ITSM Automation NG Express

Software release version: 2017.04

Administration Guide

Document release date: April 2017
Product release date: April 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

© Copyright 2017 Hewlett Packard Enterprise Development LP

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/.

Contents

Contents

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 ITOM CDF
- Administer the ITSMA suite

Administer ITOM CDF

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

- Access ITOM CDF
- Change your password
- Logs
- Manage users
- Management
- Monitor infrastructure status
- Nodes
- Manage licenses
- View the existing images
- Manage Resourses
- Security
- Restart ITOM CDF

Access ITOM CDF

Logon

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

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

   > You must use the master node host's 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. See Verify the installation.

Logout

To log out:

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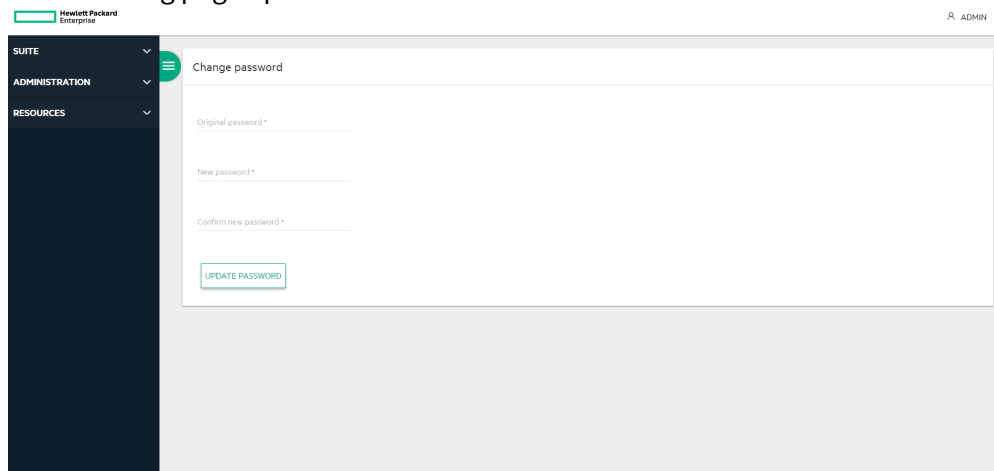2. The application closes and the LOGON screen is redisplayed.

> 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**.

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:
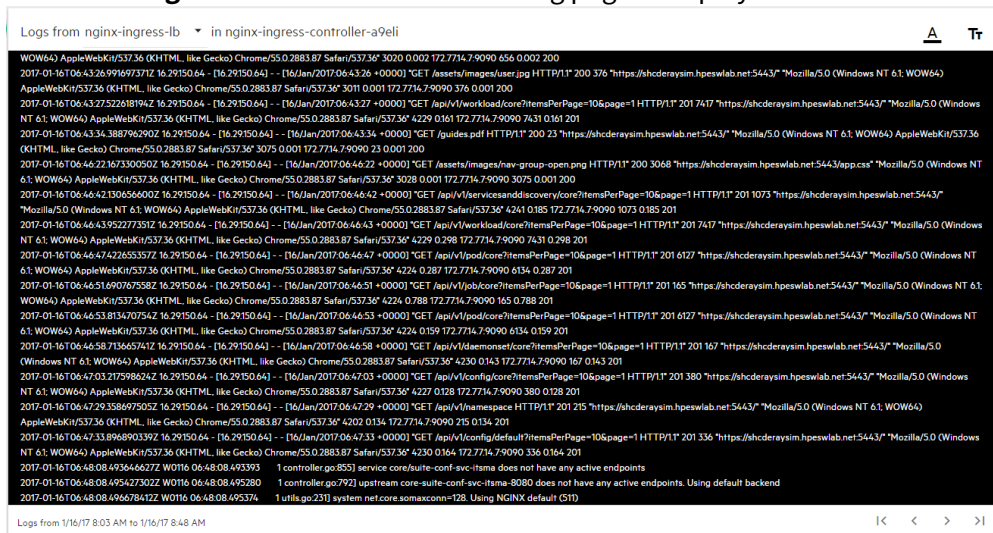
You can use the following tools:

- 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 Suite Export Logs

This section shows how to export the suite logs by gathering the logs from the suite persistent volume(s) and ZIP them up.

Export Suite Logs

1. Click **SUITE > Management** > **Export Logs**.
   The log package is downloaded to your local disk.

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.
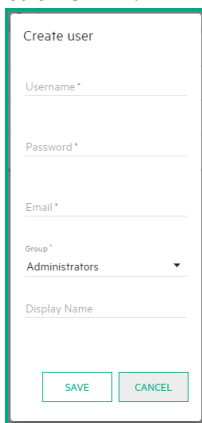
Suite Administrator

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**.

Management

The Management page provides information on how to manage and configure the installed suites.

Before the suite is installed, click **SUITE** > **Management**. The following page opens.
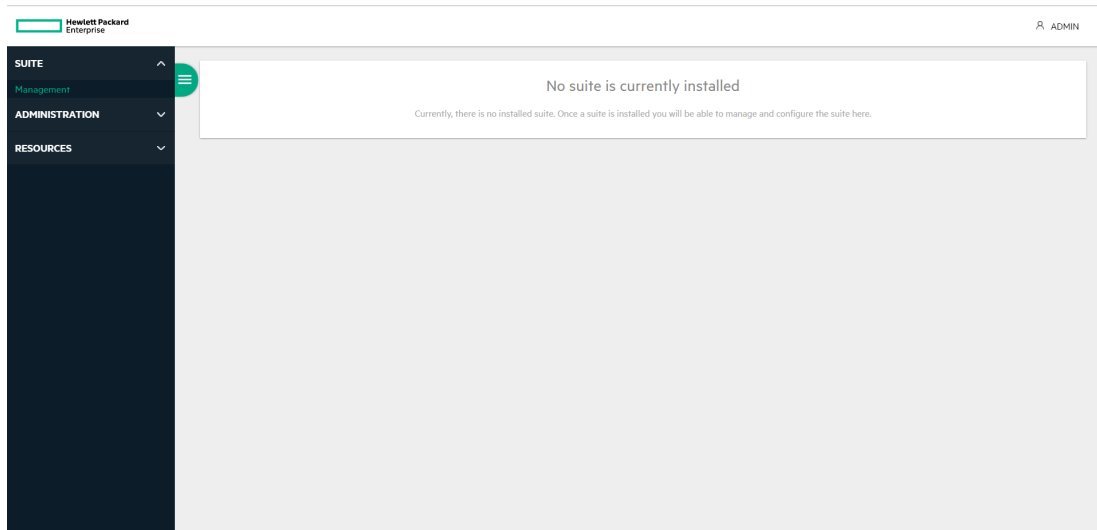
After installed suite, click **SUITE** > **Management**. The following page opens.
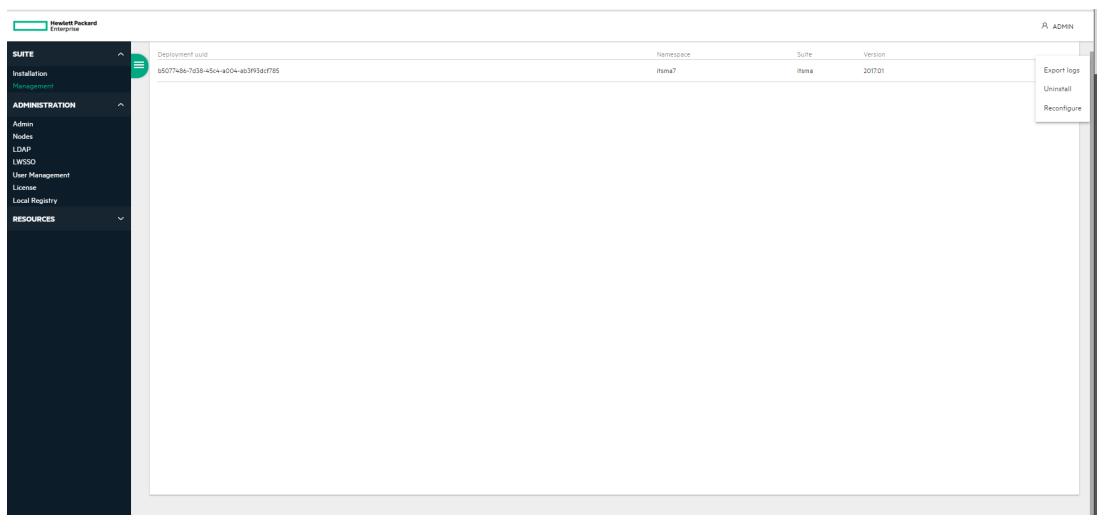
Click ⋮ : then

- Click **Export logs** to download the suite installation log to local registry.
- Click **Uninstall**, then **UNINSTALL** to uninstall the installed suite.
- Click **Reconfigure** to reconfigure the installed suite.

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**.

Namespaces				
Name	Labels		Status	Age
✓ core	-		Active	3 hours
✓ default	-		Active	3 hours
✓ kube-system	-		Active	3 hours

Nodes				
Name	Labels		Ready	Age
✓ 16.187.190.180	beta.kubernetes.io/arch: amd64 beta.kubernetes.io/os: linux kubernetes.io/hostname: 16.187.190.180 master: true role: loadbalancer		True	3 hours
✓ 16.187.190.181	Label: Worker beta.kubernetes.io/arch: amd64 beta.kubernetes.io/os: linux kubernetes.io/hostname: 16.187.190.181		True	3 hours

Persistent Volumes							
Name	Labels	Capacity	Access modes	Status	Claim	Reason	Age
itom-vol	kubernetes.io/cluster...	50Gi	ReadWriteMany	Bound	itom-vol-claim	-	3 hours

Nodes

The Nodes page provides the CPU and Memory usage history of the selected Namespace, a list of the predefined labels, and the list of nodes of the selected Namespace.

> When the CPU load is over 80%, it significantly impacts the efficiency of network transmission between the base infrastructure environment. It is recommended to control the CPU load so it is less than 80% by separating the suite instance into multiple worker nodes: adding more worker nodes and killing the pods on heavy-load nodes and deploying those pods on the newly added worker nodes.

View the existing nodes

To view existing nodes:

1. Click **ADMIN** > **Nodes**. The following page opens.
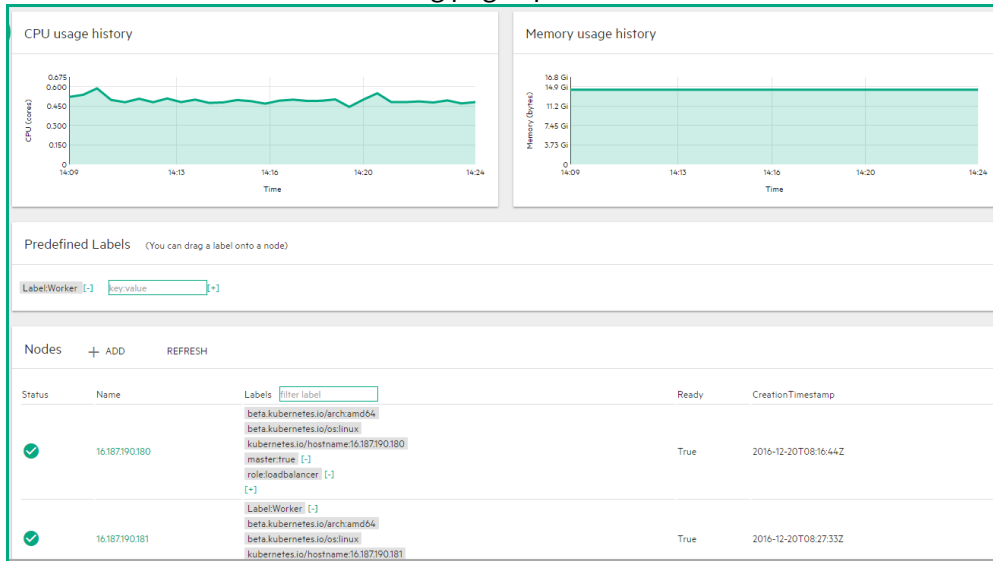
2. The area displays the CPU and memory usage of the selected namespace during the past 15 minutes, the list of the node labels, and the status, labels, readiness, and creation timestamp of the nodes corresponding to the selected namespace.
   You can do the following:

   - Define a set of labels you want to use and then assign them to nodes by dragging them to the node. See Add/delete labels and Assign labels to nodes.
   - Add a node. See Add a node.
   - **REFRESH.** Click to refresh the display.
   - Click the relevant node to see its details. See View the node details.

Add/delete labels

To add or delete labels:

1. Click **ADMIN** > **Nodes**.
2. To add a label in the **Predefined Labels** area, enter the **value** and click **[+]**. The label is added to the list.
3. To delete a label: in the **Predefined Labels** area, click **[-]** for the relevant label.

Assign labels to nodes

To manage node labels:

1. Click **ADMIN** > **Nodes**.
2. **To assign a label to a node:** drag the relevant label the **Predefined Labels** area to the relevant node in the **Nodes** area.
3. **To unassign a label:** in the **Nodes** area, click **[-]** for the relevant label and node.
4. **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

1. lick **ADMIN** > **Nodes**.
2. In the Nodes area, click **+ ADD**.

   Enter the name of the node, the name of a user that can remotely execute commands on the host - typically the root user, and the password of a user that can remotely execute commands on the host - typically the root user, and click **ADD** to remotely install the extra node.

You can also add a remote node manually as follows:

1. Copy the core platform binary file to the remote (worker) node as well as the client certificates that are required so the worker node can talk to the master node.
2. Unzip the core platform binary file.
3. Change to the relevant directory:
   cd HPESW_ITOM_Suite_Platform_<timestamp_ID>.
   The install.properties file is the same as on the master node.
4. Copy the files specified in the CLIENT_CA_FILE, the CLIENT_CERT_FILE, and the CLIENT_KEY_FILE parameters in the install.properties file from the master node to the worker node:
   a. **scp root@<master node ip>:/opt/kubernetes/ssl/ca.crt /tmp** when prompted, enter the password.
   b. **scp root@<master node ip>:/opt/kubernetes/ssl/server.crt /tmp** when prompted, enter the password.
   c. **scp root@<master node ip>:/opt/kubernetes/ssl/server.key /tmp** when prompted, enter the password.
   d. **ls /tmp** to verify that the files have been copied.
5. Run the installation: **./install**.
6. Run **docker ps** to list the current container.
7. To see what workloads are running.

   > Go to the master node and run **kubectl get nodes**. You should see two nodes.
   > Go to the master node and run **kubectl describe nodes <worker_node_IP>** to get

> detailed information about the worker node. It is only running two pods **kube-proxy** and **kube-registry**.

