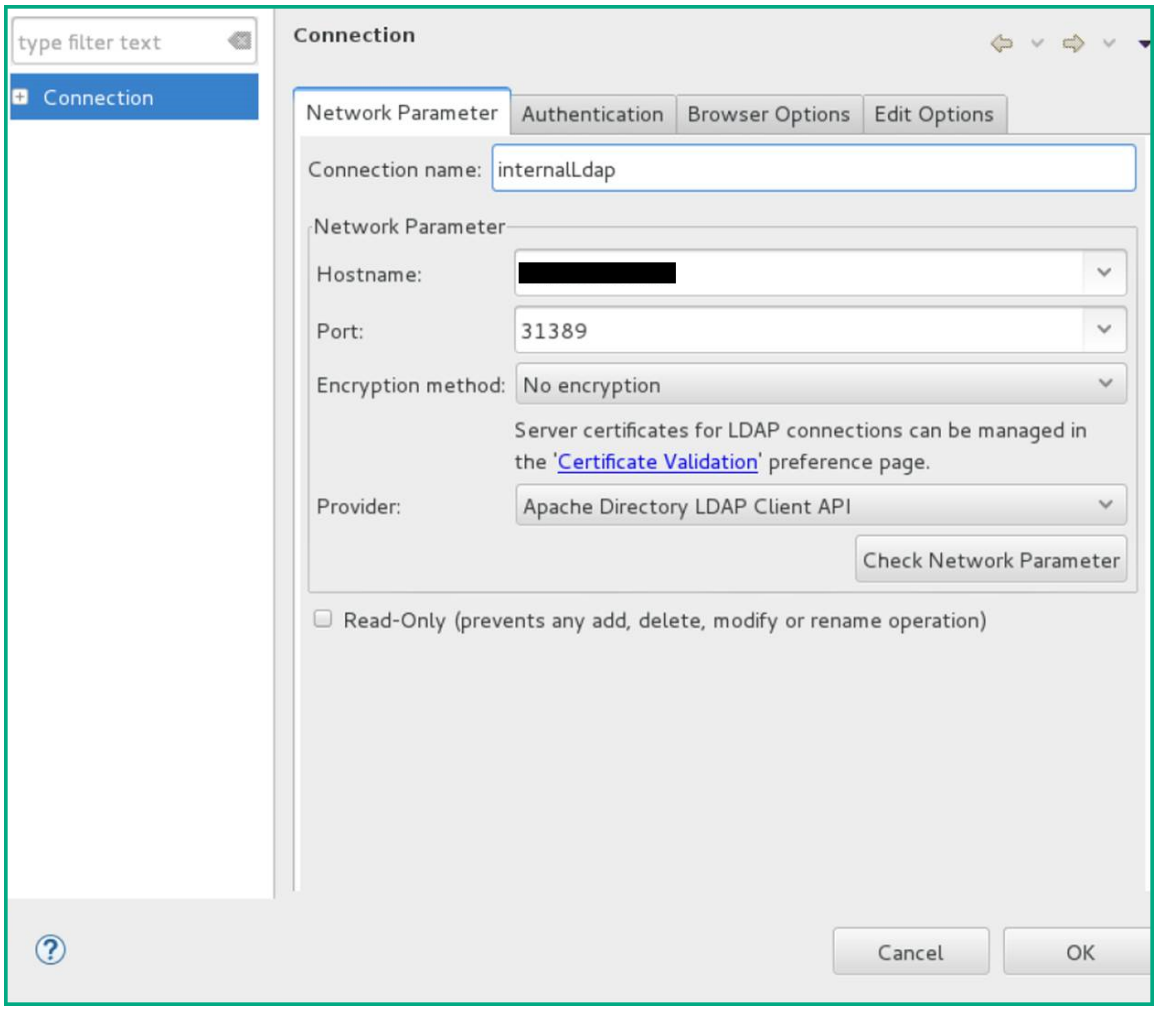
To configure users in the internal LDAP server, follow these steps:

1. Install an LDAP connection tool. For example, install Apache Directory Studio.

    The next steps use Apache Directory Studio as an example.

2. Launch Apache Directory Studio, and specify the following LDAP server connection information:
    On the **Network Parameter** tab, provide the following information:
    - **Connection name**: specify a display name for the LDAP server. For example, **internalLdap**.
    - **Hostname**: Enter the fully-qualified domain name or IP address of the master node.
    - **Port**: enter **31389**.
    - **Encryption method**: Make sure **No encryption** is selected.
    - **Provider**: Make sure that **Apache Directory LDAP Client API** is selected.

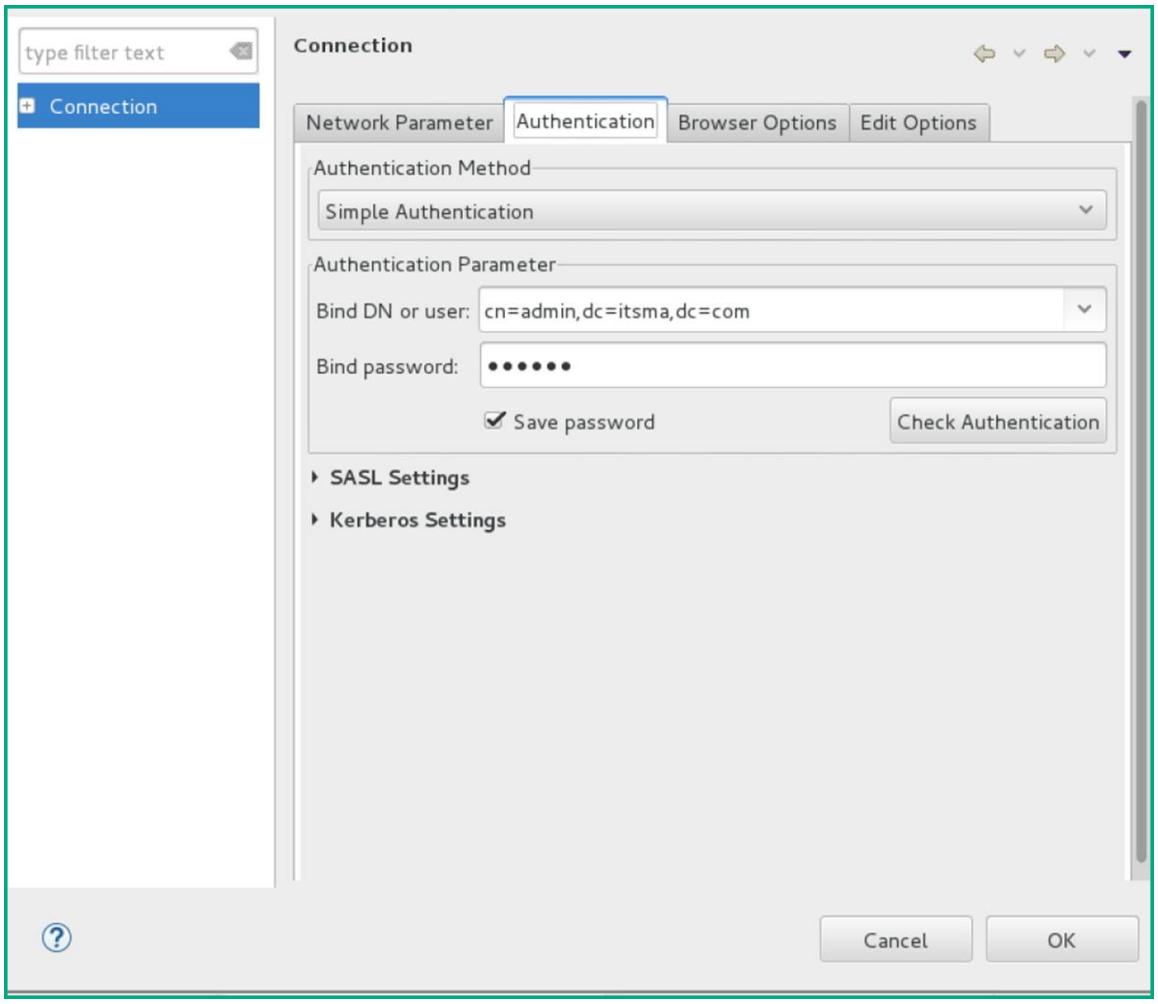
    See the following figure for an example.



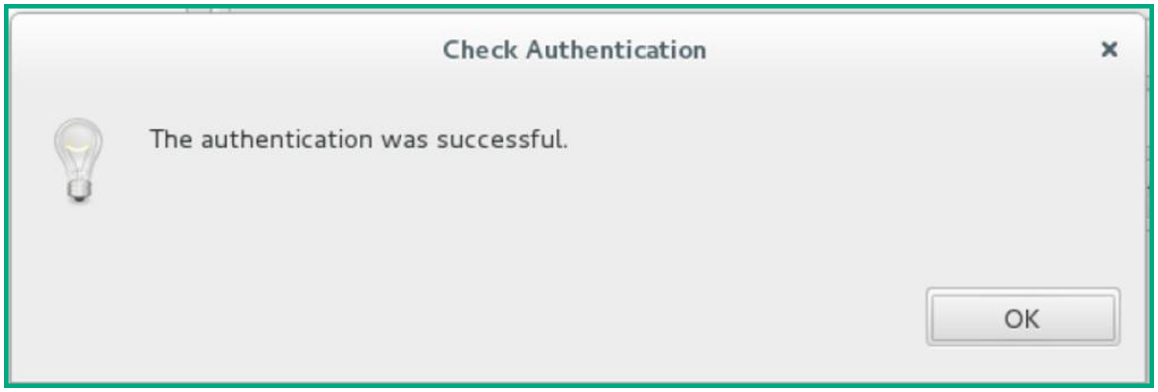
On the **Authentication** tab, provide the following information:

- **Authentication Method**: Make sure **Simple Authentication** is selected.
- **Bind DN or user**: Enter **cn=admin,dc=itsma,dc=com**.
- **Bind password**: Enter **secret**. This is the LDAP server administrator password.

See the following figure for an example.



3. Click **Check Authentication** to make sure the connection information is correct:



4. Click **OK**.
5. Add LDAP users. For details, see the OpenLDAP documentation.

Import master data

HPE provides a data import tool set, which can help you import master data from an existing Classic ITSMA system to ITSMA NG Express. You can download this toolset from HPE Marketplace.

- Purge demonstration data
- Use the data onboarding toolset to import master data
- Import user data into ITSMA

- This toolset supports master data onboarding for Service Management only.
- This toolset enables you to incrementally import data, which means you can always import additional data after an initial data import.

Purge demonstration data

Before your ITSMA system goes live, you need to purge the out-of-box demonstration data from Service Management, Smart Analytics, and UCMDB.

> To purge demonstration data, you must log in to the ITSMA Suite Portal as a suite administrator. For details, see Log in to the ITSMA Suite Portal. The following tasks assume you are already logged in to the suite portal.

Purge data from Service Management

To purge the demonstration data from Service Manager, follow these steps:

1. On the suite landing page, click **Service Management**.
2. You are automatically logged in to the Service Manager web tier client.
3. On the left-side navigator, click **System Administration** > **Base System Configuration** > **Miscellaneous** > **Purge Production Data**.
4. Make sure the **All Out of Box Data** option is selected, and then click **Next**.
5. Select the **I wish to purge all out of box data from the system** option to confirm the purge action.
6. Click **Next** to purge the data.

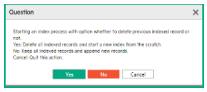
Purge indexes from Smart Analytics

To purge the indexes of the Service Manager demonstration data from Smart Analytics, follow these steps:

1. Make sure that you have already purged the demonstration data from Service Manager.
2. Click **Tailoring** > **Integration Manager**, and make sure the **SMIDOL** integration instance is enabled.

   > The **SMIDOL** instance is for the training, testing, index, and tuning processes that are triggered in Smart Analytics Configuration. Normally, one Service Manager Server has only one SMIDOL instance (named as SMIDOL*). The asterisk sign represents the sequence number, which is usually 0.

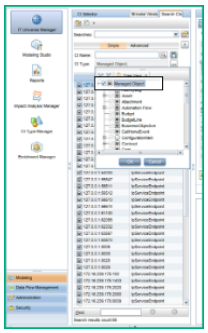
3. On the navigator, click **System Status** and make sure that the **KMReindex** schedule is started.
4. Follow these steps to index each Hot Topic Analytics configuration record:
   a. Click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Hot Topic Analytics**.
   b. Click **Search,** select a configuration record, and then click **Start Index**.
   c. Click **Yes** in the confirmation dialog that is displayed:

   
5. Follow these steps to fully re-index each Smart Ticket task:
   a. Click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
   b. From the Current Configuration List, select a task.
   c. Click **Training**, and then click **Yes** to confirm the training action.
6. Follow these steps to fully re-index each Smart Search library:
   a. Click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Search**.
   b. From the Current Knowledgebase List, select a knowledgebase.
   c. Click **Full Reindex**.

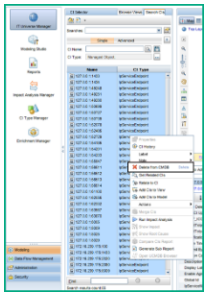
Purge data from UCMDB

To purge the demonstration data from UCMDB, follow these steps:

1. On the suite landing page, click **UCMDB Administrator**. You are automatically logged in to UCMDB.
2. Click **Modeling**, and then click **IT Universe Manager**.
3. In the CI Type field, select **Managed Object**. Click **OK**.



4. Click the search icon (magnifying glass) next to the CI Name field. A list of CIs is displayed.
5. Select all CIs, right-click the selected CIs, and then select **Delete from CMDB**.



Use the data onboarding toolset to import master data

If you have an existing Service Manager implementation, you can import the master data into your ITSMA system by using a toolset that is released on HPE Marketplace as a .zip file. This toolset comprises the following tools:

- A Microsoft Excel spreadsheet that contains a macro for exporting data to CSV files (located in the **Excel** subfolder)
- A set of files for use with HPE Connect-It, including a scenario file (DataOnBoarding.scn) and configuration files that are required for running the scenario (located in the **SM-CIT** subfolder)
- Sample CSV files (located in the **CSV** subfolder)

Limitations and known issues

- This toolset currently supports only data migration for Service Manager.
- Operator startup parameter values are not displayed correctly when you attempt to update them.
- Data is not imported into the Full Name field in the **contacts** table.

Understand the Excel spreadsheet

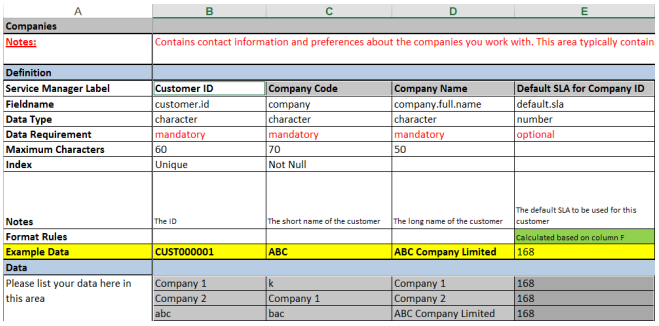
To migrate data by using the data onboarding toolset, you first need to enter your supporting data in the Excel spreadsheet provided by HPE.

The Excel spreadsheet is located in the **Excel** subfolder of the data onboarding package (.zip).

Color codes

The Excel sheet uses the following color codes.

Color	Explanation
Yellow	Yellow cells with this color contain sample data, which is not imported
Red	Cells that contain red text allow to specify additional data to import

Gray	Gray cells are automatically populated based on the value selected in another cell
Green	Green cells require you to select a value. The selected value is not get imported into the solution; instead, it is normally used to populate gray cells. For example, in the following image Column A allows you to select a value, which then populates column E. Column E is then imported into the solution. 

A	B	C	D	E
Companies				
Notes:	Contains contact information and preferences about the companies you work with. This area typically contain			
Definition				
Service Manager Label	**Customer ID**	**Company Code**	**Company Name**	**Default SLA for Company ID**
Fieldname	customer.id	company	company.full.name	default.sla
Data Type	character	character	character	number
Data Requirement	mandatory	mandatory	mandatory	optional
Maximum Characters	60	70	50	
Index	Unique	Not Null		
Notes	The ID	The short name of the customer	The long name of the customer	The default SLA to be used for this customer
Format Rules				Calculated based on column F
Example Data	**CUST000001**	**ABC**	**ABC Company Limited**	168
Data				
Please list your data here in this area	Company 1	k	Company 1	168
	Company 2	Company 1	Company 2	168
	abc	bac	ABC Company Limited	168

The Selections worksheet

The **Selections** worksheet contains predefined data from the solution. The data is used as a reference in all the other worksheets to ensure that the entered data matches the data that the toolset requires.

The following table describes the data available in the worksheet.

Column	Explanation
TimeZones	All available time zones of the suite products
Country Name	All available countries
Language Name	All available languages
Language ID	The language ID matching the language name
Customer SLA Name	The customer specific SLA Names
Customer SLA ID	The SLA ID matching the customer SLA Name
Service SLA Name	The service specific SLA Names
Service SLA ID	The SLA ID matching the service SLA Name
Location Site Category	The location site category
User Work Type	The different user types. For example, site, home, mobile
Security Roles	The security roles to give user the correct access in the modules
Contract Profiles	The user profile for the Contract Management module
Configuration Profiles	The user profile for the Configuration Management module
Operator Templates	The template use to set basic details in the operator record. For example, dashboard, default menu.
CI Display Name	The CI display name
CI Identifier	The CI ID matching the display name
Job Titles	The available job titles per department

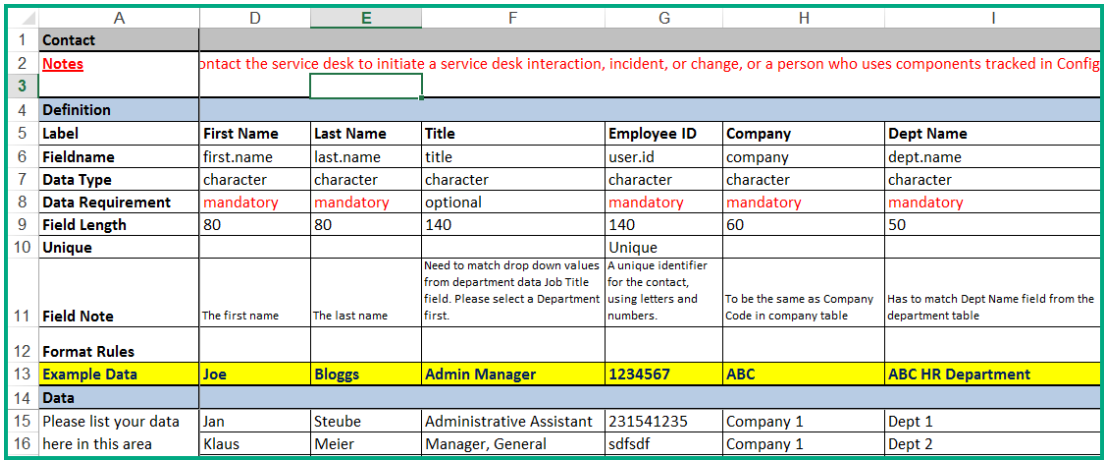
Dependencies between worksheets

Some worksheets include cross-references to data in other worksheets. These cross-references ensure data integrity throughout the spreadsheet. The ITSMA solution will import the same references between the data records into the ITSMA suite components.

The cross-references help you to select the correct record.

For example, the **Contacts** worksheet is referencing the following worksheets:

- Companies
- Location
- Departments



	A	D	E	F	G	H	I
1	**Contact**						
2	Notes	ontact the service desk to initiate a service desk interaction, incident, or change, or a person who uses components tracked in Config					
3							
4	**Definition**						
5	**Label**	**First Name**	**Last Name**	**Title**	**Employee ID**	**Company**	**Dept Name**
6	**Fieldname**	first.name	last.name	title	user.id	company	dept.name
7	**Data Type**	character	character	character	character	character	character
8	**Data Requirement**	mandatory	mandatory	optional	mandatory	mandatory	mandatory
9	**Field Length**	80	80	140	140	60	50
10	**Unique**				Unique		
11	**Field Note**	The first name	The last name	Need to match drop down values from department data Job Title field. Please select a Department first.	A unique identifier for the contact, using letters and numbers.	To be the same as Company Code in company table	Has to match Dept Name field from the department table
12	**Format Rules**						
13	**Example Data**	**Joe**	**Bloggs**	**Admin Manager**	**1234567**	**ABC**	**ABC HR Department**
14	**Data**						
15	Please list your data	Jan	Steube	Administrative Assistant	231541235	Company 1	Dept 1
16	here in this area	Klaus	Meier	Manager, General	sdfsdf	Company 1	Dept 2

Therefore, some worksheets can be completed only when some data is correctly entered in the other worksheets.

Worksheets

The Excel spreadsheet contains the following worksheets.

Information

This worksheet contains some basic information.

Companies

This worksheet contains contact information and preferences about the companies you work with.

Locations

This worksheet contains addresses and organizational information about the location of the companies. It comprises a hierarchy of records that document the company information, such as locations, sites, and buildings. The data can be used in contact records to see where a person is located.

Examples:
`Company: Customer A`

`/AT/City/Street1`

`/AT/City/Street1/Building A/Floor 1`

Contacts

This worksheet contains contact information about users who:

- Contact the service desk to initiate a service desk interaction, incident, or change
- Order from the Service Request Catalog
- Use components tracked in Configuration Management

Contact records contain reference to a company, department, and location. The unique ID for contact records is the contact name. The contact name is used as a reference in many places in the system and creates the link to the operator object. We recommend that you use a clear identifier for Contact and Operator Names.

Examples:

`Contact Name: firstname.lastname@customera.com`

`Company: Customer A`

`Department: Group 1`

`HPE Service Manager ID`:

```
Location: Floor 1
```

Departments

The department worksheet contains the data for the master data entities related to the Business-Organization of a company. You must ensure that correct organizational structure is built into the department table. The department is the next level of organizational unit after the company. The departmental structure is hierarchically organized, which means that each level references a parent department.

Departments are important for defining the correct relationship between the following records:

- SLA records and the Business Services in the Subscription Table
- Contact records and the correct Organizational Unit

Examples:

```
Company: Customer A

Customer A / Unit 1

Customer A / Unit 1

Customer A / Unit 1 / Department 1

Customer A / Unit 1 / Department 2

Customer A / Unit 1 / Department 1/ Group 1

Customer A / Unit 1 / Department 1/ Group 2

Customer A / Unit 1 / Department 2/ Group 3

Customer A / Unit 1 / Department 2/ Group 4

Customer A / Unit 2
```

Operators

This worksheet captures the operators who work with ITSMA. Although every user with access to a computer that has an active directory entry may access ITSMA, the import process should focus on operators who are actively working in the different modules in ITSMA.

Users who only access the end user portal do not need to be imported. End Users are created automatically within the suite, when the user first logs in.

To import and successfully create operator records, you must provide the following data:

- Name
- Contact ID
- Company
- Security Roles / Profiles

Other required attributes are set by a template operator and are populated at the creation of the operator record.

- Menu (Navigation Tree items)
- Time zone (should be taken from the contact record)
- Date format (defaulted date format of the time zone)

> To ensure successful authentication, the operator name has to match the <ID> in the HPE Identity Manager (IdM) server used by ITSMA.

Example:

```
Name: WZRXX212

Company: Customer A

ContactID: firstname.lastname@customera.com
```

Operator templates

ITSMA includes operator templates to ease the creation of operator records. The templates are used to fill some of the required attributes, such as the startup menu, capability words, currency, or query groups.

The following table describes out-of-box operator templates.

Template	Description
TEMPLATE_IM	Set the basic details for the Incident module
TEMPLATE_SM	Set the basic details for the Service Desk module
TEMPLATE_CM	Set the basic details for the Change module
TEMPLATE_RM	Set the basic details for the Request module
TEMPLATE_ADM	Set the basic details for Administrators

If the default settings in the operator templates do not cover your requirements, modify the templates or create new ones.

Operator Security

This worksheet captures the authorization rights of the ITSMA users.

The security model provides a consistent method of assigning permissions to users across all facets of ITSMA. It also provides standardized methods to manage user rights.

Security Roles:

A role has a set of rights and settings assigned to it. Each operator is assigned a role or roles which, along with area, determine the access rights for the operator.

Contract Profile:

The profile determines the access rights for the Contract Management module.

Configuration Profile:

The profile determines the access rights for the Configuration Management module.

Security Groups:

The operator record is used to determine the security groups of which the operator is a member and uses this information to determine the files to which the operator has limited access. When an operator queries a restricted file, Service Management reads the security group records to determine the filtering conditions to apply to the query. Service Management then returns only those records that match the filtering conditions in the security group records.

Examples:

```
change manager, change analyst
```

Vendors

This worksheet contains the list of suppliers (vendors and service providers) that support the IT solutions. This allows you to define:

- To which supplier a ticket was sent (in case there is no specified Assignment Group)
- To which supplier the Assignment Group is related (in case it is a service provider)

Examples

```
HPE, SAP, MICROSOFT
```

Assignment Groups

This worksheet captures the Assignment groups involved in Service Management process.

The naming convention for the Assignment Group is very important. A consistent and methodologically-organized naming convention facilitates the re-assignment of tickets. Additional attributes such as different levels or further classifications enable users to search for Assignment groups based on these attributes (for example, find all Assignment Groups that provide second-line support and that support the Service "Email").

Examples:

```
Service Desk EUR

Service Desk APJ

Exchange Team Level 2

Exchange Team Level 3
```

Exchange Team vendor

Assignments

This worksheets allows you to specify the members and approvers of each assignment group, and other attributes such as supported languages, supported departments, and locations.

KM Groups

This worksheet captures KM groups. KM groups allow you to relate groups of people with a specific KM profile and KM Category, which determine the rights of group members to create, review, and approve KM documents.

Examples:

KCS1 – All documents; KCSII – All documents; KCS1 – SAP; KCS2 – Service Manager

KM Group Assignment

This worksheets facilitates the setup of group members and other attributes of the KM group. You can specify the members of each group.

Holiday Group

This worksheet captures the different groups into which holidays may be organized.

For example, one group of holidays might include all holidays observed in France. This group would include worldwide holidays like Christmas and New Year's Day, together with those unique to France. A second group might also list the worldwide holidays, but add those unique to North America.

Holidays

This worksheet captures all holidays relevant to you and your partners.

Holiday Groupings

This worksheet is used to link the Holiday Group entries with the data in the Holidays table.

Work schedules

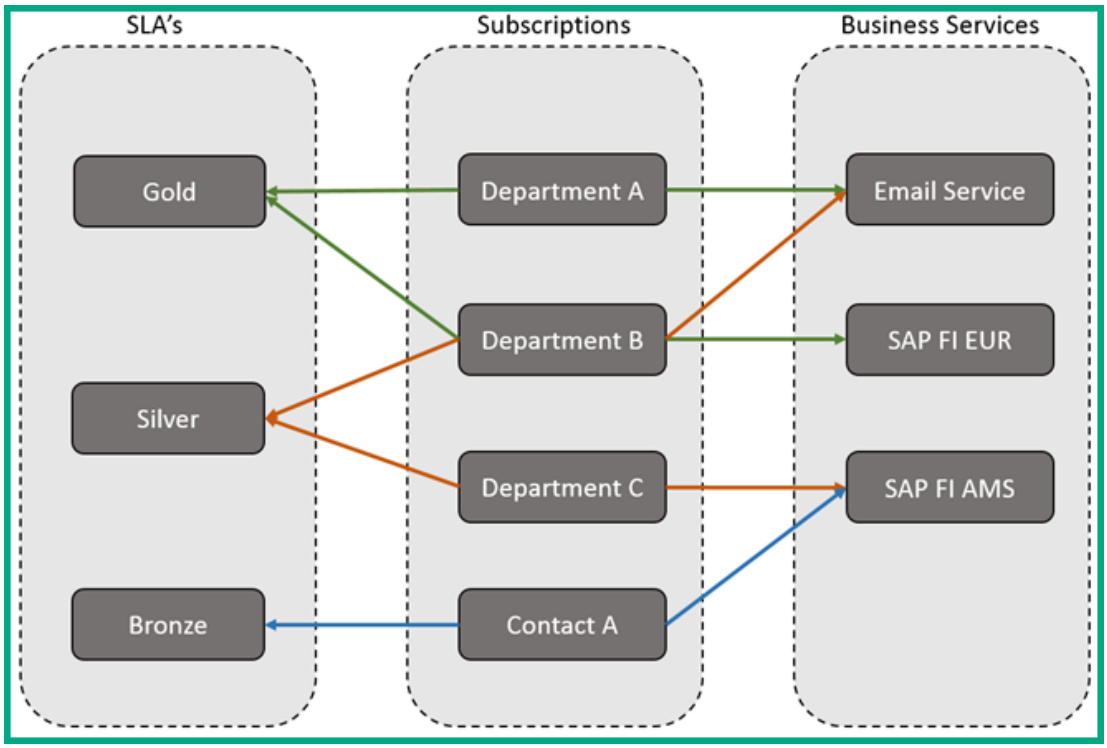
This worksheet captures the work schedules that define the work hours for users. Service Management can generate complex 24x7 schedules that span multiple time zones, include all shift and break information, accommodate any regional shift to Daylight Savings time, and automatically account for local or national holidays.

Work schedules can apply to a group, such as an assignment group, or to an individual named in the operator or contacts table. When you create schedule records, start and stop times must not overlap, and breaks must occur within the defined work shift.

Subscriptions

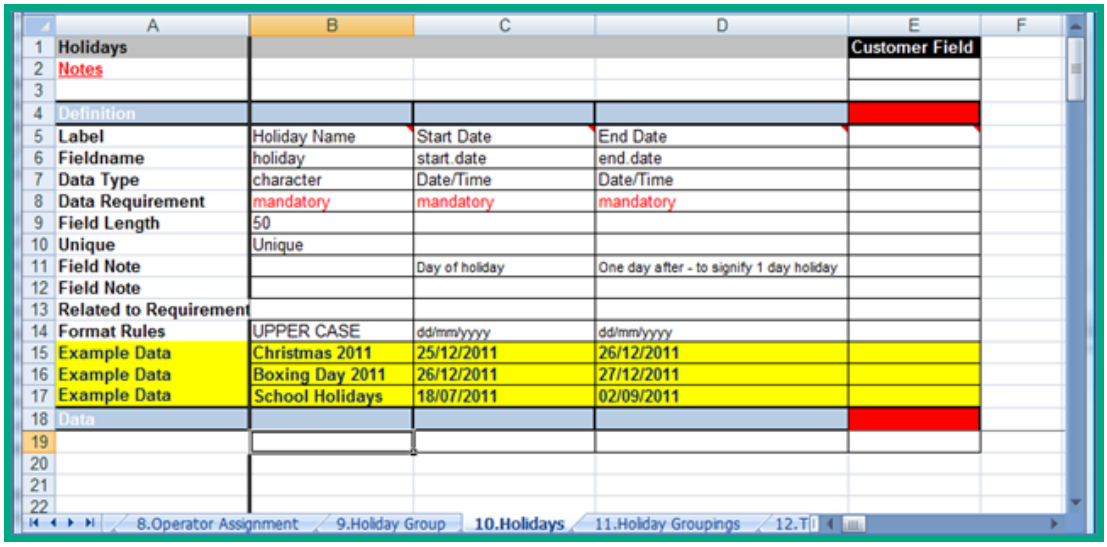
This worksheet captures the service subscriptions that track the relationships between IT customers and the services they use.

A service subscriber, either an individual user or an entire department, can request subscriptions to various services listed in Service Catalog. A subscriber’s list of subscriptions may reference access to shared services and individually assigned CIs. Subscriptions can include SLAs, history, custom options, and pending change requests.



Customize data fields

You may need to collect data from custom fields that are not included in the spreadsheet. Therefore, most of the worksheets have at least one section to capture the extra custom fields. This section is highlighted red.



	A	B	C	D	E	F
1	Holidays				Customer Field	
2	Notes					
3						
4	Definition					
5	Label	Holiday Name	Start Date	End Date		
6	Fieldname	holiday	start.date	end.date		
7	Data Type	character	Date/Time	Date/Time		
8	Data Requirement	mandatory	mandatory	mandatory		
9	Field Length	50				
10	Unique	Unique				
11	Field Note		Day of holiday	One day after - to signify 1 day holiday		
12	Field Note					
13	Related to Requirement					
14	Format Rules	UPPER CASE	dd/mm/yyyy	dd/mm/yyyy		
15	Example Data	Christmas 2011	25/12/2011	26/12/2011		
16	Example Data	Boxing Day 2011	26/12/2011	27/12/2011		
17	Example Data	School Holidays	18/07/2011	02/09/2011		
18	Data					
19						
20						
21						
22						

8.Operator Assignment | 9.Holiday Group | **10.Holidays** | 11.Holiday Groupings | 12.T

On each of the worksheets, there is a line of code that resembles the following in the Visual Basic Macro. This exports the data to a CSV file.

```
Call CreateITSMACSV(BRwin, 1, "1.Companies", "B5:E5,G5:U5,B15:E999,G15:U999", "1_Company", "")
```

- By default, the code line expects only one extra field (in the example above, this is column E). If you have more that one custom fields, you must customize the code.
- By default, the macro only exports up to row 999 in the worksheet. If you have more than 999 rows of data, you must customize the code.

Once that you have entered your data in the spreadsheet, you can export the data to CSV files. For more information about how to do this, see Export data to CSV files.

Export the master data to CSV files

To import master data into ITSMA, you must first use the the "ITSMA_Suite_Supporting_Data" spreadsheet to generate a number of CSV files. To do this, follow these steps.

> The spreadsheet contains only the main options that dictate the minimum required settings in ITSMA, and hence is not a complete replacement for direct entry into ITSMA. Many other factors and data cannot be entered through simple "yes or no" answers and are therefore not captured by the spreadsheet.

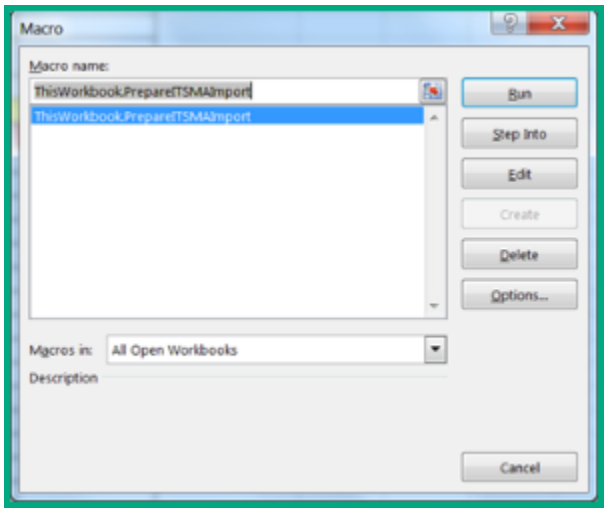
> The following steps are based on Excel 2013. If you are using a different version of Excel, the steps may slightly differ.

1. Unzip the data onboarding toolset package to a temporary directory on your local drive (for example, C:\DataOnBoarding).

   > When you unzip the package, retain the folder structure of the .zip file. Later, you will need to export data to CSV files and put the CSV files in the **CSV** subfolder. You may want to make a backup copy of the sample CSV files in the **CSV** folder, because your own CSV files will overwrite them.

2. Open the Excel spreadsheet in the **Excel** subfolder.
3. Make sure that macros are enabled in the spreadsheet (if macros are disabled, you should see a security warning. Click **Enable content** to enable macros).
4. Enter supporting data in the spreadsheet. For detailed instructions, see Understand the Excel spreadsheet.
5. Customize the "PrepareITSMAImport" macro (if required; see Understand the Excel spreadsheet), and then run the macro:
   a. On the **View** tab, click **Macros** and then select **View Macros**.
   b. If needed, select the "PrepareITSMAImport" macro and click **Edit** to edit it.

   > We recommend that you create a backup of the macro code before you edit it.

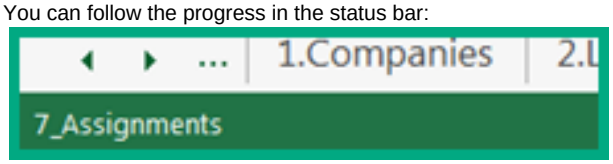
   

6. Once you have finished editing the macro, click **Run**. This directory (the directory from which you opened the spreadsheet) will generate 12 CSV files.
7. Verify the CSV files contain the correct data.
8. Copy the CSV files to the CSV subfolder (for example, C:\DataOnBoarding\CSV).

CSV file	Description
1_Company.csv	List of companies
2_Locations.csv	List of locations
3_Contacts.csv	List of departments (in a company above)
4_Departments.csv	List if contacts (in a company and dept above)

5_Operators.csv	List of operators against contacts
6_Vendors.csv	List of vendors
7_Assignments.csv	List of assignment group names
8_KMgroups.csv	The KM group names
9_Holiday Groups.csv	List of holiday group names
10_Holidays.csv	Calendar holidays (name and date)
11_Workschedules.csv	List of work schedules
12_Subscriptions.csv	Business service subscription against above dept

You can follow the progress in the status bar:



> If you execute the macro more than once, the macro overwrites existing files in the folder.

Next, you need to import the CSV files into ITSMA. See Import data from the CSV files into the ITSMA suite.

Import data from the CSV files into the ITSMA suite

Together with the data onboarding Excel spreadsheet, HPE provides a Connect-It scenario for you to easily import the generated CSV files into the ITSMA suite.

> In this release, the tool can import data into the Service Management capability only.

The Connect-It scenario consists of three main elements:

- A source connector, which helps to read the CSV files
- A destination connector, which connects to the ITSMA suite to insert and update the data
- Data mapping between the source and destination connectors to map the data from the CSV files with the database fields in the ITSMA suite

This scenario is designed for a one-time import; however, it can be used to import data on a regular basis.

To do this, perform the following steps:

- Step 1: Install Connect-It
- Step 2: Import the CSV files to the ITSMA suite
  - Task 1: Configure the source connectors
  - Task 2: Configure the custom field mapping
  - Task 3: Configure the destination connector
  - Task 4: Run the scenario
- Step 3: Verify the imported data

Step 1: Install Connect-It

We recommend that you install Connect-It 9.70, which you can download from http://www.hpe.com/software/entitlements.

For installation instructions, see the installation chapter in the Connect-It User Guide.