View the node details

1. Click **ADMIN** > **Nodes**.
2. In the Nodes area, select a node name from nodes list.
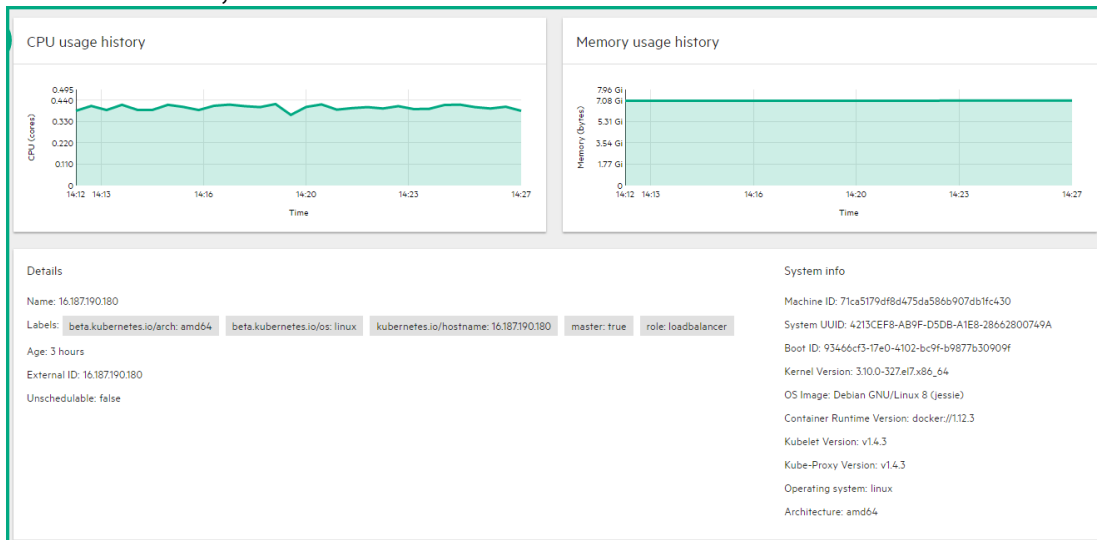
The page displays the CPU and memory usage history of the selected node for the past 15 minutes.

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 percentage of <what is in use>/<what is available>. By default, pods run with unbounded CPU and memory limits. The format is: <what is in use>/<what is available>.

Allocated resources								
CPU requests (cores)	%	CPU limits (cores)	%	Memory requests (bytes)	%	Memory limits (bytes)	%	Pods	%
0.41 / 4	10.25	0.41 / 4	10.25	770 Mi / 7.797 Gi	9.64	870 Mi / 7.797 Gi	10.90	17 / 110	15.45

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

Conditions					
Type	Status	Last heartbeat time	Last transition time	Reason	Message
OutOfDisk	False	-	a day	KubeletHasSufficientDisk	kubelet has sufficient disk space available
MemoryPressure	False	-	a day	KubeletHasSufficientMemory	kubelet has sufficient memory available
DiskPressure	False	-	a day	KubeletHasNoDiskPressure	kubelet has no disk pressure
Ready	True	-	a day	KubeletReady	kubelet is posting ready status

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 passed since the pod has been created, the cluster IP, as well as the CPU and memory usage of the

pod.
You can:

- Click a Pod name to open the Workloads - Pods page for the pod. See Pods.

- Click ≡ to view the pod log.

- Click ⋮ and select **Delete** to delete the pod.

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

	Message	Source	Sub-object	Count	First seen	Last seen
⚠	(events with common reason combined)	kubelet 16.187.191.60	-	354	7/11/16 06:25 UTC	8/11/16 11:50 UTC

Manage licenses

The License page enables you to manage your suite licenses. Note that you might have already set up some of the licenses during installation.

View existing licenses

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

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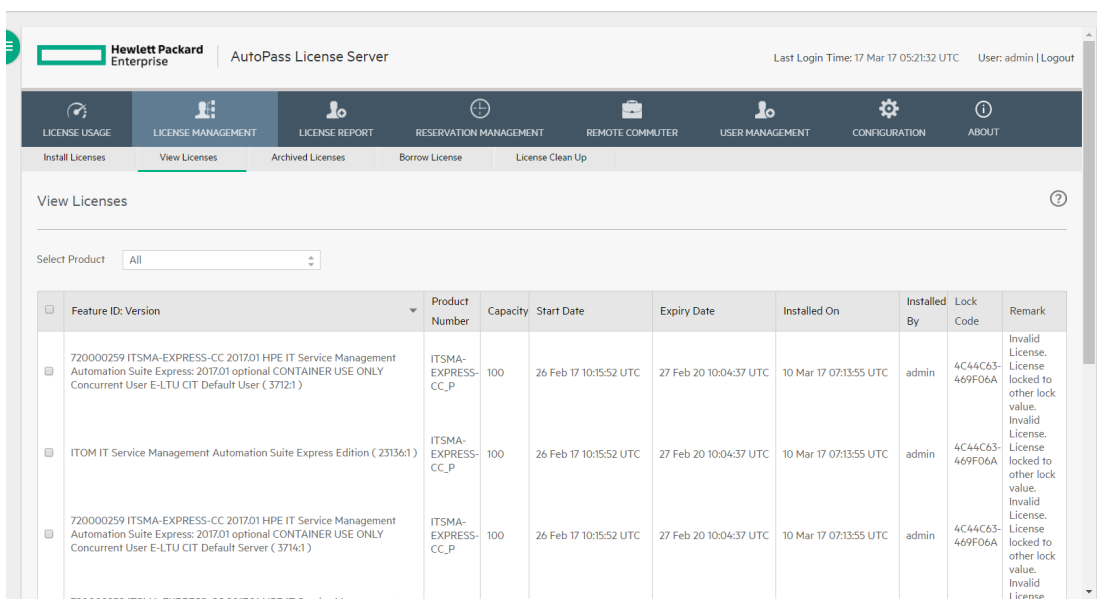
Select the relevant product in **Select Product**. The page displays the feature ID: version, product number,capacity, start date, expiry Date, the date when it was installed, and who installed it, as well as the Lock Code.

Install licenses

1. Click **ADMINISTRATION** > **License**.
   The following page opens:
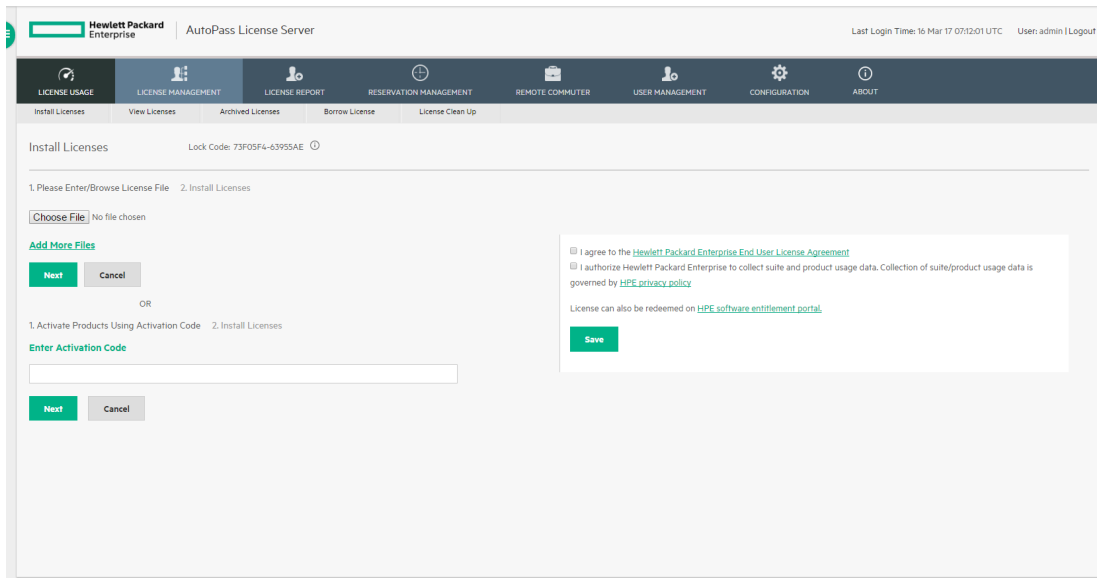
The following information is displayed:

Lock Code. The lock code and lock ID are the same.

2. Click **Choose file** to select the license file in your local system
3. Click **Add More Files** to select another license file in your local system.
4. Click the boxes to agree to the HPE End User License Agreement and authorize the suite and product usage data collecting.
5. Click **Next**.
   The following page opens and displays the licenses that have been installed.
   You can select the license keys and click **Install Licenses** to install the licenses (you can also select to go back to the previous Install Licenses page by clicking the **Back** button).

15
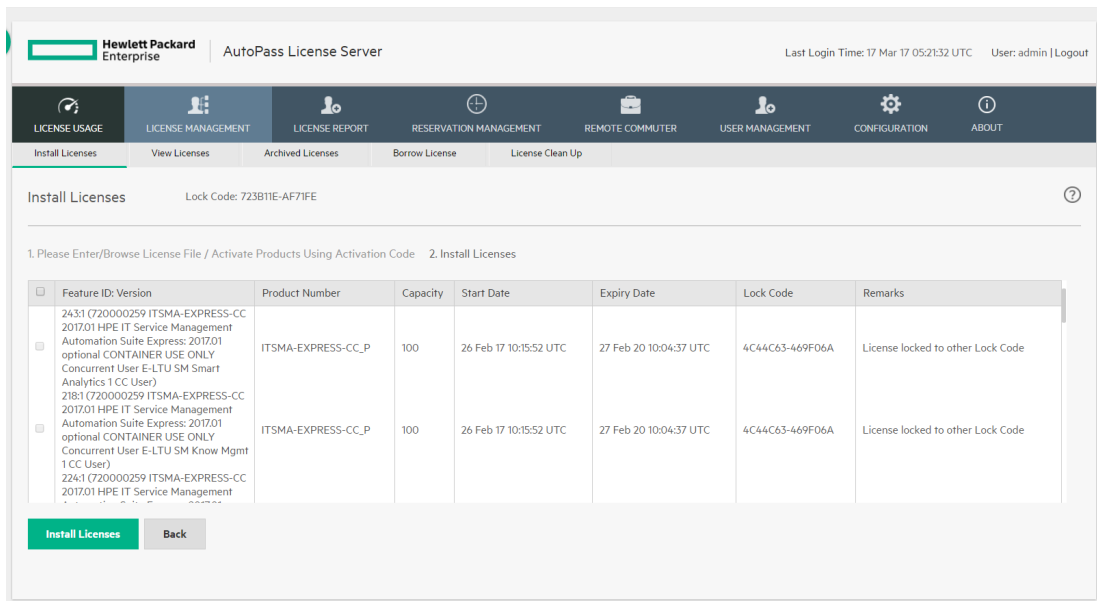
The page displays the licenses in the selected file. You must select the licenses you want to install out of the displayed licenses. After selecting, click **Install Licenses**.

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 for customers to fetch and activate the products.

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

1. Click **ADMINISTRATION** > **LICENSE REPORT**.
   The following page opens:
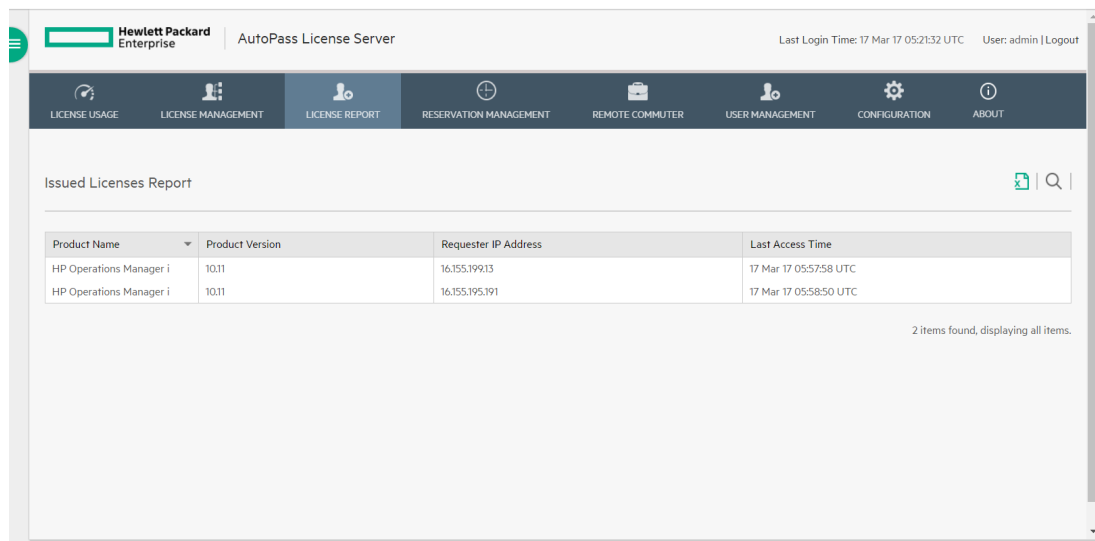
The following information is displayed:

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.

Replace an ITSMA trial license

User role: Suite Administrator

If you have not installed a perpetual license before the ITSMA installation, a built-in 30-day trial license (InstantOn) is used for the installation. If you purchase a perpetual license after installation, you can replace the trial license with the perpetual one.

To do this, follow these steps:

1. Install your new license. For details, see the "Install the suite license" section in Install an ITSMA suite license.
2. Restart the Service Management RTE application controllers:
   a. Click **RESOURCES,** and then select your <namespace>. For example, **itsma1**.
   b. Click **Workloads** > **Replication Controllers**, go to the next page, and then locate one of the following controllers:
      sm-rte
      sm-rte-integration
      sm-rte-irque
      sm-rte-scheduler

> **sm-rte-emailout**
> **sm-rte-integration-cit**
> **sm-rte-report-export**
> **sm-rte-sync**
> **sm-rte-gossip**

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

c. Click the action icon (⋮), and then click **Scale**.

d. Make a note of the value of the **Number of pods** field.

> In the next steps, you will need to change the value of this field to zero (0) and then change it back to the current value.

e. Type 0 for **Number of pods**, and then click **OK**.

> Ignore the error message in red on the page after you click the **OK** button.

f. Repeat the steps above to stop all the replication controllers in step **b**. The **sm-rte-gossip** controller must be the last one to stop.

g. Wait until the **Pods** field for each replication controller is changed to 0/0.

h. Change the value of the **Number of pods** field from 0 back to their original number for all the controllers.