> You can use a 120-day InstantOn license for a one-time data import. For information about how to activate a Connect-It InstantOn license, see the Connect-It documentation.

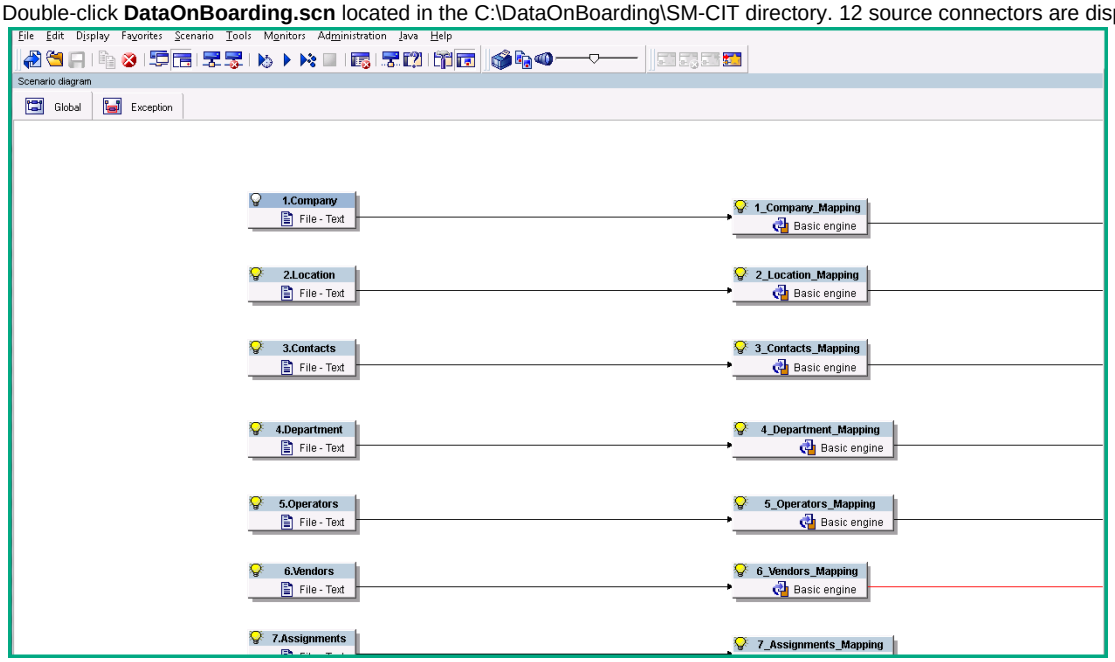
Step 2: Import the CSV files to the ITSMA suite

This step consists of the following tasks.

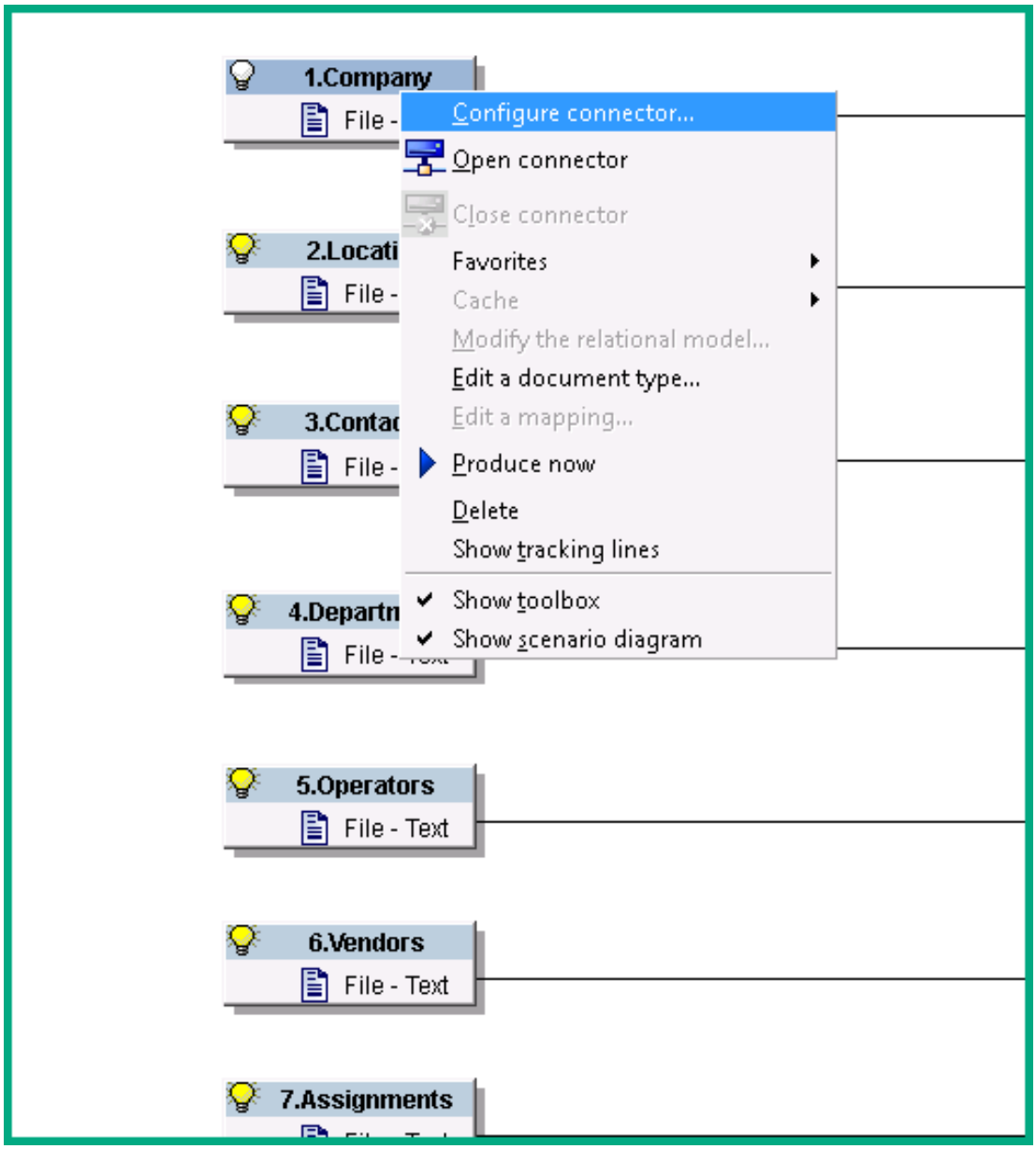
Task 1: Configure the source connectors

To do this, follow these steps:

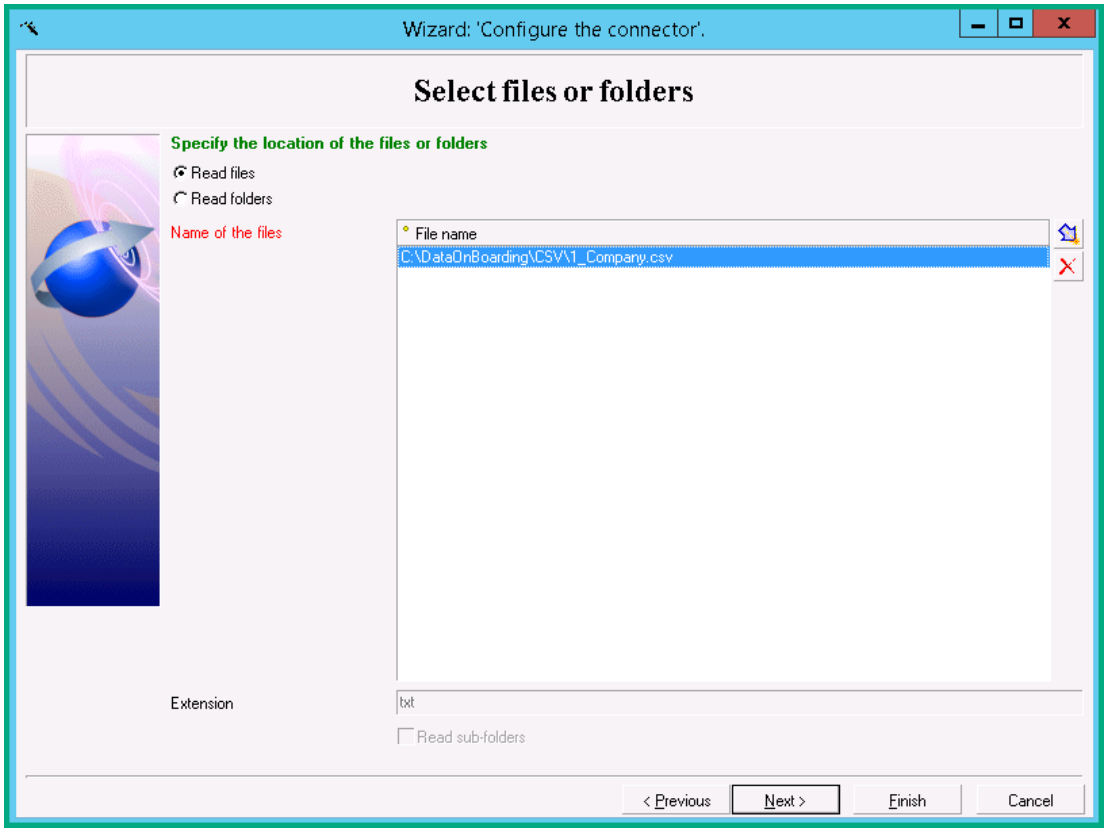
1. Double-click **DataOnBoarding.scn** located in the C:\DataOnBoarding\SM-CIT directory. 12 source connectors are displayed.



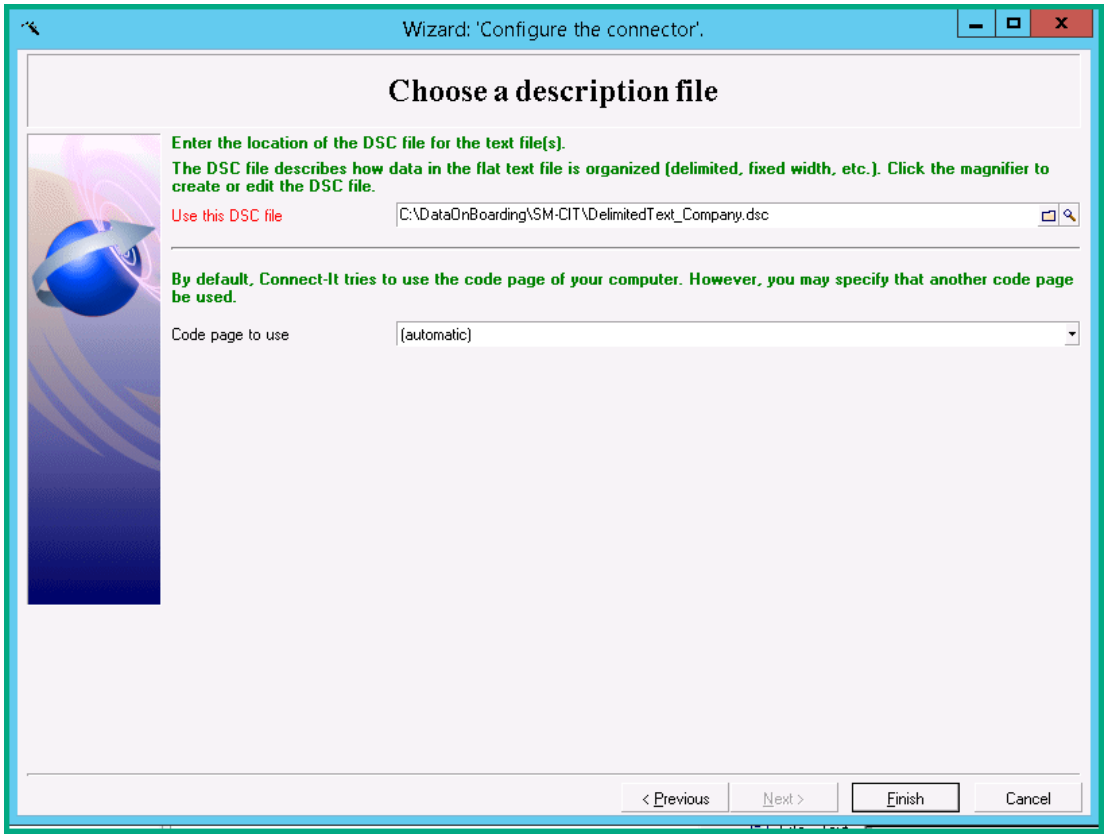
2. Configure the source connectors.
    a. Right-click the Company source connector, and then select **Configure connector**.



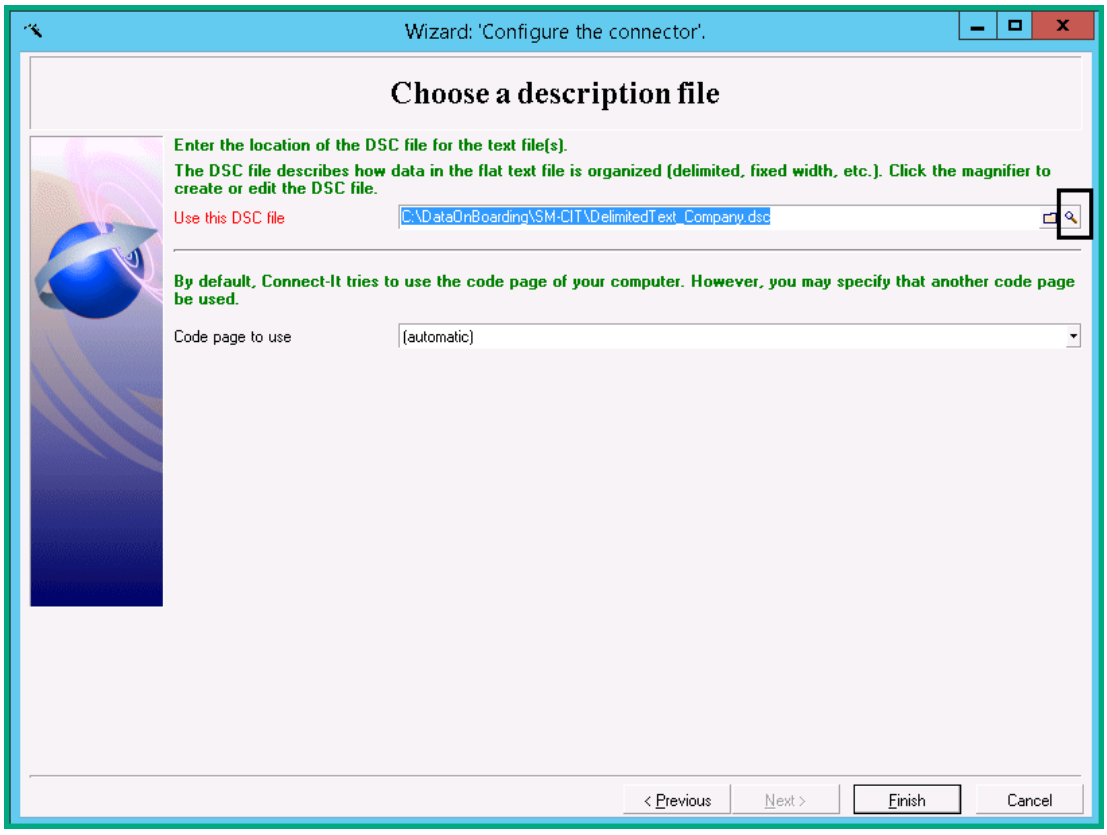
b. Click **Next** repeatedly until you see the "Select files or folders" page. Click the **File name** field and then browse to the corresponding CSV file.

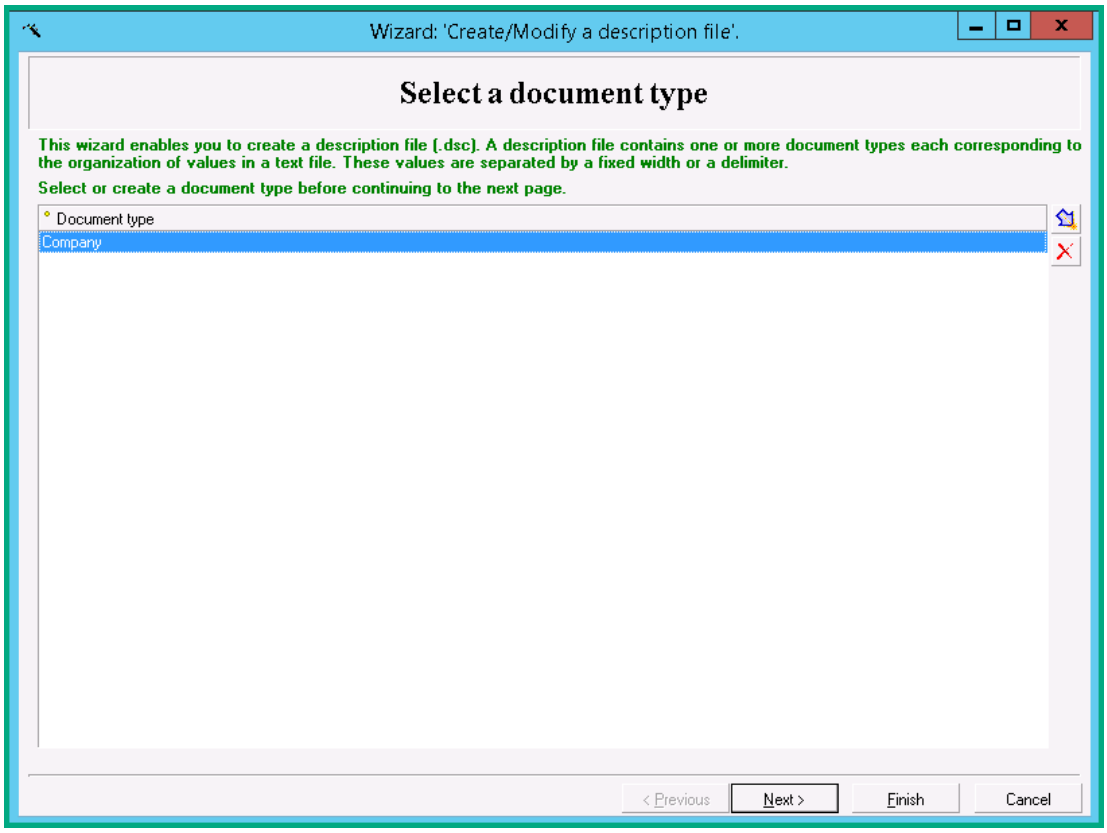


c. Click **Next** repeatedly until you see the "Choose a description file" page. Browse to the corresponding description file on your local drive.

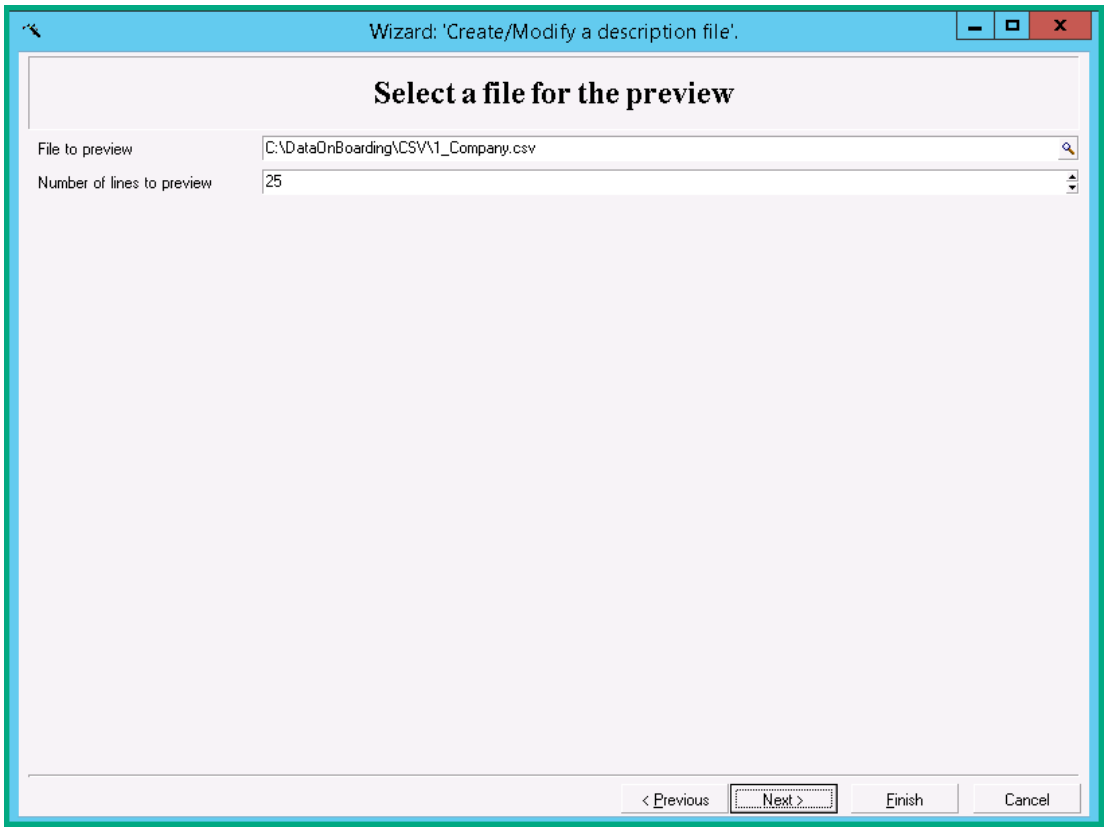


d. Click the Edit button to the right of the **Use this DSC file** field to open the "Select a document type" window.



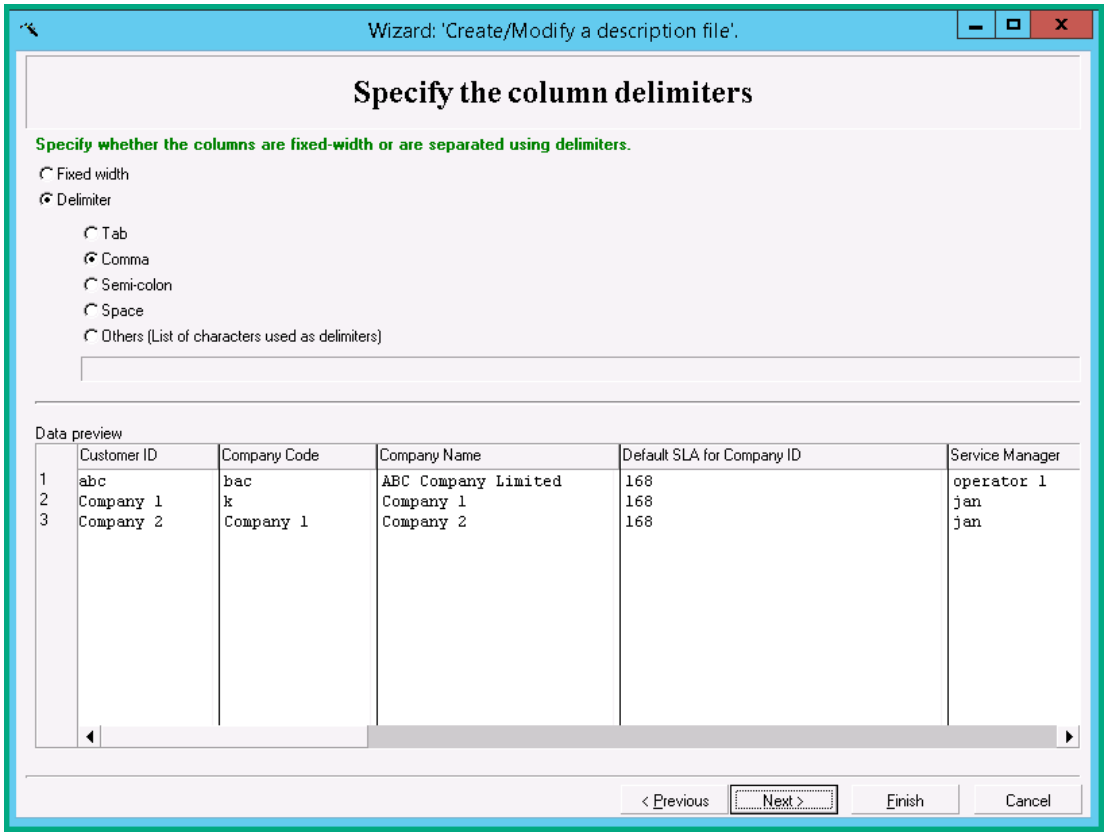


e. Click **Next**. The following page is displayed.



Click **Next**.

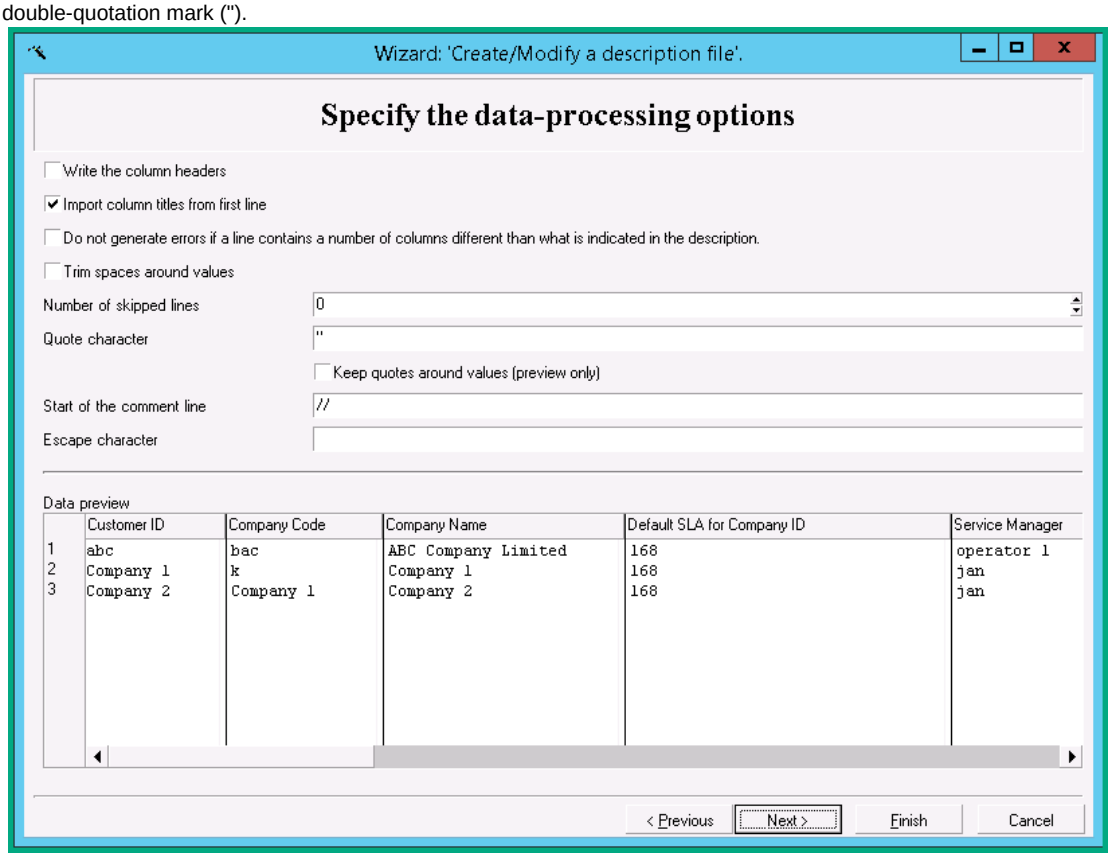
f. Make sure the **Delimiter** and **Comma** options are selected.



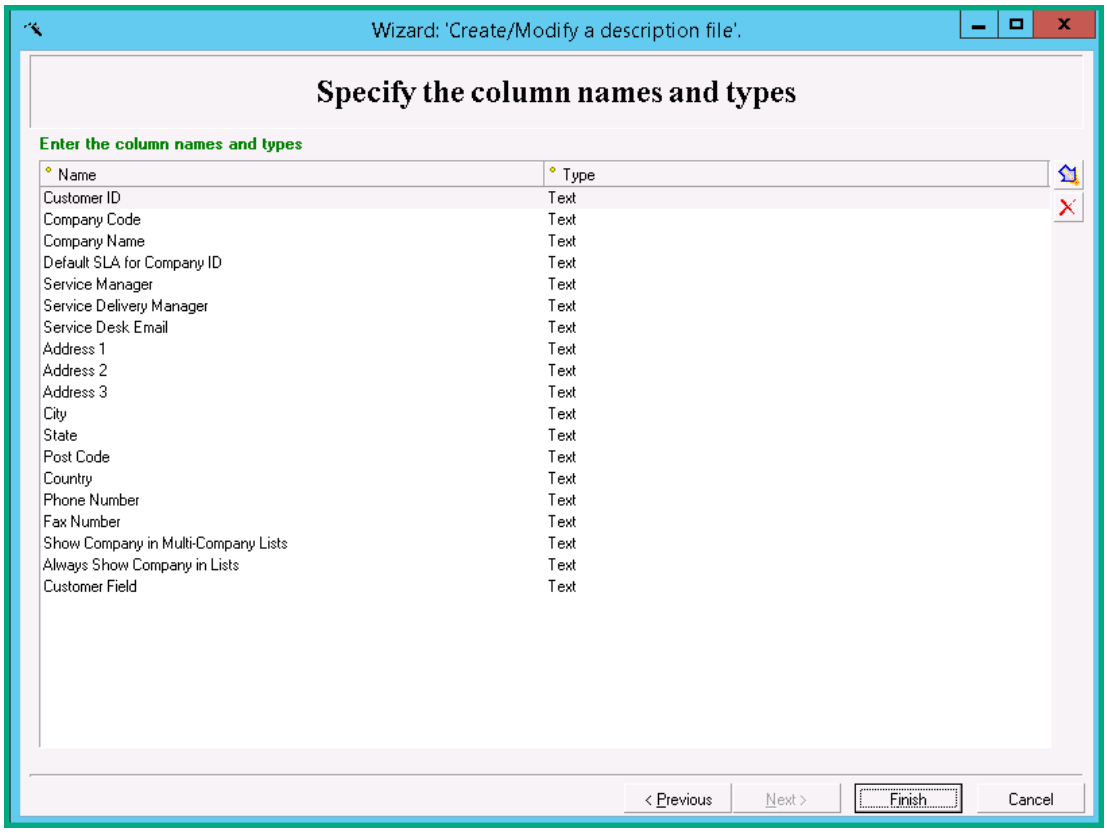
Click **Next**.

g. Make sure that the **Import column titles from first line** option is selected and the **Quote character** field is set to the

double-quotation mark (").



Click **Next**.



Click **Finish**.

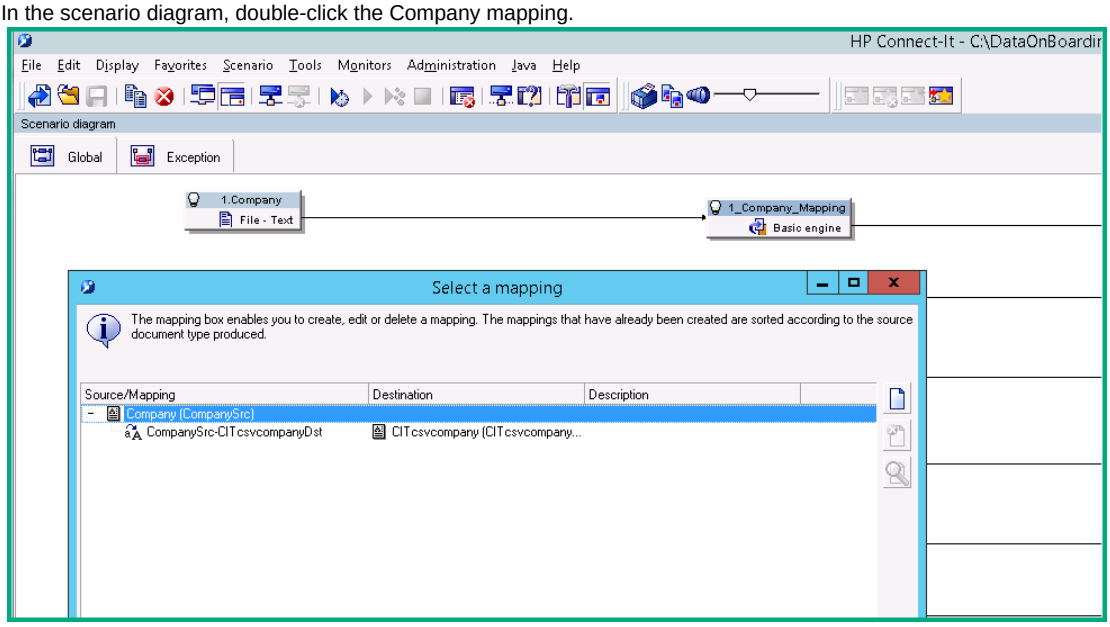
h. Check that the rest of the source connectors are automatically updated.

Task 2: Configure the custom field mapping

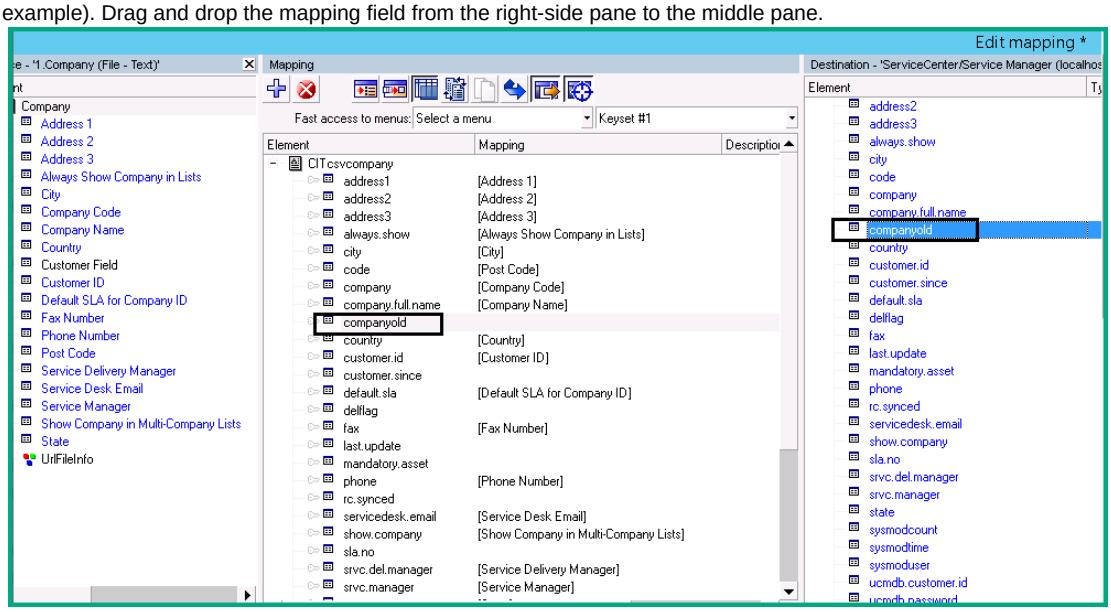
> You do not need to perform manual mapping for the out-of-box fields.

To do this, follow these steps:

1. In the scenario diagram, double-click the Company mapping.

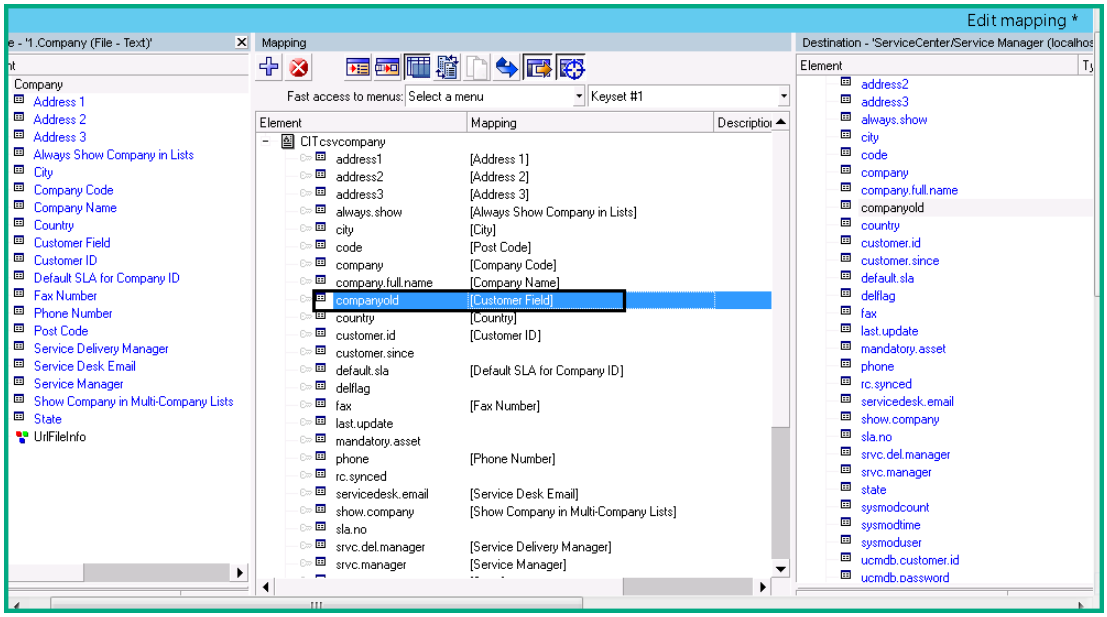


2. Double-click the mapping destination.
3. For the customer field ("Customer Field" on the left-side pane), locate the mapping field on the right-side pane (**companyold** in this example). Drag and drop the mapping field from the right-side pane to the middle pane.



> Fields on the left-side pane are from the CSV file, and those on the right-side pane are from the **company** table in Service Management.

4. Map the customer field you entered in the Excel spreadsheet to a Service Manager field.
   If the customer field is a text field, drag the customer field from the left-side pane to the middle pane to map it to the Service Manager field.