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

View the existing images

To view the existing images, click **ADMINISTRATION > Local Registry**. The following page is displayed.
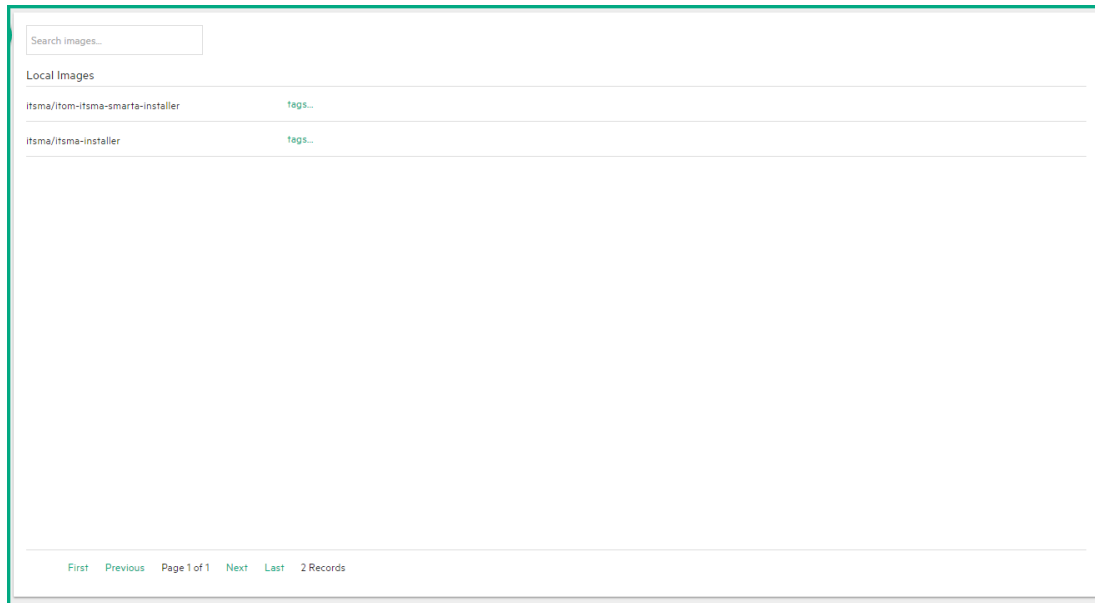
This section lists the images that are in the local registry.

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
- Workloads
- Services and discovery
- Persistent Volume Claims
- Configuration

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. See Glossary.

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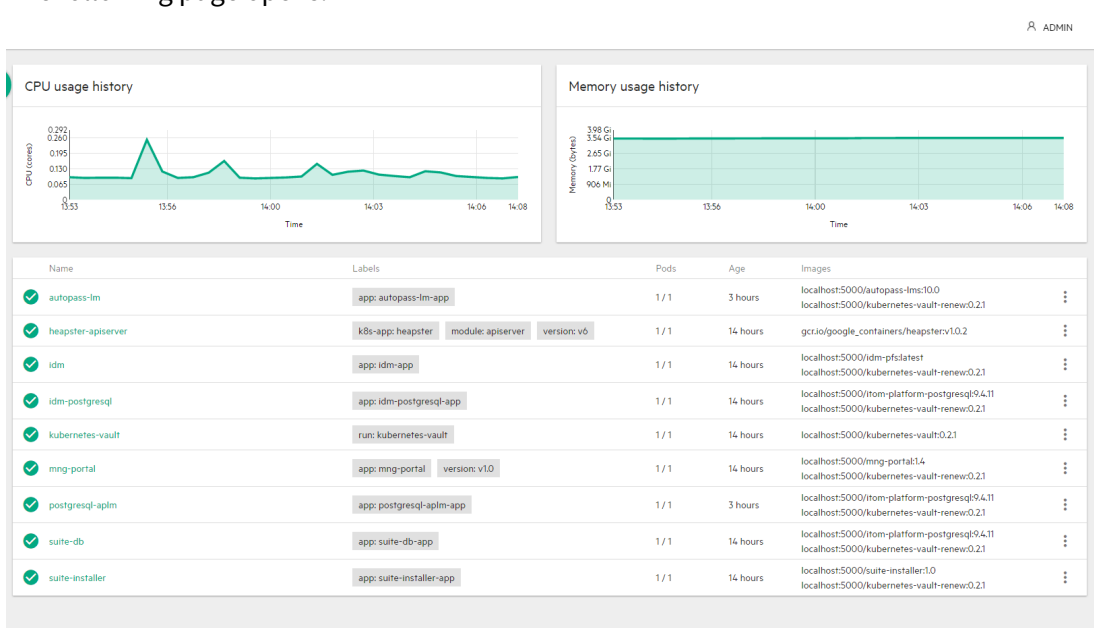
The page shows the CPU and memory usage history for the selected namespace, for the past 15 minutes, the name of the namespace, its labels, pods, the timestamp of the creation of the namespace and its images.
Click the relevant namespace to display more details. See View the namespace details.

View the namespace details

1. Click **RESOURCES** > **Namespace** and select the relevant namespace. You can also click **RESOURCES** > **Namespaces**, and click the relevant namespace.
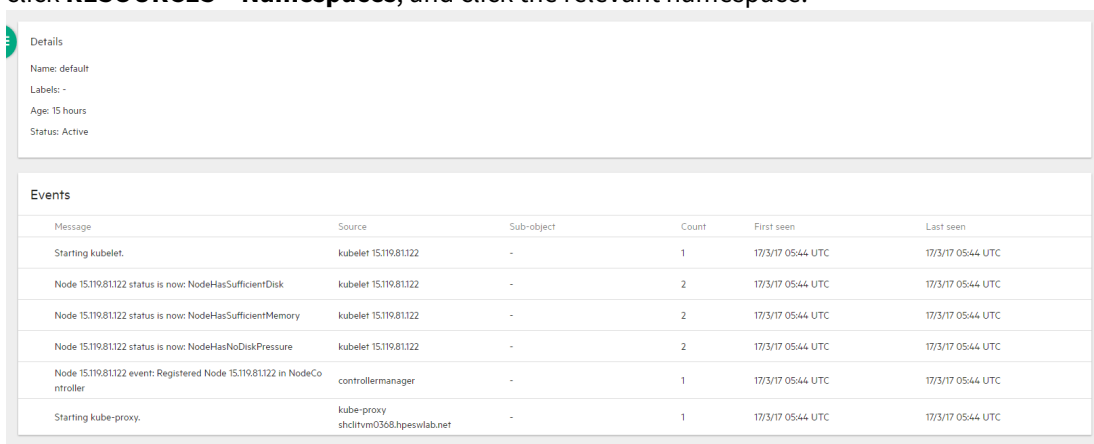
The page shows details about the namespace and details about the events occurring in the namespace.

Workloads

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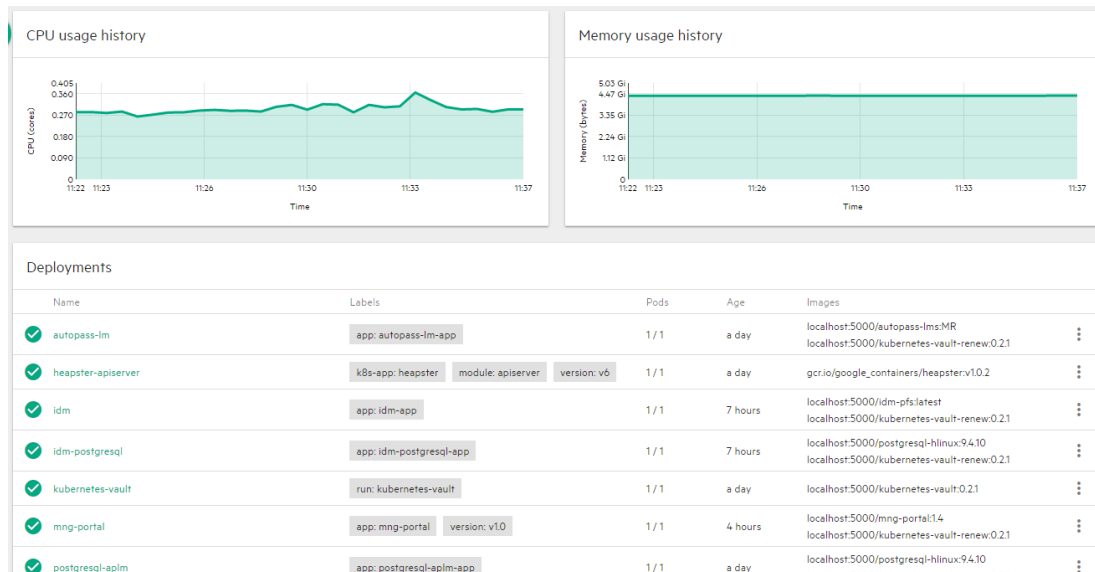
Click **RESOURCES** > **Workloads**.

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.
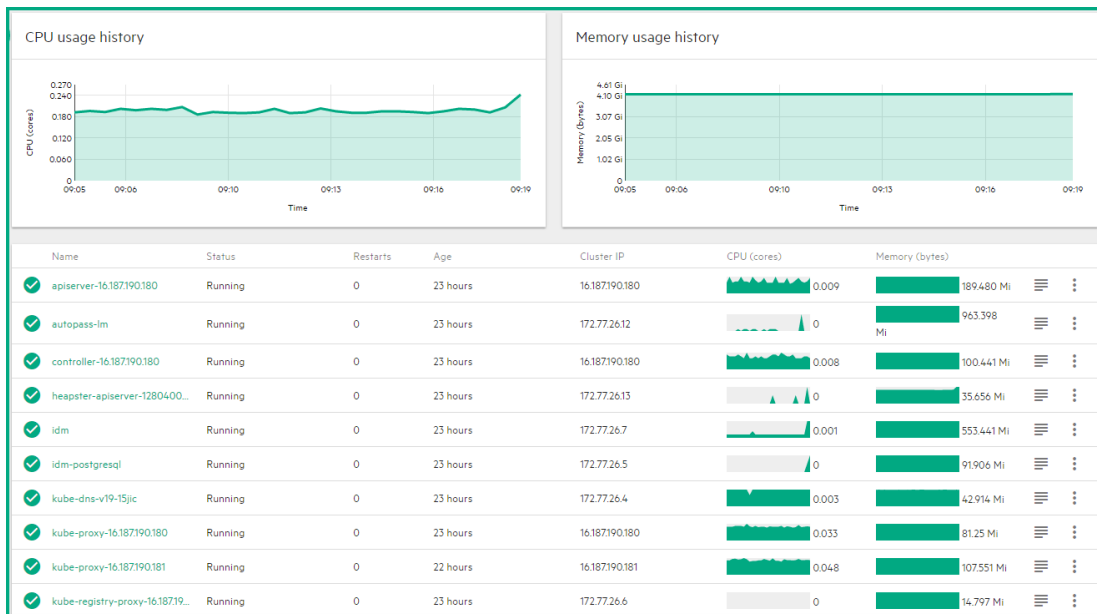
The page displays the CPU and memory usage history of the namespace the pod belongs to, namespace the pod belongs to, the name, status, number of restarts during the lifecycle of the pod, the amount of time passed since the creation of the pod, the IP address of the pod, the CPU and memory usage of the 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.
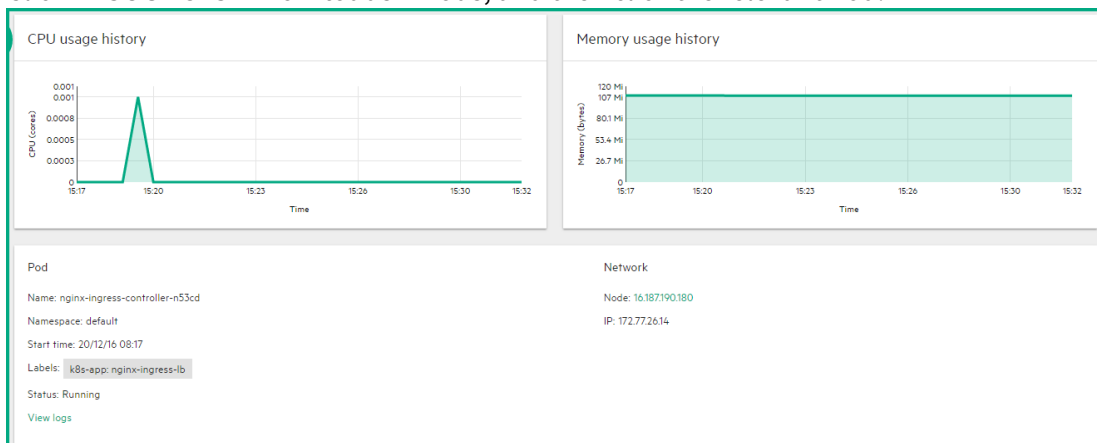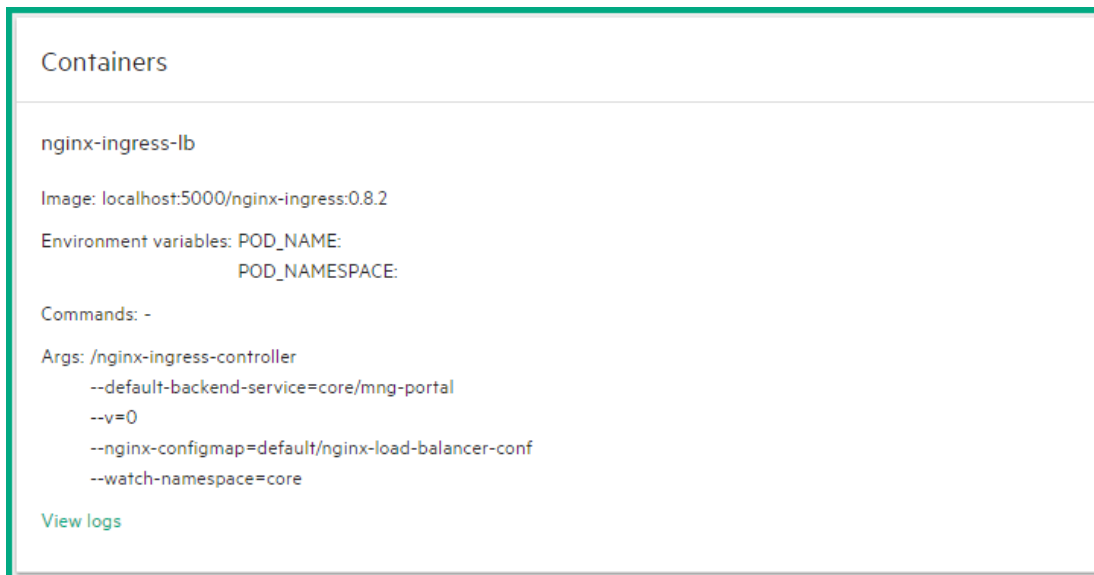
The page displays the CPU and memory usage history of the pod in the last 15 minutes, the pod details, and the network details. To display the log of the pod. See View log.