If the customer field is an array field in Service Manager, you should use a mapping script instead of the mapping method described above.
For example, the following script maps the out-of-box **secRole** field:

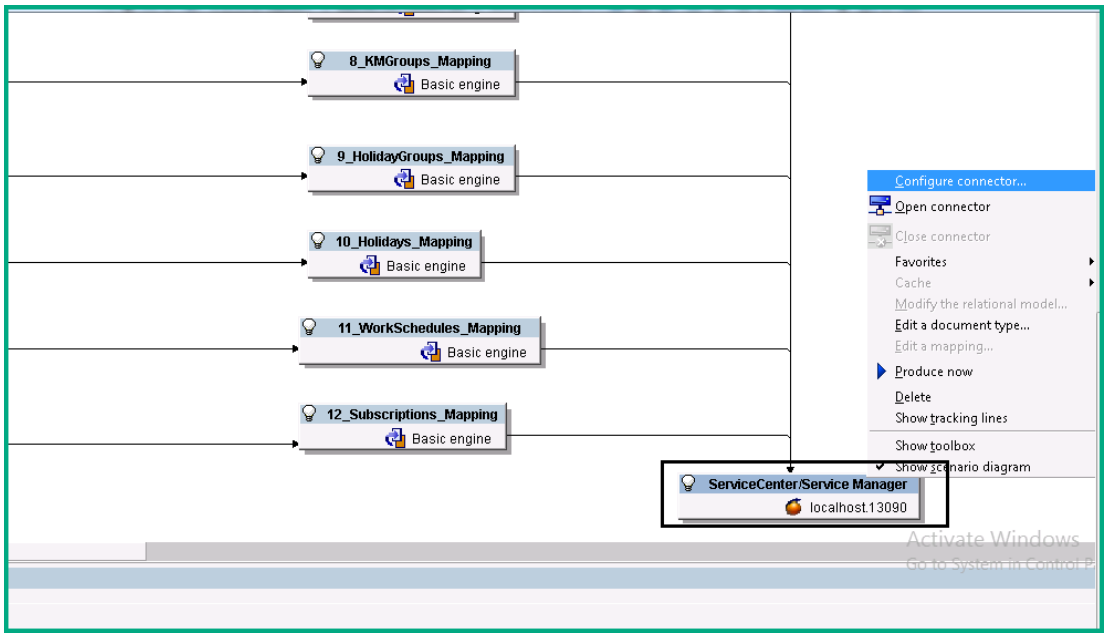
```
Dim path as String
Dim myValue as String
Dim total as Long
Dim iCounter As Integer, lSum As Long
path = ['Security Role(s)']

total=CountValues(path, "|", "")

For iCounter = 1 To total
myValue=GetListItem(path, "|", iCounter, "")
RetVal=PifSetStringVal("secRole.secRole(" & cstr(iCounter) & ").secRole", myValue)
Next
```

5. Click **OK**, and then save the scenario.
6. Repeat the same steps for the rest of the mappings in the scenario.

Task 3: Configure the destination connector

To do this, follow these steps:

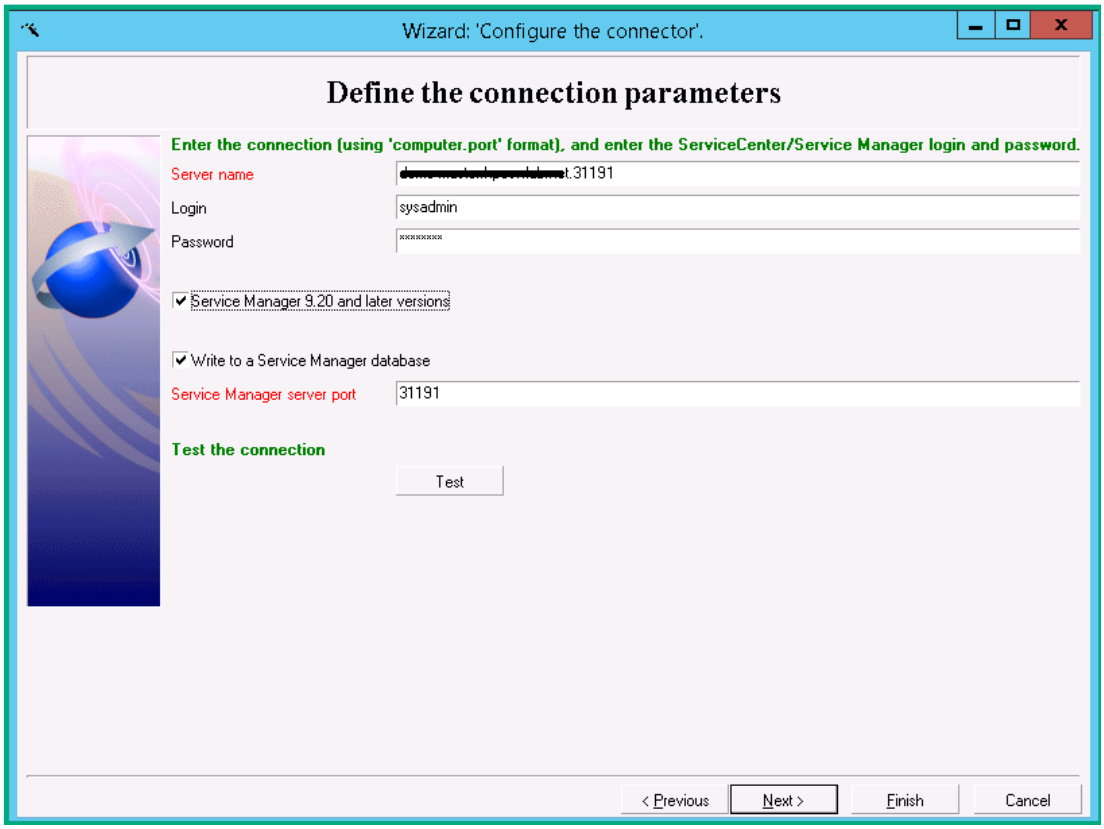
1. In the scenario diagram, right-click the **SericeCenter/Service Manager** connector, and then select **Configure connector**.



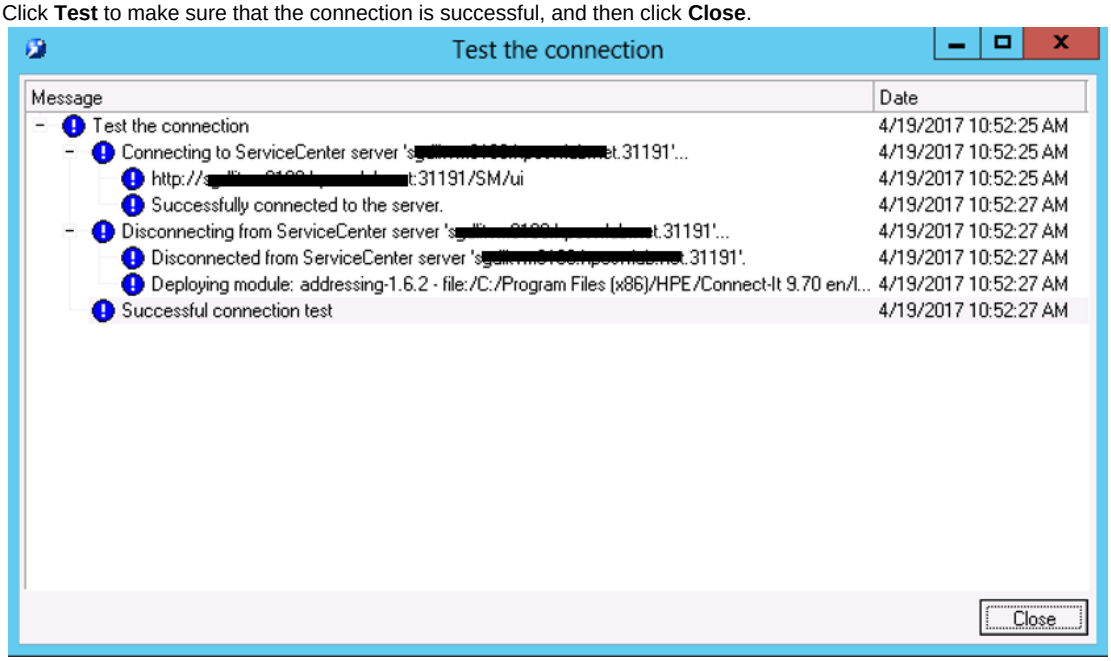
2. Click **Next** to display the **Define the connection parameters** page, and then enter the following information:
   - **Server name**: Enter a value with the following format: <*host FQDN*>.31191.
     Here, <*host FQDN*> is the fully qualified domain name or IP address of the ITSMA master node, and 31191 is the Service Management and Connect-It integration port.
   - **Login** and **Password**: Enter the user name and password of an ITSMA suite administrator user (for example, the **sysadmin** use r).
   - **Service Manager server port**: enter **31191**.

     > In ITSMA, this is the SM-CIT integration port instead of the SM RTE port. See also ITSMA node ports.

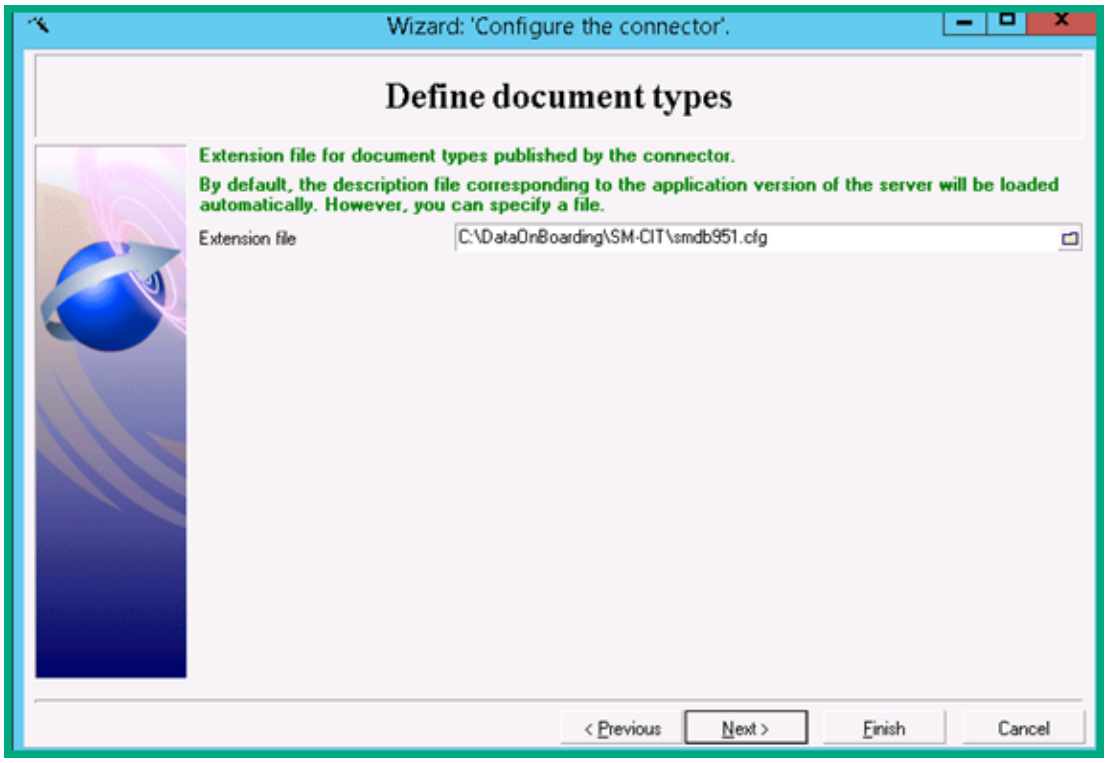
   - Make sure the following options are selected:
     - **Service Manager 9.20 and later versions**
     - **Write to a Service Manager database**



3. Click **Test** to make sure that the connection is successful, and then click **Close**.



4. Return to the wizard screen, and click **Next** repeatedly until the **Define document types** page is displayed. Select to the **smdb951.cfg** file located in the C:\DataOnBoarding\SM-CIT directory, and then click **Finish**.

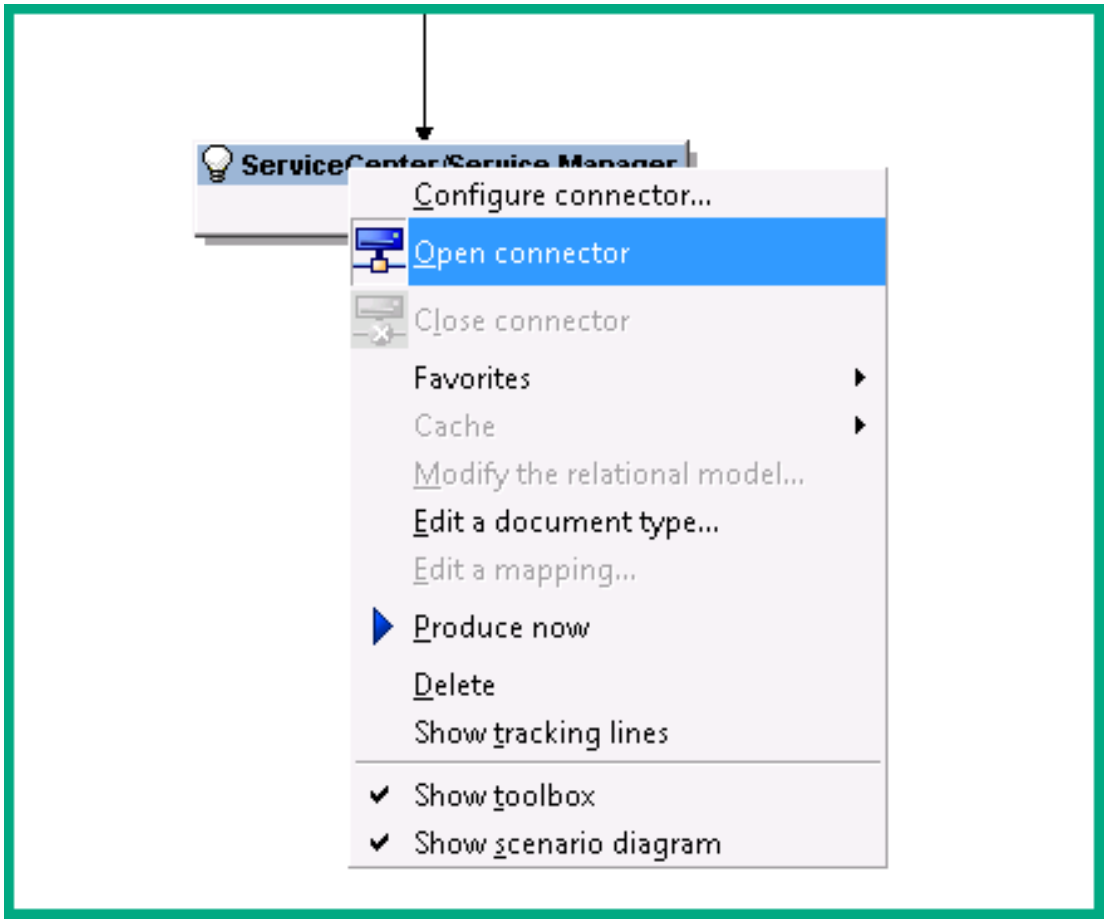


Task 4: Run the scenario

> Each CSV file is prefixed with a number. You must import the CSV files in ascending numerical order.

To do this, follow these steps:

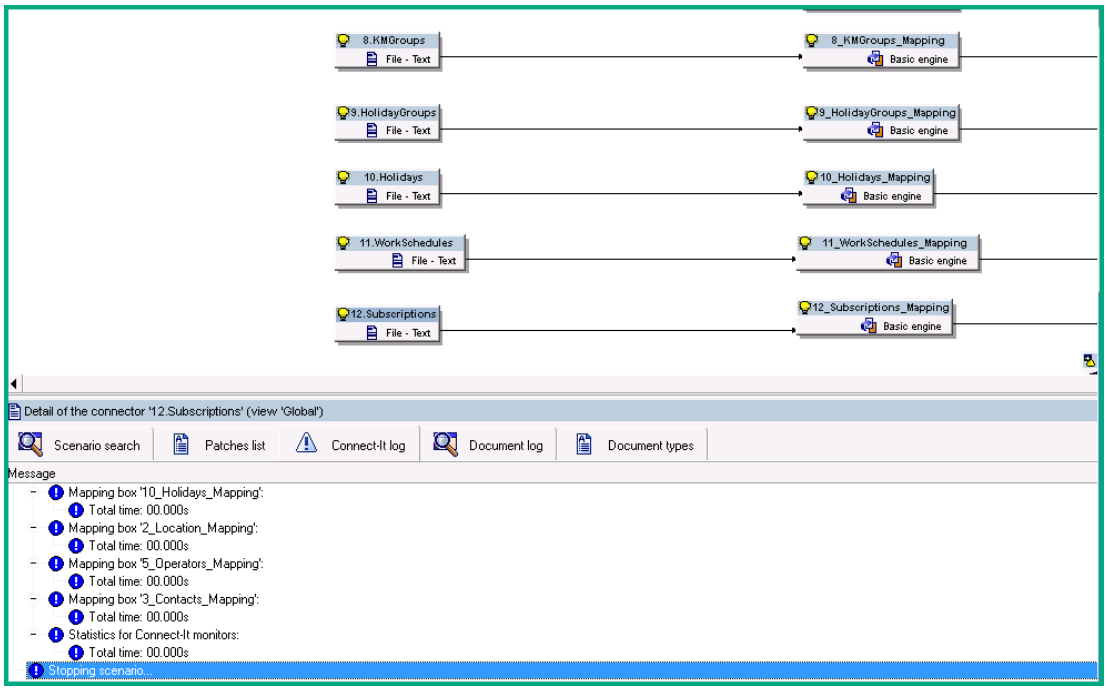
1. In the scenario diagram, right-click **Service Center/Service Manager**, and then select **Open connector**.



2. Right-click the Company source connector, and select **Produce now** to import the data.
3. Continue to produce data for the rest of the source connectors in the following order.

> To produce Subscription data, configuration items (CIs) must exist in your ITSMA system. If you have purged the out-of-box data from the system, be sure to create your own CIs in the system.

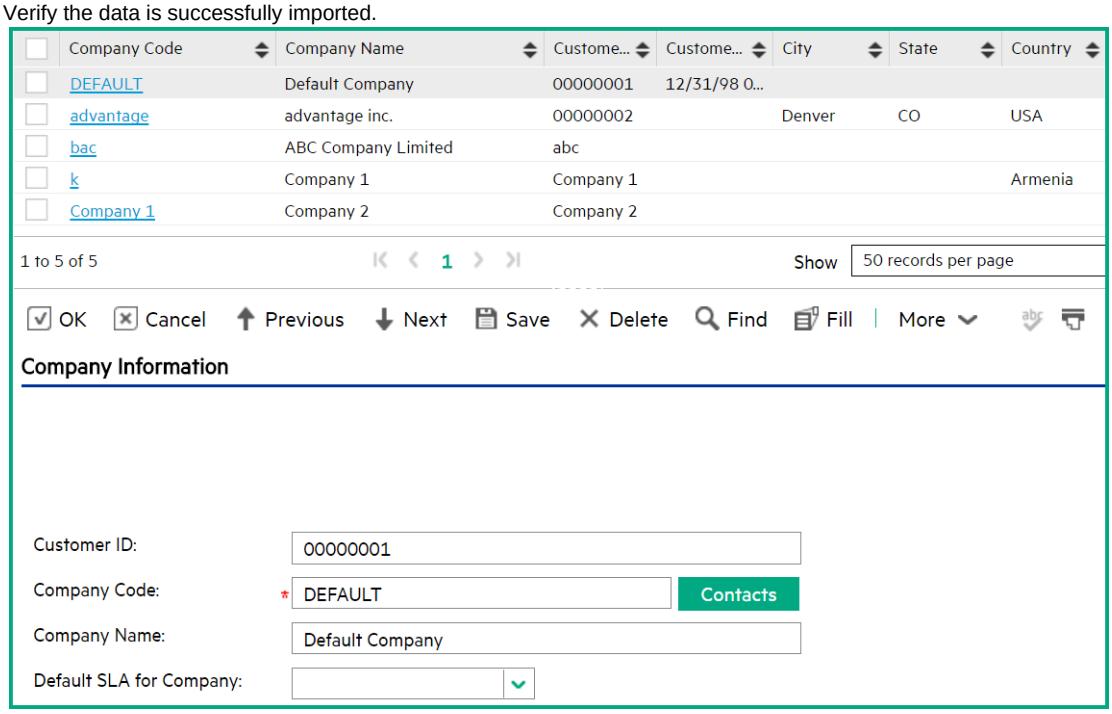
- 2.Location
- 3.Contacts
- 4.Departments
- 5.Operators
- 6.Vendors
- 7.Assignments
- 8.KMGroups
- 9.HolidayGroups
- 10.Holidays
- 11.WorkSchedules
- 12.Subscriptions

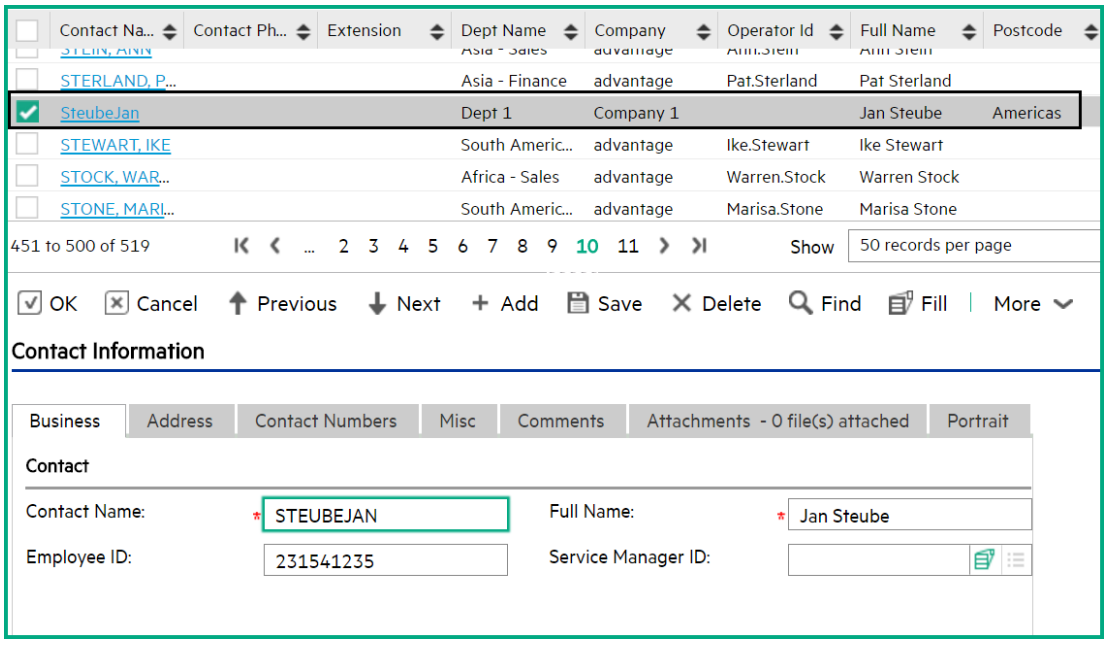


Step 3: Verify the imported data

After the data onboarding scenario is executed, follow these steps to verify the data is successfully imported into ITSMA:

1. Log in to ITSMA as **sysadmin**:
   https://*<EXTERNAL_ACCESS_HOST>*/main
2. Click **Service Management**.
3. Enter **db** in the command line, and then press Enter to open the Database Manager.
4. In the Table field, enter the name of a corresponding table. For example, enter **company** or **contacts**.
5. Verify the data is successfully imported.



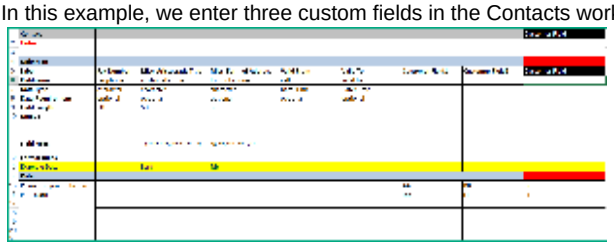


To troubleshoot any issues, see Troubleshoot data onboarding.

Extend the toolset to import more custom fields

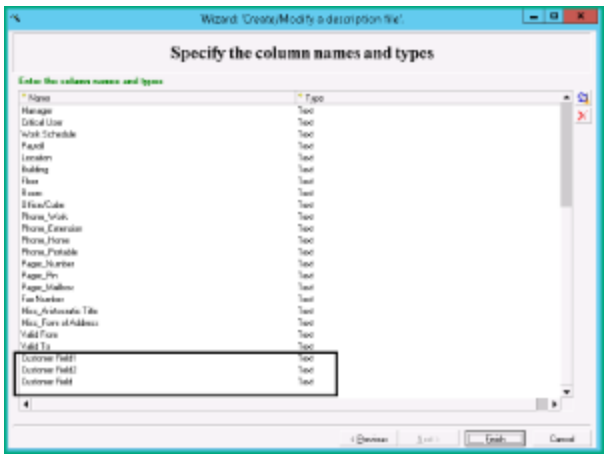
By default, the data onboarding Excel spreadsheet allows you to specify one custom field. If you have more than one custom field, follow these steps.

> The following steps use the Contacts worksheet as an example.

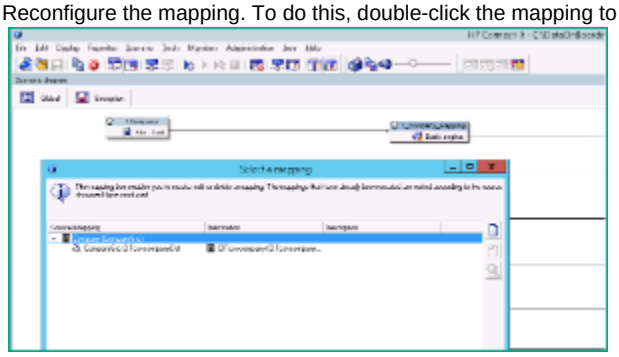
1. Enter your data, including the custom fields in the Excel spreadsheet. For instructions, see Understand the Excel spreadsheet.
   In this example, we enter three custom fields in the Contacts worksheet: Custom Field1, Custom Field2, and Custom Field.
   
2. Update the data onboarding macro according to your data entries. For instructions, see Understand the Excel spreadsheet.
   In this example, we update the code line for Contacts in the macro as follows:

   ```
   Call CreateITSMACSV(BRwin, 3, "3.Contacts", "B5:L5,B15:L999,N5:AN5,N15:AN999", "3_Contacts", "AJ:AK")
   ```

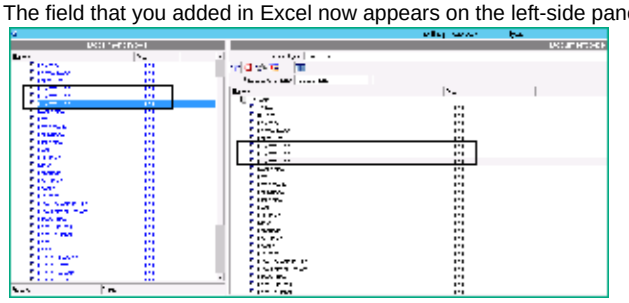
3. Run the data onboarding macro to export the data to CSV files. See Export the master data to CSV files.
4. Double-click the DataOnBoarding.scn file (located in the C:\DataOnBoarding\SM-CIT directory) to open the scenario in Connect-It.
5. Reconfigure the source connector. For detailed steps, see Export the master data to CSV files.
   In this example, right-click the Contacts connector and select **Configure connector**. Follow the configuration wizard to complete the configuration. Make sure the following page is displayed, which indicates the custom fields that you added are loaded into Connect-It.



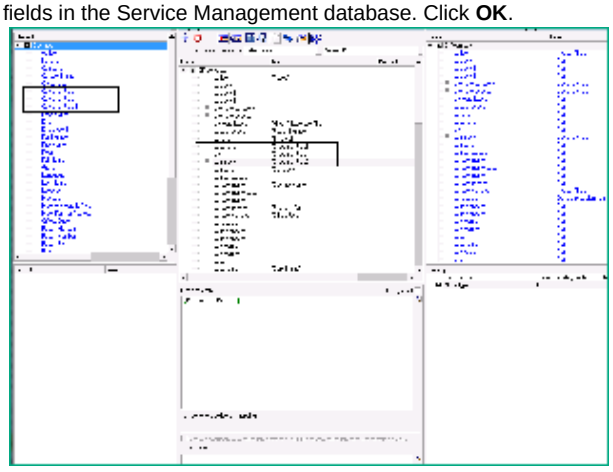
6. Reconfigure the mapping. To do this, double-click the mapping to open the following window, and then double-click the highlighted part.



The field that you added in Excel now appears on the left-side pane. Drag and drop the field to the right-side pane, and then click **OK**.



Double-click the Contacts mapping, and then drag and drop the custom fields to the middle pane to map them to their corresponding fields in the Service Management database. Click **OK**.



7. Run the data onboading scenario and verify the imported data. For details, see Import data from the CSV files into the ITSMA suite.

Troubleshoot data importing issues

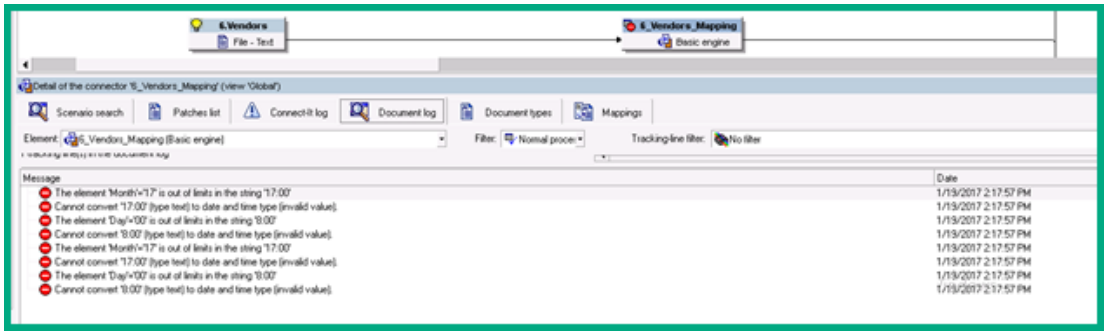
Troubleshoot Connect-It

You may encounter the following issues in Connect-It when you import data.

"The record being added contains a duplicate key" error

This error occurs when you re-run the data onboarding scenario in Connect-It to re-import Departments data.
To solve this issue, delete the imported data from the dept table in Service Management, and then re-import the departments data.

"Invalid value" error

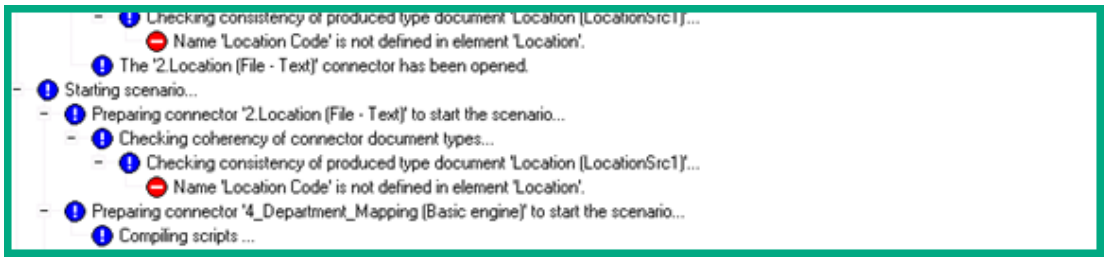


- *Root cause*: You have entered invalid values in the Excel spreadsheet.
- *Solution*: Check the relevant data entries in the Excel spreadsheet and correct mistakes.

"More columns found than expected" error

- *Root cause*: You have added one or more columns to the Excel spreadsheet and exported the data to CSV files, and then run the data onboarding scenario without reconfiguring the source connector and the mapping. The error occurs because the newly added data is not reloaded to the scenario.
- *Solution*: If you update a CSV file, you need to reconfigure the source connector and the mapping to reload the updated data, and then run the scenario again.

"Name is not defined in element" error



- Root cause: You have updated a column header in the Excel spreadsheet and exported the data to CSV files, and then run the data onboarding scenario without reconfiguring the source connector and the mapping. The error occurs because the newly added data is not reloaded to the scenario.
- Solution: If the update is correct, you need to reconfigure the source connector and the mapping to reload the updated data, and then run the scenario again. If the update is made by mistake, change the name back to the correct value and then run the scenario again.

Troubleshoot ITSMA

Follow these guidelines to troubleshoot problems that occur when you import master data into ITSMA.

Monitor the eventin queue

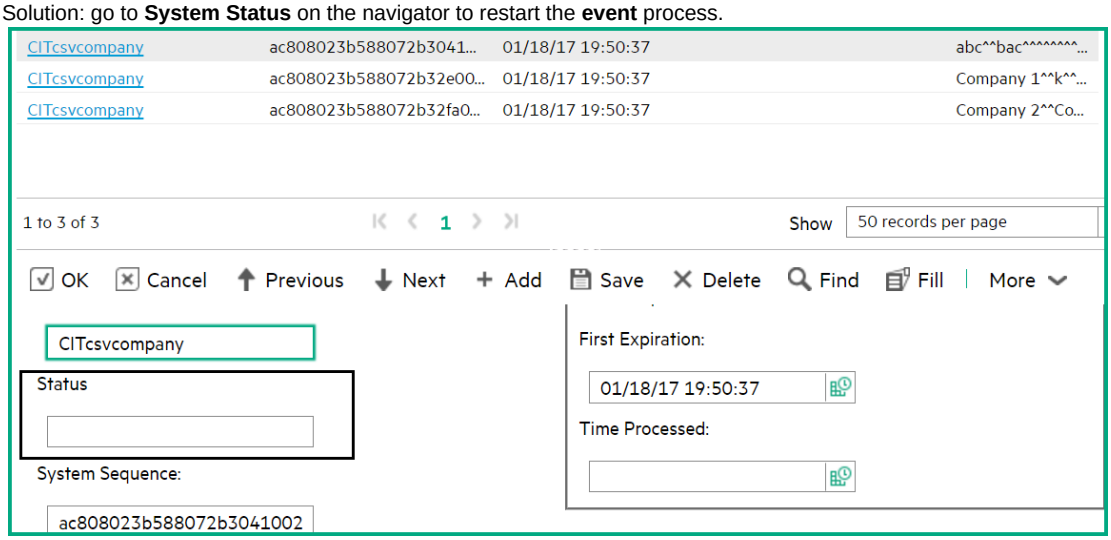
Once you have imported data into ITSMA by using the master data onboarding tool set, the system creates **eventin** records to insert the data into the database and executes the records based on a scheduler. You can use the **eventin** queue to monitor the status of the import: once the data is inserted into the Service Management database, the eventin records should disappear from the **eventin** queue.

To access the *eventin* queue, do the following:

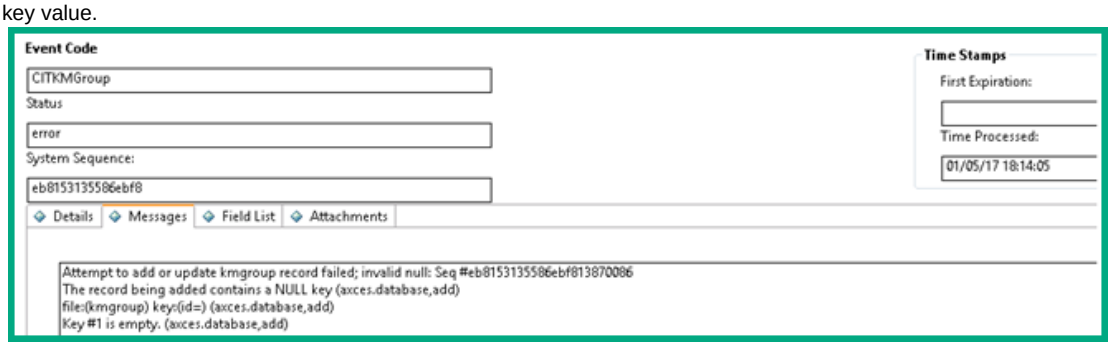
1. On the ITSMA suite landing page, click **Service Management**.
2. Type **db** in the command line box, and press Enter to open the Database Manager.
3. In the Table field, enter **eventin**, and then click **Search**.

If **eventin** records remain in the queue, try the following solutions, depending on the status of the record:

- If the Status field is empty: the record is not executed.
  Solution: go to **System Status** on the navigator to restart the **event** process.



- If the Status field is "error": errors occurred when the system attempted to insert the data into the database.
  Solution: debug the error according to the error messages. For example, the following figure shows an error caused by an empty primary key value.

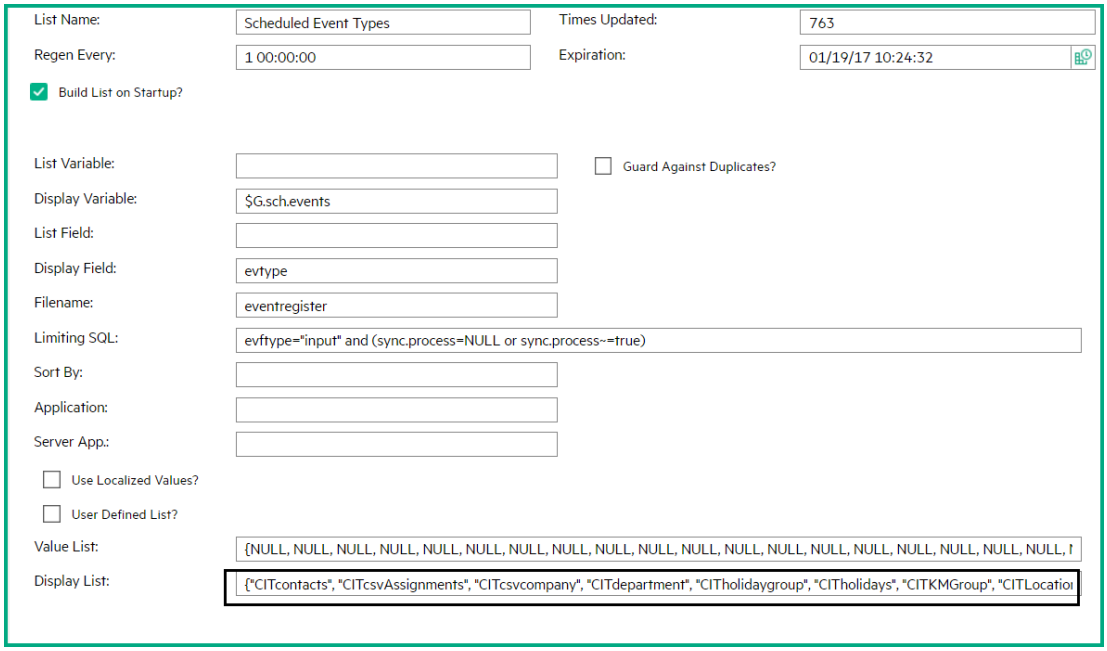


Check the Scheduled Event Types global list

To import data successfully, make sure the **Scheduled Event Types** global list contains the event registration. To do this, follow these steps:

1. On the ITSMA suite landing page, click **Service Management**.
2. Type **gl** in the command line, and then press Enter.
3. In the Name field, enter **Scheduled Event Types**.
4. Click **Search**.
5. Make sure that the Display List field contains the following values:

```
"CITcontacts", "CITcsvAssignments", "CITcsvcompany", "CITdepartment", "CITholidaygroup",
"CITholidays",
"CITKMGroup", "CITLocation", "CIToperator", "CITSubscriptions", "CITvendors", "CITWorkShedules"
```



6. Go to **System Status**, and then restart the **event** process.

Import user data into ITSMA

Import user data into Service Management

When LDAP users attempt to log in to ITSMA for the first time, ITSMA does not automatically synchronize the users to Service Management. You need to use the data onboarding toolset to import user data to Service Management first before LDAP users can log in to Service Management.

For details about how to import user data, see Use the data onboarding toolset to import master data.

> You can download this toolset from here. This toolset supports incremental data import. You can always run the toolset to import new user data.

Import user data into CMDB

Users from the LDAP server are created in CMDB on the fly when LDAP users perform the following tasks:

- Access Service Management and launch an embedded UCMDB Browser widget
- Access CMDB Browser
- Access CMDB

However, before these LDAP users can log in to UCMDB, you must configure additional necessary LDAP parameters in the UCMDB JMX Console in addition to the LDAP configuration in ITSMA. For more information, see Configure LDAP for CMDB.

> If you are using the internal LDAP server, users from the LDAP server are created in CMDB with the group named "itpeople" and a default role (that is, the **SuperAdmin** role inherited from "itpeople"). You must manually create other groups and roles in CMDB and create other user permissions. For more information, see the UCMDB Help Center.

User data onboarding in Service Portal

Service Portal uses the HPE Identity Manager (IdM) instance embedded in ITSMA for user authentication. The IdM roster loader runs periodically to load LDAP users to IdM; on the other hand, full and delta user synchronizations from IdM to the Service Portal frondend (which is based on HPE Service Anywhere) are executed to create Service Portal ESS users.

The process of end user self-registration in Service Portal is as follows:

1. The user logs in to Service Portal. The user is authenticated by the LDAP server.
2. At the backend, the user is loaded to IdM and is created as a Service Portal ESS user.

However, you need to manually configure LDAP groups in Service Portal. For details, see Configure LDAP for Service Portal.

Configure Email

User role: Suite Administrator

Follow the instructions in this topic to configure both outbound and inbound email for ITSMA.

Outbound email

The email service enables the system to send email notifications to any mail server that supports Simple Mail Transfer Protocol (SMTP). Configuring the email service is mandatory before you can use email related features such as the Service Management email notifications and survey.

To configure email service, follow these steps:

1. Log on to the ITSMA Suite Configuration user interface as the **sysadmin** user:
   https://<EXTERNAL_ACCESS_HOST>/itsmaconfig
2. Click **CONFIGURATION** > **Email Service**.

   > If you are using non-containerized Service Manager (mixed mode scenario 1), you will not see the **Email Service** menu item in the suite configuration interface. You need to configure email in your external Service Management system.

3. Configure your email service settings as described in the following table.

Setting	Description
SMTP Server Host	Specifies the name of the SMTP server host that is used for sending email notifications. The value for the parameter can be the IP address, machine name, or DNS name of the SMTP server .
SMTP Server Port	Specifies the communications port that the SMTP server uses.
User Name Password	Specifies the user name and password of an existing account that the ITSMA suite uses to bind to the SMTP server.
Mail From	Specifies the descriptive name or other identifier of the sender an e-mail. This parameter should be set in the format of email address.
Enable SSL&TLS	Select this option to enable SSL/TLS for SMTP operations. If th option is set to true, see Email with SSL certificate to configure SSL.

4. Click **Test** to make sure you can successfully connect to the SMTP server.
5. Click **Apply** to save your configuration. A dialog box that lists the items to be changed is displayed.
6. Review the listed items, and then click **Confirm**.

   > After your confirmation for applying the changes, the system restarts the related services.

Inbound email

The Smart Email solution offered by ITSMA can process inbound emails and automatically create requests in the containerized Service Management. ITSMA retrieves emails from an external mail server. By default, Smart Email is not enabled in ITSMA.

To enable Smart Email, follow these steps:

> *If the external mail server is using a secure protocol (IMAPS, POP3S, or HTTPS for EWS)*
>
> To enable Smart Email, you need to copy the certificate of the external mail server to a subfoler under the ITSMA global NFS share directory, and then restart the sm-rte-emailout pod. This is not needed if the external mail server is not using a secure protocol.

1. Configure SSL certificate. See Email with SSL certificate.

2. Set up Smart Email in Service Management. For details, see the Set up inbound email topic and related topics in the *Smart Email* section in the Service Management Help Center.

Configure SSL for outbound or inbound email

To configure SSL for outbound or inbound emal, follow these steps:

1. Upload the mail server's certificate (for example, smtp.cer) to the ***<ITSMA global NFS share directory>*/certificate/source** folder (see Set up three NFS shares for ITSMA).
   For example, upload the certificate to this folder: /var/vols/itom/itsma/itsma-itsma-global/certificate/source.
   The system automatically re-generates itsma-truststore.jks and itsma-cer.pem in the **ca-trust** folder (for example: **/var/vols/itom/itsma/itsma-itsma-global/certificate/ca-trust**).

   If the system fails to update itsma-cer.pem, you can import the certificate by using the following commands:

   ```
   cd /var/vols/itom/itsma/itsma-itsma-global/certificate
   export PATH=.:$PATH
   keytool -importcert -trustcacerts -alias <alias> -keystore
   ca-trust/itsma-truststore.jks -file source/<certificate_name>
   ```

2. Browse to a VM in cluster, and then restart the **sm-rte-emailout** pod. For example:

   ```
   kubectl get pod -n itsma1 | grep sm-rte-emailout
    itsma1      sm-rte-emailout-1377400934-5dvqr                2/2
     Running   0          21h
   kubectl delete pod sm-rte-emailout-1377400934-5dvqr -n itsma1
   ```

   The system will restart the following sm-rte-emailout in a few minutes.
3. Log in to the Service Management user inteface, and send an email for testing.

Replace the certificate for ITSMA

In a production environment, you are recommended to replace the out-of-box Nginx certificate for ITSMA with your own certificate that is signed by your corporate CA or a third-party CA.

To do this, follow these steps:

1. Prepare a certificate file (for example, tls.crt) and a private key file (for example, tls.key) in .pem format.
   The certificate's CN value must be the FQDN defined in the <EXTERNAL_ACCESS_HOST> parameter, and the certificate must be signed by your corporate root CA or a third-party root CA.
   The following figure shows the content of an example private key file (tls.key):

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAkyNty0/aMBlacHp5P44hkfZ68QFCrEYW+uB+bPAZmZQsu9Uu
3w6URSB/JyIAoIu5Q2S67PrebnhPARrwMM4REjzfEqz2vKMZWCtO9S0EsGPfT5mm
W7XfVZ/y54QoHfGsouP3NJLU58hoxid9EquXaswLKvD4jDlBMQlICPvAaJjy/uUo
bVw8Vu6c6WEJVj/0FiWk3ajamzW0kyOLrHfmRX0soFXHrHyYIZ61jwky3HUs+QbY
zJVPxV2OTJb2Ug0tGVRZn2KixUD5IX3XbT0Hh75Ae6Jx5ZMODFkhGfzoCJK6jLnQ
NemdMGSIdP9VhL8OfJRBc6IcLV3H7s1877XmIQIDAQABAoIBADSDaoYrg7Wy9sI6
E9gJBBYyIAKv7nnJsh3rzXNX5esYJTcMiOP3MhfR10/CJPMnqwFQjB5UEtreeWPt
l1fz08fsjbj+njkJBNyg6Fc8r/W8T1D7h5InwQOwSGM0mZTGUlT4g5vx46atsic2
pL7rGul01W+H/U0eihPUOi9qmms50C1vX5cGOxD/N9P33mV0IHqjTjpocvO6Z+mc
SLDCf2tBykYjxUiHTokQoqRdpcmk/kGtuQDlE2fKDPgrqypr2rRGadIw4cU68ahf
sJfcJOYC0CCMRkUUTMCDFoHAxbSIgYDMH2is0FcvHXhzzlrM2CFAxCUYvM1GAJML
UDS4K1kCgYEA1PxjucEVyy0a7N1IK+0bZpo2XbvKebqFM5mCeCfxCkFSBRsYH7A3
KEIrc2gCq8YrFv780jE9GDjomfpxCpR5aILjDesCifzrI04Yk9xteivXqwolMtF2
+dPnJKHPhQ+MB/InUygxvN4KINlxASs+XAdzm0Ca/CWmQG5dtb6L9zsCgYEAsNqm
PVRH0fI5VZuhlX0UHT9NdbHfohXNB68i7DE+0YinVvpk3fC0/0SnxmYm927H6K35
ApKFrbi+47RFzK2WKdkVnuD6mD66lXSkZ7XiQnNkOqbfsoKPEUGpnmDZy7j5f27t
ooq6VrOBbUgkaxYc9RxPrMSKduNqPQsb7UeeWlMCgYAaJ6RXe06h1LgpvkLOoh9r
SiTC/fyvVihlXcSX3M/M4pif5+PegFVFrFqJoYwya/N+r3F8nm9SOirWPdsD4ZfH
LcuUOffl2hlGDKEYB0mqZxfk+Sn4Q6DIrS0FYpmJTY90qlgJ7jWta9bykcE+04Ck
7IVV22ks7bKs1uDLIMsvYQKBgCkV0pLi1oB+jjVGH4az9Q1KXHtgJDzqZaRIWouW
cSqKXZ3GM9KfjdzTnUppBtpqoQR8DiI72dRe2/HYOnLvTLhSF0S+rVjbEcuQunTh
ezvGxN0fUU6OKCBxKa+CfnZmdYfWRFyDcACeWQ4DOXqrO3Tx68yOKECwWkjuIMHB
5pbDAoGBAL/4O2fd5Cupo2uGchDgTJKCw9x6siRQit99dz+/C7I6cL95pa4irQiw
1wogzD8RMxD+vgNfIMNRAsMSV9e6B5klF4vbdHtVEnQvvDWmBkkeQiWOI8CoMPr7
kplYcynicmXC1EA8rlbew4j0thRel/Y5IieNF5DNXNMQON9GbY2V
-----END RSA PRIVATE KEY-----
```

The following figure shows the content of an example certificate file (tls.crt):

2. Download the tls.crt and tls.key files to a temporary directory on the master node, and then use the following commands to encode the certificate (tls.crt) and the private key (tls.key):
   # base64 -w 0 tls.crt > tls_base64.crt
   # base64 -w 0 tls.key > tls_base64.key
   The content of your **tls_base64.crt** should resemble the following:

   The content of your **tls_base64.key** should resemble the following:

3. Go to /var/vols/itom/core/suite-install/itsma/output/itom-ingress-x.x.x.xxx/yamls, and then edit the secret.yaml file as follows:
    a. Replace the tls.crt:"xx…xxx" part with the content of the tls_base64.crt file.
    b. Replace the tls.key:"xx…xxx" part with the content of the tls_base64.key file.
    See the following figure for an example.

```
apiVersion: v1
kind: Secret
metadata:
  name: nginx-itsma-secret
  namespace: itsma1
data:
  tls.crt: "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUVlRENDQW1BQ0NRREkra0o1RWNDdWpEQU5CZ2txaGtpRzl3MEJBU
XNGQURDQmlURUxNQWtHQTFVRUJoTUMKVlZNeEN6QUpCZ05WQkFnVEFrTkJNUkl3RUFZRFZRUUhFd2xUWVc0Z1JHbGxaMjh4RFRBTEJnTl
ZCQW9UQkVoUQpVMWN4RERBS0JnTlZCQXNUQTBKVVR6RWNNQm9HQTFVRUF4TVRjM1Z5ZG1WeUxtaHdaWE4zYkdGaUxtNWxkREVlCk1Cd0d
DU3FHU0liM0RRRUpBUllQZFhObGNrQmtiMjFoYVc0dVkyOXRNQjRYRFRFM01EY3hNVEE1TlRnek0xb1gKRFRjd01EY3hNREE1TlRnek0x
b3djakVMTUFrR0ExVUVCaE1DV2tneEN6QUpCZ05WQkFnVEFsTklNUXN3Q1FZRApWUVFIRXdKVFNERU5NQXNHQTFVRUNoTUVTRkJUVnpFT
U1Bb0dBMVVFQ3hNRFFsU1BNU3d3S2dZRFZRUURFeU56CmFHTXRhWFJ6YldFdGMzVnBkR1V0WTJRdE1UUXhMbWh3WlhOM2JHRmlMbTVsZE
RDQ0FTSXdEUVlKS29aSWh2Y04KQVFFQkJRQURnZ0VQQURDQ0FRb0NnZ0VCQUpNamJjdFAyakFaV25CNmVUK09JWkgyZXZFQlFxeEdGdnJ
nZm16dwpHWm1VTEx2Vkx0OE9sRVVnZnljaUFLQ0x1VU5rdXV6NjNtNTRUd0VhOERET0VSSTgzeEtzOXJ5akdWZ3JUdlV0CkJMQmozMCta
cGx1MTMxV2Y4dWVFS0IzeHJLTGo5elNTMU9mSWFNWW5mUktybDJyTUN5cncrSXc1UVRFSlNBajcKd0dpWTh2N2xLRzFjUEZidW5PbGhDV
lkvOUJZbHBOMm8ycHMxdEpNamk2eDM1a1Y5TEtCVng2eDhtQ0dldFk4SgpNdHgxTFBrRzJNeVZUOFZkamt5VzlsSU5MUmxVV1o5aW9zVk
ErU0Y5MTIwOUI0ZStRSHVpY2VXVERneFpJUm44CjZBaVN1b3k1MERYcG5UQmtpSFQvVllTL0RueVVRWE9pSEMxZHgrN05mTysxNWlFQ0F
3RUFBVEFOQmdrcWhraUcKOXcwQkFRc0ZBQU9DQWdFQVFpMnVtRGtBcjlMNWVvbzJUdk5tbmJGR1pvM1VEY2YyWVp1eGVSdm5nS08wYnk1
cwpKOWF3UEZHRFhhQU5KZlFiMDgwL1VOTml6TkQ5eXY4eW5vcUhNUzRZeWdWbUFETnZsTVl1WDh0ZVdEZVJqS1hmCjFHaXJZRVltbHdRU
25PZWJwS0pReWticW1BNjlNM21rSGJjOS9NeE1kT2ZGeUpGNENLZ1QrbHZtNXhMdzdaMm8KMGFrbFZ6WVV1NnF3Z1prWHZHMmFtVnJJeT
JmblpkTmdiU2E5NkVNam5ybFQ5TkIwMWwwN1FwQ0RxU1dNc0FLdgpPQkh1L3laSnRQSFVKQlRaMWo0RHpjdDQxc09JM0luazdYQkZmZWN
CakE3b09pQTdTRW5jYjNHY3k2WkZWUHlaCmlHWjJaZ1pMbTJRb0NxOEFFNTVHZHE3UkpFTGhHZGMrb0hYRWl6L0dtcEhjbDB4NnJWRTNB
ejNPMUxaNDRQRVcKVjZ3MEFwVDR5bklGVUZrUVMyU0tvbTFEd1kwaHRhNTZHRDRqUGc3YlRXK31IQkllMVlmSjVTMmFUODA5UVJqWApIS
0doTkdJdTZpbXMvZ2o4TGxKd1YvbHlMSy9oN3FxUkExYitNTzZuTkh4UHZiTHM4Vi95NCtMTXE2NHN6N2syCkpmandRdFUrMXppM3NwUH
FLd3ZqRFJZWm9mdlJ1Qmt6czBiNUI1MU53RnpVdUZpSEFrQThaN01lYUnpUeWM3MGgKV0VWSWZ5dTZVKzJERHRaT0tVL09IYk5PbnpOVTZ
jQWZPRVRIWFZoeWZjeWtHVU00dWk3S1dtZ2FOZkNYaGZtSwprbUJnaGxFaTdPNmNzbjZRSEdOdFMvbVUyNTZ5NHVTOEN3Wi9FMkJBS0or
WnNwejVOOFkzV1ZmVDFNQT0KLS0tLS1FTkQgQ0VSVElGSUNBVEUtLS0tLQo="
  tls.key: "LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFb3dJQkFBS0NBUUVBa3lOdHkwL2FNQmxhY0hwNVA0NGhrZ
lo2OFFGQ3JFWVcrdUIrYlBBWm1aUXN1OVV1CjN3N1VSU0IvSnlJQW9JdTVRMlM2N1ByZWJuaFBBUnJ3TUO0UkVqemZFcXoydktNWldDdE
85UzBFc0dQZlQ1bW0KVzdYZlZaL3k1NFFvSGZHc291UDNOSkxVNThob3hpZDlFcXVYYXN3TEt2RDRqRGxCTVFsSUNQdkFhSmp5L3VVbwp
iVnc4VnU2YzZXRUpWai8wRmlXazNhamFtelcwa3lPTHJIZm1SWDBzb0ZYSHJIeVlJWjYxandreTNIVXMrUWJZCnpKVlB4VjJPVEpiMlVn
MHRHVlJabjJLaXhVRDVJWDNYY1QwSGg3NUFlNkp4NVpNT0RGa2hHZnpvQ0pLNmpMblEKTmVtZE1HU0lkUDlWaEw4T2ZKUkJjNkljTFYzS
DdzMTg3N1htSVFJREFRQUJBb01CQURTRGFvWXJnN1d5OXNJNgpFOWdKQkJeU1BS3Y3bm5Kc2gzcnpYTlg1ZXNZS1RjTW1PUDNNaGZSMT
AvQ0pQTW5xd0ZRakI1VUV0cmV1V1B0CmwxZnowOGZzamJqK25qa0pCTnlnNkZjOHIvVzhUMUQ3aDVJbndRT3dTR00wbVpUR1VsVDRnNXZ
4NDZhdHNpYzIKcEw3ckd1bDAxVytIL1UwZWloUFVPaTlxbW1zNTBDMXZYNWNHT3hEL045UDMzbVYwSUhxalRqcG9jdk82WittYwpTTERD
ZjJ0QnlrWWp4VWlIVG9rUW9xUmRwY21rL2tHdHVRRGxFMmZLRFBncnF5cHIyclJHYWRJdzRjVTY4YWhmCnNKZmNKT1lDMENDTVJrVVVUT
UNERm9IQXhiU0lnWURNSDJpczBGY3ZIWGh6emxyTTJDRkF4Q1VZdk0xR0FKTUwKVURTNEtsa0NnWUVBMVB4anVjRVZ5eTBhN04xSUsrMG
JacG8yWGJ2S2VicUZNNW1DZUNmeENrRlNCUnNZSDdBMwpLRUlyYzJnQ3E4WXJGdjc4MGpFOUdEam9tZnB4Q3BSNWFJTGpEZXNDaWZ6ckk
wNFlrOXh0ZWl2WHF3b2xNdEYyCitkUG5KS0hQaFErTUIvSW5VeWd4dk40S0lObHBU3MrWEFkem0wQ2EvQ1dtUUc1ZHRiNkw5enNDZ1lF
QXNOcW0KUFZSSDBmSTVWWnVobFgwVUhUOU5kYkhmb2hYTkI2OGk3REUrMFlpblZ2cGszZkMwLzBTbnhtWW05MjdINkszNQpBcEtGcmJpK
zQ3UkZ6SzJXS2RrVm51RDZtRDY2bFhTa1o3WG1Rbk5rT3FiZnNvS1BFVUdwbm1EWnk3ajVmMjd0Cm9vcTZWck9CY1Vna2F4WWM5UnhQck
1TS2R1TnFQUXNiN1VlZVdsTUNnWUFhSjZSWGUwNmgxTGdwdmtMT29oOXIKU2lUQy9meXZWaWhsWGNTWDNNL000cGlmNStQZWdGVkZyRnF
Kb1l3eWEvTityM0Y4bm05U09pcldQZHNENFpmSApMY3VVT2ZmbDJobEdES0VZQjBtcVp4ZmsrU240UTZESXJTMEZZcG1KVFk5MHFsZ0o3
ald0YTlieWtjRSswNENrCjdJV1YyMmtzN2JLczF1RExJTXN2WVFLQmdDa1YwcExpMW9CK2pqVkdINGF6OVExS1hIdGdKRHpxWmFSSVdvd
VcKY1NxS1haM0dNOUtmamR6VG5VcHBCdHBxb1FSOERpSTcyZFJlMi9IWU9uTHZUTGhTRjBTK3JWamJFY3VRdW5UaAplenZHeE4wZlVVNk
9LQ0J4S2ErQ2ZuWm1kWWZXUkZ5RGNBQ2VXUTRET1hxck8zVHg2OHlPS0VDd1dranVJTUhCCjVwYkRBb0dCQUwvNE8yZmQ1Q3VwbzJ1R2N
oRGdUSktDdzl4NnNpUlFpdDk5ZHorL0M3STZjTDk1cGE0aXJRaXcKMXdvZ3pEOFJNeEQrdmdOZklNTlJBc01TVjllNkI1a2xGNHZiZEh0
VkVuUXZ2RFdtQmtrZVFpV09JOENvTVByNwprcGxZY3luaWNtWEMxRUE4cmxiZXc0ajB0aFJlbC9ZNUlpZU5GNUROWE5NUU9OOUdiWTJWC
i0tLS0tRU5EIFJTQSBQUklWQVRFIEtFWS0tLS0tCg=="
```

4. Re-generate the secret:
   # kubectl delete -f secret.yaml
   # kubectl create -f secret.yaml
5. Re-start the Nginx:
   # kubectl delete -f itom-nginx-ingress-deployment.yaml
   # kubectl create -f itom-nginx-ingress-deployment.yaml

Configure SAML SSO

ITSMA NG Express 2017.07 supports Single Sign-On (SSO) based on the SAML 2.0 protocol. Using the HPE Identity Manager (IdM) instance that comes with ITSMA and an external Identity Provider (IdP), this solution enables SSO between ITSMA and other HPE applications (for example, other containerized HPE ITOM suites).

Currently, the SAML SSO solution supports only Microsoft Active Directory Federation Services (ADFS) 2.0 or 3.0 as the IdP. ADFS helps you use single sign-on (SSO) to authenticate users to multiple, related web applications over the life of a single online session. Once ADFS is installed and configured to authenticate users from an LDAP directory, you are ready to add the IdM metadata to ADFS as a trusted relying party.

> The screenshots in this section are from ADFS 3.0, and may slightly differ from those in ADFS 2.0.

> **Prerequisite**
> ITSMA must use an LDAP connection for SAML SSO, and ITSMA and the IdP (currently, ADFS only) must connect to the same LDAP server.

To configure SAML SSO for ITSMA, perform the following steps.

Step 1: Export the public key portion of the ADFS federation service certificate

SAML SSO requires two-way SSL between ITSMA and ADFS. This step will export the public key from the ADFS certificate. In a later step, you will upload this key into ITSMA so that the ITSMA IdM can decrypt SAML responses from ADFS.

1. From your operating system, start Active Directory Federation Services.
2. Right-click **Federation Service**, and then click **Properties**.
3. On the **General** tab, under **Communicating certificate**, click **View**.
4. In the **Certificate** dialog box, select the **Details** tab.
5. On the **Details** tab, click **Copy to File**.
6. Click **Next**.
7. On the **Export Private Key** page, make sure that **No, do not export the private key** is selected, and then click **Next**.
8. On the **Export File Format** page, select **DER encoded binary X.509 (.CER)**, and then click **Next**.
9. On the **File to Export** page, specify the certificate file in **File name**, and then click **Next**.

Step 2: Upload the ADFS communication public key to ITSMA

You need to upload the ADFS communication public key that you exported previously to the following directory in the ITSMA installation:

{itsma_global_volume}/certificate/idm

Where: {itsma_global_volume} is the global NFS share directory that you configured for the suite installation. This directory is used to store global data of ITSMA. For more information, see Set up three NFS shares for ITSMA.

For example, copy the ADFS public key to the following folder:
/var/vols/itom/itsma/itsma-itsma-global/certificate/idm/

Step 3: Enable SAML 2.0 in ITSMA

> Before you proceed, make sure that LDAP settings are correctly configured in ITSMA (see Configure an external LDAP server). This is a prerequisite for configuring SAML SSO for ITSMA.

1. Launch the **Suite Configuration** utility as the sysadmin user:
   https:<EXTERNAL_ACCESS_HOST>/itsmaconfig
2. Navigate to **Configuration** > **Accounts** > **LDAP & SAML**.
3. Switch on the **Enable SAML 2.0** button on the upper right corner.
4. Specify a value for **IDP Metadata URL**. This value must use this format: https://<ADFS host>/federationmetadata/2007-06/federationmetadata.xml.
5. Click **Test** to make sure the URL is correct.
6. Click **Apply**.

Step 4: Download the IdM metadata of ITSMA

> Make sure that you have already enabled SAML in ITSMA, otherwise the IdM metadata is not available to download.

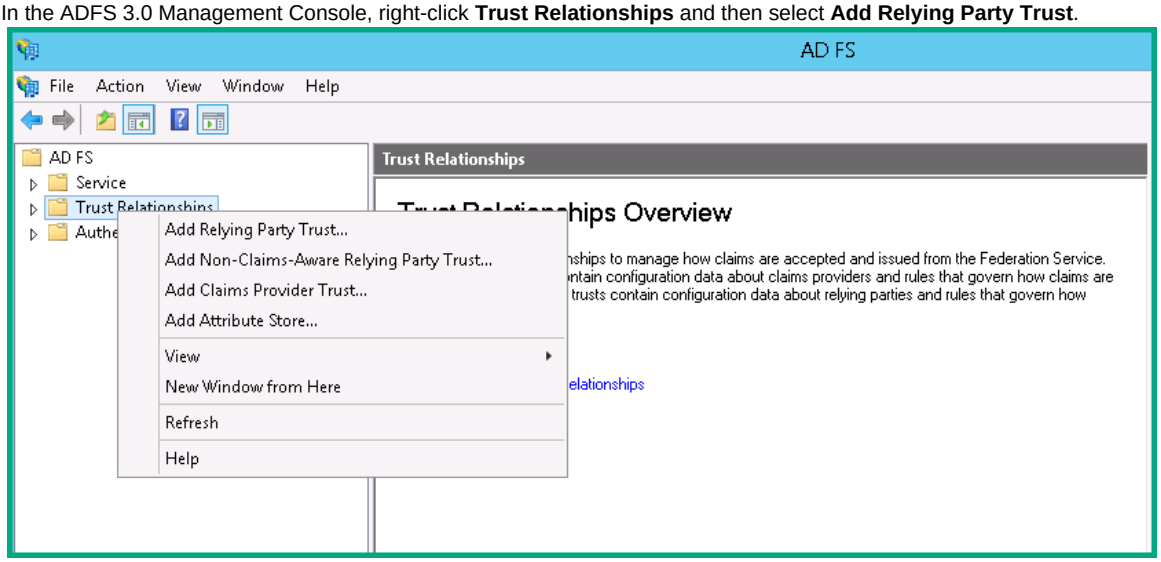
Download the suite's IdM metadata using the following URL: https://<EXTERNAL_ACCESS_HOST>/idm-service/saml/metadata.

The metadata is downloaded as an XML file (for example, spring_saml_metadata.xml).

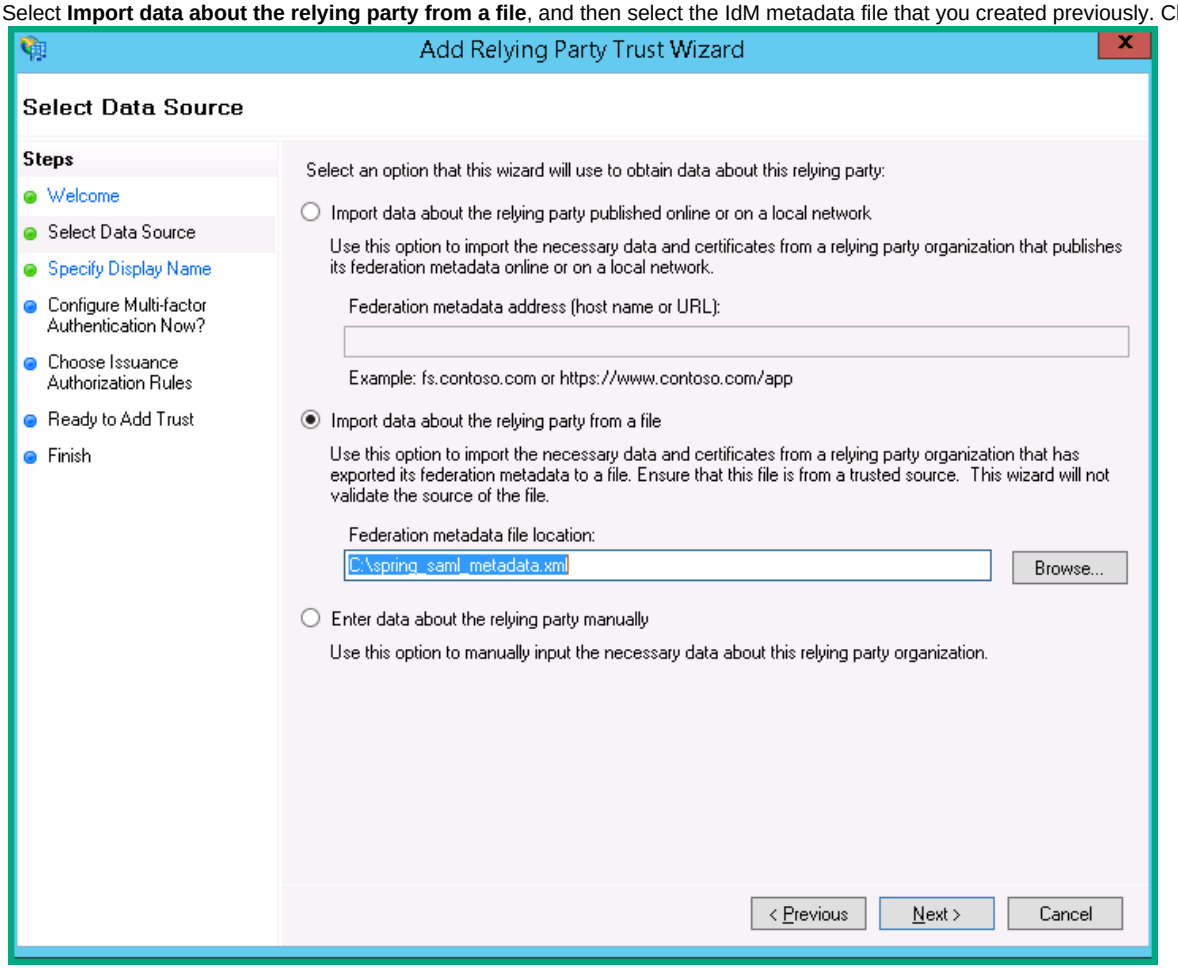
Step 5: Add the metadata file as a new relying party trust in ADFS

This step will add the metadata file that you have downloaded in the previous step as a new relying party trust in ADFS.

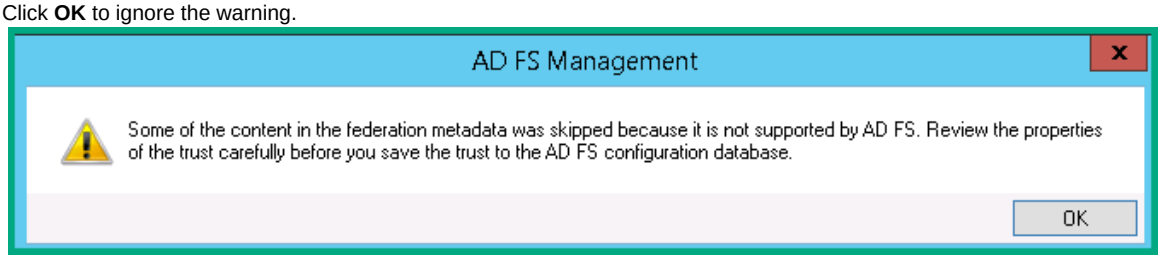
1. In the ADFS 3.0 Management Console, right-click **Trust Relationships** and then select **Add Relying Party Trust**.



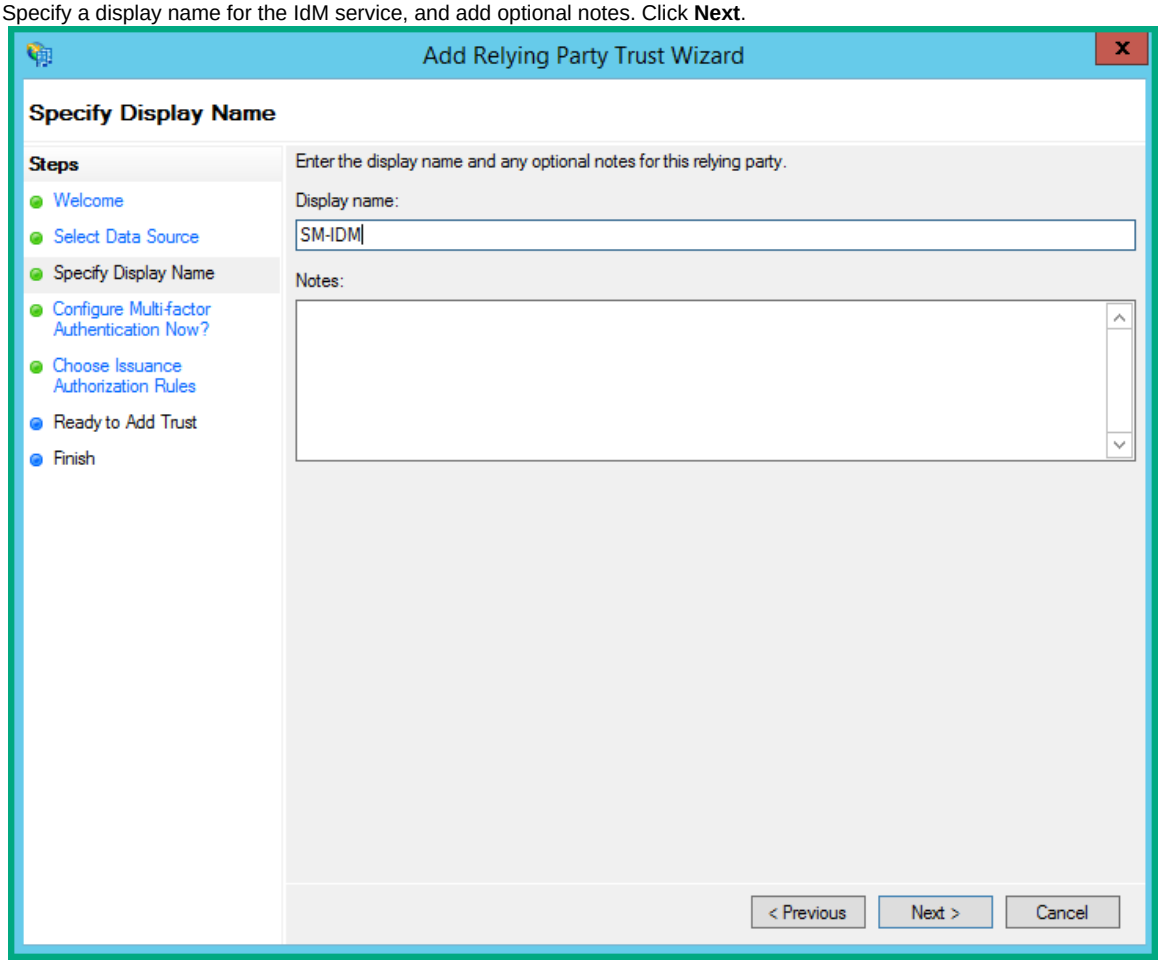
2. Select **Import data about the relying party from a file**, and then select the IdM metadata file that you created previously. Click **Next**.



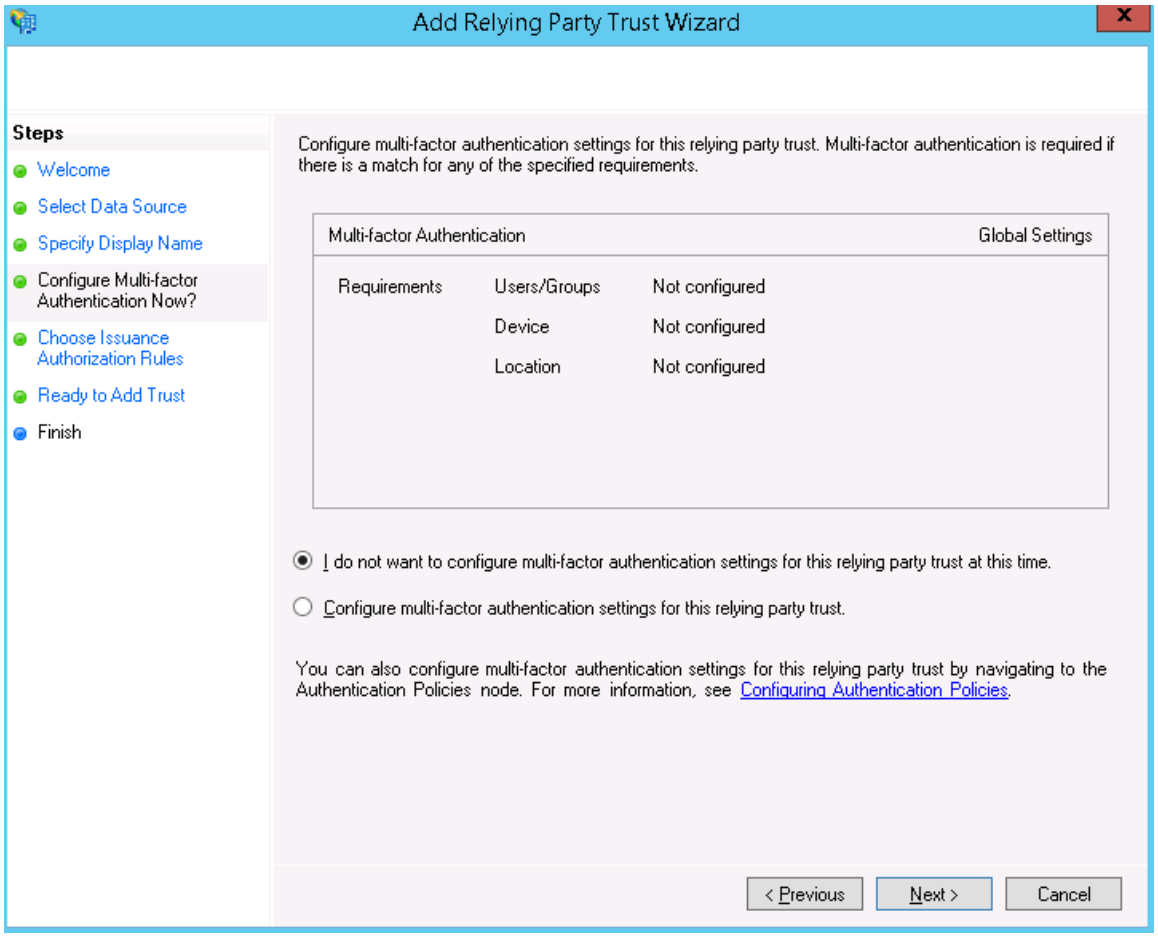
3. The wizard may display a warning, indicating that some content of the metadata is not supported. You can safely ignore this warning. Click **OK** to ignore the warning.



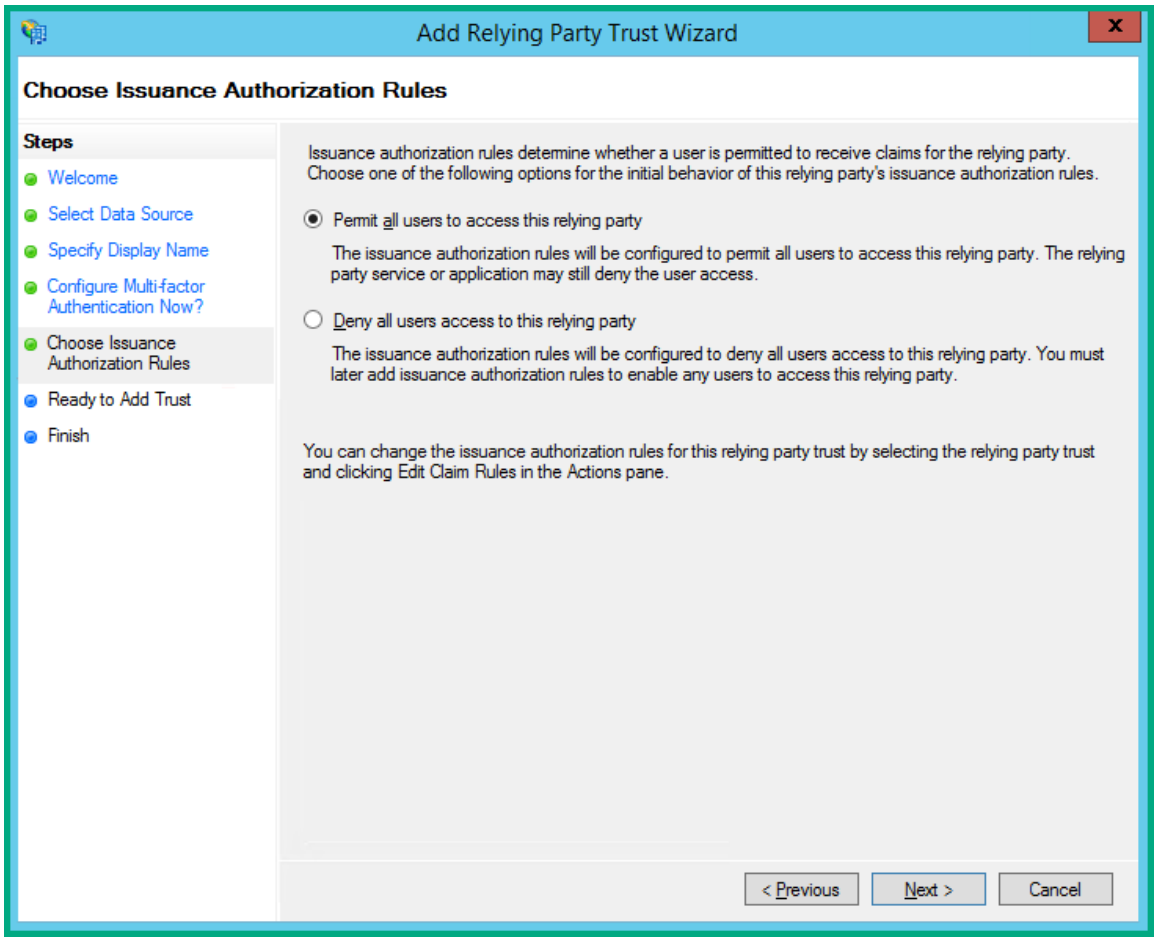
4. Specify a display name for the IdM service, and add optional notes. Click **Next**.



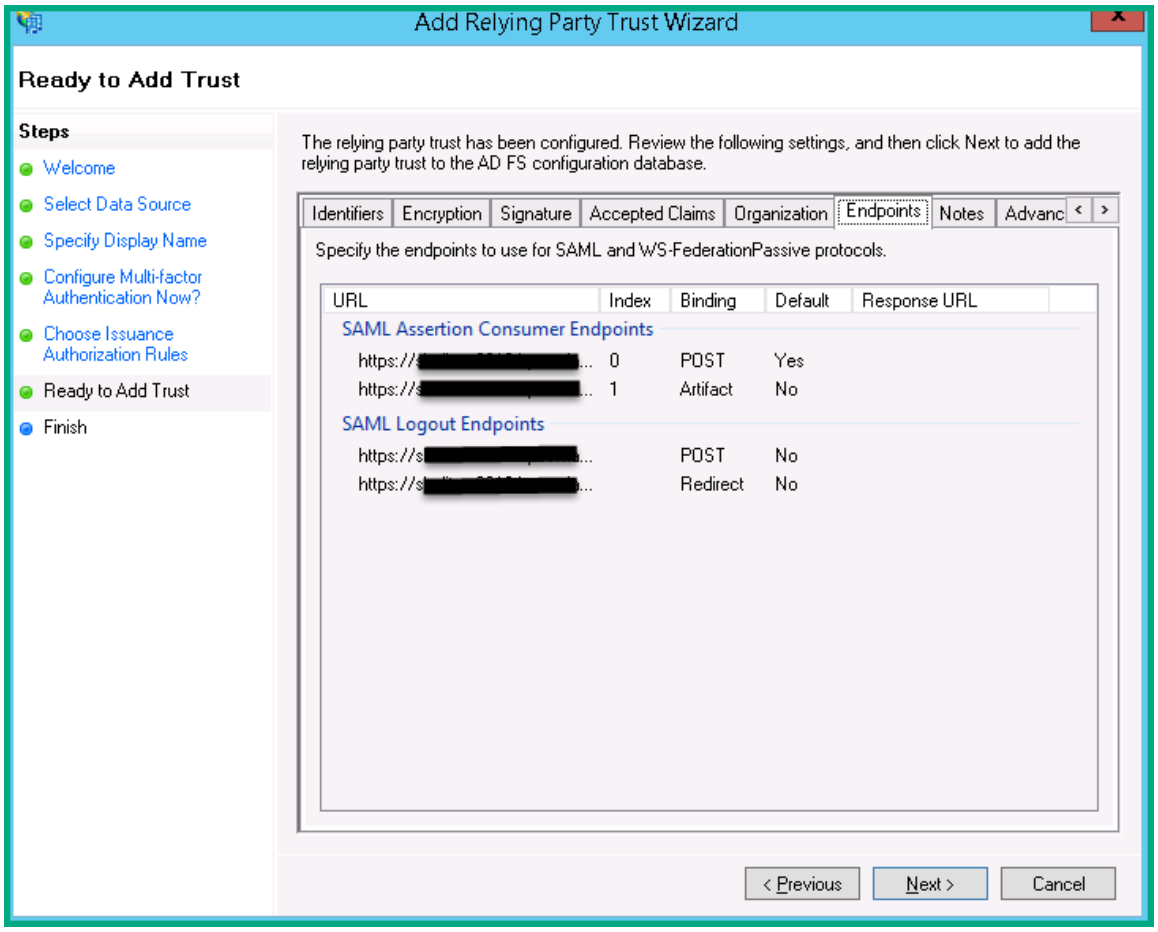
5. Make sure that the **I do not want to configure multi-factor authentication setting for this relying party trust at this time** option is selected, and then click **Next**.



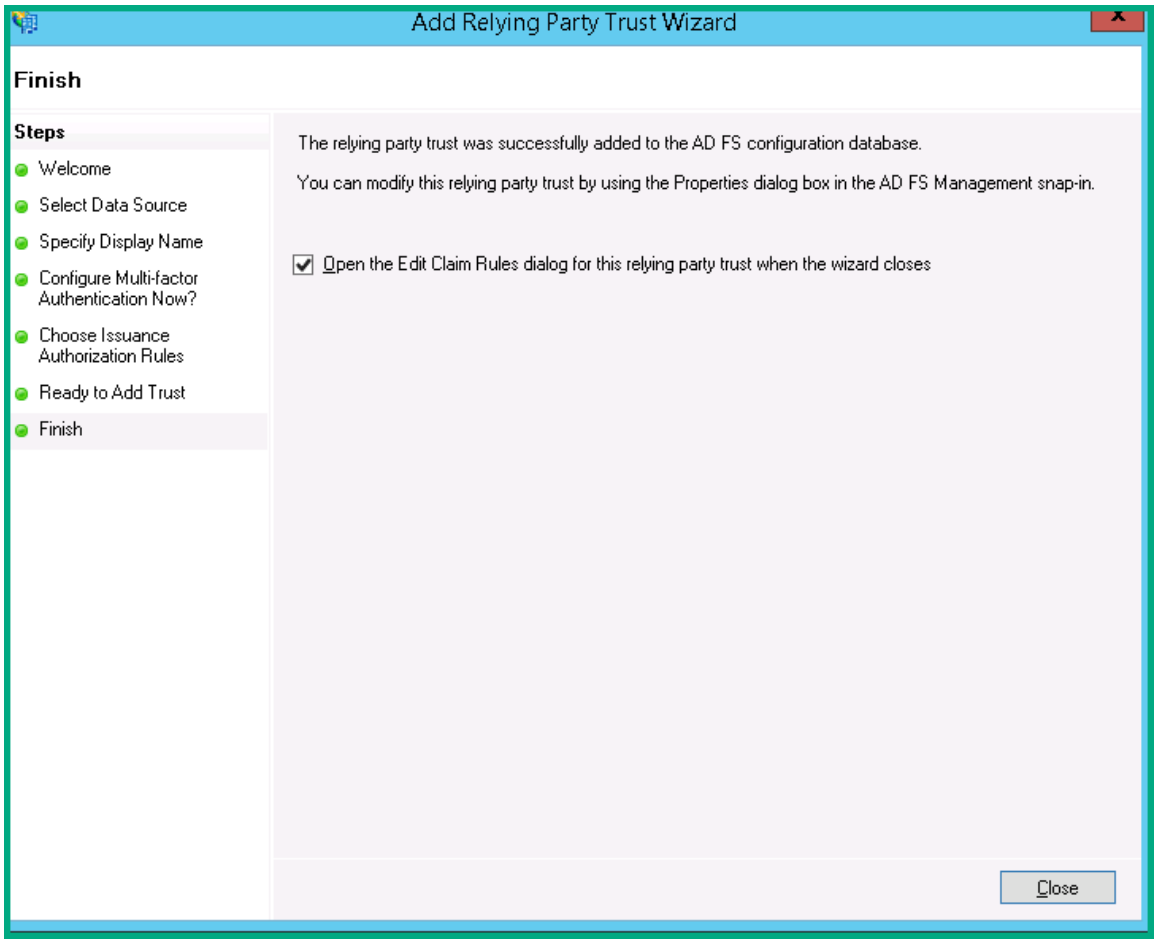
6. Select the **Permit all users to access this relying party** issuance authorization rule.



7. You are now in the Ready to Add Trust step. Check that the **Endpoints** tab contains multiple endpoint values. If not, verify that your metadata was generated with https protocol URLs.

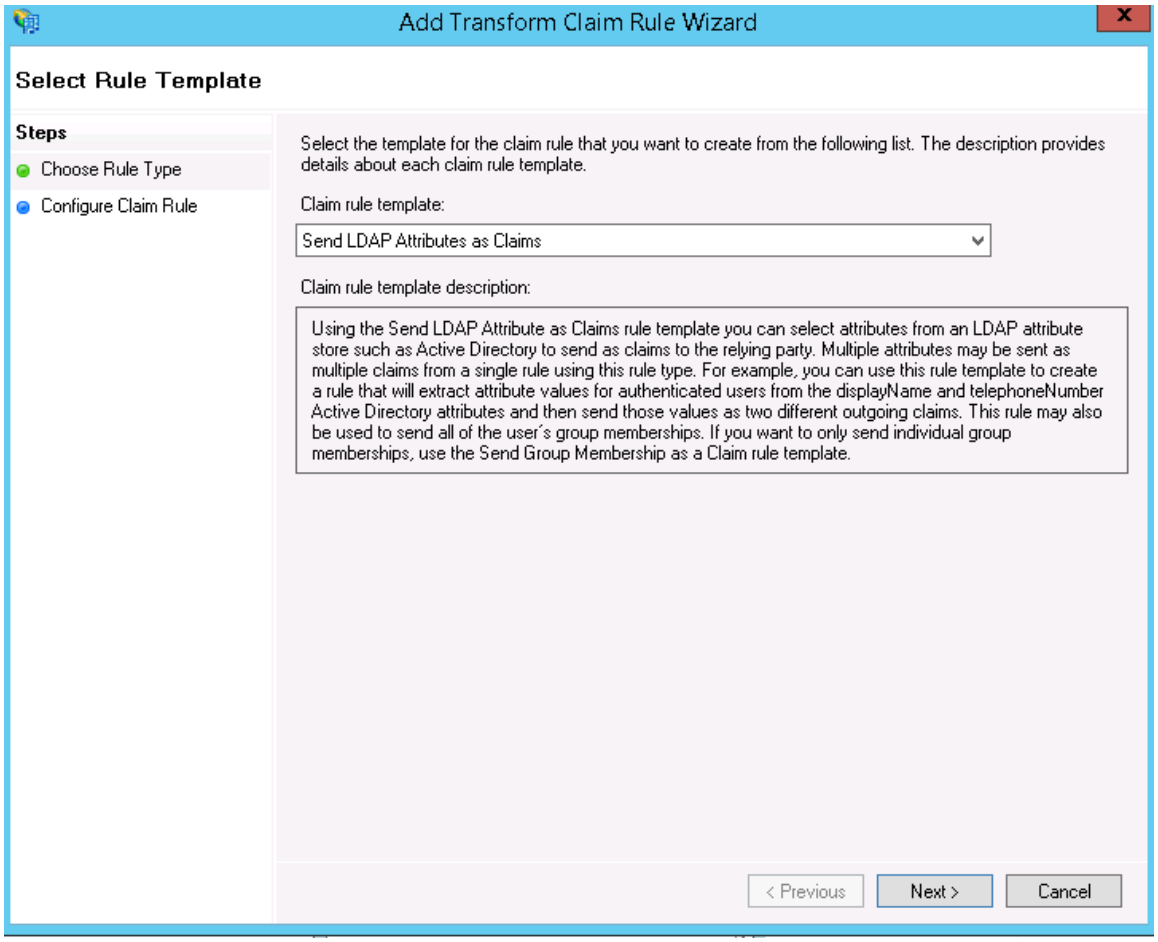


8. Leave the **Open the Edit Claim Rules dialog** checkbox selected, and then click **Close** to close the wizard.

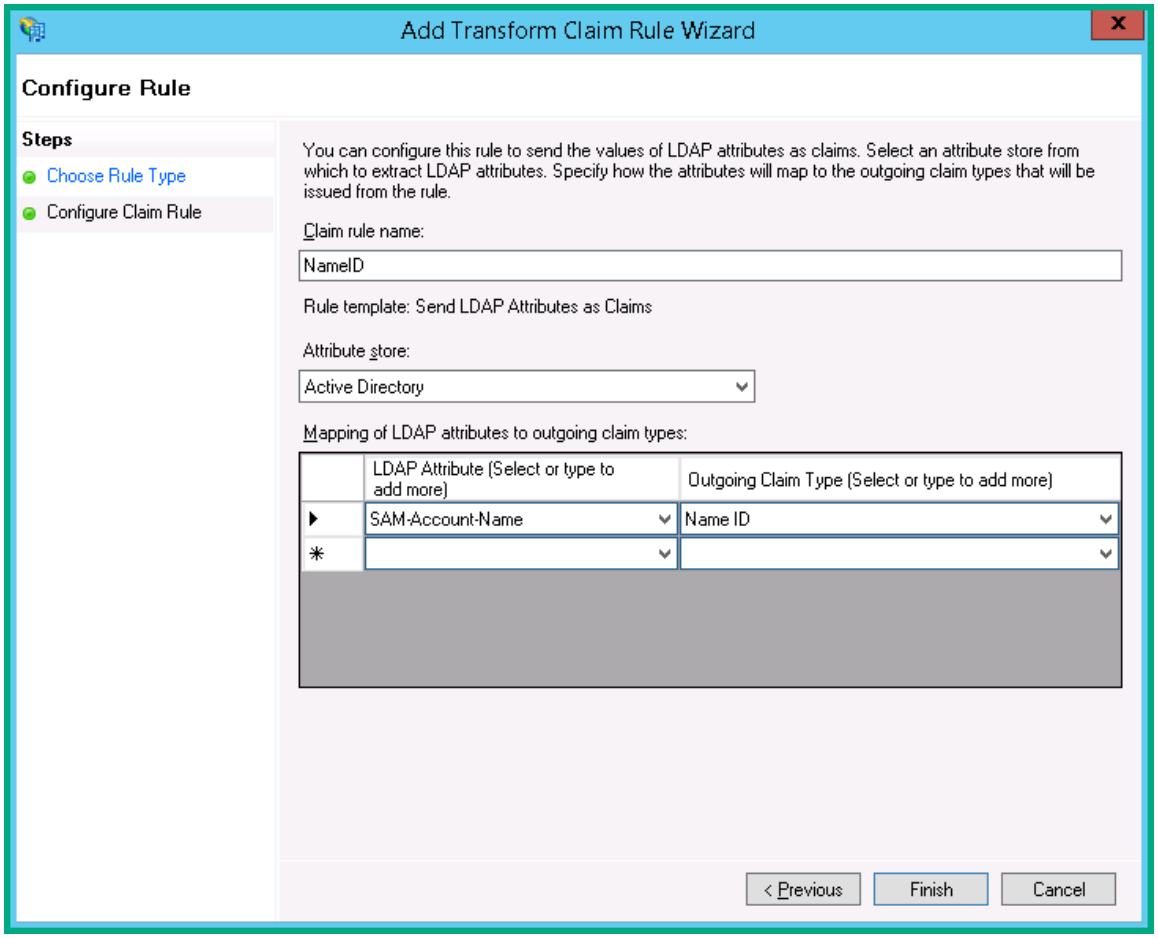


The Add Transform Claim Rule wizard opens.

9. Continue to configure the NameID element as part of the Subject in the SAML Response message as follows:
    a. Select **Add Rule**, and then select **Send LDAP Attributes as Claims**. Click **Next**.



b. Specify the following fields to configure the claim rule:
   - Claim rule name: enter **NameID**
   - Attribute store: select **Active Directory**
   - LDAP Attribute: select **SAM-Account-Name**
   - Outgoing claim type: select **Name ID**



c. Close the wizard and the **Apply the claim rules** window.

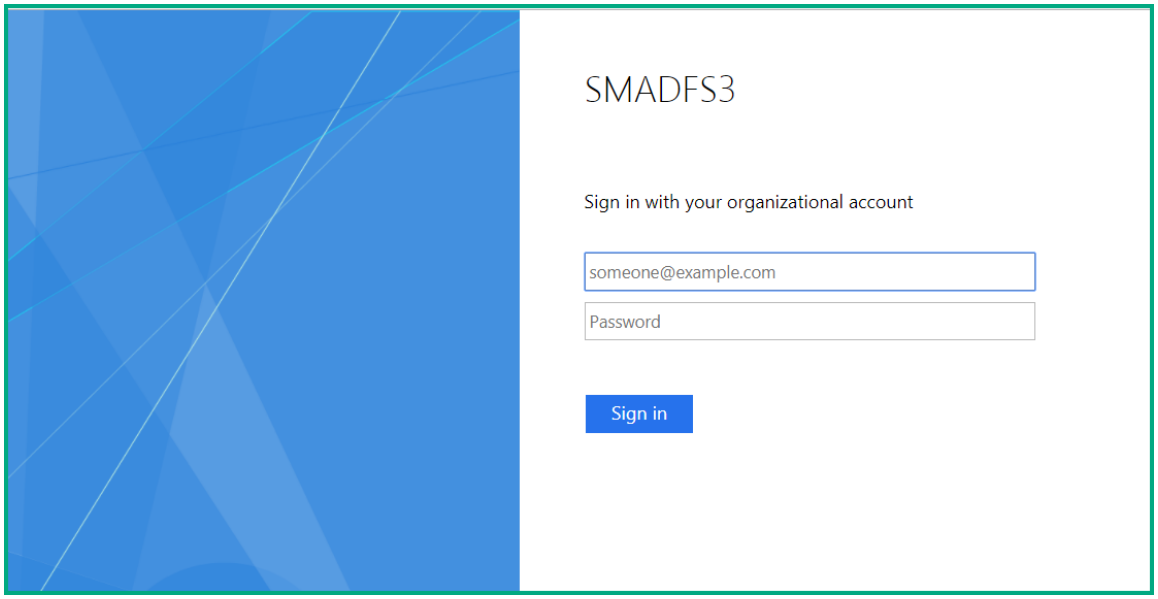
> In ADFS 3.0, you may need to configure the Name ID as a PassThrough claim.

Step 6: Verify SAML SSO

1. Launch one of the following ITSMA login URLs from your browser:
   https://<EXTERNAL_ACCESS_HOST>/main (for non-ESS users)
   https://<EXTERNAL_ACCESS_HOST>/saw/ess (for ESS users)

   > **Login URL for sysadmin**
   > The **sysadmin** user is a seeded user, which is stored in the suite's IdM database instead of the LDAP server and hence cannot be authenticated by ADFS. If SAML SSO is enabled, the **sysadmin** user can only use the following login URL:
   > https://<EXTERNAL_ACCESS_HOST>/itsmaconfiglogin.

2. Check that you are directed to an ADFS login page, as shown in the following example figure:



3. Enter your LDAP user name and password to log in.

Configure the Service Portal mobile app

ITSMA Service Portal provides a mobility solution that is based on a native Android mobile app published on Google Play and HPE Marketplace. Before end users can use the mobile app to do their daily work, the suite administrator must set up the mobility solution.

Prerequisites

- An access server is already set up if your organization is using a DMZ network. For details, see (Optional) Set up Access Server for a DMZ network.
- The ITSMA suite is already installed. For details, see Install the ITSMA suite (on-premises).

Once the prerequisites are met during the suite installation. After the suite installation, the suite administrator can perform the following tasks to set up the mobile app so that end users can use the mobile app in their daily work.

- Replace the out-of-box ITSMA Nginx certificate
- Enable ITSMA suite mobile notifications

Replace the out-of-box ITSMA Nginx certificate

The out-of-box Nginx certificate in ITSMA is signed by a private CA. You may want to replace the certificate with your own one, which is signed by your corporate root CA or a third-party root CA. For more information about how to replace the out-of-box Nginx certificate for ITSMA, see Replace the certificate for ITSMA.

> If you do not do this or if your corporate root CA is a private CA, when users attempt to log in to ITSMA using the mobile app, the HTTPS connections are considered "untrusted" by Android and thus blocked. If this is the case, users need to import the private root CA certificate to their mobile device by following Google's instructions: https://support.google.com/nexus/answer/2844832.

Enable ITSMA suite mobile notifications

If your organization is using a proxy server to access the Internet, you can follow the instructions below to enable the ITSMA suite to send notifications to Google Play. These notifications are then sent to user's Smartphones when connected to Google Play.

> If your organization is not using a proxy server to access the Internet, this task is not needed.

Before you proceed, make sure that the mobile app is working correctly.

> You can repeat the following procedure if the proxy settings are changed.

1. Log in to the ITSMA suite master node.
2. Run the following command:

```
kubectl get deployment  itom-xservices-platform  -n `kubectl get namespaces
-o=custom-columns=NAME:.metadata.name --no-headers |grep itsma` -o yaml
>/tmp/itom-xservices-platform.yaml
```

3. Edit the /tmp/itom-xservices-platform.yaml file as follows:
    a. Modify the section from

    - name: GCM_PROXY_HOST

    - name: GCM_PROXY_PORT

    to

    - name: GCM_PROXY_HOST

      value: '<proxy server address>'

    - name: GCM_PROXY_PORT

      value: '<proxy server port number>'

    For example:

    - name: GCM_PROXY_HOST

      value: 'proxy.yourcompany.com'

    - name: GCM_PROXY_PORT

      value: '8080'

    > - Use the Spacebar key instead of the Tab key to align the first letter of 'value' to the first letter of 'name' on the line above.
    > - Remember to put the proxy server address and port number within single quotation mark.

    b. Remove the whole line starting with 'pod.alpha.kubernetes.io/init-containers'.
    c. Remove the whole line starting with 'pod.beta.kubernetes.io/init-containers'.
    d. Save the file.
4. Run the following command to apply the changes.

```
kubectl replace --force -f /tmp/itom-xservices-platform.yaml
```

> This stops ITSMA services for several minutes. We recommend that you make such changes during non-business hours.

5. Wait for the changes to be applied. Run the following command to verify if the suite is up and running:

```
kubectl get pods   -n `kubectl get namespaces -o=custom-columns=NAME:.metadata.name --no-headers
|grep itsma` |grep xservices
```

   All items should be Running.
6. Run the following command and check if the proxy host and port are configured correctly:

```
kubectl get deployment  itom-xservices-platform  -n `kubectl get namespaces
-o=custom-columns=NAME:.metadata.name --no-headers |grep itsma` -o yaml
```

Configure log level for debugging

User role: Suite Administrator

The suite administrator can configure the debugging log level for the following components or features of the suite:

- Service Management
- CMDB
- Smart Analytics
- Service Portal
- IDM
- Chat

> - The log level for Service Management and CMDB can only be configured on the suite configuration page when you install

ITSMA in full containerized mode.
- After your confirmation for applying the changes, the system restarts the related services.
- Once debugging is enabled, additional logging information is written to the suite logs, which you can download from ITOM Container Deployment Foundation (CDF).

Configure the Service Management log level

To configure the debugging log level, follow these steps:

1. On the suite landing page, click **Suite Configuration**.
2. Click **CONFIGURATION** > **Debug** > **Log Level**.
3. Click the **Service Management** tab.
4. In the **Server** section, update the parameters by selecting a value in the drop-down list, and then click the **Update** button. Or, you can directly modify the parameter values in the text area.

   SM server log level parameters

   Some values are available for quick selection in the the drop-down list. If you wan to specify other possible values that are not in the drop-down list, you can directly modify the values in the text box.

Parameter name	Default value	Possible values	Description
sqllimit	10	Number of seconds For example: 1, 2, 3, 4, 5, 10, 20, 30, 60	This parameter defines the time limit for requests to the RDBMS. If a particular request exceeds the time limit defined by this parameter, the ITSMA Service Management server writes a message to the server log file documenting the name of the user making the request, how long it took, and the actual SQL query.
debugdbquery	5	Number of seconds or 999 for a full query debug. For example: 1, 2, 3, 4, 5, 10, 20, 999	This parameter causes the Service Management server to record database queries, timings, and results information that exceed the time threshold you specify in this parameter value in the log file.
cache_clean_interval	3600	1800, 2700, 3600	This parameter defines the interval the Service Management server waits before clearing the cache of infrequently used entries.

webservices_sessiontimeout	1800	15, 30, 60, 120, 300, 600, 900, 1800, 3600	This parameter defines the number of seconds that the server waits for a WebService API client request before the server assumes that the client session has timed out and closes the connection. If a Service Management connection is kept alive, a value that is 30 seconds shorter than the value of the connectionTimeout parameter is automatically applied for the timeout limit of the web service session. Otherwise, the value set in the webservices_sessiontimeout parameter is applied. If a Service Management connection is kept alive, the minimum timeout limit (15 seconds) is then applied for the web service session when the timeout limit for the Service Management connection is less than 45 seconds.
connectionTimeout	180000	45000, 60000, 90000, 180000	This parameter defines the number of milliseconds that the server waits for a Service Management client request before the server assumes that the client connection has timed out and closes the connection. • The timeout limit for the connectionTimeout parameter should be longer than that for the webservices_sessiontimeout parameter. Otherwise, the client session could not be reused. It is recommended that you set the connectionTimeout parameter to a value of no less than 60000 milliseconds. • A value that is 30 seconds shorter than the value of the connectionTimeout parameter is automatically applied for the timeout limit of a web service if the Service Management connection is kept alive.
smartemailTimeout	45000	30000, 45000, 60000, 90000, 180000	This parameter defines the number of milliseconds that the Smart Email process waits for a connection to the mail server to be established. When the defined timeout value is reached, the Smart Email process stops trying to connect to the mail server until the next time when the Service Management Smart Email scheduler starts again.

sqldebug		0 (Disable), 1 (Enable)	This parameter causes the ITSM A Service Management server to write information about RDBMS connections to the server log file. If enabled, the server writes the time to login to the RDBMS (*sqllogintime*) and the time it takes to perform a query request (*sqlquerytime*).
debughttp		0 (Disable), 1 (Enable)	This parameter causes the Service Management server to write HTTP SOAP requests and responses to the following log files. • logs\sm.log • RUN\HTTP.log **Important:** Enabling this parameter significantly reduces available system resources because the log files the server produces contain all HTTP traffic, including HTTP headers and attachments. For this reason, we recommend that you not enable this parameter on production systems, but rather in test environments only.
debugjavascript		1, 2, 3	This parameter causes the HPE Service Manager server to write JavaScript debugging messages to the log file. Its value can be 1, 2, or 3. • 1: Prints log information when an object is compiled, created, or disposed. • 2: In addition to the output of *debugjavascript:1*, prints log information when the garbage collector of the server's internal JavaScript engine is started or stopped. • 3: Forces the JavaScript engine to run garbage collection before running any JavaScript scripts. This setting is intended only for developers, and must not be used in production environments.
debugrest	0	0 (Disable), 1 (Enable)	This parameter enables the Service Management server to write detailed log trace for RESTful web services diagnostics. By default, this feature is disabled. To use this debugging parameter, set it to 1, then restart the Service Management server and re-run the RESTful web service application.

logdebuglevel	1	0 = DEBUG, 1 = INFO(default), 2= WARN, 3 = ERROR, 4 = FATAL	This parameter defines the log level of the JRTE codes. If the value of this parameter is equal to or larger than 1, all JVM options are logged in sm.log when the Service Management server is starting.
debugjni		0 (Disable), 1 (Enable)	This parameter provides detailed debugging in the Java Native Interface implementation.
log4jDebug		com.hp.ov.sm.common.oom.LowMemoryHandler	This parameter enables certain java packages to be started in debug mode. By default, none of the java packages will be run in debug mode.
enablecoredump		0 (Disable), 1 (Enable)	Unused in this release
rtm		0, 1, 2, 3, 4, 5	This parameter causes the Service Management server to write Response Time Monitor (RTM) performance statistics to the log file.
maxlogsize	20 (Size in MB)	5, 10, 20, 40, 60, 80, 100	This parameter defines the maximum size to which a log file can grow before Service Management rotates to a new log file. The system creates a new log when the current file reaches the indicated size. This parameter requires the use of the *numberoflogfiles* parameter.
numberoflogfiles	10	0 to 100	This parameter specifies the number of the log files. Service Management switches the log when the log size reaches the maximum size defined by the *maxlogsize* parameter. When this happens, the current log file is archived to the log file ending with 1, and the existing log files are renamed to the next higher number, so that the archive log file n+1 always contains older data than archive file n. To disable log switching, set its value to zero (0).

5. In the **Webtier** section, update the parameters by selecting a value in the drop-down list, and then click the **Update** button. Alternatively, you can directly modify the parameter values in the text area.

SM webtier log level parameters

If no value is listed in the drop-down list for a parameter, you need to update the value directly in the text area.

Parameter name	Default value	Possible values	Description
session-timeout	15	Number of minutes	This parameter defines the default session timeout interval for all sessions created in the Service Management web tier. It is best practice to lower the session-timeout value to 2 minutes if you experience Service Management web client sessions lingering for a longer period of time than expected.

viewrecordlist	true	true, false	Enabling this parameter causes web clients to display the record list/detail view for search results. Enabling this parameter from here forces all web clients to display the record list/detail view. Enabling the this parameter from the web browser URL only displays the record list/detail view on that particular web client.
querySecurity	true	true, false	Enabling this parameter causes the Service Management web tier to verify the security key of a URL query generated by the Service Management server, and, if valid, authorize the query. Disabling this parameter allows any user with logon permissions, the skills to create a query, and access to the Service Management URL to extract data from any Service Management table.
jsDebug	false	true, false	This parameter enables the web client to load unminified JavaScript files. However, when this parameter is enabled, the web client also displays to end users an error message that includes full stack trace. For this reason, do not enable this parameter in production environments to avoid disclosure of sensitive information.

6. Click **Apply.**

- By default, customized branding files and settings are stored in the following folder: **{itsma_global_volume}/logs/sm-9.52/webtier**.
- By default, the path to the exported dashboard report is: **{itsma_global_volume}/logs/sm-9.52/report-export**.

{itsma_global_volume} is the global NFS share directory that you set up during installation (For example: **/var/vols/itom/itsma/itsma-itsma-gloabl**). For more information, see Set up three NFS shares for ITSMA.

Configure the CMDB log level

1. On the suite landing page, click **Suite Configuration**.
2. Click **CONFIGURATION** > **Debug** > **Log Level**.
3. Click the **CMDB** tab.
4. In the **Server**, **UD**, and **Browser** sections, select a module, specify its log level, and then click **Update**. Repeat this step to specify the log levels for further modules.
   CMDB log level module

   Server:

Module name	Default value
ucmdb-api.properties.loglevel	ERROR
mam.properties.loglevel	INFO
security.properties.loglevel	INFO
cmdb-framework.properties.loglevel	ERROR
cmdb.properties.cla.loglevel	INFO
cmdb.properties.loglevel	ERROR
logstash.statistics.properties.loglevel.history	ERROR

cmdb.properties.notification.loglevel	INFO
reconciliation.properties.loglevel	ERROR
cmdb.properties.tqlscheduler.loglevel	INFO
cmdb-framework.properties.urmLogLevel	WARN
cmdb_soaapi.properties.loglevel	ERROR
security.properties.loglevel.cm	INFO
security.properties.loglevel.lwsso	ERROR
ui-server.properties.loglevel	ERROR
security.properties.loglevel.authorization	INFO
mam.web.properties.loglevel	ERROR
cmdb.properties.search.loglevel	INFO
fcmdb.properties.loglevel	INFO
cmdb.properties.downgrade.loglevel	INFO
cmdb.properties.quota.loglevel	INFO
logstash.statistics.properties.loglevel.datain	ERROR
fcmdb.gdba.properties.loglevel	ERROR
fcmdb.push.properties.loglevel	ERROR
mam.properties.loglevel.monitoring	INFO
multiple.cmdb.properties.loglevel	INFO
security.properties.loglevel.wink	ERROR
ui-server.properties.spring	ERROR
logstash.statistics.properties.loglevel.search	ERROR
logstash.statistics.properties.loglevel.tql	ERROR

Universal Discovery (UD):

Module name	Default value
discovery.framework	INFO
discovery.library	INFO
discovery.probe.agents	INFO
discovery.library.results.resultprocess	INFO
discovery.library.dal	INFO
discovery.probe.agents.probemgr.workflow	INFO

Browser:

Module name	Default value
ucmdb_browser.level	WARN
ucmdb_browser_search.level	WARN
jvm_stats.level	ERROR

statistics.level	INFO
rpcCalls.level	INFO

You can select from the following log levels for each module:

- INFO: An event for informational purposes
- WARN: An event that might possible lead to an error
- TRACE: A fine-grained debug message, typically capturing the flow through the application
- DEBUG: A general debugging event
- ERROR: An error in the application, possibly recoverable
- FATAL: A severe error that will prevent the application from continuing
- OFF: No events will be logged

5. Click **Apply**.

Configure the Smart Analytics log level

1. On the suite landing page, click **Suite Configuration**.
2. Click **CONFIGURATION** > **Debug** > **Log Level**.
3. Click the **Smart Analytics** tab, and then specify a log level. You can select one of the following log levels:
   - INFO (default): An event for informational purposes
   - DEBUG: A general debugging event
4. Click **Apply**.

Configure the Service Portal log level

1. On the suite landing page, click **Suite Configuration**.
2. Click **CONFIGURATION** > **Debug** > **Log Level**.
3. Click the **Service Portal** tab, and then specify a log level. You can select from the following log levels:
   - INFO (default)
   - WARN
   - TRACE
   - DEBUG
   - ERROR
4. Click **Apply**.

Configure the IdM log level

1. On the suite landing page, click **Suite Configuration**.
2. Click **CONFIGURATION** > **Debug** > **Log Level**.
3. Click the **IDM** tab, update the parameters by selecting a value in the drop-down list, and then click the **Update** button. Or, you can directly modify the parameter values in the text area.

Parameter	Default value
idm_auth_debug	INFO
idm_debug	INFO

You can select from the following log levels:

- INFO (default)
- WARN
- TRACE
- DEBUG
- ERROR

4. Click **Apply**.

Configure the Chat log level

a. On the suite landing page, click **Suite Configuration**.
b. Click **CONFIGURATION** > **Debug** > **Chat**.
c. Click the **Chat** tab, and then specify a log level. You can select from the following log levels:
   - INFO
   - WARN
   - TRACE

- DEBUG
- ERROR

d. Click **Apply**.

Change the ITSMA suite administrator password

User role: Suite Administrator

The Suite Administrator (**sysadmin**) has full administrator privileges for the suite. During the installation, you configured a password for this user. You can change this password after the installation.

The initial password for the Suite Administrator user role was set when the suite was installed. To change the password, follow these steps:

1. Log in to the ITSMA Suite Configuration user interface as the **sysadmin** user:
   https://<EXTERNAL_ACCESS_HOST>/itsmaconfig
2. Click **Operation** > **Admin Password.**
3. Enter the old and new passwords for the **sysadmin** user.

   > The password must be 10 to 30 characters in length and contain all of the following types of characters: uppercase letters, lowercase letters, numbers, and special characters.

4. Click **Update**.

Service Portal administration

This section describes Service Portal administration tasks.

- Customize Service Portal
- Import Service Manager catalog item entitlement to Service Portal

Customize Service Portal

You can design the look and feel of Service Portal.

- Configure Service Portal display theme setting
- Configure Service Portal feature settings

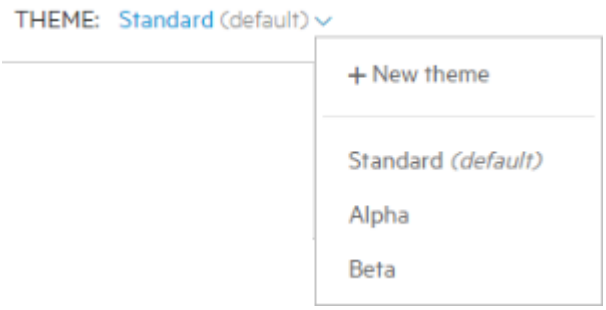
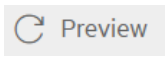
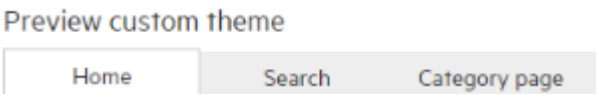
Configure Service Portal display theme setting

ITSMA suite provides a default display theme for the Service Portal. You can create a custom display theme to suit your company's look and feel.

Themes settings page user interface

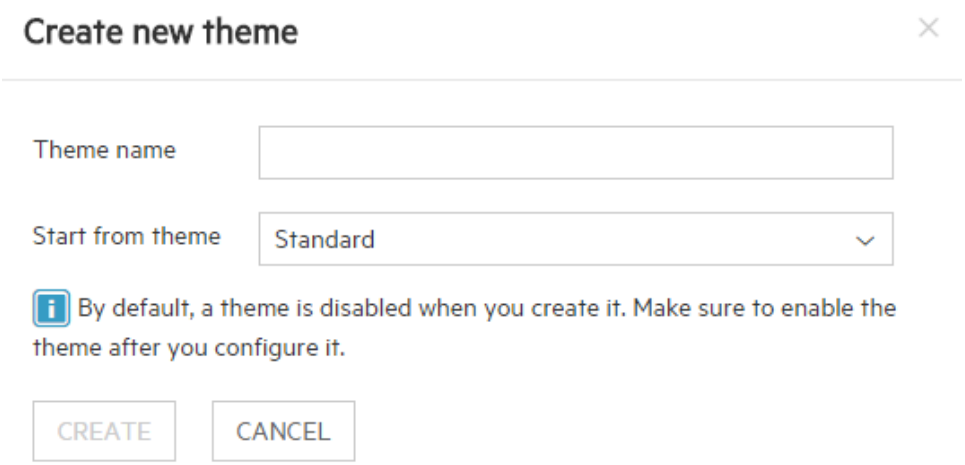
On Service Portal main page, click 
and select **Theme Settings**.

Interface Item	Description
Theme	The theme for the Service Portal that is displayed. By default, the out-of-the-box **Standard (default)** theme settings are displayed. 

Theme selection	Click to display a drop-down list of themes. You may select a previously created theme, or create a theme. 
	When you update a setting, you can click **Preview** to display the change. The setting is only previewed and not saved until you click **Save**. 
	When you have selected a theme other than the default, click **More** to display the following options: • **Rename** - select to rename the theme. • **Delete** - select to delete the theme. • **Enable** - select to enable the theme. Only available for selection when the theme is disabled. • **Disable** - select to disable the theme. Only available for selection when the theme is enabled. • **Set as default** - select to set the theme as the default. Only available for selection when the theme is enabled.
Preview custom theme	You can select which part of the Service Portal user interface the theme settings are previewed on.
Settings tab	Area where you define the settings for the theme.

Add a new theme

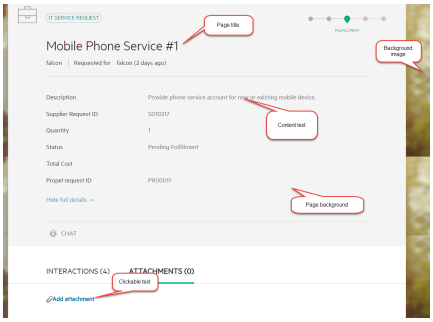
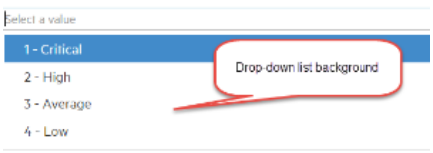
1. On Service Portal main page, click  and select **Theme Settings**.
2. Click and select **+ New Theme**.
   The **Create New Theme** dialog box is displayed.

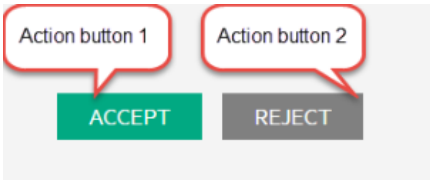
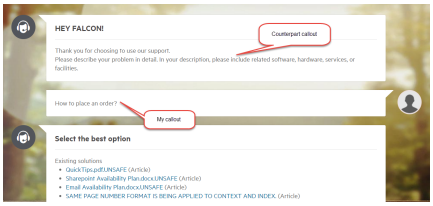
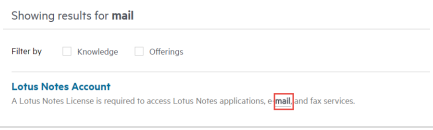
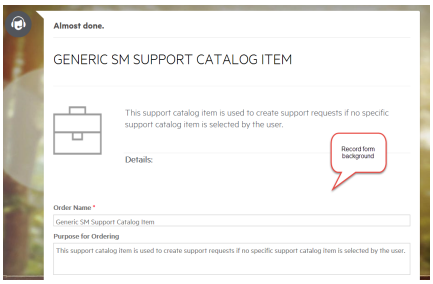


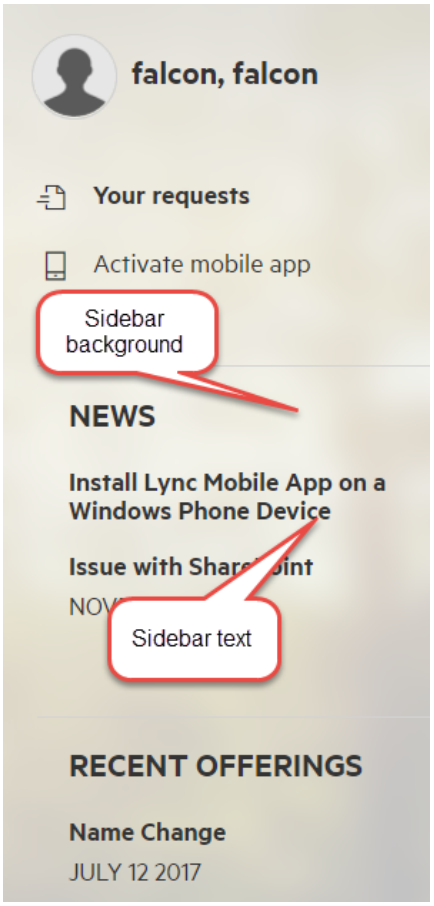
3. Type a suitable name for the theme.
4. From the drop-down list, select the theme to provide the initial settings that you want to customize.
   For example, assume you previously created a custom theme named Alpha. You now want to create a similar theme, based on Alpha, but perhaps with changes to the text color, and background. First, you would give your new theme a name. Then, you would select Alpha from the drop-down list. If you want to create a theme based on the Standard theme, you would select Standard from the drop-down list.
5. Click **Create**. The theme displays, but is disabled.
6. To enable the theme, click **More**, and select **Enable**.
7. Edit the settings as required. For more information, see
8. Click **Save**.
9. To make the theme the default, click **More**, and select **Set as default**.

Edit theme settings

The following table describes the theme settings:

Section	Fields	Affected area of Service Portal display
Header	• Name • Font/Text size/Text color/Bold • Logo • Background	
Action ribbon	• Search box background • Ribbon button foreground • Ribbon button background • Ribbon button hover • Ribbon text • Ribbon text hover	
Global page setting	• Background image • Page background • Page title • Section title • Content text • Link • Link mouseover • Clickable text	
	• Dropdown list background	

Buttons	• Submit button text • Submit button background	
	• Action button text • Action button 1 background • Action button 2 background	
	• Buttons disabled color	
Callout	• My callout background • My callout text • Counterpart callout background • Counterpart callout text	
MISC	• Search keyword highlight	
	• Record form background	
	• Live chat bar text color • Live chat bar background color	

	• Sidebar text • Sidebar background • Sidebar background blur This setting blurs the image selected for the background of the sidebar. You can enter a two digit number. 0 displays the image as it is and 99 blurs the image till it is nearly opaque. 9 is the default setting.	

Configure Service Portal feature settings

ITSMA suite provides default feature settings for the Service Portal. You can change the following feature settings:

- Self-Service settings
  - Feature selection
  - Ribbon promotion
  - Portal loading page
  - Mobile app
  - Portal profile page on first login
- Virtual agent and email integration
  - Suggested links in email and support suggestion
- Miscellaneous
  - Select category page type

Self-Service settings

Feature selection

By default, Q&A and Ideas are disabled, select **On** to enable a feature.

And the following features are enabled, select **Off** to disable a feature and remove all reference to it from the portal.

- Request on behalf
- Shopping cart
- Live chat

Ribbon promotion

In the **Ribbon promotion** section, you can select which of the following links display in the top ribbon of the Service Portal:

- Ask friends
- Help friends
- Suggest idea
- Your services and assets
- Your approvals
- Request on behalf

You can select up to four links to display.

Portal loading page

By default, the Service Portal light startup landing page is enabled. In the **Enable portal loading page** field, you can disable this by selecting **Off**.

If this option is enabled, on startup a standardized light landing page displays for users. While the portal loads in the background, users can:

- Start typing a request description
- Track their open requests:
    - View open requests
    - Accept or reject proposed solutions
    - Provide more information
- View news

If users do not interact with the light landing page, it automatically closes when the portal loads.

Mobile app

By default, the ability to log in to the Service Portal using the mobile app is disabled. In the **Enable mobile app** field, you can enable this by selecting **On**.

In the **Mobile QR code URL** field, you can customize the website URL placed into the mobile app QR code, default website URL is used if this field is left blank.

Portal profile page on first login

On the Service Portal, there is a profile page for the user to complete. By default, this displays automatically when the user logs in for the first time. In the **Show portal profile page on first login** field, you can disable this by selecting **Off**.

Virtual agent and email integration

Suggested links in email and support suggestion

On the Service Portal, the ability to display links to the following, in specially prepared email messages and virtual agent support, is enabled by default. In this section, you can disable each type by selecting **Off**.

- Articles
- Q&A
- News
- Offerings

Miscellaneous

Select category page type

On the Service Portal, when a user clicks on a category tile, a page is displayed with three tabbed sections. You can configure the default section that is displayed. Select the appropriate option in the **Category page type** field, as detailed in the following table.

Option	Description
FEATURED (Out-of-the-box default)	A list of items in the following order: • All new items • Recommended offerings • Popular offerings • Article There may be up to 30 items in this section.

OFFERINGS	A list of offerings in the following order: • Recommended offerings • Popular offerings There may be up to 20 items on each page of this section.
ARTICLES	A list of articles in the following order: • Recommended articles • Other articles There may be up to 20 items on each page of this section.

Import Service Manager catalog item entitlement to Service Portal

Service Manager catalog Item capability words and access filters can be imported to Service Portal of ITSMA. In Service Portal, the access control of catalog items is achieved using user groups, and therefore, a user group is created for each capability word and access filter imported from Service Manager.

To import the capability words and access filters from Service Manager to Service Portal, follow these steps.

1. Log in to the Service Portal administration portal as **sysadmin**: https://<EXTERNAL_ACCESS_HOST>/propel/launchpad.
2. Click **Supplier**, and then verify that the supplier is properly set for Service Manager. For more information about how to set a supplier, refer to the Service Manager Help Center.
3. Click the supplier for SM.
4. On the detail page of the supplier, check the **User Auto Entitlement** checkbox and save.
5. Go back to the **Service Portal** page, click **Catalog Connect**, and then verify that there is at least one aggregation with the offering type **S ervice Offering** or **Support Offering**.
6. In Service Manager, in the navigation tree, expand **Miscellaneous**, and then click **System Status**.
7. Click **Start Scheduler**.
8. On the **Select startup record** page, click **propel** to start the scheduler.

   > If you want to change the schedule interval, you need to modify the **PropelSync** schedule before you start the scheduler.

9. After you start the scheduler, a user group is created for each Service Manager capability word, and its name starts with “SM_”, for example, “SM_AlwaysAdmin.” Likewise, a user group is created for each access filter, and its name starts with “SM_AF-”, for example, “SM_AF- 6664B6BEB9F75971.” Meanwhile, if a user exists in IDM and has a certain capability word(s) or meets a certain access filter, the user will be add to the corresponding user group.
10. Wait a few minutes, go back to the Service Portal Admin page, and then click **Identity**.
11. Click the organization of ITSMA.
12. On the detail page of the organization, click the **Groups** tab, and make sure that all Service Manager capability words and access filters have been imported.
13. Go back to the **Service Portal** page, click **Catalog Connect**, and then restart all the aggregations so that they run with the user groups imported from Service Manager.
14. Go back to the **Service Portal** page, click **Catalog Items**, and then click a catalog item.
15. On the **Access Control** page, verify that **Access Control Rule 1** has the user groups imported from Service Manager capability words. Also verify that **Access Control Rule 2** has the user groups imported from Service Manager access filters.
16. After you finish all these steps, Service Manager Service Catalog capability words and access filters have been imported to Service Portal of ITSMA.

After the Service Manager catalog item entitlement is imported, end users can search their entitled offerings in Service Portal. In addition, end users can also search their entitled KM articles and hot news in Service Portal. The KM entitlement is based on Service Manager KM entitlement.

Variables used in access filters

If an access filter leverages a variable, in order for this access filter to be imported and effective in Service Portal, you need to open the **variableI nfos** table with the Database Manager, and then add the variable to this table.

While adding a variable, the following rules apply:

- **Variable Name** must be identical to the variable name specified in the access filter.
- When the variable points to a field in the **operator** table, **Table Name** must be **operator**, **Field Name** must be the field the variable points to, **Join Tables** must be **operator**, **Base Query Type** must be **operatorBaseQuery**.
- When the variable points to a field in the **contacts** table, **Table Name** must be **contacts**, **Field Name** must be the field the variable points to, **Join Tables** must be **operator** and **contacts**, **Base Query Type** must be **contactsBaseQuery**.
- When the variable points to a field in the **Subscription** table, **Table Name** must be **Subscription**, **Field Name** must be the field the variable points to, **Join Tables** must be **operator, contacts,** and **Subscription**, and **Base Query Type** must be **subscription BaseQuery**.

Smart Analytics administration

As the Suite Administrator, you can perform the following administration tasks for Smart Analytics.

Functional comparison of classic and containerized Smart Analytics

The followng table provides a functional comparison of Classic and containerized Smart Analytics:

Function	Classic Smart Analytics	Containerized Smart Analytics
Stop word	Configure this function in the <*Language name*>.dat file in the <*Smart Analytics Installation*>/langfiles directory.	Configure this function in the <*Language name*>.dat file in the <*Smart Analytics NFS root folder*>/data/idol/langfiles/ directory.
Stop Phrase	Configure this function in the qssp.db file in the <*Smart Analytics Installation*>/Content1/main directory.	Configure this function in the qssp.db file in the <*Smart Analytics NFS root folder*>/data/idol/st/content[1,2]/main/ directory.
Synonyms	Configure this function in the synonym.txt file in the <*Smart Analytics Installation*>/ directory.	Configure this function in the synonym.txt file in the <*Smart Analytics NFS root folder*>/config/idol/synonym directory.
Data cleansing	Configure this function in Service Manager by clicking **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Data Cleansing**.	Configure this function in Service Manager by clicking **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Data Cleansing**.
Connector (HTTP/SharePoint/File System)	Install Connector with CFS either on the same computer as the Smart Analytics server or on a different computer. Configure connector to connect with Smart Analytics Server Port. The default port number is 9000.	Due to performance perspective and SharePoint connector limitation (SharePoint connector can be installed on Windows only), connector with CFS must be installed outside the Container. The installation method for Connector with CFS is as same as that in Classic mode. Refer to Configure external connectors to work with Smart Analytics in ITSMA suite for detailed instructions. Configure the connector to connect to Smart Analytics Mix Proxy Port (the default port number is 31370 in the 2017.07 release). Configure the connector to connect to the exposed DIH port (the default port number is 31370 in the 2017.02 and 2017.04 releases).
Scale out Smart Search content	1. Install the content server. 2. Edit the trusted client settings in the level2proxy\IDOLServer.cfg file on the Smart Analytics proxy server. For detailed instructions, see *SM Help Center > Add a content server for Smart Search*. 3. Use the Service Manager Smart Analytics Assistant (SAA) utility to add this content.	Click **Operation** > **Smart Analytics** > **Add Content Group**.
Redistribute	Click the **Redistribute** button in the Service Manager Smart Analytics Assistant.	Click the **Redistribute** button after you successfully add a content group. This button is enabled automatically.

Scale out Smart Ticket and Hot Topic Analytics	1. Install the content server. 2. Edit the <*Smart Analytics Installation*>/IDOL/IDOLServer.cfg file. Detail can be found in *Service Manager Help Center* > *Add a content server for Smart Ticket and Hot Topic Analytics*.	Not supported.
Index	Connect to the Smart Analytics main server.	Connect to DIH directly in containerized mode. Connect to the Mix Proxy in mixed mode.
Search	Connect to the Smart Analytics main server.	Connect to DAH directly in containerized mode. Connect to the Search service in mixed mode.
Smart Analytics Assistant (SAA)	Use the **saa** command in Service Manager to open the Smart Analytics Assistant page.	Click **Operation** > **Smart Analytics**, and then expand the **Smart Analytics Assistant** section.
Smart Ticket Tuning	Configure this function in Service Manager by clicking the **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket** > **Tuning** tab. For detailed instructions, see *Service Manager Help Center* > *Configure Smart Ticket*.	Configure this function in Service Manager by clicking the **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket** > **Tuning** tab. For detailed instructions, see *Service Manager Help Center* > *Configure Smart Ticket*.
Extend Smart Ticket/Hot Topic Analytics/Smart Search to other modules	Configure this function in Service Manager. For detailed instructions about how to extend Hot Topic Analytics, see *Service Manager Help Center* > *Enable Hot Topic Analytics for other modules*. For detailed instructions about how to extend Smart Ticket, see *Service Manager Help Center* > *Extend Smart Ticket to other modules*.	Configure this function in Service Manager. For detailed instructions about how to extend Hot Topic Analytics, see *Service Manager Help Center* > *Enable Hot Topic Analytics for other modules*. For detailed instructions about how to extend Smart Ticket, see *Service Manager Help Center* > *Extend Smart Ticket to other modules*.
OCR	Connect to the Image Server by clicking **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Configuration**. The default port number is 18000.	Connect to the Image Server in the container. The default port number is 31395. You must apply both CompatibleForNG_Plus_SM941.unl and CompatibleForNG_SM941to952.unl to SM 9.41 in the Mixed mode. For more information, see Install ITSMA in mixed mode (scenario 1) > *Task 6: Configure integration with external Service Manager* > *Apply unload files to Service Manager*.
Restart IDOL services	1. Execute the **StopAll.sh** script in the <*Smart Analytics Installation*>/scripts/ directory. 2. Execute the **StartAll.sh** script in the <*Smart Analytics Installation*>/scripts/ directory.	Run the following commands on the master node: 1. Execute the **kubectl get pod --all-namespaces | grep smarta** command to show all pods status. 2. Execute the **kubectl delete pod <pod_name> -n <*namespace*>** command to stop the services.
License	Smart Analytics module license.	ITSMA express license for fully containerized mode. Smart Analytics module license for external SM in the Mixed mode.

SSL	Two-way SSL is supported.	SSL is disabled by default. To switch between one-way SSL and two-way SSL, se e Configure SSL for ITSMA in mixed mode. • The outbound request of search service supports one-way SSL only.

Add Smart Analytics content groups

If the capacity of the existing smart search content groups is not enough for the indexed data, you can easily add content groups for Smart Search.

The system does not display **Service Management Content Group** under either of the following circumstances:

- The installation and configuration process is not finished.
- The external SM has no Smart Analytics licenses.

To add Smart Analytics content groups, follow these steps:

1. On the suite landing page, click **Suite Configuration**.

   For ITSMA, do not use the Smart Analytics Assistant utility available in the containerized Service Management or in the external Service Management to add Smart Search content groups.

2. Click **Operation** > **Smart Analytics.**
3. View the capacity of the current content groups for Smart Search. The system provides on-screen recommendations for adding new content groups based on the current document count and capacity of the existing content groups.
4. If you decide to add a new content group, click **Add New Content Group**.

   When the system successfully adds a content group, the DIH service will restart so that the Smart Search feature stops working until the process is finished. If the system fails to add a new content group, the DIH service will not restart and you can continue to use Smart Search without any downtime.

   If the "Adding a new content group" status hangs for more than 10 minutes, some error might have occurred in the backend. See the "Failed to scale out the content server" section in Smart Analytics troubleshooting.

5. Click **Redistribute Documents** to balance data distribution.

   After you add a new content group, you are recommended to redistribute documents to improve query performance.

Use Smart Analytics Assistant

Smart Analytics Assistant is a tool that enables administrators to perform IDOL administrative actions in Smart Analytics. This tool provides a command line on the user interface enables the administrator to send IDOL actions to Smart Analytics components. For example, you can use this tool for content server maintenance, to check the system status, and for troubleshooting.

To use Smart Analytics Assistant, follow these steps:

1. Log in to the ITSMA Suite Configuration user interface as **sysadmin**: https://<EXTERNAL_ACCESS_HOST>/itsmaconfig.
2. Click **Operation** > **Smart Analytics.**
3. Expand the **Smart Analytics Assistant** section.
4. Double-click a Smart Analytics component in the **Service Manager Components** or **Service Portal Components** list.
   Service Manager Components

Name	Host	Port	Component description

Smart Search DAH 1	smarta-ss-dah1-svc	9060	Supports query action for Service Manager Smart Search
Smart Search DIH	smarta-ss-dih-svc	31370	Supports index action for Service Manager Smart Search
Mixed Mode Level Two Proxy	smarta-mix-l2proxy-svc	31380	Supports query and index action for Service Manager Smart Search in mixed mode
Smart Search CFS	smarta-ss-cfs-svc	31360	Sends index action for attachment and external connector to IDOL
Image Server	smarta-ss-imgsvr-svc	18000	Analyzes and extracts content in image
Smart Search DAH	smarta-ss-dah-svc	9060	Load balancer for Smart Search DAH(n)
Smart Search Content 1a	smarta-ss-con-1a-svc	10010	Stores indexed records for Service Manager Smart Search
Smart Search Content 1b	smarta-ss-con-1b-svc	10010	
Smart Search Content 2a	smarta-ss-con-2a-svc	10010	
Smart Search Content 2b	smarta-ss-con-2b-svc	10010	
Smart Ticket & Hot Topic Analytics Proxy	smarta-st-proxy-svc	31390	Supports query and index action for Service Manager Smart Ticket and Hot Topic Analytics
Mixed Mode Main Proxy	smarta-mix-proxy-svc	31370	Transfers request from consumer to IDOL in mixed mode
Smart Ticket & Hot Topic Analytics Content 1	smarta-st-con-1-svc	10010	Stores indexed records for Service Manager Smart Ticket and Hot Topic Analytics
Smart Ticket & Hot Topic Analytics Content 2	smarta-st-con-2-svc	10010	
Smart Search Agentstore	smarta-ss-agent-svc	9050	Agentstore used by IDOL Server to store agents and profiles

Service Portal Components

Name	Host	Port	Component Description
Service Portal DAH	smarta-smsp-dah-svc	9060	Supports query action for Service Portal search
Service Portal DIH	smarta-smsp-dih-svc	31370	Supports index action for Service Portal search
Service Portal QMS	smarta-smsp-qms-svc	16000	Supports type-ahead in Service Portal search
Service Portal Content 1a	smarta-smsp-con-1a-svc	10010	Stores indexed records for Service Portal search
Service Portal Content 1b	smarta-smsp-con-1b-svc	10010	

5. Select an action from the drop-down list. The system automatically populates the <*Host*> and <*port*> values in the action examples with the corresponding values that you can find from the **Service Manager Components** or **Service Portal Components** list.
6. Click **Run**.

Follow these steps to manually restore the Category data for Smart Analytics:

1. Stop smarta-mix-proxy (in mixed mode), or stop smarta-st-proxy (in fully containerized mode).
2. Back up the Category data. To do this, follow the steps that are appropriate for your deployment:
    a. To back up Category data in containerized Smart Analytics, use the **Backup Component** action in Smart Analytics Assistant in the suite.
    b. To back up Category data in external Smart Analytics, use the **Backup Component** action in the external Smart Analytics Assistant.
    By default, the Smart Analytics server Category Port is 9020.
3. Restore the Category data. To do this, follow these steps:
    a. Copy the *.zip backup file generated in the previous step to the <*Smart Analytics NFS root folder*>/data/idol/mix/proxy directory on the NFS server.
    b. Delete all files and folders in the <*Smart Analytics NFS root folder*>/data/idol/mix/proxy directory.
    c. Unzip the backup file and replace the existing files.
    d. Run the **chmod -R itsma:itsma <*Smart Analytics NFS root folder*>/data/idol/mix/proxy** command to grant the container pod

access rights to this folder.

4. Start smarta-mix-proxy (in mixed mode), or start smarta-st-proxy (in fully containerized mode).

Note that some action commands only work with certain Smart Analytics components in the suite. Refer to the following table for detailed descriptions.

Action name	Action example	Description	Allowed component	Allowed port	
View Status	http://<Host>:<port>/action=GetStatus	Requests details of all components. Check whether all components are up and running; checks how many documents are in each database.	all	<Host>:<ACI_Port>	
View Action History	http://<Host>:<port>/action=GRL&format=xml	Displays a log of requests, including the date and time that a request was made, the client IP address that made the request, and the internal thread that handled the action.	all	<Host>:<ACI_Port>	
View Index Status	http://<Host>:<port>/action=indexerGetStatus	Checks the status of index actions in the Smart Analytics index queue.	dih	smarta-<*ss/st*>-dih-svc:31370	
			l2proxy	**Mixed mode**	smarta-mix-l2proxy-svc:31380
				fully containerized	None
			content	<CONTENT_SERVICE>:10010	
			main proxy	**Mixed mode**	smarta-mix-proxy-svc:31370
				fully containerized	smarta-st-proxy-svc:31390
View Root Category Detail	http://<Host>:<port>/action=CategoryGetHierDetails	Displays the root categories after training.	category	**Mixed mode**	smarta-mix-proxy-svc:31390
				fully containerized	smarta-st-proxy-svc:31410
Back up Component	http://<Host>:<port>/action=BackupServer&path=/var/backup	Creates a backup that can be used to restore the component's state. You can use this action for the Content, Category, Agent, and Community components, but you must send the action to the component ACI port rather than to the IDOL Proxy port. The backup file is stored in the path that you specified.	content	<CONTENT_SERVICE>:10010	
			mainproxy	**Mixed mode**	smarta-mix-proxy-svc:31370
				fully containerized	smarta-st-proxy-svc:31390
			category	**Mixed mode**	smarta-mix-proxy-svc:31390
				fully containerized	smarta-st-proxy-svc:31410
Restore Content Server	http://<Host>:<port>/action=RestoreServer&filename=/var/backup/***.zip	Restores the content of a content server that was previously backed up.	content	<CONTENT_SERVICE>:10010	
Synchronize Category	http://<Host>:<MainProxyACIPort>/action=CategorySyncCatDRE	Synchronize and build the category after you restore the Category component. When running this action for **Smart Ticket & Hot Topic Analytics Proxy** in fully	category	**Mixed mode**	smarta-mix-proxy-svc:31390

		containerized mode, you must manually enter port number 31410 in the action examples.		**fully containerized**	smarta-st-proxy-svc:31410
Back up Database	http://<Host>:<indexPort>/DREEXPORTIDX?filename=c:/BackupFolderName/FilePrefix&DatabaseMatch=<Database_name>&HostDetails=true	Exports all the index documents for a database from the Smart Analytics content server to a series of compressed files in the defined backup directory. This action backs up individual databases. If you want to backup all databases on a content server, use the action Backup Component as mentioned above.	dih	smarta-<*ss*/*st*>-dih-svc:31371	
			lv2 proxy	**Mixed mode**	smarta-mix-l2proxy-svc:31381
				fully containerized	None
			main proxy	**Mixed mode**	smarta-mix-proxy-svc:31371
				fully containerized	smarta-st-proxy-svc:31391
			content	<CONTENT_SERVICE>:10011	
Restore Database	http://<MainProxyHost>:<IndexPort>/DREADD?FileName=/var/backup/***.idx&DREDbName=***&CreateDatabase=True	Restores the index IDX exported before. If no DREDbName is specified, use the dbname of the indexed file.	dih	smarta-<*ss*/*st*>-dih-svc:31371	
			lv2 proxy	**Mixed mode**	smarta-mix-l2proxy-svc:31381
				fully containerized	None
			main proxy	**Mixed mode**	smarta-mix-proxy-svc:31371
				fully containerized	smarta-st-proxy-svc:31391
			content	<CONTENT_SERVICE>:10011	

The system does not display the **Service Manager Components** list under either of the following circumstances:

- The installation and configuration process is not finished.
- The external Service Manager has no Smart Analytics licenses.

For ITSMA, always use the Smart Analytics Assistant (SAA) utility available in the Suite Configuration user interface. Do not use the SAA utility available in the containerized Service Management or in the external Service Management.

Add trusted clients for Smart Analytics

To improve security, you can restrict access to Smart Analytics to specific Service Manager servlet FQDNs or addresses. Only those Service Manager servlets whose hostnames or IP addresses are listed as trusted clients can send requests and receive responses from the containerized Smart Analytics.

To add a Smart Analytics trusted client, follow these steps:

1. On the suite landing page, click **Suite Configuration**.
2. Click **Operation** > **Smart Analytics.**
3. Expand the **Add a Trusted Client** section. The default value is *, which means all Service Manager servers can connect to the containerized Smart Analytics.
4. Type the FQDN or IP address of a Service Manager servlet in the text field. You can separate multiple FQDNs or IP addresses by commas. Do not add any spaces between the FQDNs or IP addresses and commas.
   For example, **abc0123.lab.net,15.192.87.1,15.192.87.2,15.192.87.3**

   You must add worker nodes as trusted clients. Run the **kubectl get nodes --show-labels** command to find the IP addresses of the worker nodes.

   Do not add the master node FQDN or IP to the Trusted Client field.

5. Click **Apply**, and then click **Yes** in the pop-up window to confirm.
   It may take some time for the configuration to take effect. Wait until the Service Manager components under the Smart Analytics Assistant tab are online again.

> If the hostname or IP address of a Service Manager servlet is changed, you must manually update the information in the trusted clients list. Also, you must perform a full reindex manually after you change the Service Manager data volume. If you do not, Smart Search results from the old volume may be returned.

Configure external connectors to work with Smart Analytics in ITSMA suite

To enable search actions among different data sources, you need to configure different external connectors and servers to work with Smart Analytics in the ITSMA suite.

> If you are working with Service Manager 9.41, You need to update the IDOLTOKEN length value to 100. To do this, follow these steps:
>
> 1. Log on to Service Manager as a system administrator.
> 2. Type **dbdict** in the Service Manager command line, and then press Enter.
> 3. Search for kmknowledge.
> 4. Select IDOLToken, and then update the length value from 60 to 100.
> 5. Click **Save**.

- Configure SharePoint Connector
- Configure HTTP Connector
- Configure File System Connector

Configure SharePoint Connector

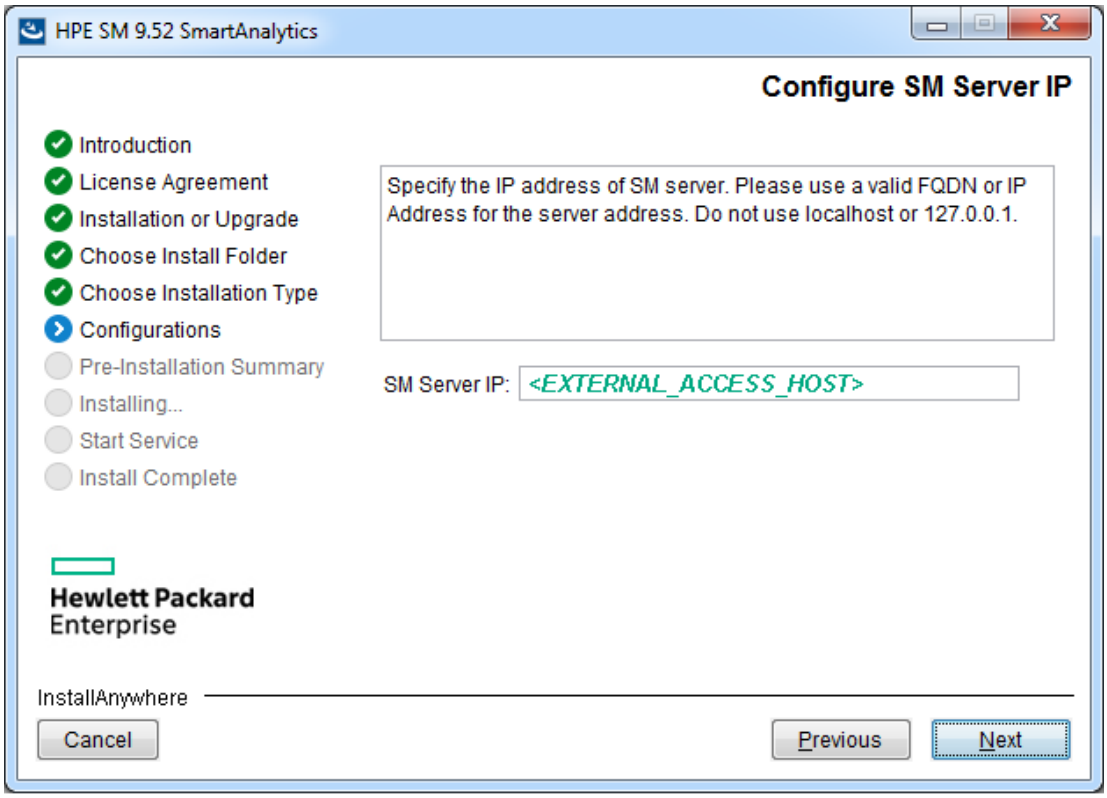
> - If you have never installed Smart Analytics SharePoint connectors before, perform Task 1, Task 2, and Task 4.
> - If you have already installed and configured SharePoint Connector with a CFS server, perform Task 3 and Task 4 (Step 4 to Step 6).

To enable search actions in SharePoint, you must install and configure the SharePoint connector with CFS outside the containerized environment. To do this, perform the following tasks:

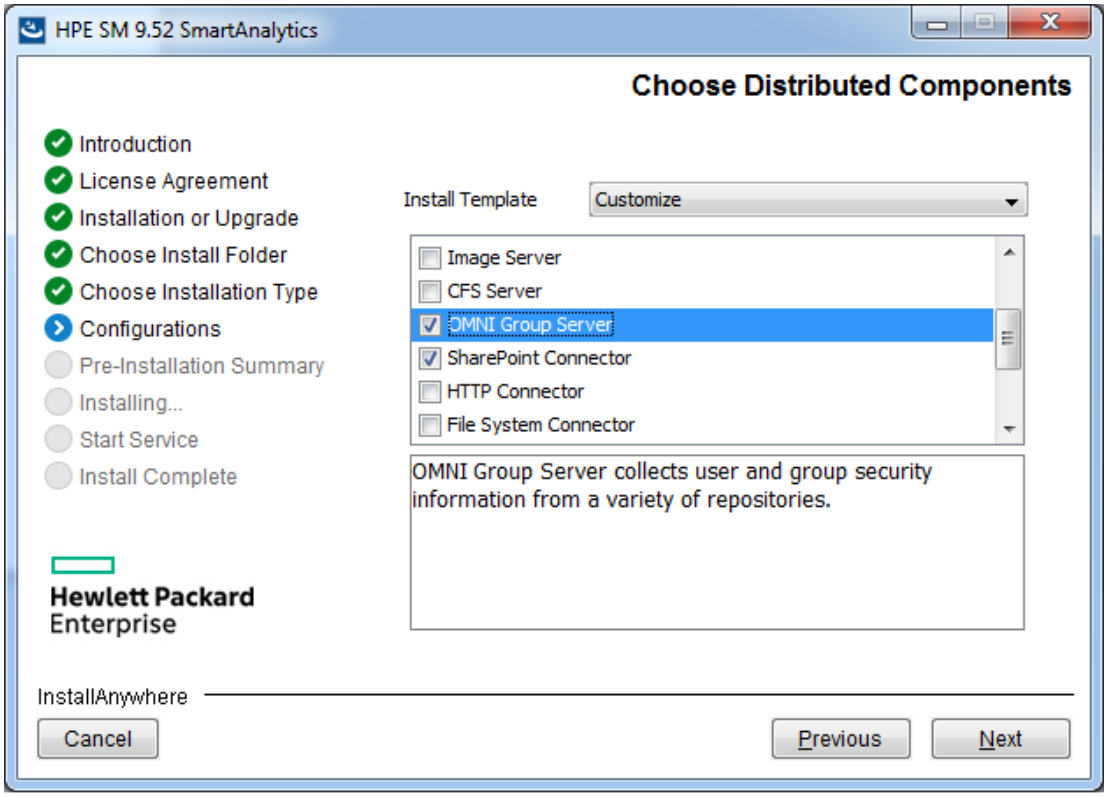
Task 1: Install SharePoint with a CFS server

Follow these steps:

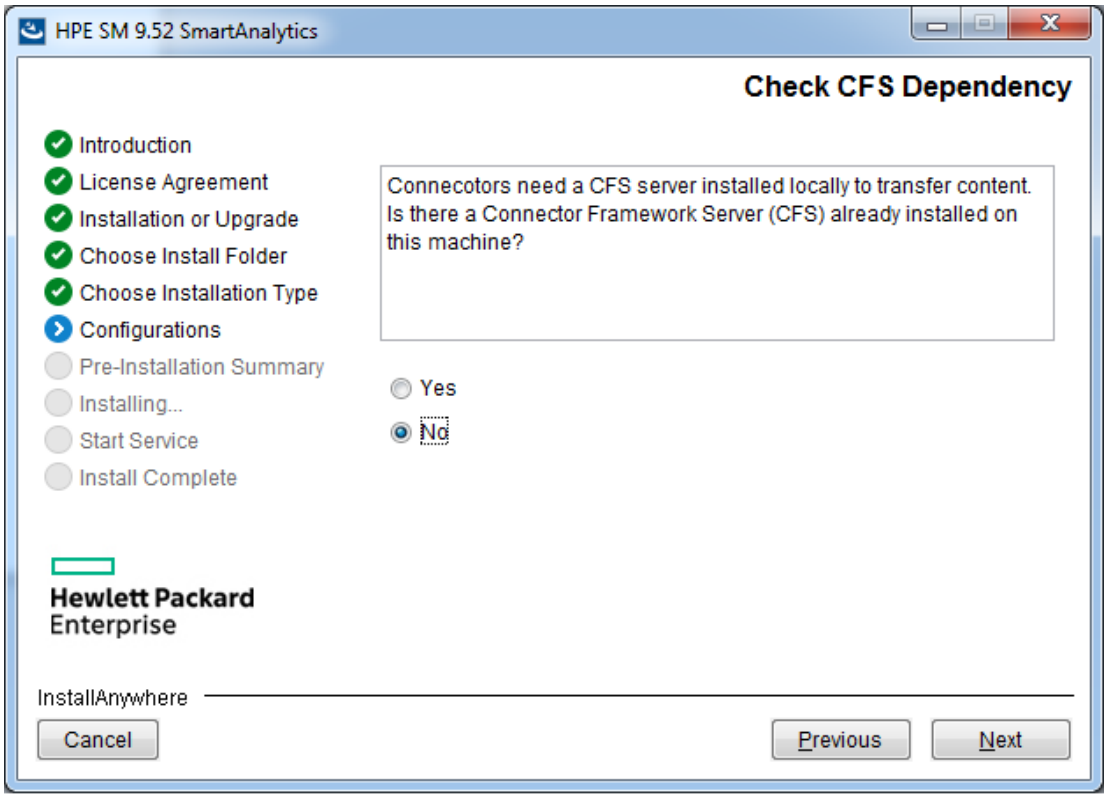
1. Save the Smart Analytics 9.52 installer from http://www.hpe.com/software/entitlements to your computer, and then unzip this installation package.
2. Unpack the .zip file, and then double-click the setup application (setupSmartAnalyticsWindowsX64.exe).
3. The HPE SM 9.52 SmartAnalytics Setup wizard opens. Read the introduction, and then click **Next**.
4. Read the license agreement, select **I accept the terms of the License Agreement**, and then click **Next**.
5. Select **New Installation**, and then click **Next**.
6. Choose an installation folder, and then click **Next**. The default installation folder is C:\Program Files(x86)\HPE\Service Manager 9.52\SmartAnalytics.
7. Select **Advanced** Install as your installation type, and then click **Next**.
8. Enter the external access host in the **SM Server IP** field, and then click **Next**.



9. Select **Customize** in the Install Template drop-down list, and then select **OMNI Group Server** (for Security SharePoint) and **SharePoint Connector**. Click **Next**.

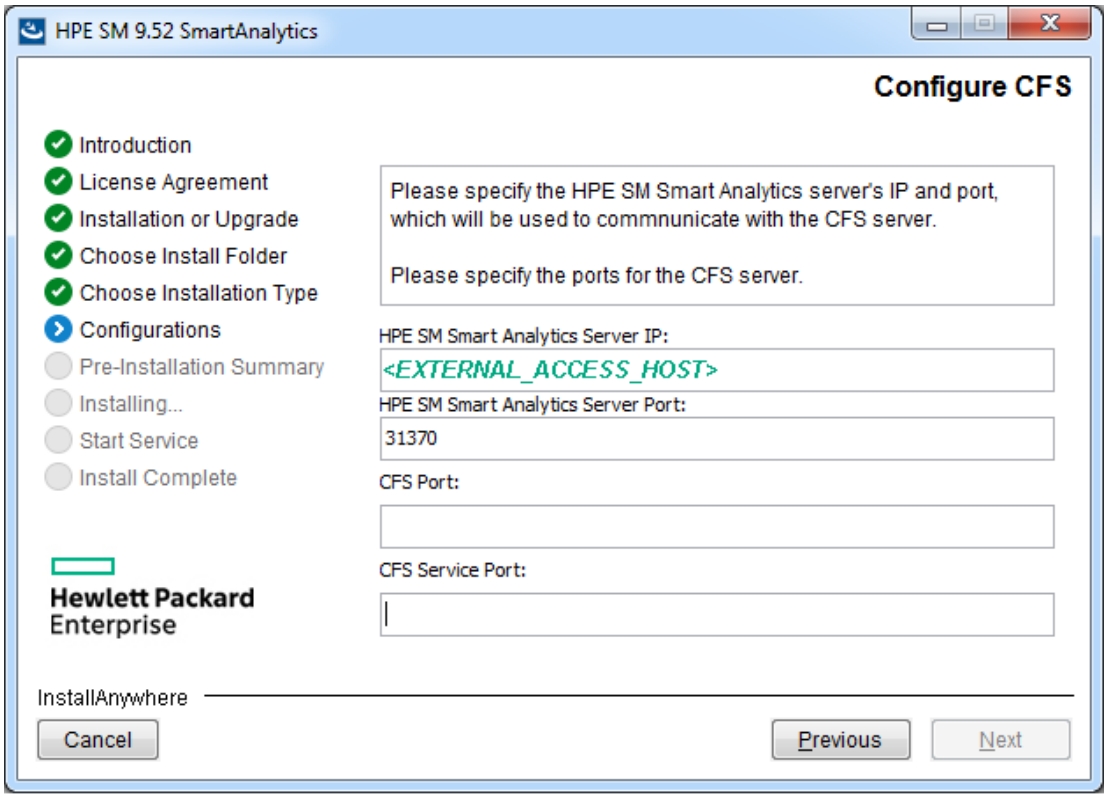


10. Select **No** if there are no CFS servers installed on this computer. Otherwise, select **Yes**.



You must install the external SharePoint connector and the CFS server on the same computer.

11. Enter the SM Smart Analytics Server IP and port as follows, and then enter the CFS Server port and Service port. Click **Next**.
    SM Smart Analytics Server IP: **<EXTERNAL_ACCESS_HOST>**
    SM Smart Analytics Server Port: **31370**
    CFS Port: **7000**
    CFS Service Port: **7001**



> If you have modified the CFS Port from 7000 to another number, you need to update the value for the IngestPort parameter to the modified port number in the Connector configuration file (such as SharepointRemoteConnector.cfg). The file should resemble the following:
> [Ingestion]
> IngestHost=127.0.0.1
> IngestPort=7000

12. Enter the OMNI Group Server Port and Service Port (for Security SharePoint), and then click **Next**.
13. Configure the LDAP Repository information, and then click **Next**. If you want to index SharePoint without security, skip the configuration, and then click **Next** directly.
14. Configure the SharePoint Connector information, and then click **Next**.
15. Click **Install** to install OMNI Group Server (for Security SharePoint), SharePoint Connector and CFS Server.

Task 2: Configure the SharepointRemoteConnector.cfg file

Follow these steps:

1. Go to <SharePoint Installation directory>/SharepointRemoteConnector, and then open the SharepointRemoteConnector.cfg file with a text editor.
2. Configure the [FetchTasks] and [MyTask] sections as needed.