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.
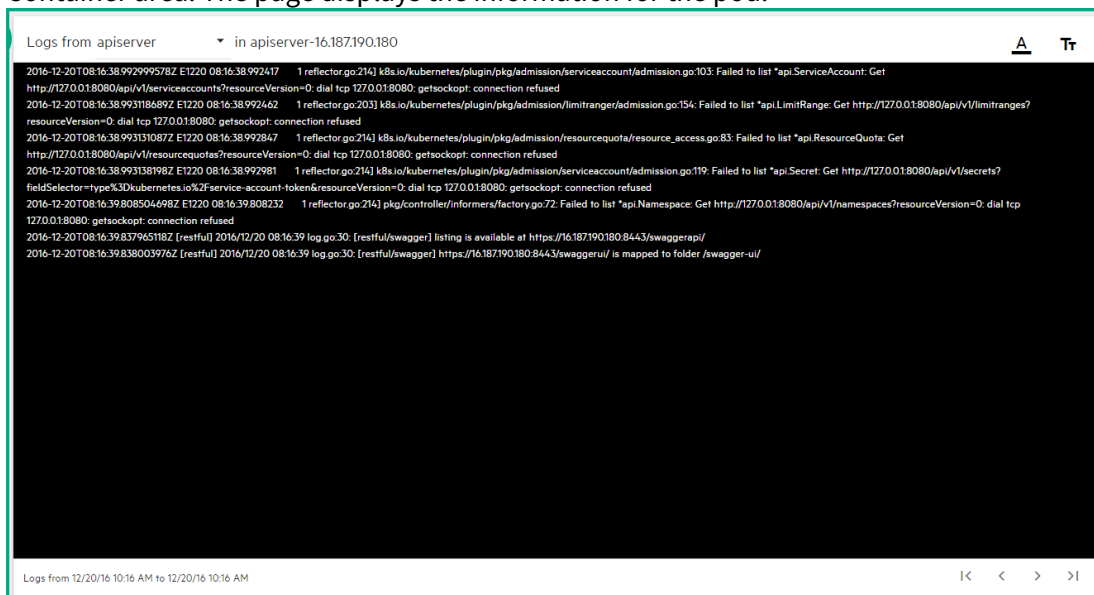
You can use the following tools:

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

23

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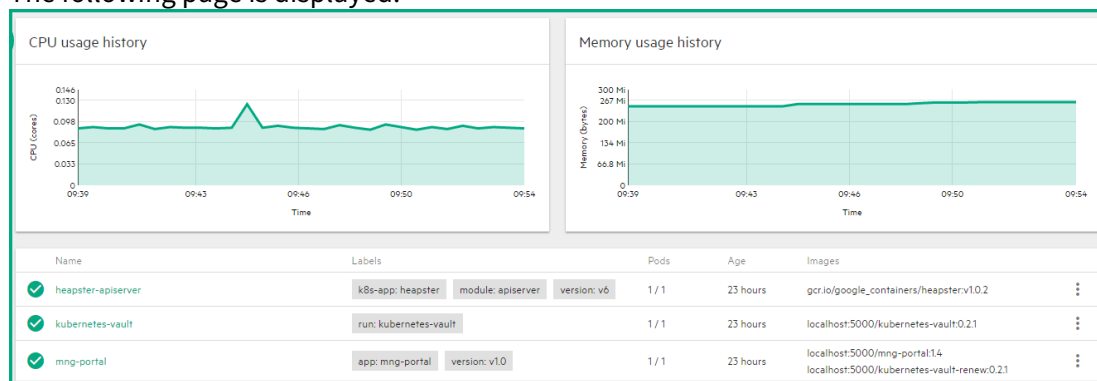
The page displays the CPU and memory usage history of the selected namespace during the past 15 minutes, the name of the available deployments, their labels, the number of pods, the creation timestamp of the deployment, and its images.
You can:

- 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:
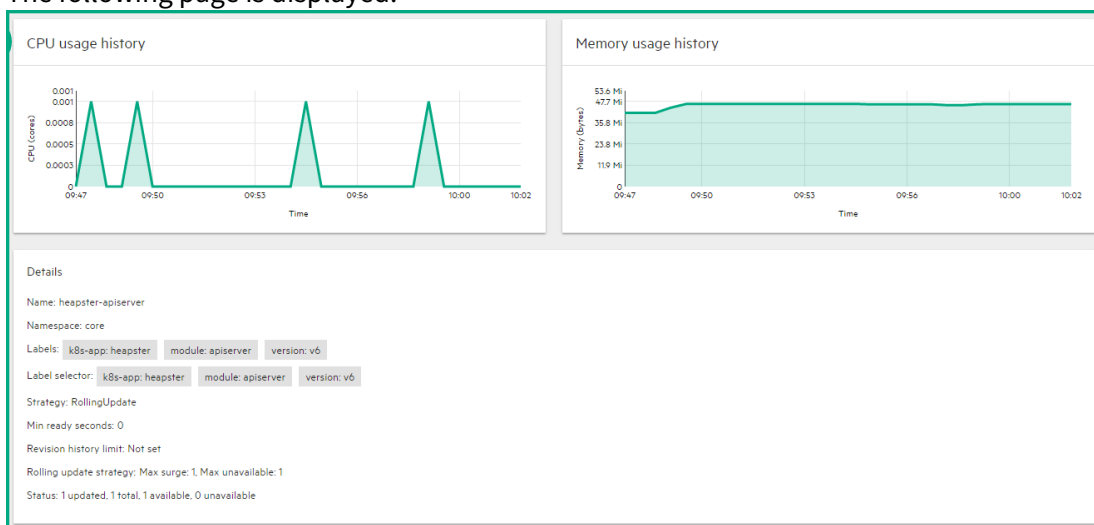
    The page displays the CPU and memory usage history of the selected deployment during the past 15 minutes, and details about the selected deployment.
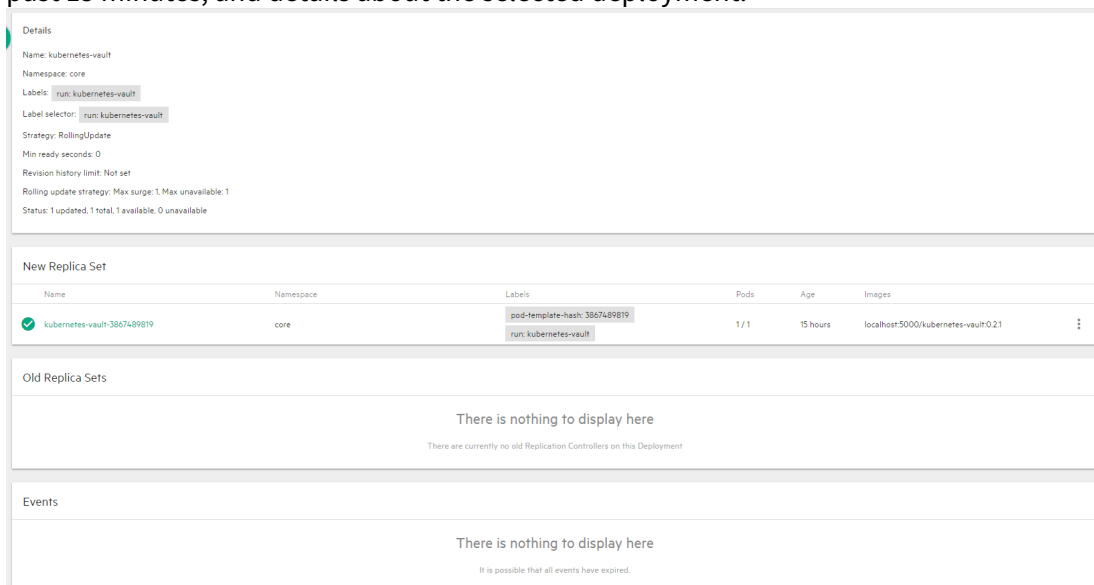
    The page displays details about the new replica set, the old replica sets, and the events that took place.

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.

26

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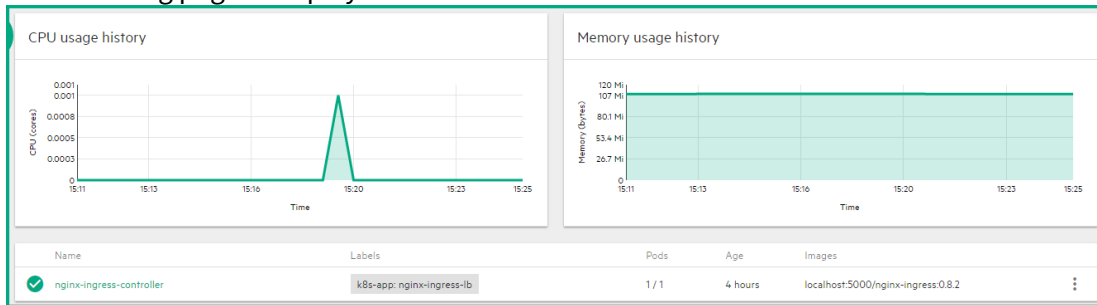
The page displays the CPU and memory usage of the selected namespace during the past 15 minutes, and the list of replication controllers with their name, labels, pods, age, and images of the replication controllers associated with the selected namespace.
You can:

- 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**.

Set desired number of pods

Replication controller nginx-ingress-controller will be updated to reflect the desired count.
Current status: 1 created, 1 desired

Number of pods *

CANCEL   OK
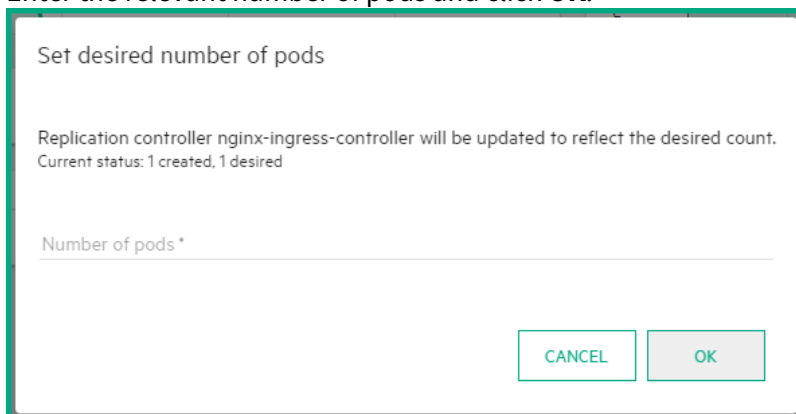
View the replication controller details

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

2. Click ⋮ and select **View details**, or click the relevant Replication Controllers.
   The following page opens.
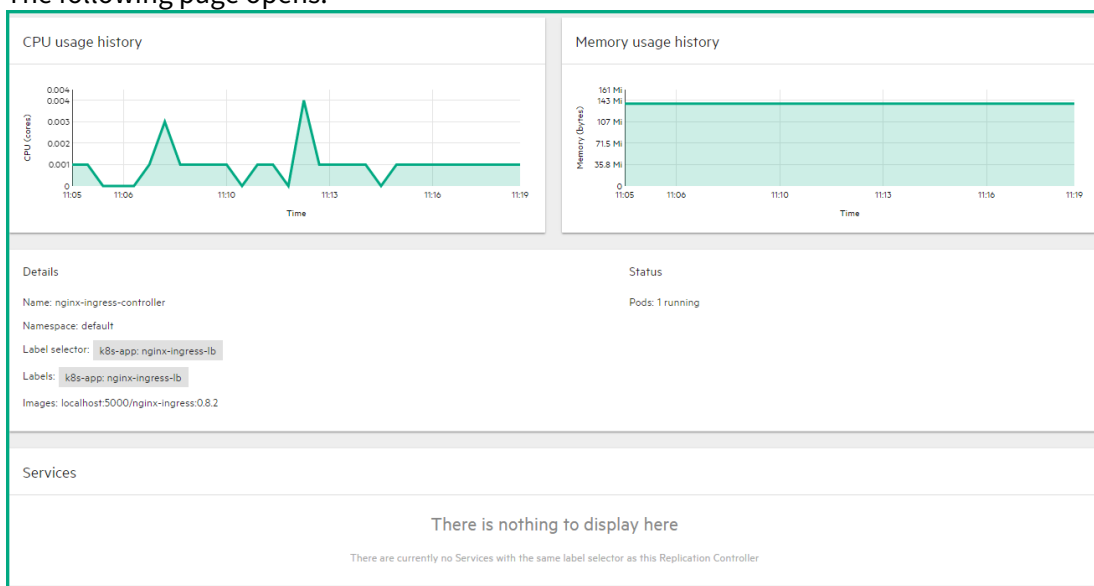
It displays the CPU and memory usage history of the selected replication controller for the past 15 minutes, the details of the selected replication controller, and the services provided by the selected replication controller.

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.

See Glossary.

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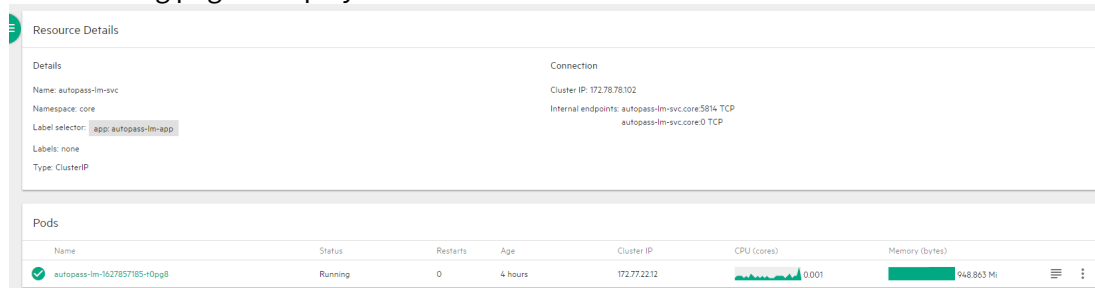
The page displays details about the service and the connection as well as information about the related pods.

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.

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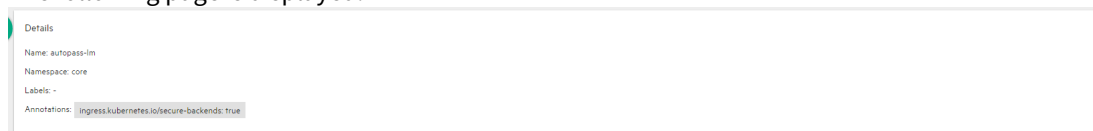
The page displays details of the selected ingress and its related pods.

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:

Name	Volume	Labels	Age
✓ itom-vol-claim	itom-vol	kubernetes.io/cluster-service: true	16 hours

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.