```
[FetchTasks]
Number=1
0=MyTask

[Default]

[MyTask]
SharepointOnline=false
SharepointUrlType=SiteCollection
SharepointUrl=http://sgdlitvm0821.asiapacific.hpqcorp.net/
Username=caojiao
Password=9sTvwsLGmpmYjIyM8A

IndexSites=true
IndexLists=true
IndexFolders=true
IndexAttachments=true
IndexUserProfiles=false
MappedSecurity=true
EncryptACLEntries=true
//Domain=DOMAIN
IncludeProviderNameInACLs=true
GroupServerDebugOutputFile=SynchronizeGroupsDEBUG.log
ScheduleCycles=-1
UseEmailAsGroupName=true
```

3. Restart your SharePoint Connector Server.
4. (Mixed mode only) If you want to use OMNI Group Server (for Security SharePoint), continue with the following steps. Otherwise, go to Task 4.

> The fully containerized mode does not support OMNI Group Server for SharePoint Connector.

   a. Go to <SharePoint Installation directory>/OmniGroupServer, and then open the OmniGroupServer.cfg file with a text editor.
   b. Configure the [LDAP] and [Sharepoint] sections as needed.

```
[LDAP]
ActiveDirectory=True
GroupServerLibrary=ogs_ldap.dll
//GroupServerCycles=1
LDAPServer=S81W0060.asiapacific.hpqcorp.net
LDAPPort=389
LDAPUserBase=OU=CN,OU=Users,OU=Accounts,DC=asiapacific,DC=cpqcorp,DC=net
LDAPGroupBase=CN=PDL-HPSW-RnD-SH-SM@hp.com,OU=Managed Groups,OU=Accounts,DC=asiapacific,DC=cpqcorp,DC=net
//UserFilter=(objectClass=hpEmployee)
//GroupFilter=(objectClass=hpGroup)
LDAPUsername=jiao.cao@hpe.com
LDAPPassword=9sTvwsLGmpmYjIyM8A

ExtractDomainFromDN=true
LDAPMode=Group
PageSize=10000
KeyUserName=sAMAccountName
LDAPEnableReverseLookup=true
```

```
103  [SharePoint]
104  GroupServerJobType=Connector
105  ConnectorHost=127.0.0.1
106  ConnectorPort=36000
107  ConnectorTask=MyTask
108
```

c. Restart the OMNI Group Server.
d. Go to the Mix Proxy directory in Container (for example, /var/vols/itom/itsma/itsma-itsma-smartanalytics/config/idol/st/mixProxy), and then edit the proxy.cfg file.
e. Uncomment **GooupServerHost** and **GroupServerPort**, and then update the values to OMNI Group Server Host and Port, respectively.

```
474  [SharePoint]
475  // Authentication
476  Library=C:\Program Files (x86)\HP\Service Manager 9.41\SmartAnalytics/modules/user_ldapsecurity
477  V4=TRUE
478  EnableLogging=TRUE
479  DocumentSecurity=True
480  CaseSensitiveUserNames=False
481  CaseSensitiveGroupNames=False
482  SecurityFieldCSVs=username,group
483  DocumentSecurityType=SharePoint
484  GroupServerHost=16.187.189.94
485  GroupServerPort=5057
486  GroupServerRepository=Combine
487  //SyncRolesFromGroups=true
488  EnableLogging=TRUE
489  EscapedEntries=true
```

f. Restart the Mix Proxy server.

> Run the following commands on the master node to stop the Mix Proxy server:
>
> **kubectl get pod --all-namespaces | grep smarta-mix-proxy**
>
> **kubectl delete pod <pod_name> -n <namespace>**

Task 3: Configure the CFS connector, Smart Analytics server host, and port

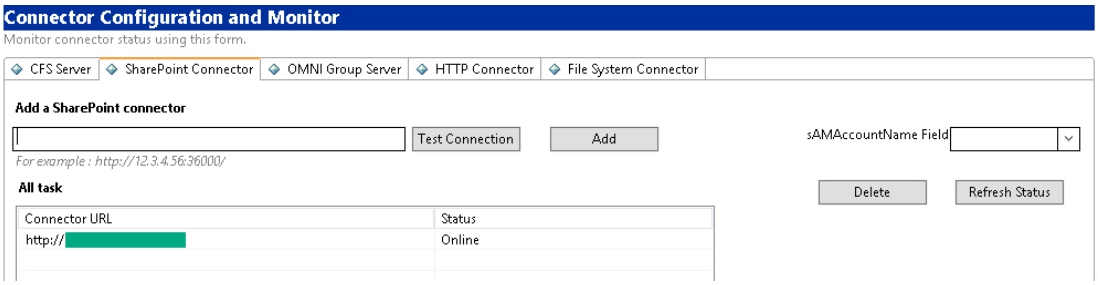
To modify the existing configuration and connect to Smart Analytics in Container, follow these steps:

1. Go to <CFS Installation directory>/CFS, and then open the CFS.cfg file with a text editor.
2. Locate the [IdolServer] section, and then modify the host and port as follows:

   [IdolServer]
   Host=<EXTERNAL_ACCESS_HOST>
   Port=31370
   DefaultDatabaseName=News
   //SSLConfig=SSLOption1
3. Save your changes, and then restart the CFS service.

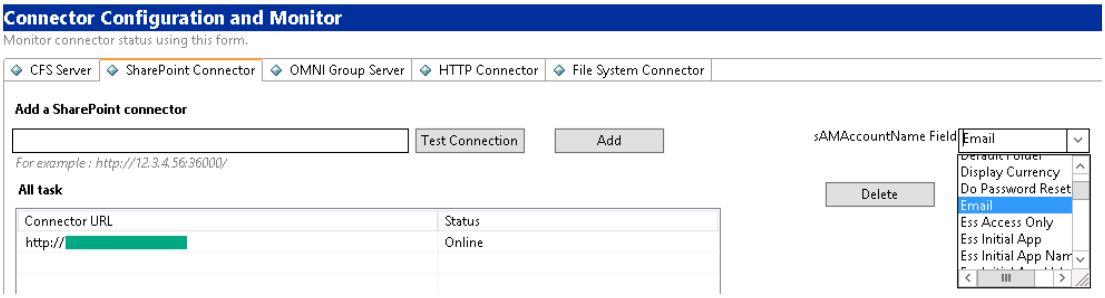
Task 4: Configure SharePoint Connector in Service Manager

1. Log on to Service Manager, and then click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Search**. The Smart Search configuration page opens.
2. Click the **Connector Configuration** link to open the connector configuration page.
3. Go to the SharePoint Connector tab, and then perform the following actions:
   a. Type a configured SharePoint connector URL in the Add a SharePoint connector field (for example: http://192.168.255.255:36000/). You can skip this step if you have configured this URL in Service Manager before.



> The "/" at the end of the URL is mandatory. Make sure that SharePoint is online.

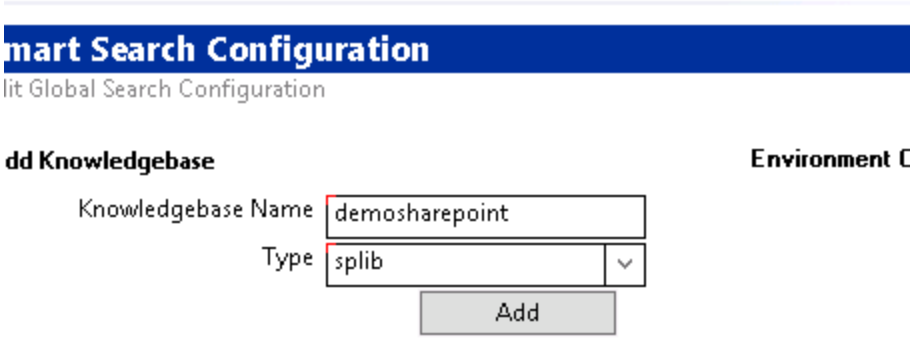
b. Choose the field type from the sAMAccountName Field drop-down list. This field is the mapping field of SharePoint and Service Manager users.



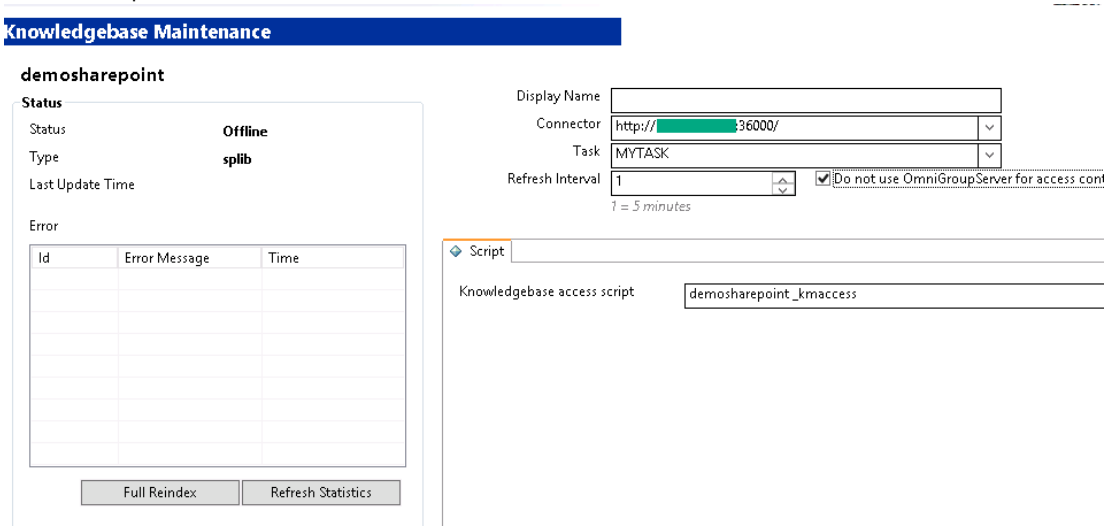
4. (For Security SharePoint) Go to <SharePoint Installation directory>/OmniGroupServer, and then open the OmniGroupServer.cfg file with a text editor.
5. Set the value of FieldName0 to the option you selected for the **sAMAccountName Field** drop-down list.

```
ExtractDomainFromDN=true
LDAPMode=Group
PageSize=10000
KeyUserName=sAMAccountName
LDAPEnableReverseLookup=true

KeyGroupName=mail
KeyMember=member
LDAPDebugLogging=TRUE
FieldKey0=sAMAccountName
FieldName0=Email
FieldKey1=mail
FieldName1=mail
FieldKey2=cn
FieldName2=cn
GroupServerMaxDatastoreQueue=100000
//remove domain prefix for groups
GroupServerOp0=StartAfter
GroupServerOpParam0=0;\
GroupServerOpApplyTo0=GROUP
//Just to avoid unnecessary queries for members that don't exist.
//This might not have any effect if the group members are properly managed.
DisableUserFromDNSearch=TRUE
DisableGroupFromDNSearch=TRUE
```

6. Restart the Omni Group server.
7. Do the following to add a splib library for the SharePoint connector. You can skip this step if you have added a splib library in Service Manager before.
   a. Open the Smart Search Configuration page.
   b. Enter the Knowledgebase Name.
   c. Select splib in the Type drop-down list.
   d. Click **Add**. The Knowledgebase Maintenance page opens.



8. Enter a Connector and Task, and then select the **Do not use OmniGroupServer for access count** check box if you are not configuring an Omni Group Server.



9. Click **Save**.
10. Click **Full Reindex** and **Refresh Status**.

> You need to create multiple libraries for each task if you have configured multiple tasks in the SharepointRemoteConnector.cfg file.

11. You can perform a search when the status changes to Indexing and the Doc Count for this library is greater than 1.

> Log off and then log back on to Service Manager if you can not find the library in your Smart Search library list.

Configure HTTP Connector

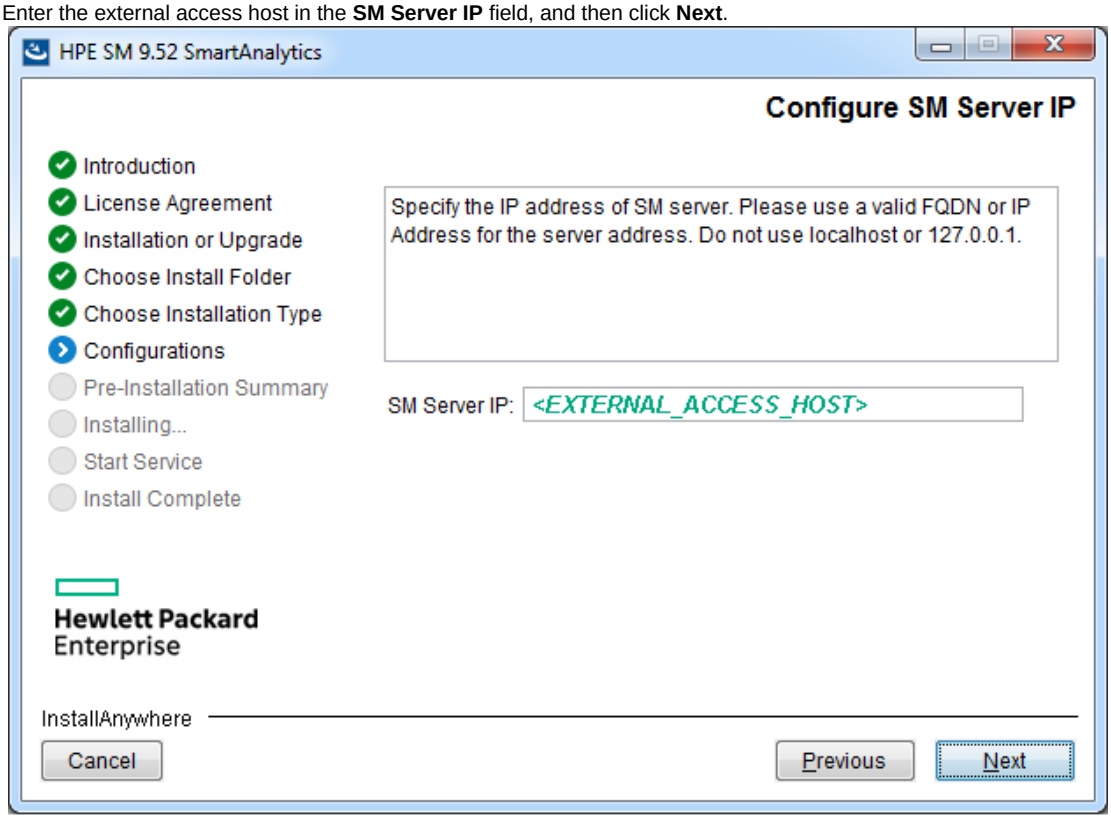
> - If you have never installed Smart Analytics HTTP connectors before, perform Task 1, Task 2, and Task 4.
> - If you have already installed and configured HTTP Connector with CFS server, perform Task 3 and Task 4 (Step 5 and Step 6).

To enable search actions in web sites, you must install and configure the HTTP Connector with CFS out of Container. To do this, perform the following tasks:

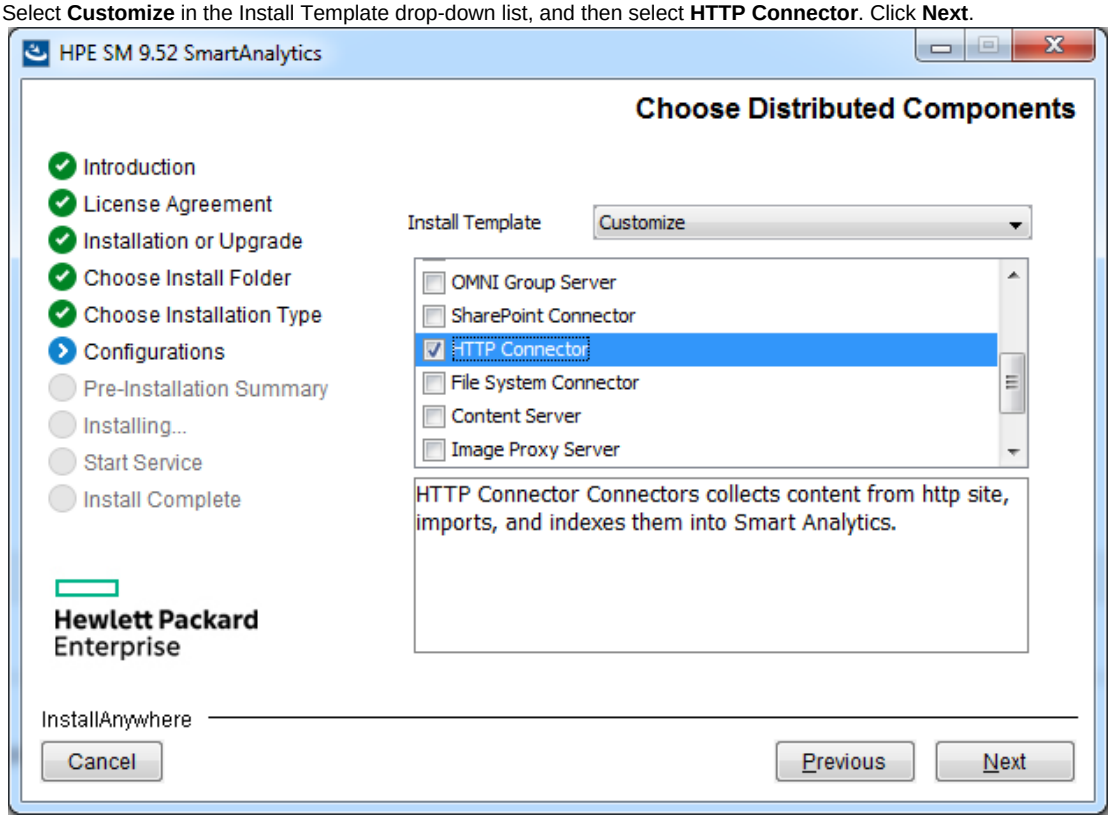
Task 1: Install HTTP Connector with a CFS server

1. Download the Smart Analytics 9.52 installer from http://www.hpe.com/software/entitlements, and then unzip this installation package.
2. Unpack the .zip file and then double-click the setup application (setupSmartAnalyticsWindowsX64.exe).
3. The HPE Service Manager 9.52 SmartAnalytics Setup wizard opens. Read the introduction, and then click **Next**.
4. Read the License Agreement. To continue the installation, select **I accept the terms of the License Agreement**, and then click **Next**.
5. Select **New Installation**, and then click **Next**.
6. Choose an installation folder, and then click **Next**. The default installation folder is C:\Program Files(x86)\HPE\Service Manager 9.52\SmartAnalytics.

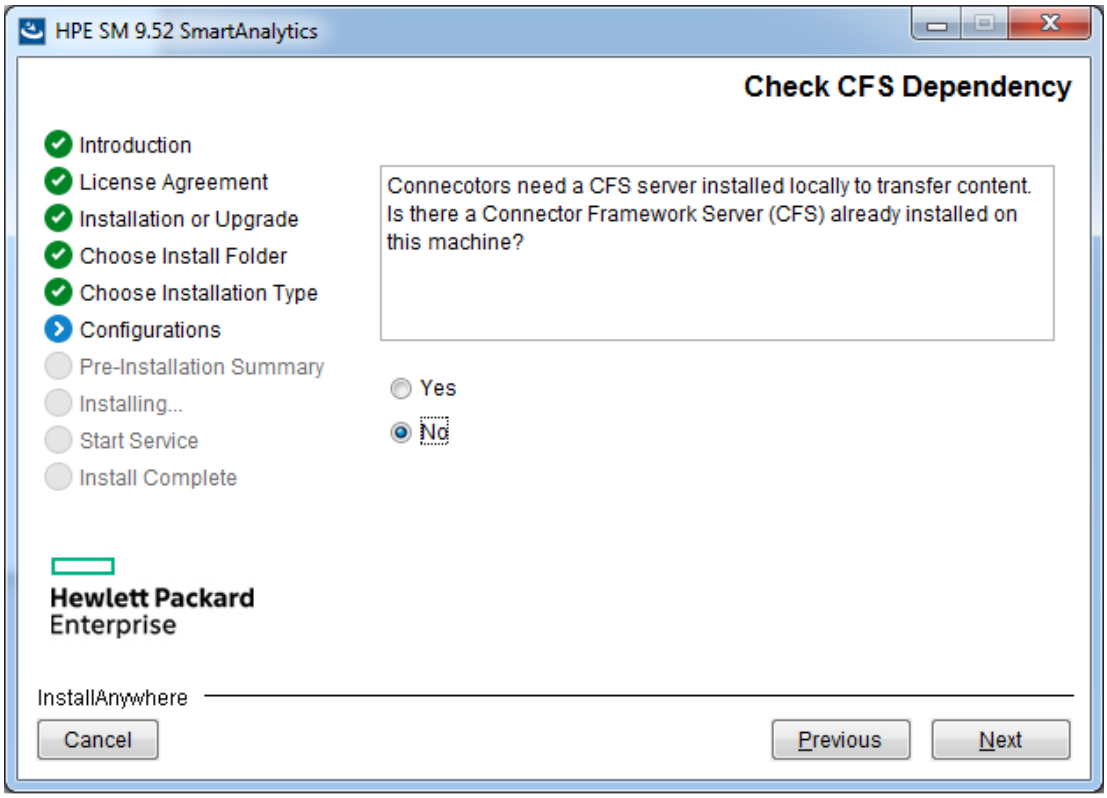
7. Select **Advanced Install** as your installation type, and then click **Next**.
8. Enter the external access host in the **SM Server IP** field, and then click **Next**.



9. Select **Customize** in the Install Template drop-down list, and then select **HTTP Connector**. Click **Next**.

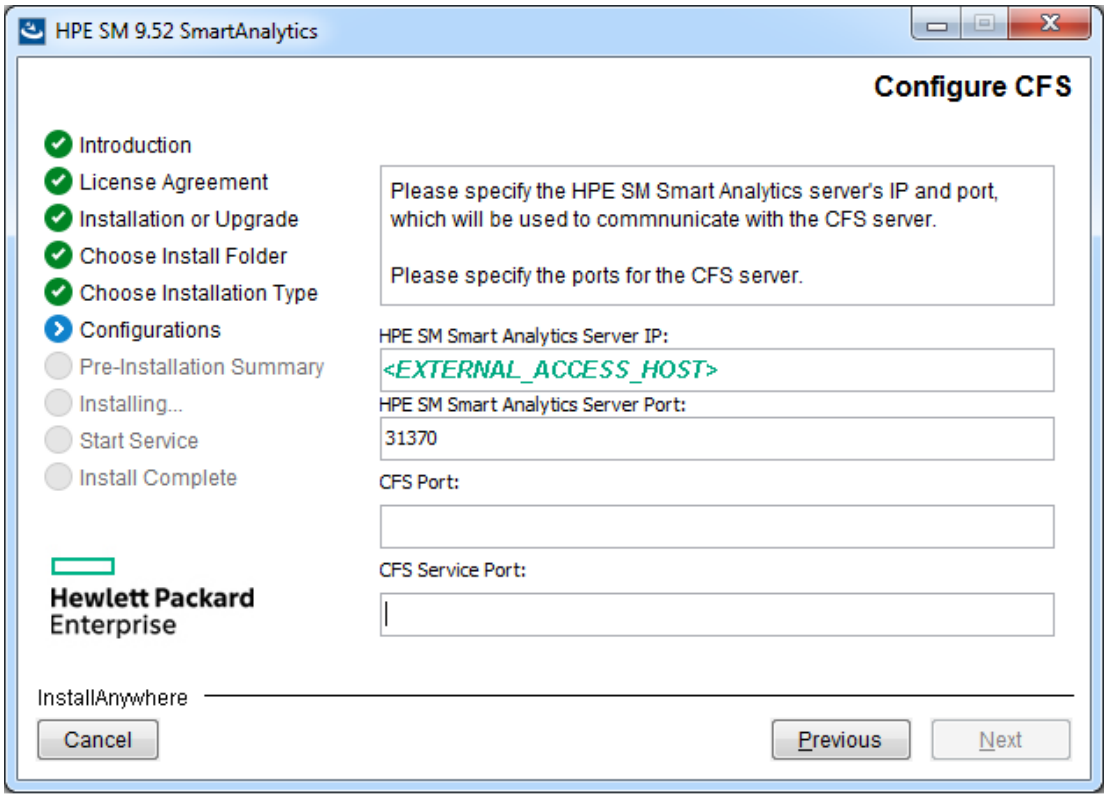


10. Select **No** if there are no CFS servers installed on this computer. Otherwise, select **Yes**.



> You must install the external HTTP connector and the CFS server on the same computer.

11. Enter the Service Manager Smart Analytics Server IP and port as follows, and then enter the CFS Server port and Service port. Click **Next**.
    Service Manager Smart Analytics Server IP: **<EXTERNAL_ACCESS_HOST>**
    Service Manager Smart Analytics Server Port: **31370**
    CFS Port: **7000**
    CFS Service Port: **7001**



If you have modified the CFS Port from 7000 to another, you need to update the value for the IngestPort parameter to the modified port number in the Connector configuration file (such as httpconnector.cfg). The file should resemble the following:
[Ingestion]
IngestHost=127.0.0.1
IngestPort=7000

12. Configure the HTTP Connector Server Port and HTTP Connector Service Port, and then click **Next**.
13. Click **Install** to install the HTTP Connector and CFS Server.

Task 2: Configure the httpconnector.cfg file

1. Go to <HTTP Connector Installation directory>/HTTPConnector, and then open the HTTPConnector.cfg file with a text editor.
2. Configure the [FetchTasks] and [MYSITE] sections as needed.