Details

Name: itom-vol-claim

Namespace: core

Status: Bound

Volume: itom-vol

Labels: kubernetes.io/cluster-service: true

Capacity: {"storage":"50Gi"}

Access modes: ReadWriteMany

> 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:

Name	Age
default-token-76u5r	16 hours
nginx-default-secret	16 hours

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.

Data

ca.crt: -----BEGIN CERTIFICATE-----
JIE9zCCAt+gAwIBAgIJAJTbWfhTmIZ7MA0GCSqGSIb3DQEBCwUAMBIxEDAOBgNV
BAMMB2hwZS5jb20wHhcNMTcwMzE2MTUwNjEwWhcNMTgwMzE2MTUwNjEwWjASMRAw
DgYDVVQQDDAdocGUuY29tMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
s8co3PDninfDOgV/QsBKwC1g49ZyPZg2vbvUSLHqaHyxpzvPzrJRCScFutKLpI
ePZ3hWw+e/+V7DPKCccDgTU5ZO6vEYPYt+fRVI0/fcnU/ppXfpTGmJET9VKMumuL
QOkl8RBp4aD7wsSBfCEZKtiVqoeHAA4tErwFHv7jMCRPpiP35FhIclVQCRPz9yRk
x7nYBcUAUtkDT2FlmOluGZBE0Pdd/oCphZiRf8bujKT0kap1Dk+9qqVeDgQ8fniS
WrK57BiCacKzleUwHSo5qUGALCgz5e2EhPyPCNxaWpEfLzP8rDXopZEc15zfInXy
cVIrW3CCgdNqjExmlFWkLpqq/QcXBdnSK9qWoJOeun1DJg1+MKSL1MwfjkGru7hH
KH5n8e9PNvPpzZS77kUeHIAl1khjvONNwz+TJeebnWpbBhfStLT4b6XxnTGbngHM
MdWTwDdznB1Qse4ODrHKu9Jd5cTigH5c+Ycjb5xOMh5Zz/4JXZ8CaJCeK9+HvHtx
UJOhp9gSKsJiX/pNnWGKnFbkLmaOspiW.rssC1YhHb9LQioQ7Qf+LhzYVrtLVCen
MovJpBSGYYbGc6VwSqCN9yiG6DsVusmrlxiODlRkpWZPWuyqBqsmynGlovs/i9O
1xuBJLK5Mtz55Jvk33GbPRs6/8AO5jqOzIpisx5jR5L8CAwEAAaNQME4wHQYDVR0O
BBYEFJ0/xf6lH6JxGqFf7vguUUWFB2yXM8BGA1UdIwQYMBaAFJ0/xf6lH6JxGqFf
7vguUUWFB2yXMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADgglBAEXFpPvZ
rAZV9TTmLjTifj5bHmhuB1nb+G2jcQKxNgINA9spowPtR/PWkAFI9vCynosaOwgg
DlqSQdYKU/8qNIyINtgp0XGbnTX+DA6uQxYW53FA8rdKIV/MgWqb5FMHaBprBHi7
Rpr/rGBsJgY6hOPBS6VJcNiQql9OnXiaYL/fExxQdg8dLqY0bB/4cJYSsconBMgn
gjEYb6OP+582LGIBhfdiMAhwzfMfMZ9OW+OhGb+RQw/EL5CBkM4JgxCG5TtpWuStF
DbKmjZZXC8Re0VpUaRqo/fcCN3oy1vJfuHnilmo4ZJhy9AH4NnMXiNGCkNOwO0Gn
WCo79ewebdmitFVi07v2ahBmH2W/hHjTgIiZyFuMrkkA9tqSvrKICvtxl5m9kdta
FX5pco9BsN4xo6oJm6azcf4CD7dRk/5Z8SFpl4deDwNmy2qtMkz0aOK9c3PYDbGR
8uxgiF7xiGIHIEAWN0FJqdCHHdaV5CRGPK5GB/ZnKNLVB6wQjuas5Jqeqgop NQ29
4BF+0lk4dciw7u7e2iY0fIASKYqylcAsmbiFsWj0ZahPu7dPjM/6mjY0NqWawXz4
IFqYk2pO08pLcy91JzcOY8JRN7EkrLsFf3e5LZiVR4vMfvodbZFDI+fafBUQqe
UbiB1hFFNQMx6onxEVxdLf7kAhd1sYe5Zy3
-----END CERTIFICATE-----

namespace: core

token: ey.JhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NicnZpY2VhY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJjb3JlIiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6ImRlZmF1bHQtdG9rZW4tNzZ1NXIiLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3VudC5uYW1lIjoiZGVmYXVsdCIsImt1YmVybmV0ZXMuaW8vc2VydmljZWFjY291bnQvc2VydmljZS1hY2NvdW50LnVpZCI6Im1lMmmM4YmNiLTBhNWEtMTFlNy1hYmQ3LTAwNTA1NmIzMzMyOSIsInN1YiI6InN5c3RlbTpzZXJ2aWNlYWNjb3VudDpjb3JlOmRlZmF1bHQifQ.EVeBpfKiqPq71EXVeWJRU4CCkUMuPuRDDh2N7AxhU2Ui5Q6scJwDr4ZNfr7AdC7U2IR9RDzr0QKXiVybaMaPGoL9xVzWJGW0i8MIZeNiPqY1Ay_IJFxuAsYICyHgwvBXkvUurjaol-
QQsXAjne32eVlccWouUnJY_OvxdD_H8NZHxOHZdqr2SowuqUebiWWBRqA5OUvgrAyfYrl3aggskfIMm42iTlavOsA9_Z9fztkVg8iiV8GeN25bokiiKRmu5LwW81O96Om9fJKUuNOq4eSnnffgZ94KyUaNeOisa1hOilaondsCVPewfXRgP2q4XMOYLpxeHNN8eLlTVPJiV4BnB2uqvO_HL7GcA-
h7n24HU0yZ7BvHQbqQH5yRkDDgEJXX_aG2pYel4zf1iiOENpFYcuTcYCOLJCV9pFSR3D2-JnmwAa34pmweNzn56JOxynBCYAu_qeLJaxnyx33RJCE0N-Xnki1teCAXtA2HRNQiZjzzORaiIWfuRj6-
ibKX7X7s7wD8wFAvvh6ic6jiappAyFhZbbsrzAfAgVdIF1g0n2a_yq8GLz6vhdDtmbxFaXo0ADAEkQa_NpTJv_hNWlfr2FCPQnEetopBV1gJMxF-OuVrgO9mSUuwBunt-57XpntadXEGrgmEleW1mQVefSfQrQg1iridl3r8kC9GXi

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:

Name	Labels	Age	
autopass-config	-	16 hours	⋮
base-configmap	-	16 hours	⋮
kube-vault-configmap	-	16 hours	⋮
suite-conf-cm-itsma	-	4 hours	⋮

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:

Details

Name: base-configmap
Namespace: core
Labels: -

Data

API_SERVER: 15.119.81.121
ETCD_ENDPOINT: https://15.119.81.121:4001
EXTERNAL_ACCESS_HOST: shclitvm0367.hpeswlab.net
INGRESS_HOST: 15.119.81.121
MASTER_API_PORT: 8080
MASTER_API_SSL_PORT: 8443
NFS_SERVER: 15.119.81.121
SYSTEM_NAMESPACE: core

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

This section provides information on network and communication security.

Secure topology

ITOM CDF is designed to be part of a secure architecture, and can meet the challenge of dealing with the security threats to which it could potentially be exposed.

Several measures are recommended to securely deploy ITOM Container Deployment Foundation (CDF):

- Use of the TLS/SSL communication protocol

Replace the Certificate of Ingress Service with a Customized Certificate

Users can replace the certificate and private key of **Ingress Service** with a customized certificate and private key. Follow the steps below:

1. Generate a certificate and private key for the **host name**, of which host the **Ingress Service** is running on. And put it somewhere on the master node.
2. On master node, delete a secret with command:
   kubectl delete secret nginx-default-secret -n core
3. On the master node, recreate the secret with a new certificate and private key.
   echo "
   apiVersion: v1
   kind: Secret
   metadata:
     name: nginx-default-secret
     namespace: core
   data:
     tls.crt: `base64 <certificate file name with absolute path> |tr -d \"\n\"`
     tls.key: `base64 <private key file name with absolute path> |tr -d \"\n\"`
   " | kubectl create -f -
4. On master node, delete and recreate the ingress service.
   kubectl delete -f ${K8S_HOME}/objectdefs/nginx-ingress.yaml
   kubectl create -f ${K8S_HOME}/objectdefs/nginx-ingress.yaml

FAQ

Question

Are exceptions required to be added to the firewall policy?

Answer

Browsers access HPE ITOM Container Deployment Foundation (CDF) via HTTPS ports (TCP/5443). End users need to add it to the firewall exception policy.

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 & Inactivity timer timeouts

Authorization Configuration

For detailed information on authorization configuration, refer to the ITOM CDF Online Help Center in the ITOM CDF Portal top right corner.

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.

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**

For detailed information, please refer to the online help topic, Working with Secure Sockets Layer (SSL) in a Production Environment. See the ITOM CDF Online Help Center in the ITOM CDF top right corner.

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.

Security logs

This section provides information related to 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.

For detailed information, please refer to the online help topic, Tracing and Logging in the ITOM Container Deployment Foundation (CDF) Online Help Center in the ITOM CDF top right corner.

Network and Communication Security

HPE recommends that you add the iptables rules listed below to the following below tables.

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

Required ports	Service	Target server to configure the rules	Direction	Short description
111	NFS	NFS server	Nodes -> NFS Server	NFS server port access by all nodes

2049	NFS	NFS server	Nodes -> NFS Server	NFS server port access by all nodes
2380	Etcd	Master Node	Master <-> Master	Etcd service port for etcd cluster communication
4194	Kubernetes	All Nodes in Cluster	Localhost only	Cadvisor for local kubelet
5000	Private Registry	All Nodes in Cluster	Localhost only	Registry port for local host
5443	MngPortal	Ingress Node	All -> Ingress Node	The port exposed on ingress node. All clients could access this port
8443	kubernetes	Master Node	Nodes -> Master	API server port for client connection
10250	kubernetes	All Nodes in Cluster	Nodes -> Nodes	Kubernete port for internal communication
10251	kubernetes		Nodes -> Nodes	Kubernete port for internal communication
10252	kubernetes		Nodes -> Nodes	Kubernete port for internal communication
10255	kubernetes		Nodes -> Nodes	Kubernete port for internal communication
20048	NFS	NFS server	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. The Master Node on: 10.10.10.10

To add an 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
```

Administer the ITSMA suite

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

- Change the ITSMA suite administrator password
- Configure an external LDAP server
- Master data onboarding
- Configure Email
- Configure log level for debugging
- Add Smart Analytics content groups
- Set up Service Portal
- Bind the internal PostgreSQL database to a dedicated worker node
- Apply PostgreSQL parameter updates in ITSMA
- ITSMA node ports
- Customize the ITSMA login page
- Configure users for the internal LDAP server

Change the ITSMA suite administrator password

User role: Suite Administrator

The **sysadmin** user 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.

To change the password for the **sysadmin** user, follow these steps:

1. On the suite landing page, click **Suite Configuration**.
2. Click **Operation** > **Admin Password.**
3. Enter your old and new passwords for the "sysadmin" user.

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

4. Click **Update**.

Configure an external LDAP server

User role: Suite Administrator

The ITSMA suite is designed to integrate with an LDAP server for user authentication.

The internal LDAP server in the suite is only for demonstration purposes. For production environment, you can configure an external LDAP server from the **Suite Configuration** page.

> The ITSMA suite has a seeded user named **sysadmin**, which is stored in the suite's IdM database. Make sure that your external LDAP server does NOT contain a **sysadmin** user account.

To configure an external LDAP server, follow these steps:

1. On the suite landing page, click **Suite Configuration**.
2. Navigate to **CONFIGURATION** > **Accounts** > **LDAP**.
3. Configure your external LDAP server settings as described in the following table.

Setting	Description
Hostname or IP Address	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).
User ID	The fully distinguished name of any user with authentication rights to the LDAP server. If the LDAP server does not require a User ID or password for authentication, this value can be omitted.
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.
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.
User Name Attribute	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.
Enable SSL	Select this option to enable SSL connection to the LDAP server.

4. Click **Test** to make sure you can successfully connect to the LDAP server.
5. Click **Apply** to save your configuration.

> After your confirmation for applying the changes, the system restarts the related services. If the system fails to restart some of the services, click **Revert** to revert all changes that you just made.

6. Wait until the background services are restarted. Go to Service Management, Service Portal, and CMDB to check the LDAP settings and perform additional configurations.

> For Service Management LDAP settings, you need to perform the following additional tasks after you apply the changes in this Suite Configuration page:
> - For the "contacts" file from Service Management LDAP settings (**System Administration** > **Ongoing Maintenance** > **System** > **LDAP Mapping**), update the

> **operator.id** field mapping to the value as specified in the **User Name Attribute** parameter in the table in step 4.
> - For the "operator" and "contacts" files, make sure that the existing LDAP mapping for the SM fields matches the attributes of your new LDAP server. For more information, see "Define file and field-level mappings to an LDAP server" in the Service Manager help center.

> For Service Portal, you need to perform some additional tasks in the Service Portal Management Console to set up external LDAP. For details, see Configure LDAP for Service Portal.

> For CMDB, make sure that all the necessary LDAP parameters are correctly configured in CMDB before using LDAP users for login. For more information, see the "LDAP Mapping" section in the UCMDB help center.

7. Log out of the ITSMA Suite Portal and try logging in using an LDAP account to verify the LDAP server.

Configure LDAP for Service Portal

1. Log on to Service Portal Management Console:
   https://*<master node FQDN>*/propel/launchpad/org/Provider
   (user name/password: **admin**/**propel**)
2. Click the **Identity** application in the Launchpad.
3. In the Organization List view, click the **ITSMA**.
4. Update LDAP in Service Portal to use external LDAP:
   a. In the Organization Details view, click **Authentication**. The Authentication view is displayed and all of the authentication configurations for the organization are listed.
   b. Click the **Edit** button of **ITSMALDAP**.
   c. Update the LDAP settings to be consistent with what you have updated for the suite level LDAP changes in the Suite Configuration page, and then click **Save**.

   > If the **User Name Attribute** in the suite configuration page is set to sAMAccountName, you need to manually change the **User Search Filter** parameter in the Service Portal LDAP settings to sAMAccountName={0}.

   > Make sure that the **Full Name** field in the Service Portal LDAP Attributes is the same as the mapping value specified for the contact.name field of the "contacts" file in the Service Management LDAP mapping.

> For more information on configuring LDAP settings, see the "Configure an LDAP server" section in the "Configure LDAP" topic from the Service Manager Help Center.

5. Add Group that is used to 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 either of the following:
        LDAP Representation - for which you type the Distinguished Name and select the Authentication configuration.
        Database Representation - for which you manually add Associated Users to the group. Note, see Concepts for details of manually adding users to a Database Representation group.
        Calculated Representation - for which you first specify a Reference User, and then a set of User Profile Attributes is displayed. Next, you add attributes to the Calculation Criteria. Finally, to complete the criteria for the Calculated Representation group, you select the Combining Criteria — either all criteria must match or at least one criteria must match.
    d. Click the **Save** button to finish and save your new group.

6. Add 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, for the role that you want to associate with a group, click **Add 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.

Master data onboarding

A master data onboarding tool set ships with the ITSMA suite release. This tool set can help you import master data from an existing Classic ITSMA system to ITSMA NG Express.

- Purge demonstration data
- Use the data onboarding tool set to import master data
- User data onboarding in ITSMA

> This tool set supports master data onboarding for Service Management only.

> This tool set supports incremental data import, which means you can always import new 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 Manager, Smart Analytics, and UCMDB.

> To purge demonstration data, you must log in to the ITSMA Suite Portal as a suite administrator first. 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 Manager

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.

> Next, continue with purging indexes from Smart Analytics.

Purge indexes from Smart Analytics

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

1. Make sure 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, which are triggered in Smart Analytics Configuration. Normally, one Service Manager Server has only one SMIDOL instance named as SMIDOL*. The asterisk sign is the sequence number, which is usually 0.

3. From the navigator, click **System Status** and make sure the **KMReindex** schedule is started.
4. Perform indexing for each Hot Topic Analytics configuration record:
   a. Click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Hot Topic Analytics**.
   b. Click **Search**.
   c. Select a configuration record, and then click **Start Index**.
   d. Click **Yes** in the confirmation dialog that is displayed:
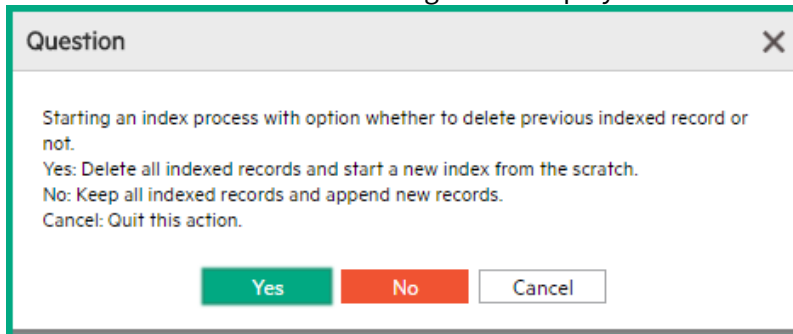
5. Perform a full re-index for each Smart Ticket task:
   a. Click **System Administration** > **Ongoing Maintenance** > **Smart Analytics** > **Smart Ticket**.
   b. From the Current Configuration List, select a task.
   c. Click **Training**.
   d. Click **Yes** to confirm the training action.

6. Perform a full re-index for 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**.
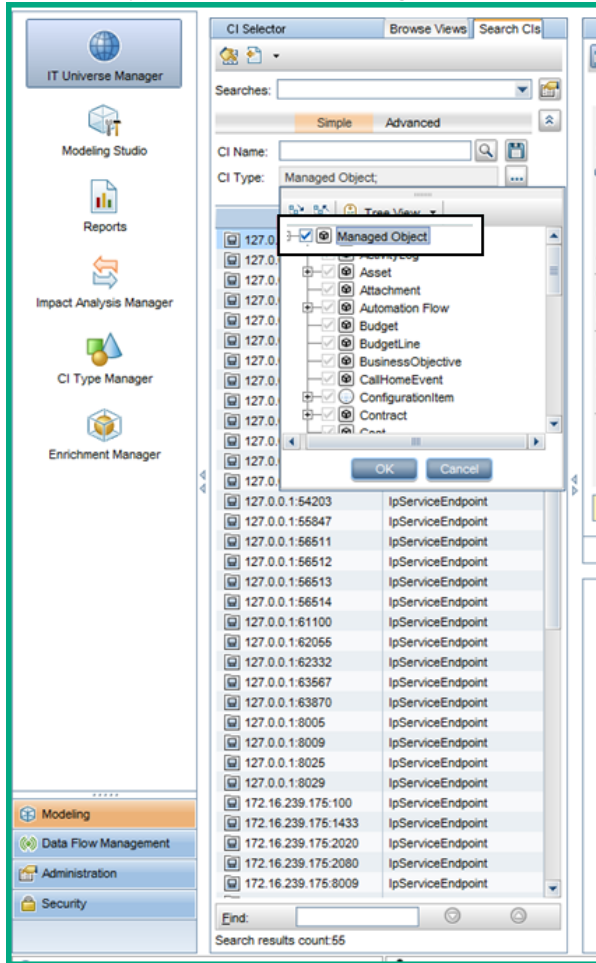
4. Click the search icon (magnifying glass) next to the CI Name field. A list of CIs is displayed.

5. Select all CIs, right-click the mouse, and then select **Delete from CMDB**.
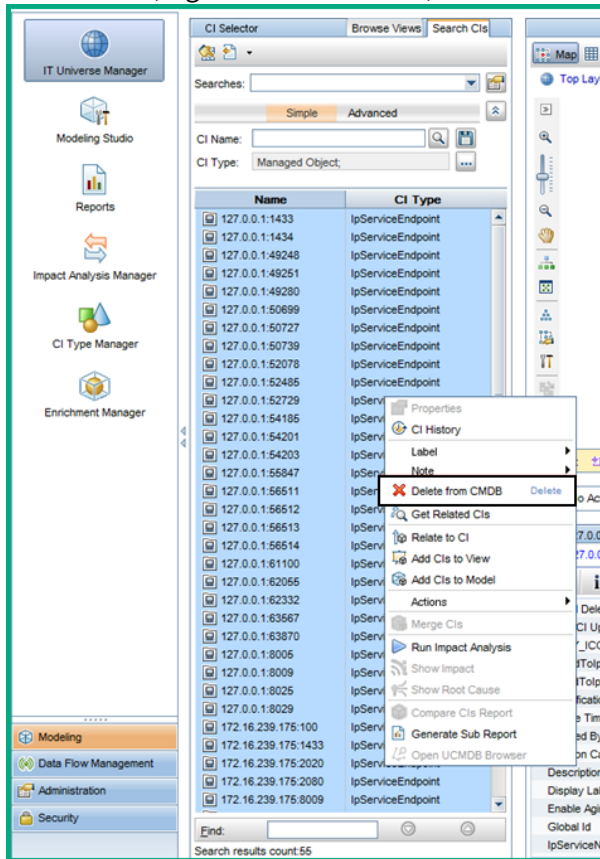
Use the data onboarding tool set to import master data

If you have an existing Service Manager implementation, you can import the master data into your ITSMA system by using a tool set that ships with the ITSMA suite as a .zip file. This tool set comprises the following tools:

- An Microsoft Excel spreadsheet with 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 required for running the scenario (located in the **SM-CIT** subfolder)
- Sample CSV files (located in the **CSV** subfolder)

> In this release, this tool set supports data migration only for Service Manager. For known issues with this tool set, see Known issues.

Understand the Excel spreadsheet

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

This section describes the "ITSMA_Suite_Supporting_Data" spreadsheet used to capture the supporting data for each of the modules for the ITSMA suite.

The Excel spreadsheet is located in the **Excel** subfolder of the data onboarding package (.zip). Click each tab (worksheet) and read the following instructions.

Color codes

The Excel sheet uses the color codes described in the following table.

Color	Explanation
Yellow	Cells with this color contain sample data, which is NOT imported
Red	Cells in red, allow to specify additional data to import
Grey	These cells are automatically populated based on the value selected in another cell
Green	These cells indicate that they only require you to select a value. The selected value does not get imported into the solution; instead, it is normally used to populate a cell marked with the grey color. For example: Column A allows you to select a value, which then populates column E. Column E is then imported into the solution.

The Selections worksheet

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

Data available in this worksheet is described in the following table.

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, 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 operator template to set basic details of the operator record, like 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 the worksheets

Some worksheets reference data from other ones. Their cross references are put in place to ensure that the entered data is correctly referenced. The ITSMA solution will import the same references between the data records into the ITSMA suite components.

The references help to allow the selection of 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	<u>Notes</u>	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

This means, in some cases, that a worksheet can only be completed when some data is correctly entered in the other worksheets.

Worksheets

The following describes the worksheets in the Excel spreadsheet.

Information

This worksheet contains some basic information.

Companies

The Company record represents the highest organizational unit for which a complete self-contained set of accounts can be drawn. A company will represent a customer and RIT itself as organization. It contains contact information and preferences about the companies you work with.

Examples:

- Customer A
- Customer B
- Customer C

Locations

Contains addresses and organizational information about the location of the companies. It is a hierarchy of records to document the following information of a company: locations, sites, buildings, and so on. The data can be used in contact records to see in which place a person is located.

Examples:

`Company: Customer A`

`/AT/City/Street1`

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

Contacts

Contains contact information about users who contact the service desk to initiate a service desk interaction, incident, or change, a person orders from the Service Request Catalog or someone who uses components tracked in Configuration Management.

A contact record is linked to a company, department and location. The Unique id for contacts is the contact name. The contact name is used as reference in many places in the system and creates the link to the operator

object. To easily link contacts with operators it's recommended to use clear identifier for Contact and Operator Names (see examples below).

Examples:

Contact Name: firstname.lastname@customera.com (Email address, in this example)

Company: Customer A

Department: Group 1

HP Service Manager ID: this is the operator Id to logon in Service Manager

Location: Floor 1

Departments

The department shows the data we would expect for the master data entities related to the Business-Organization of a company, as per the model of the overview section. I should be ensured that organizational structure is built within the department table. The department represents the next level of organizational units, after the company record. The department structure is hierarchical organized, which means each level is referenced with a parent department.

Each department is related to a company as a first level. This allows a clear distinction and selection of the required data.

Departments are important for the correct relation of the following records:

- SLA records with the Business Services in the Subscription Table.
- Contact records to the correct Organizational Unit, whereas each contact can only be linked to one department

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

The operator represents a person (internal and external), which actively works with the system. In theory every person having access to a computer has an active directory entry may have access to the ITSMA Suite. The import process should focus on operators actively working in the different modules in the ITSMA Suite. End Users which only access the end user portal don't need to be imported. End Users are created automatically within the suite, upon first login.

To import and successfully create operator records the following data should be provided:

- Name

- Contact ID
- Company
- Security Roles / Profiles

Other required attributes are set through 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 the ITSMA suite.

Example:

`Name: WZRXX212` (Windows Login ID. E.g. Unique value in the LDAP structure)

`Company: Customer A`

`ContactID: firstname.lastname@customera.com` (link to the contact record)

Template operators

As part of this solution template operators are provided to ease the creation of operator records. Template operators are used to prefill some of the required attributes, such as the startup menu, capability words, currency or query groups. Out-of-box template operators are described in the following table.

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 these template operators are not covering your requirements, adjust these template operators or create new ones.

Operator Security

This worksheet helps to associate the correct authorization rights to users using the suite.

The security model provides a consistent method of assigning permissions to users across all facets of ITSMA data and accounts for out-of-box rights that can be configured for a specified role within an area. 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 right for the contract management module.

Configuration Profile:

The profile determines the access right 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 Manager reads the security group records to determine the filtering conditions to apply to the query. Service Manager then returns only those records that match the filtering conditions in the security group records.

Examples:

```
change manager, change analyst
```

Vendors

The Vendor master data contains the list of suppliers (vendors and service providers) that help supporting the IT solutions. This allows defining:

- To which supplier a ticket was sent to in the case there is no specific Assignment Group for it
- To which supplier the Assignment Group is related in the case it is a service provider

Examples