```
55  [FetchTasks]
56  Number=1
57  0=MYSITE
58
59  [MYSITE]
60  URL=https://en.wikipedia.org/wiki/Main_Page
61  DIRECTORY=HTTPconnector
62  CantHaveCSVs=*.css,*.js
63  CantHaveCheck=1
64  //StayOnSite=True
65  //Depth=99
66  ProxyHost=proxy.[redacted].com
67  ProxyPort=8080
68  //FOLLOWROBOTPROTOCOL=FALSE
69  //----Login with form----
70  //LOGINMETHOD=FORMPOST
71  //LOGINURL=https://login.com/
72  //LOGINUSERFIELD=os_username
73  //LOGINUSERVALUE=USERNAME@COMPANY.COM
74  //LOGINPASSFIELD=os_password
75  //LOGINPASSVALUE=PASSWORD_ENCRYPTED
76  //LoginSubmitField=ButtonID
77  //----HTTP digest authentication----
78  //DigestUsername=USERNAME
79  //DigestPassword=PASSWORD_ENCRYPTED
80  //----NTLM authentication----
81  //NTLMUsername=USERNAME
82  //NTLMPassword=PASSWORD
```

3. (Optional) To configure multiple tasks, configure the .cfg file as follows:

   [FetchTasks]
   Number=2
   0=MYSITE1
   1=MYSITE2
   [MYSITE1]
   ...
   [MYSITE2]
   ...
   The file should resemble the following:

```
[FetchTasks]
Number=2
0=MYSITE
1=WikibyJ

[MYSITE]
URL=https://en.wikipedia.org/wiki/Main_Page
DIRECTORY=HTTPconnector
CantHaveCSVs=*.css,*.js
CantHaveCheck=1
//StayOnSite=True
//Depth=99
ProxyHost=proxy.[redacted].com
ProxyPort=8080
//FOLLOWROBOTPROTOCOL=FALSE
//----Login with form----
//LOGINMETHOD=FORMPOST
//LOGINURL=https://login.com/
//LOGINUSERFIELD=os_username
//LOGINUSERVALUE=USERNAME@COMPANY.COM
//LOGINPASSFIELD=os_password
//LOGINPASSVALUE=PASSWORD_ENCRYPTED
//LoginSubmitField=ButtonID
//----HTTP digest authentication----
//DigestUsername=USERNAME
//DigestPassword=PASSWORD_ENCRYPTED
//----NTLM authentication----
//NTLMUsername=USERNAME
//NTLMPassword=PASSWORD

[WikibyJ]
URL=https://en.wikipedia.org/wiki/Main_Page
DIRECTORY=HTTPconnector
CantHaveCSVs=*.css,*.js
CantHaveCheck=1
//StayOnSite=True
//Depth=99
ProxyHost=proxy.[redacted].com
ProxyPort=8080
//FOLLOWROBOTPROTOCOL=FALSE
//----Login with form----
```

4. Restart the HTTP Connector Server.

Task 3: Configure the CFS connector, Smart Analytics server host, and port

To modify the existing configuration and connect to containerized Smart Analytics, follow these steps:

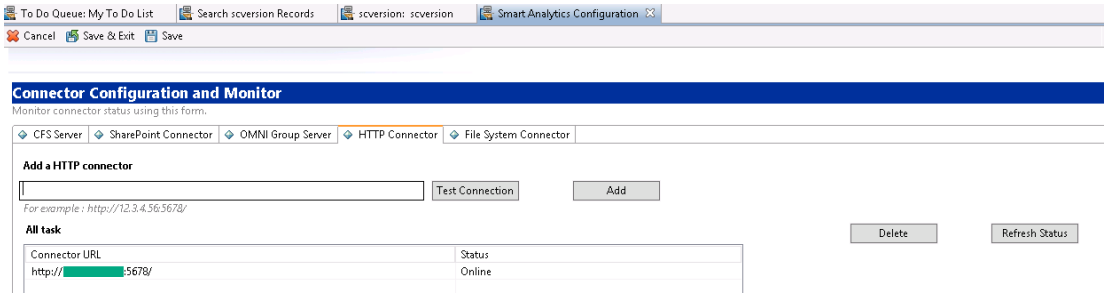
1. Go to <CFS Installation directory>/CFS, and then open the CFS.cfg file with a text editor.
2. Locate the [IdolServer] section, and then modify the host and port as follows:

   ```
   [IdolServer]
   Host=<EXTERNAL_ACCESS_HOST>
   Port=31370
   DefaultDatabaseName=News
   //SSLConfig=SSLOption1
   ```
3. Save your changes, and then restart the CFS service.

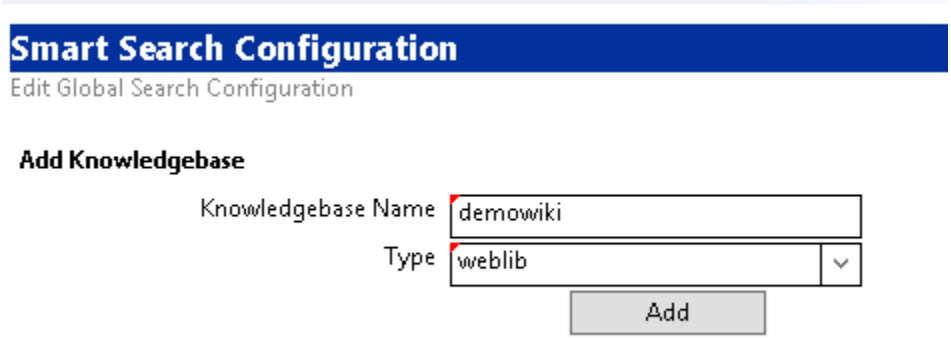
Task 4: Configure HTTP Connector in Service Manager

1. Log on to Service Manager, and then click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Search**. The Smart Search configuration page opens.
2. Click the **Connector Configuration** link to open the connector configuration page.
3. Go to the **HTTP Connector** tab, perform the following actions:
    a. Type a configured HTTP connector URL in the **Add a HTTP connector** field, for example: http://192.168.255.255:5678/. You can skip this step if you have configured this URL in SM before.

> The "/" at the end of the URL is mandatory.
> Make sure the HTTP Connector's status is online.

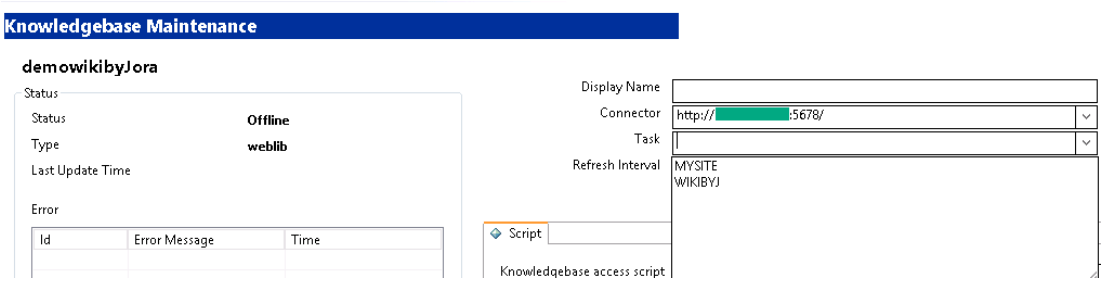


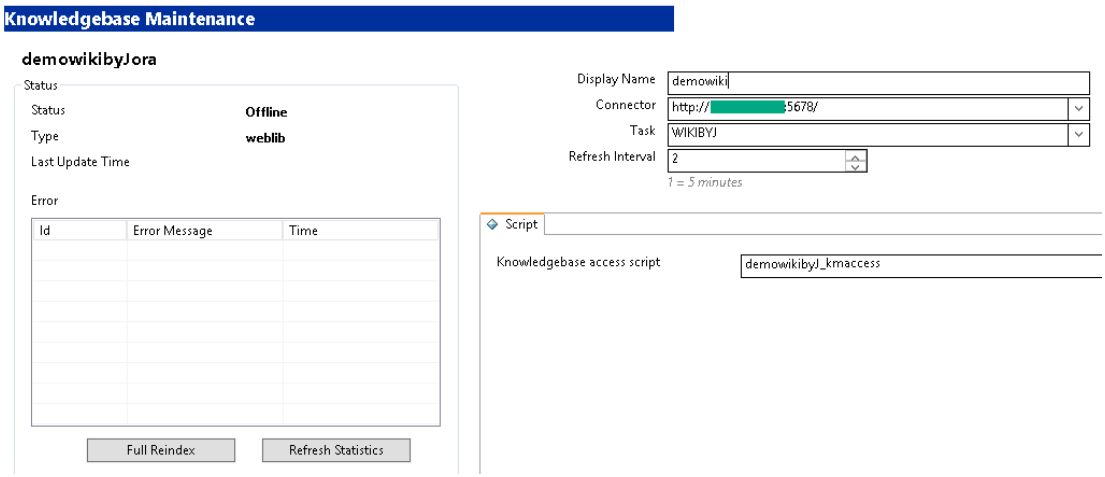
    b. You can click **Test connection** to test the URL connection status, and click **Add** to add this URL to the current list.
4. Add a weblib library for the sharepoint connector (you can skip this step if you have added a weblib library to Service Manager before). To do this, follow these steps:
    a. Go to the Smart Search Configuration page.
    b. Enter a Knowledgebase Name.
    c. Select weblib in the Type drop-down list.
    d. Click **Add**. The Knowledgebase Maintenance page opens.



5. Enter a Connector and Task, and then click **Save**.
6. Click **Full Reindex** and **Refresh Status**.

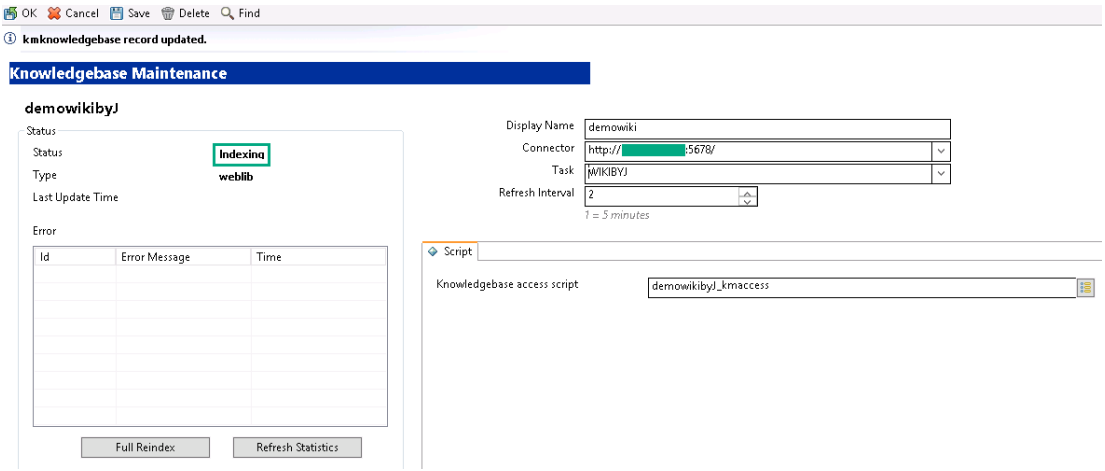
> You need to create multiple libraries for each task if you have configured multiple tasks in the HTTPConnector.cfg file.





7. You can perform a search when the status changes to Indexing and the Doc Count for this library is greater than 1.

> Log off and then log back on to Service Manager if you can not find the library in your Smart Search library list.



Current Knowledgebase List

Knowledgebase Na...	Type	Display Name	Interval	Index Status	Doc Count	Last Index Time
Catalog_Library	sclib	Catalogs	1	Finished		11/05/15 22:11:07
Change_Library	sclib	Changes	1	Finished	36	11/05/15 22:11:11
Contact_Library	sclib	Contacts	1	Finished		11/05/15 22:11:49
Department_Library	sclib	Departments	1	Offline		
Device_Library	sclib	Configuration Items	1	Offline		
Incident_Library	sclib	Incidents	1	Finished		11/05/15 03:35:12
Interaction_Library	sclib	Interactions	1	Finished		11/05/15 03:35:22
Knowledge_Library	sclib	Knowledge Library	1	Finished		11/11/15 02:07:40
KnownError_Library	sclib	Known Errors	1	Offline		
Location_Library	sclib	Locations	1	Offline		
Problem_Library	sclib	Problems	1	Offline	2	
Request_Library	sclib	Requests	1	Offline		
demowikibyJora	weblib	demowiki	2	Indexing	100	

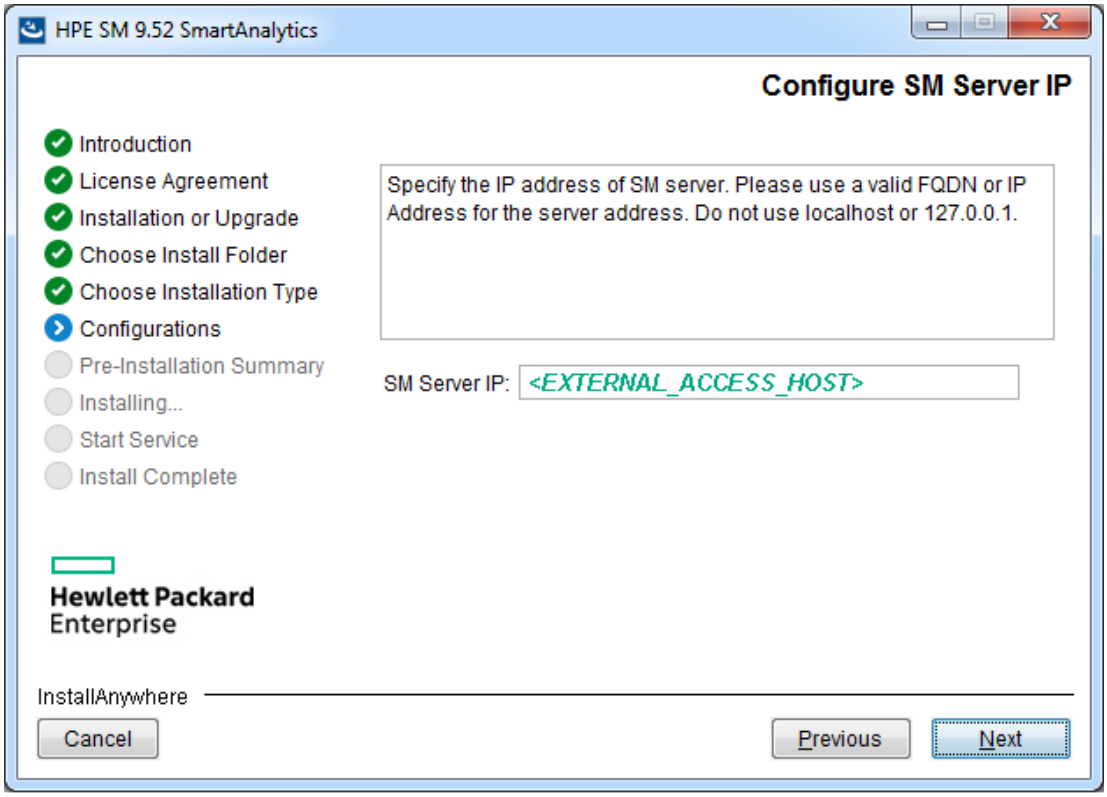
Configure File System Connector

> - If you have never installed Smart Analytics File System connectors before, perform Task 1, Task 2, and Task 4.
> - If you have already installed and configured File System Connector with CFS server, perform Task 3 and Task 4 (Step 5 and Step 6).

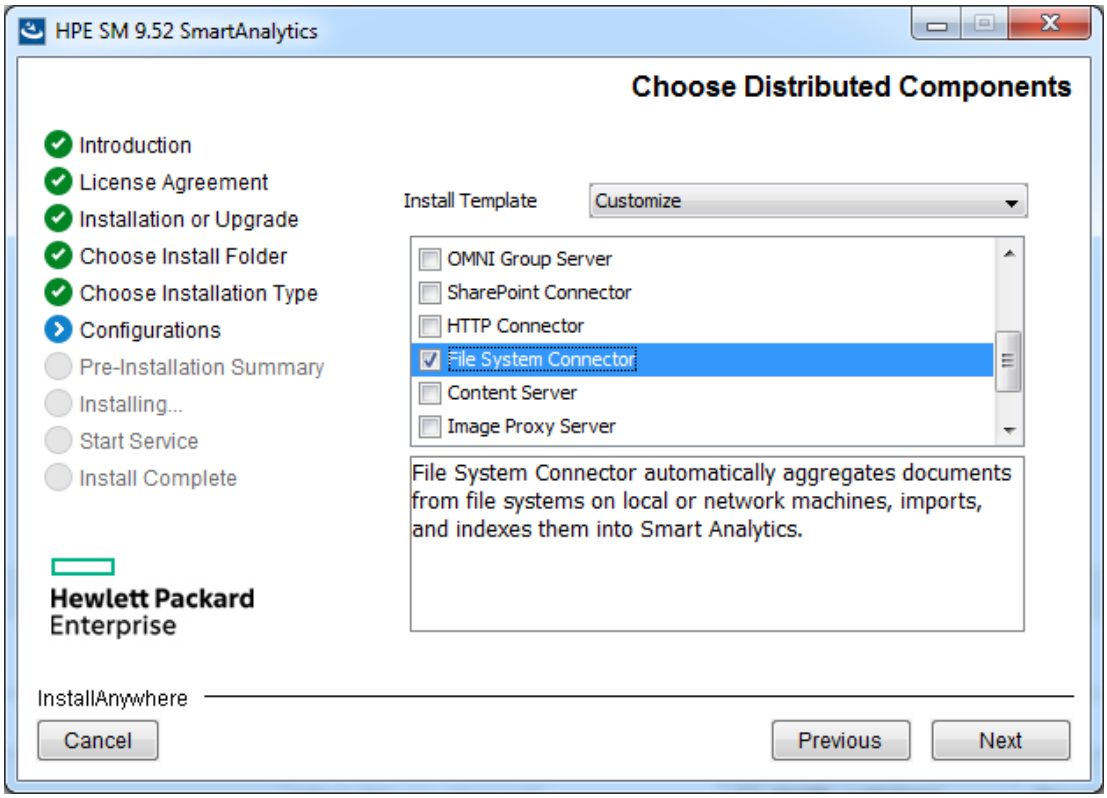
To enable search actions in file systems, you must install and configure the File System Connector with CFS out of Container. To do this, perform these tasks:

Task 1: Install File System Connector with a CFS server

1. Download the Smart Analytics 9.52 installer from http://www.hpe.com/software/entitlements, and then unzip this installation package.
2. Unpack the .zip file and then double-click the setup application (setupSmartAnalyticsWindowsX64.exe).
3. The HPE Service Manager 9.52 Smart Analytics Setup wizard opens. Read the introduction, and then click **Next**.
4. Read the License Agreement. To continue the installation, select **I accept the terms of the License Agreement**, and then click **Next**.
5. Select **New Installation**, and then click **Next**.
6. Choose an installation folder, and then click **Next**. The default installation folder is C:\Program Files(x86)\HPE\Service Manager 9.52\SmartAnalytics.
7. Select **Advanced** Install as your installation type, and then click **Next**.
8. Enter the external access host in the **SM Server IP** field, and then click **Next**.

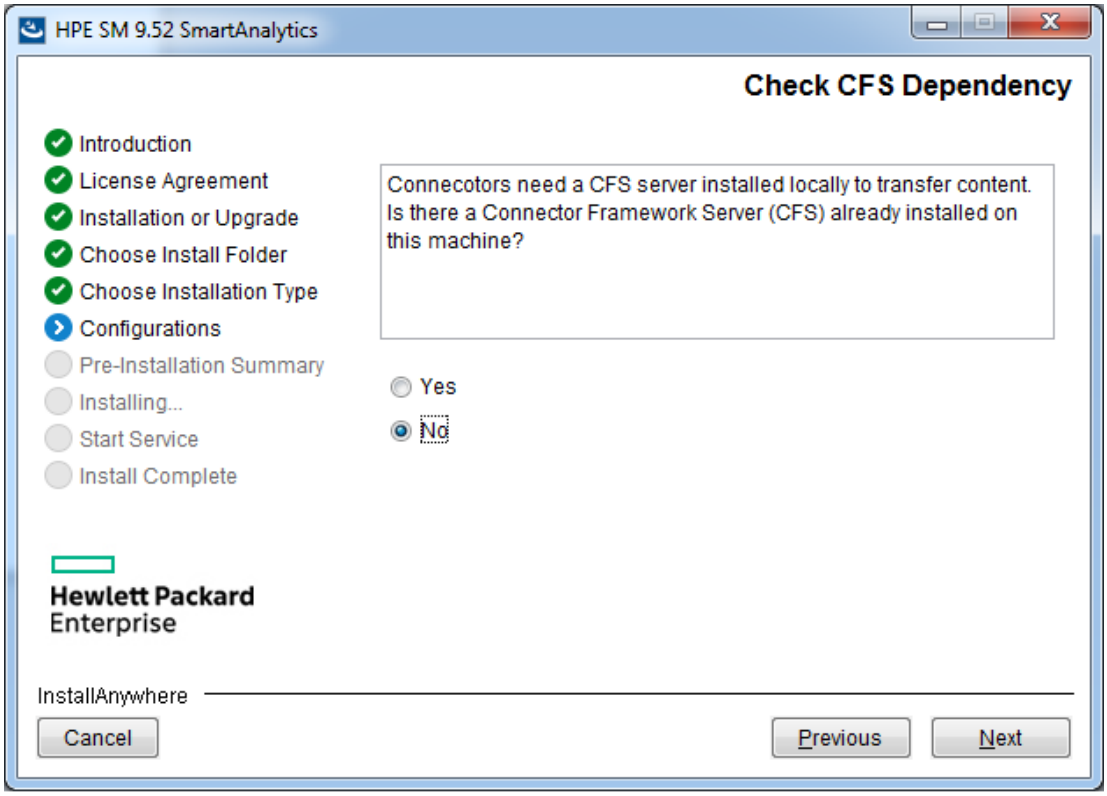


9. Select **Customize** in the Install Template drop-down list, and then select **File System Connector**. Click **Next**.



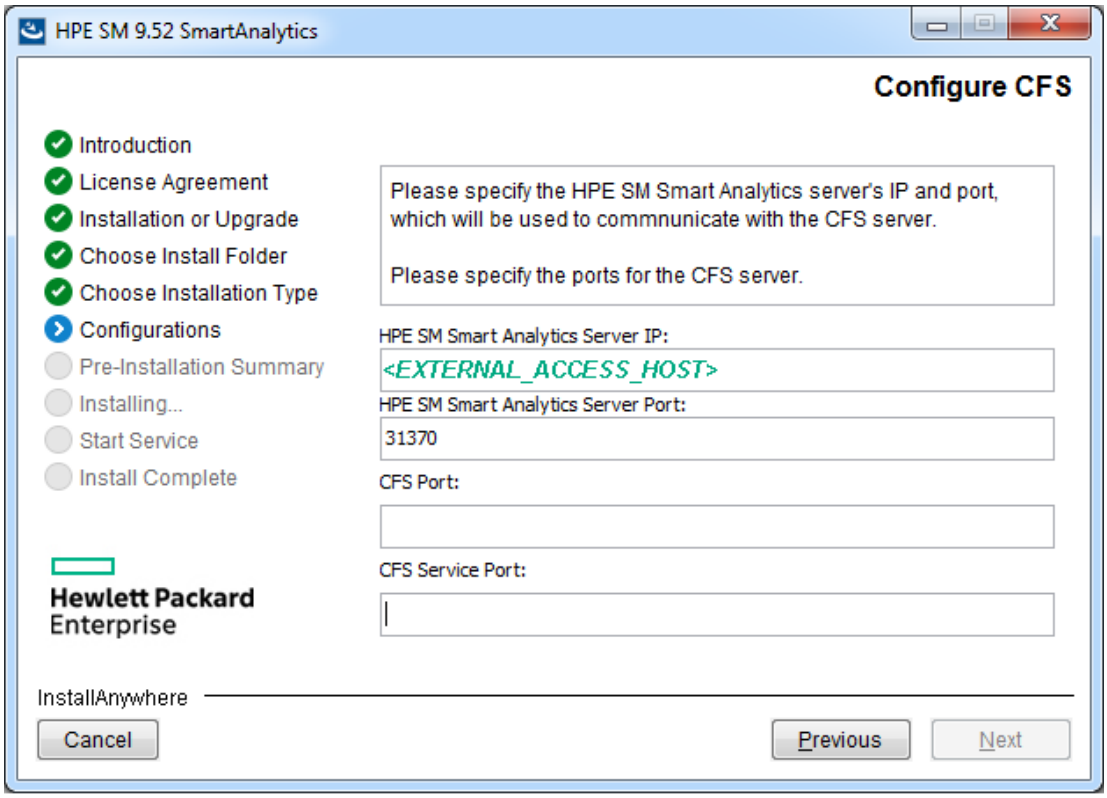
10. Select **No** if there are no CFS servers installed on this computer. Otherwise, select **Yes**.

> You must install the external File System connector and the CFS server on the same computer.



11. Enter the Service Manager Smart Analytics Server IP and port as follows, and then enter the CFS Server port and Service port. Click **Nex t**.
    SM Smart Analytics Server IP: **<EXTERNAL_ACCESS_HOST>**

SM Smart Analytics Server Port: **31370**
CFS Port: **7000**
CFS Service Port: **7001**



> If you have modified the CFS Port from 7000 to another, you need to update the value for the IngestPort parameter to the modified port number in the Connector configuration file (such as filesystemconnector.cfg). The file should resemble the following:
> [Ingestion]
> IngestHost=127.0.0.1
> IngestPort=7000

12. Configure File System Connector Server Port and Service Port, and then click **Next**.
13. Click **Install** to install the File System Connector and CFS Server.

Task 2: Configure the filesystemconnector.cfg file

1. Go to <File System Connector Installation directory>/FileSystemConnector, and then open the filesystemconnector.cfg file with a text editor.
2. Configure the [FetchTasks] and [MyTask] sections as needed.

```
[FetchTasks]
Number=1
0=MyTask

[MyTask]
//specifies the interval (in seconds) between scheduled synchronize actions.
ScheduleRepeatSecs=300
//specifies whether the connector searches sub-folders.
DirectoryRecursive=TRUE
//The DirectoryPathCSVs parameter specifies a comma-separated list of folders to search for files.
DirectoryPathCSVs=\\J7\ShareDirectory
//A regular expression that specifies the folders to search for files. The connector only searches folders:
//that are within the location specified by DirectoryPathCSVs
//where the full path of the folder matches the regular expression
//where the full path of all parent folders (up to the folder specified by DirectoryPathCSVs) match the regular expression.
PathCrawlRegex=.*
//A regular expression that specifies the folders to ignore. The connector ignores any folders where the path matches the regular expression.
//If a folder is ignored, all of its subfolders are also ignored.
//PathNoCrawlRegex=
//The DirectoryFileMatch parameter limits the files that are retrieved by the connector. The value of this parameter is a wildcard expression
//The filename of a file must match the wildcard expression, otherwise the file is ignored. default to all files
DirectoryFileMatch=*.pdf,*.doc,*.ppt,*.txt,*.log

```

3. Restart your File System Connector Server.

Task 3: Configure the CFS connector, Smart Analytics server host, and port

To modify the existing configuration and connect to containerized Smart Analytics, follow these steps:

1. Go to <CFS Installation directory>/CFS, and then open the CFS.cfg file with a text editor.
2. Locate the [IdolServer] section, and then modify the host and port as follows:

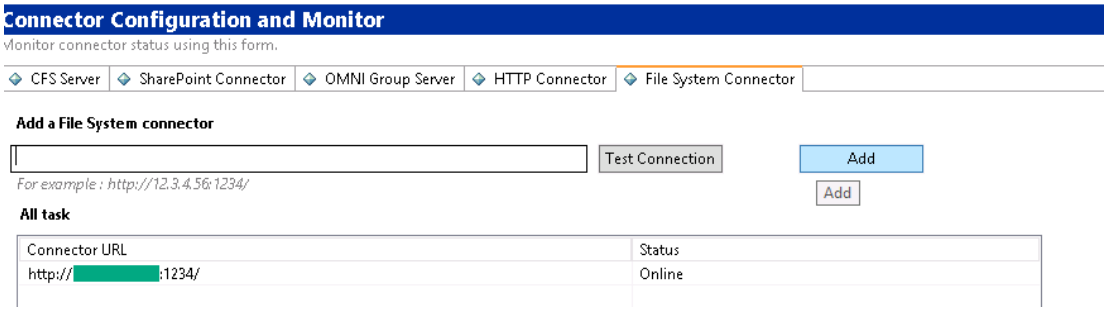
   ```
   [IdolServer]
   Host=<EXTERNAL_ACCESS_HOST>
   Port=31370
   DefaultDatabaseName=News
   //SSLConfig=SSLOption1
   ```
3. Save your changes, and then restart the CFS service.

Task 4: Configure File System Connector in SM

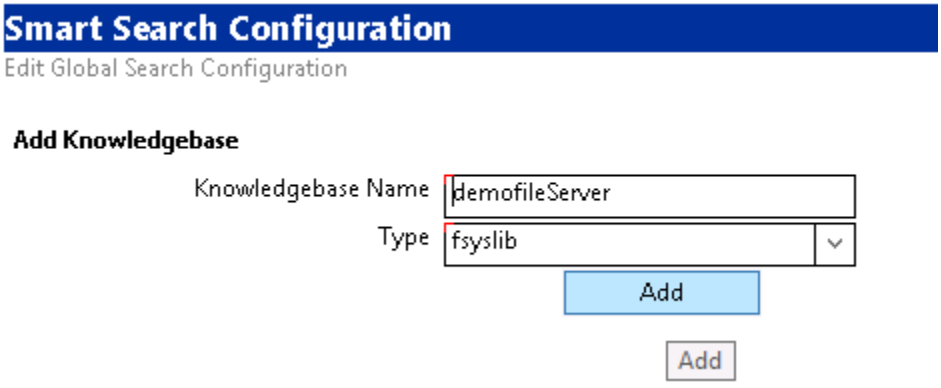
Log on to Service Manager, and then click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Search**. The Smart Search configuration page opens.

1. Click the **Connector Configuration** link to open the connector configuration page.
2. Go to the **File System Connector** tab, and then perform the following actions:
   a. Type a new file system connector URL in the **Add a File System connector** field (for example: http://192.168.255.255:1234/). You can skip this step if you have configured this URL in Service Manager before.

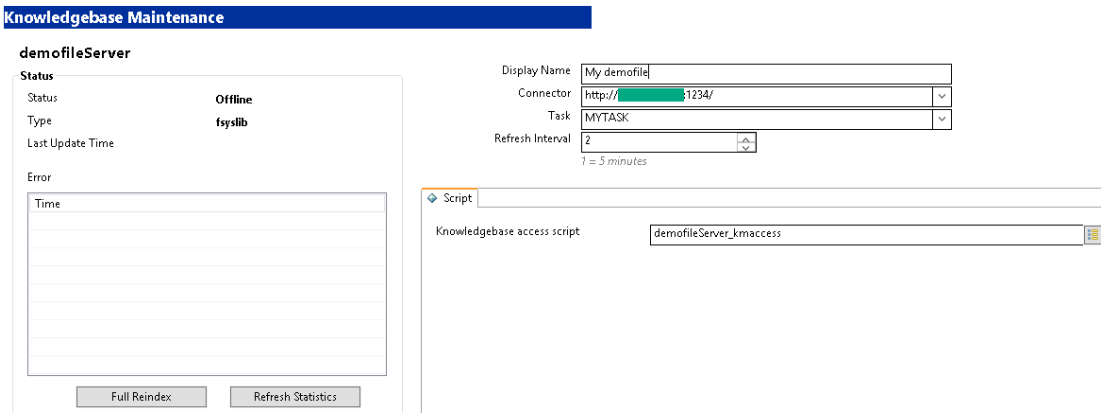
   > The "/" at the end of the URL is mandatory. Make sure the File System Connector's status is online.

   b. You can click **Test connection** to test the URL connection status, and click **Add** to add this URL to the current list.
3. Add a fsyslib library for the sharepoint connector (you can skip this step if you have added a fsyslib library in Service Manager before). To do this, follow these steps:
   a. Go to Smart Search Configuration page.
   b. Enter a Knowledgebase Name.
   c. Select fsyslib in the Type drop-down list.
   d. Click **Add**. The Knowledgebase Maintenance page opens.

4. Enter a Connector and Task, and then click **Save**.
5. Click **Full Reindex** and **Refresh Status**.



6. You can perform a search when the status changes to Indexing and the Doc Count for this library is greater than 1.

> Log off and then log back on to Service Manager if you can not find the library in your Smart Search library list.

Set stop words, stop phrases, and synonyms for Smart Analytics

This topic includes the following tasks:

- Update Smart Analytics stop words
- Set stop phrases for Hot Topic Analytics
  - Fully containerized mode
  - Mixed mode
- Update Smart Analytics synonyms

Update Smart Analytics stop words

To update Smart Analytics stop words, follow these steps:

1. On the master node, run the following command to access the <*Smart Analytics NFS root folder*>/data/idol/langfiles folder:
   cd <Smart Analytics NFS root folder>/data/idol/langfiles
   The stop words lists are saved as the <*language name*>.dat file in this folder.
2. Run the following command to add a new word or modify an existing word in a language file:
   vim <*language name*>.dat
3. Select ESC, and then enter **:wq** to save the changes and exit.
4. Restart all Smart Analytics services in the container. To do this, follow these steps:
   a. Run the **kubectl get pod --all-namespaces | grep smarta** command to get all Smart Analytics pod's status.
   b. Run the **kubectl delete pod <pod_name> -n <namespace>** command to stop the services.
5. Train and perform a full reindex of Smart Ticket, Hot Topic Analytics, and Smart Search. To do this, follow these steps:
   a. From Service Management, go to **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**. Select a record in the Current Configuration List, and then click the **Training** button.
   b. From Service Management, go to **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Hot Topic Analytics**. Select a record in the Current Configuration List, and then click the **Start Index** button.
   c. From Service Management, go to **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Search**. Select a record in the Current Configuration List, and then click the **Full Reindex** button.

Set stop phrases for Hot Topic Analytics

Adding stop phrases is a way to hide particular words or phrases from appearing in the Hot Topic Analytics topic map. The stop phrases are still retained in the Smart Analytics data set.

Fully containerized mode

To update stop phrases for Hot Topic Analytics in containerized mode, follow these steps:

1. From Service Management on the master node, click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Hot Topic Analytics**.
2. Click **Stop Phrase**. The **Configure IDOLStop Phrase** page opens.
3. Add the words or phrases that you identified as stop phrases to this page. These words or phrases must exactly match the key words to

find hot topics, and each word or phrase must start with a new line.

- Do not use wildcards in stop phrases.
- Stop phrases are case-sensitive by default, and the corresponding configuration is defined in the IDOL/IDOLServer.cfg file as follows:
  QuerySummaryStopPhraseMode=9

  To set the stop phrases to be case-insensitive, update the configuration as follows:
  QuerySummaryStopPhraseMode=41

4. Click **Save**. The system automatically saves the stop phrases in alphabetical order. Alternatively, you can click **Save & Exit** to close the **Configure IDOL Stop Phrase** page.
5. Run Hot Topic Analytics again. The stop phrases are no longer displayed in the topic map.

Mixed mode

External Service Manager 9.41, 9.50, and 9.51 with containerized Smart Analytics

To update stop phrases for Hot Topic Analytics in Mixed mode (external Service Manager 9.41, 9.50, and 9.51 with containerized Smart Analytics), follow these steps:

1. On the master node, run the following command to access the <Smart Analytics NFS root folder>/data/idol/st/content1/main folder:
   cd <Smart Analytics NFS root folder>/data/idol/st/content1/main
   The stop words lists are saved in the qssp.db file in this folder.
2. Run the following command to add a new word or modify an existing word:
   vim qssp.db
3. Select ESC, and then enter **:wq** to save the changes and exit.
4. Continue to follow *step 1* to *step 3* to update the file in the <*Smart Analytics NFS root folder*>/data/idol/st/content2/main folder.
5. Restart HPE Smart Analytics HTA and the containerized Smart Ticket content server. To do this, follow these steps:
   a. Run the **kubectl get pod --all-namespaces | grep smarta-st-con** command to get all content server pod's status.
   b. Run the **kubectl delete pod <pod_name> -n <namespace>** command to stop the services.

External Service Manager 9.52 with containerized Smart Analytics
To update stop phrases for Hot Topic Analytics (external Service Manager 9.52 with containerized Smart Analytics), see Fully containerized mode
.

Update Smart Analytics synonyms

To update Smart Analytics synonyms, follow these steps:

1. On the master node, run the following command to access the <*Smart Analytics NFS root folder*>/config/idol/synonym folder:
   cd <Smart Analytics NFS root folder>/config/idol/synonym
   The synonyms are saved in the synonyms.txt file in this folder.
2. Run the following command to add a new word or to modify an existing synonym in this file:
   vim synonyms.txt
3. Select ESC, and then enter **:wq** to save the changes and exit.
4. Restart all Smart Analytics services in the container. To do this, follow these steps:
   a. Run the **kubectl get pod --all-namespaces | grep smarta** command to get all Smart Analytics pod's status.
   b. Run the **kubectl delete pod <pod_name> -n <namespace>** command to stop the services.
5. Train and perform a full reindex of Smart Ticket, Hot Topic Analytics, and Smart Search. To do this, follow these steps:
   a. From Service Management, go to **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**. Select a record in the Current Configuration List, and then click the **Training** button.
   b. From Service Management, go to **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Hot Topic Analytics**. Select a record in the Current Configuration List, and then click the **Start Index** button.
   c. From Service Management, go to **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Search**. Select a record in the Current Configuration List, and then click the **Full Reindex** button.

Roll back from containerized Smart Analytics

The Smart Analytics migration tool consists of three scripts: 1-StopSMApods.sh, 2-MergeConfiguration.sh, and 3-StartSMApodsRestoreContentData.sh. Your roll-back procedures varies depending on which scripts you have executed in the migration process. See the following scenarios:

- If you have executed 1-StopSMApods.sh only, perform step 4 and 7.
- If you have executed both 1-StopSMApods.sh and 2-MergeConfiguration.sh, perform step 1, 2, 3, 4, and 7.
- If you have executed all three scripts, perform all the following steps.

Follow these steps to roll back Smart Analytics data:

Step 1: Recover configuration files

1. Log on to the NFS server.
2. Browse to the <Smart_Analytics_NFS>/config/idol directory, and then search for all files whose names end with "cfg_backup". For example, Content.cfg_backup.
3. Run the **mv -f <File_Name>.cfg_backup <File_Name>.cfg** command.

The following list includes some typical backup files:

./ss/content1a/Content.cfg_backup
./ss/content1b/Content.cfg_backup
./ss/content2a/Content.cfg_backup
./ss/content2b/Content.cfg_backup
./st/content1/Content.cfg_backup
./st/content2/Content.cfg_backup
./st/mixProxy/proxy.cfg_backup

Step 2: Recover stop words, stop phrases, and synonyms

1. Log on to the NFS server.
2. Browse to the <Smart_Analytics_NFS>/data/idol/langfilese directory, and then run the **find . -name *.dat_backup** command to search for all files whose names end with "dat_backup".
3. Run the **mv -f <File_Name>.dat_backup <File_Name>.dat** command to recover stop words.
   The following list includes some typical backup files:

   ./russian.dat_backup
   ./portuguese.dat_backup
   ./arabic.l-r.dat_backup
   ./chinese.dat_backup
   ./czech.dat_backup
   ./dutch.dat_backup
   ./english.dat_backup
   ./french.dat_backup
   ./german.dat_backup
   ./hebrew.dat_backup
   ./hungarian.dat_backup
   ./italian.dat_backup
   ./japanese.dat_backup
   ./polish.dat_backup
   ./spanish.dat_backup
   ./swedish.dat_backup
   ./turkish.dat_backup
4. Browse to the <Smart_Analytics_NFS>/data/st/content1/main directory and the <Smart_Analytics_NFS>/data/st/content2/main direct ory, and then run the **mv -f qssp.db_backup qssp.db** command in the two folders respectively to recover the stop phrases.
5. Browse to the <Smart_Analytics_NFS>/config/idol directory, and then run the **mv -f ./synonym/synonym.txt_backup ./synonym/synonym.txt** command to recover the synonyms.

Step 3: Recover Smart Ticket data

1. Log on to the NFS server.
2. Browse to the <Smart_Analytics_NFS>/data/idol/mix/proxy/category directory.
3. Run the following commands:
   rm -rf category
   mv -r category_backup category

Step 4: Restart all related components

1. Log on to the ITSMA suite master node, and then browse to the folder in which 2-MergeConfiguration.sh is located.
2. Run the following command:
   for i in `ls yamls`; do if [[$i = "ss"* || $i = "st"*]]; then kubectl create -f yamls/$i; fi done
3. Run the following command to check the pods' status:
   kubectl get pods --all-namespaces | grep smarta
4. When all pods' status is Running, run the following commands:
   kubectl create -f yamls/l2proxy.yaml
   kubectl create -f yamls/proxy.yaml

Step 5: Recover Hot Topic Analytics data

1. Log on to the ITSMA suite master node, and then run the following command to get a list of Hot Topic Analytics content server pods.
   kubectl get pods --all-namespaces | grep st-con
   For example:

NAME	READY	STATUS	RESTARTS	AGE
smarta-st-con-1-3678744724-mf0dd	1/1	Running	0	1h
smarta-st-con-2-1017065627-tkt9w	1/1	Running	2	4h

2. Run the following command to enter the pod:
   kubectl exec -it <NAME> -n <NAMESPACE> sh

3. Browse to the /var/data directory, and then run the **ls** command to find all files in the folder.
   There should be at least one file with the name of Backup-<TIME>-smarta-st-con-1-<RANDOM>-10010-0.idx. Record the name.
4. Run the following command:
   curl http://127.0.0.1:10011/DREADD?<FILE_NAME>&createdatabase=true

Step 6: Re-index Smart Search data

Re-index the Smart Search data in Service Manager.

Step 7: Remove useless files

1. Log on to the NFS server.
2. Browse to the <Smart_Analytics_NFS> directory.
3. Run the following commands, and then remove all the listed files.
   find . -name *_backup
   find . -name BackupContent*