```
HPE, SAP, MICROSOFT
```

Assignment Groups

The Assignment group represents a team of people involved in Service Management process to which tickets can be assigned. Incidents, Problems, Changes, Requests, etc. are assigned to these groups as work from their members is required.

The naming convention for the Assignment Group is a very important aspect, since it allows all parties of the "Support Organization" to have harmonized group names which allow faster and more accurate (re)-assignment. However, the group name is only one main characteristic of the group that should allow finding the right home for a ticket. Additional attributes like 1st level, 2nd level or further classifications, are the ones making the difference, as the user can search for Assignment Groups based on their 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 is allowing to easily setup the group members and other attributes for the assignment group. You can specify the members or approvers of each group, but also other attributes like supported languages, supported departments or locations.

Languages, departments, and locations are required to make best use of the Assignment Rule engine.

KM Groups

The KM Group is similar to an Assignment Group; however the specialty is that it allows relating the group with a specific KM profile and KM Category to give the group members rights for the creation, review and approval of KM Documents.

Examples:

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

KM Group Assignment

This worksheets is allowing to easily setup the group members and other attributes for the KM group. You can specify the members of each group.

Holidays

The following diagram illustrates how Holidays and Holiday Groups are related. In the example below we have two holiday groups, Germany and China. Each group is linked with the particular holidays in each country.
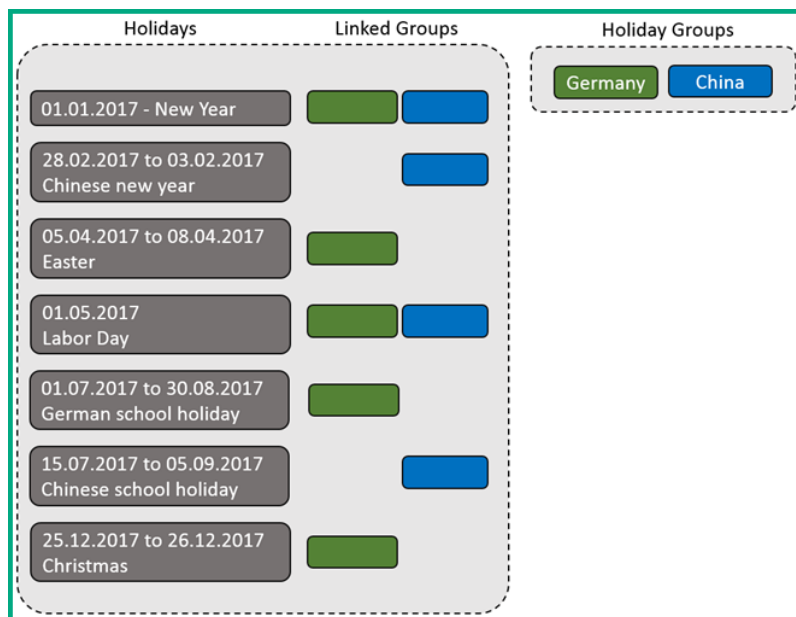
Holiday Group

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

Holidays

The **Holidays** worksheet allows you to enter all holidays relevant for 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

A work schedule defines the work hours for one or more operators. HPE Service Manager can generate a complex 24x7 schedule that spans multiple time zones, includes all shift and break information, accommodates any regional shift to Daylight Savings time, and automatically accounts for local or national holidays. Service Manager uses the following information to create a work schedule:

- Shift and break information

- Holiday information (optional)

Service Manager Uses work schedule information in various calculations. One of the more important calculations is when to trigger a SLA alert that an incident is about to breach a SLA.

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

Service subscriptions 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.

Each subscription can be associated with one Service SLA. The subscription table stores the SLA ID for the Service SLA associated with the subscription. HPE Service Manager supports multiple Service SLAs when an interaction, a change request, an incident, or a problem record is created.

A power user can search for and view the Service SLA title when viewing a subscription record. A self-service user can view the Service SLA in a read-only find field. When a self-service user clicks the Find button, a detail window opens that contains the Service SLA ID, title, and description.

The following diagram depicts the relationships between SLA, Subscriptions and Business Services.
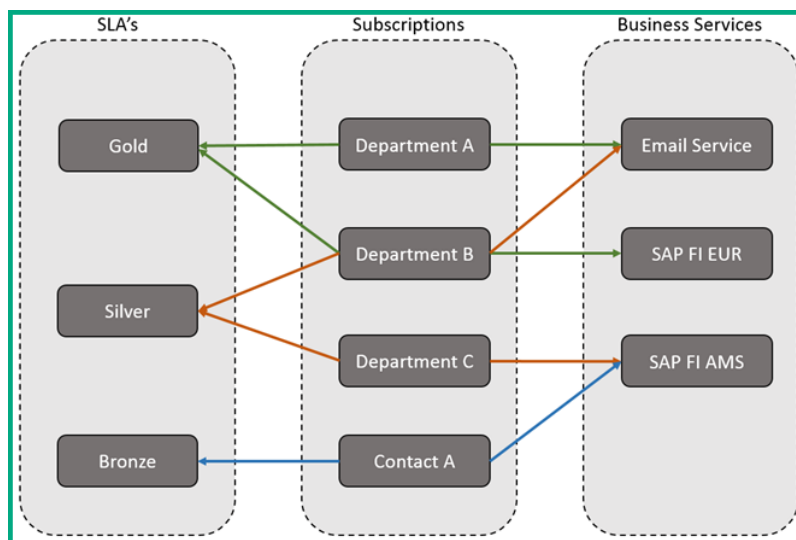
Customizing the data fields

The Excel spreadsheet should suffice to collect customer data in most cases; however, you can customize the tool if you have extra custom fields to collect.

Most of the worksheets therefore have at least one RED section to capture the extra customer fields:

For each of the tabs (worksheets), there is a line of code in the Visual Basic Macro to export the data to a CSV file. See also the comments in the macro code itself.

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

- It is clear from the above code line that only one extra field is expected (column E). You need to customize this code line if you have more customer fields.
- Furthermore, the macro only exports up to line 999. Therefore, you also need to customize this code line if you have more data lines.

Next, you are ready to enter supporting data in the Excel spreadsheet and export the data to CSV files. For details, see Export data to CSV files .

Export data to CSV files

This section explains how the "ITSMA_Suite_Supporting_Data" spreadsheet provided by HPE can be used to generate a number of CSV files that you can import into your ITSMA suite system.

The import files are CSV files that must be loaded into the ITSMA solution through HPE Connect-It. The user to import the data will require sufficient rights to execute these imports, and is therefore typically reserved to those who have administration rights.

The spreadsheet contains only the main options that dictate the minimum required settings in the ITSMA suite, and hence is in no way a complete replacement for direct entry into the ITSMA solution. There are a multitude of other factors and data that can be fine tuned. These settings cannot be entered through simple Yes or No answers and are hence not part of the spreadsheet.

To export the CSV files, follow these steps:

> 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 tool set package to a temporary directory on your local drive. For example:
   C:\DataOnBoarding

   > When unzipping the package, keep 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. Enable macros 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.
   For example, in the Contacts worksheet, we add a customer field named "Region".

	A	AH	AI	AJ	AK	AL
1	Contact					Customer Field
2	Notes					
3						
4	Definition					
5	Label	Misc_Aristocratic Title	Misc_Form of Address	Valid From	Valid To	Region
6	Fieldname	aristocratic.title	form.of.address	valid.from	valid.to	
7	Data Type	character	character	Date/Time	Date/Time	
8	Data Requirement	optional	optional	optional	optional	
9	Field Length	50	30			
10	Unique					
11	Field Note	e.g. Lord; Lady; Your Worship	e.g. Mr; Mrs; Miss; Ms			
12	Format Rules					
13	Example Data	Lord	Mr			
14	Data					
15	Please list your data here					Americas
16	in this area					EMEA
17						
18						
19						
20						
21						

5. If needed, customize the "PrepareITSMAImport" macro as needed. For detailed instructions, see Understand the Excel spreadsheet.
   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.

   > Before editing, copy the code lines of the macro to a text file for backup. If the code is lost, you can recreate the macro using the text file.
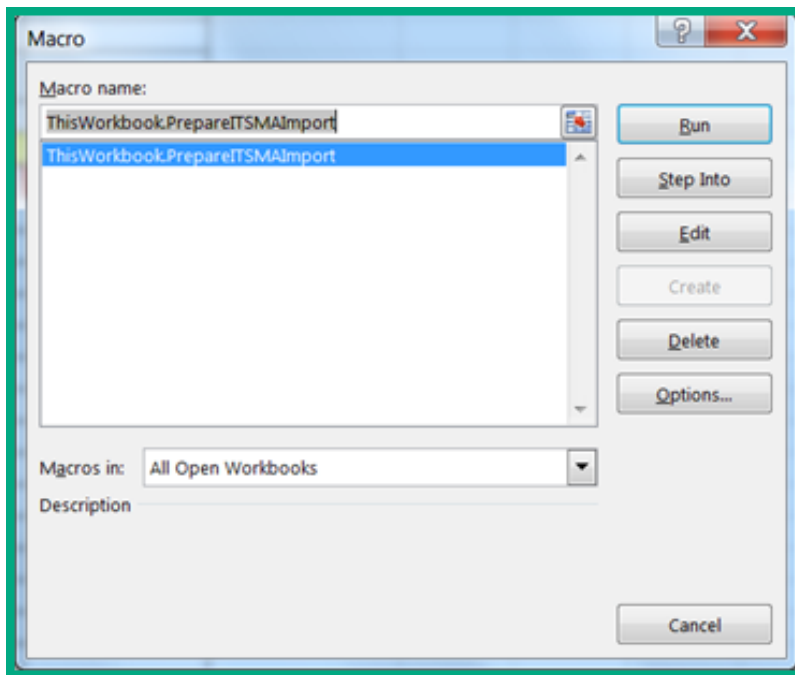
> If a worksheet contains more than one customer field or more than 999 lines,
> you need to update the "Call CreateITSMACSV" code line for the worksheet.
>
>

6. Once you have finished editing the macro, click **Run**.
   This will generate 12 CSV files in the current directory, which in theory is "My Documents" or
   the directory from which you opened the spreadsheet.
   If you execute the macro several times, the macro will overwrite existing files in the folder.
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:
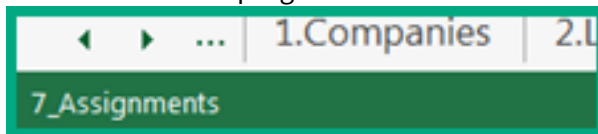
> If you execute the macro several times, the macro overwrites existing files in the folder.

Next, you need to import the CSV files into the suite. 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.

Once the CSV files for import are ready, you can run this Connect-It scenario to import the files into the ITSMA suite.

> In this release, this tool supports data import only for the Service Manager capability in the ITSMA suite.

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

You are recommended to 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 one-time data onboarding. 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 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.
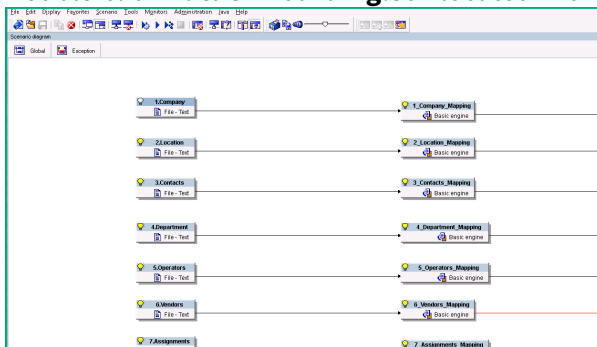
   12 source connectors are displayed.
2. Configure the source connectors.

a. Right-click the Company source connector, and then select **Configure connector**.
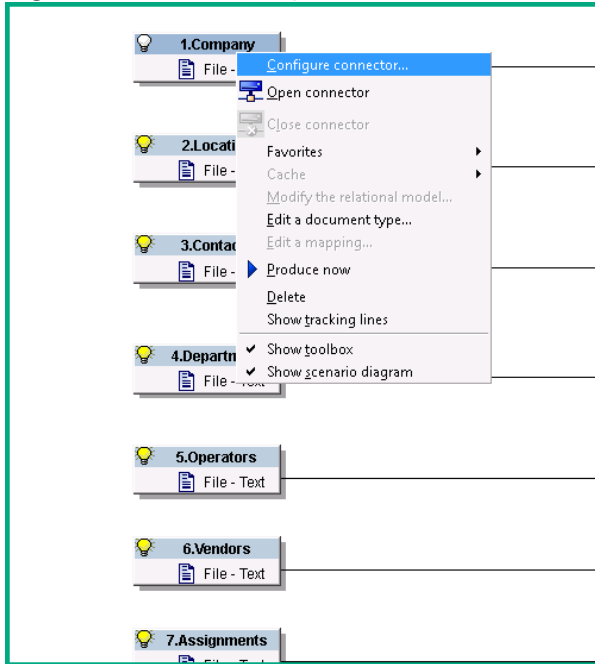
b. Click **Next** repeatedly until you see the "Select files or folders" page. Click the **File name** field and then browse to the corresponding CSV file.
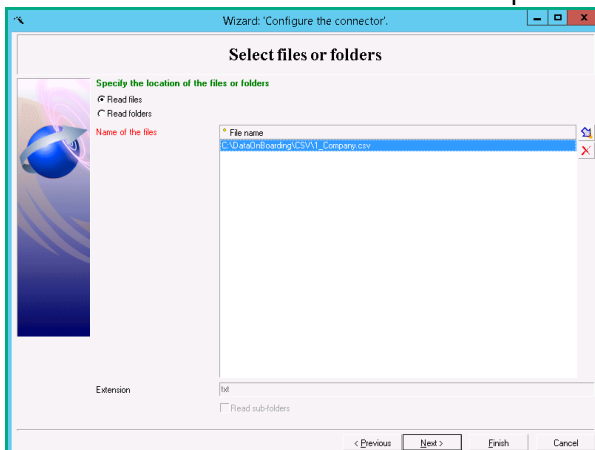
c. Click **Next** repeatedly until you see the "Choose a description file" page. Browse to the corresponding description file on your local drive.
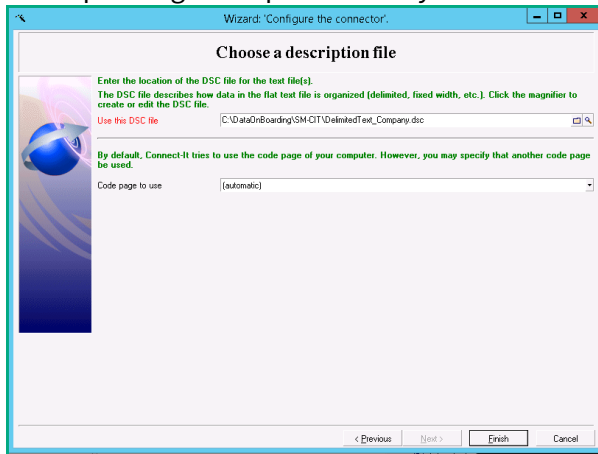
d. Click the Edit button to the right of the **Use this DSC file** field to open the "Select a document type" window.
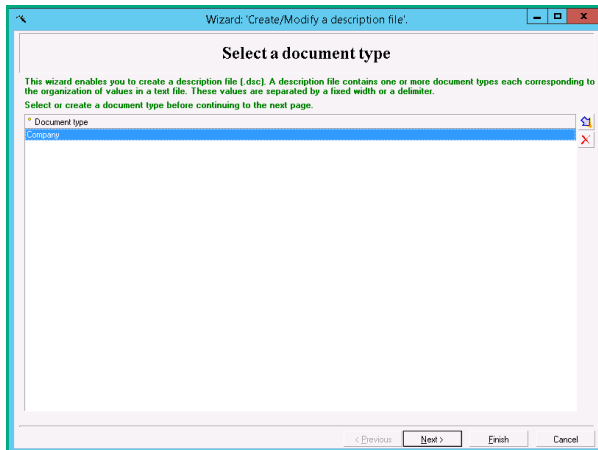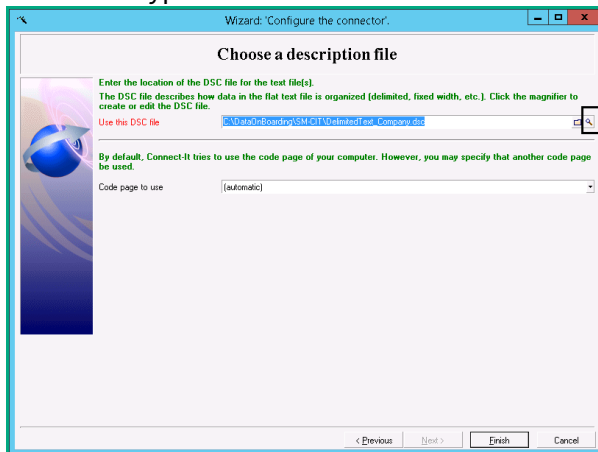
e. Click **Next**.
The following page is displayed.
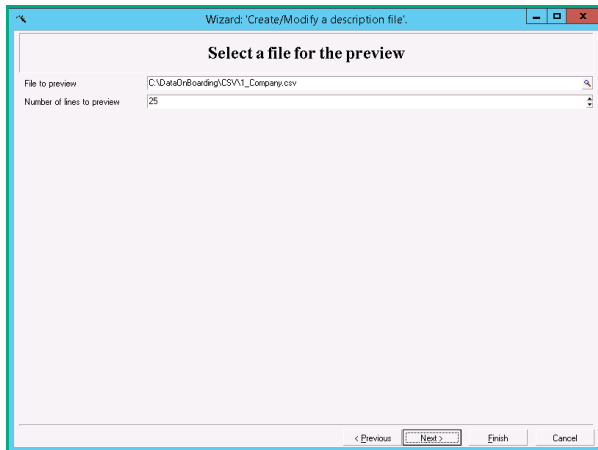
Click **Next**.

f. Make sure **Delimiter** and **Comma** are selected.
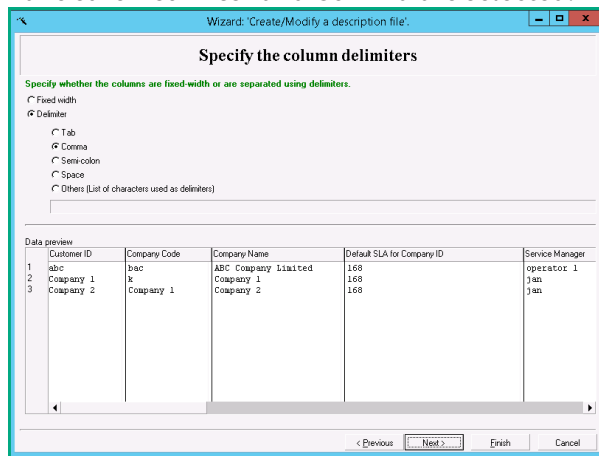
Click **Next**.

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 (").
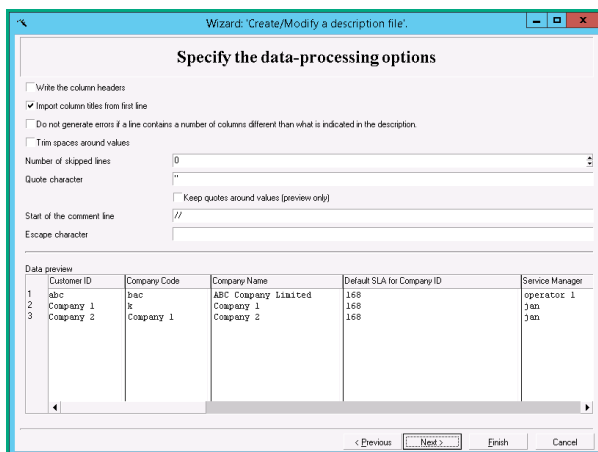
Click **Next**.
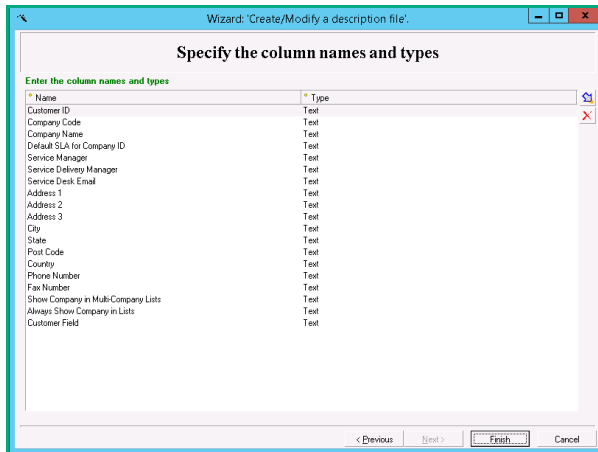
> Click **Finish**.

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

Next, continue with configuring the data mappings between each source connector and the destination connector.

Task 2: Configure field mapping

In this task, you will configure mapping for customer fields that you entered in the Excel spreadsheet.

> Manual mapping for the out-of-box fields are not required.

To do this, follow these steps:

1. In the scenario diagram, double-click the Company mapping.
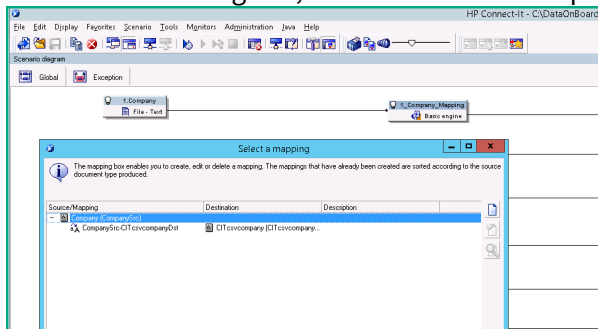
2. Double-click the mapping destination.
3. For the customer field ("Customer Field" on the left-side pane), locate the mapping field on the right-side pane (**companyold** in this example). Drag and drop the mapping field from right-side pane to the middle pane.
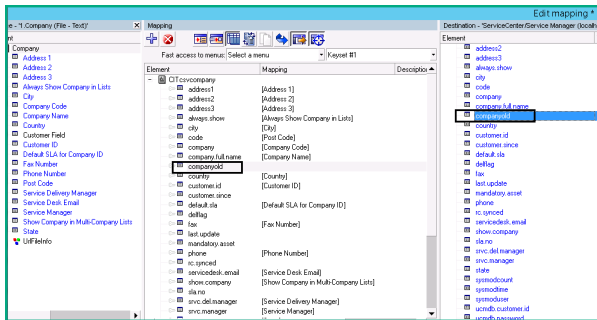
> Fields on the left-side pane are from the CSV file, and those on the right-side pane are from the **company** table in Service Manager.

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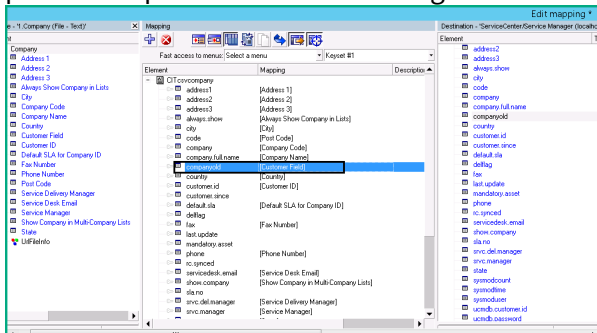
If the customer field is an array field in Service Manager, you should use a mapping script instead of the mapping method described above.
As an example, here is a mapping script for the out-of-box **secRole** field in Service Manager:

```
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** at the lower right corner of the window and then save the scenario.
6. Repeat the same steps for the rest of the mappings in the scenario.

Next, continue with configuring the destination connector so that Connect-It can connect to the ITSMA suite.

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**.
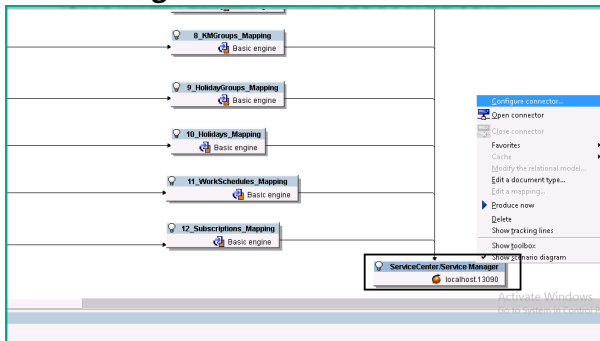
2. Click **Next** to enter the **Define the connection parameters** page, and then enter the following information:

    - **Server name**: Enter a value with the following format: *<host FQ*DN>.31191.
      Here, *<host FQ*DN> is the fully qualified domain name or IP address of the ITSMA master node, and 31191 is the SM-CIT integration port.
    - **Login** and **Password**: Enter the user name and password of an ITSMA suite administrator user (for example, the **sysadmin** user).
    - **Service Manager server port**: enter **31191**.

    > In the ITSMA suite, this is the SM-CIT integration port instead of the SM RTE port.

    - Make sure the following options are selected:
        - **Service Manager 9.20 and later versions**
        - **Write to a Service Manager database**
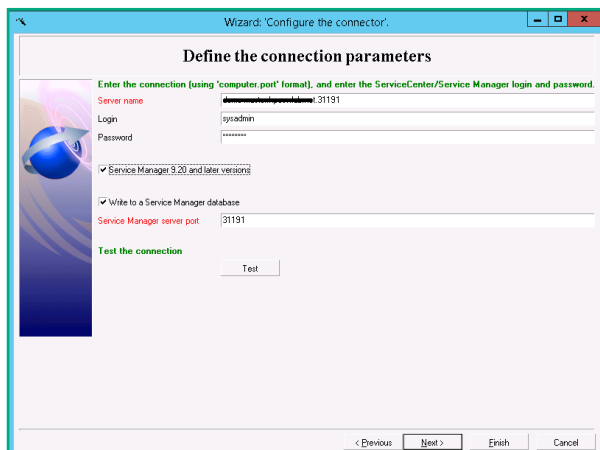
3. Click **Test** to make sure that the connection test is successful.
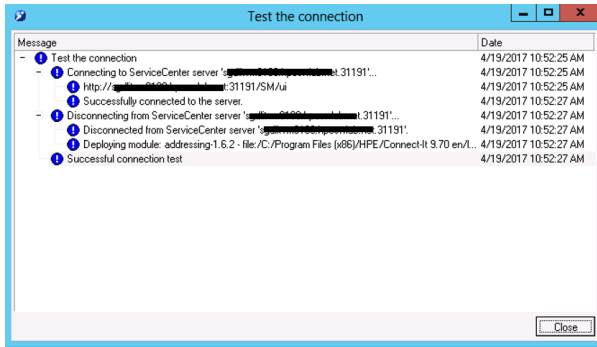
Click **Close**.

4. Return to the wizard screen, and click **Next** repeatedly until you see the **Define document types** page.

Browse to the **smdb951.cfg** file located in the C:\DataOnBoarding\SM-CIT directory, and then click **Finish**.
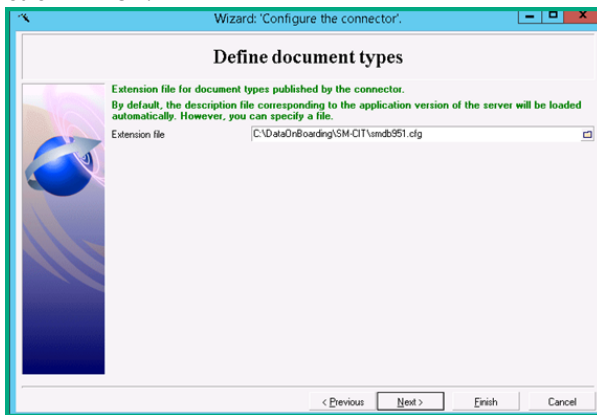
Next, run the scenario to import the data.

Task 4: Run the scenario

> Each CSV file is prefixed with a sequence number (1, 2, and so on). Be sure to import the CSV files in the correct order (import "1" first, then "2", and so on).

To do this, follow these steps:

1. In the scenario diagram, right-click **Service Center/Service Manager**, and then select **Open connector**.
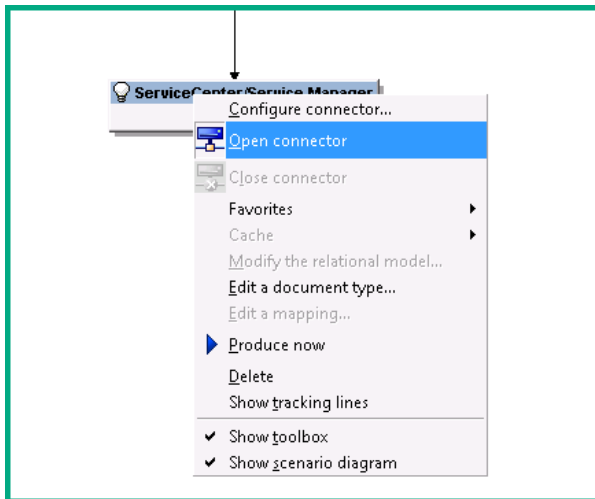
2. Right-click the Company source connector, and select **Produce now**.
   Wait until the data import is complete.
3. Continue to produce data for the rest of the source connectors in the following order:

> To produce Subscription data, configuration items (CIs) are required to 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. This is because Subscription data is connected with CIs, and subscription data import will fail without CIs.

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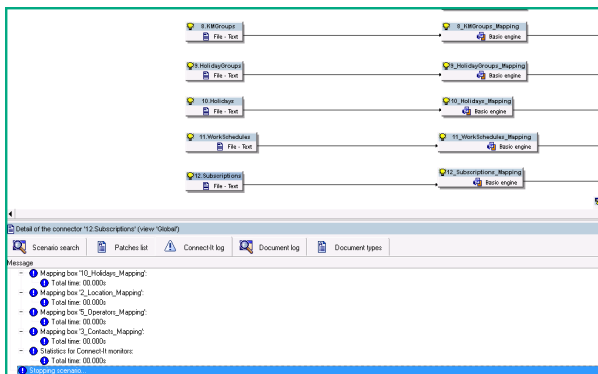
Step 3: Verify the imported data

After the data onboarding scenario is executed, verify the data is successfully imported into the ITSMA suite:

1. Log into ITSMA as **sysadmin**:
   https://<master node FQDN>/main
2. Click **Service Management**.
3. Enter **db** in the command line, and 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.
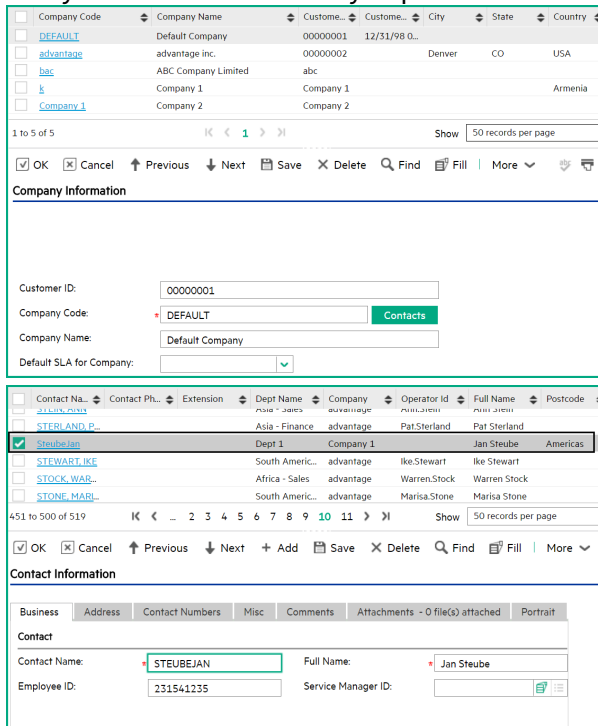
If any issues are found, see Troubleshoot data onboarding.

Extend the tool set to import more customer fields

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

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

1. Enter your data, including the customer fields in the Excel spreadsheet. For instructions,
   see Understand the Excel spreadsheet.
   In this example, we enter three customer fields in the Contacts worksheet: Customer Field1,

Customer Field2, and Customer 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 data to CSV files.

4. Double-click DataOnBoarding.scn 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 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 customer fields that you added are loaded into Connect-It.
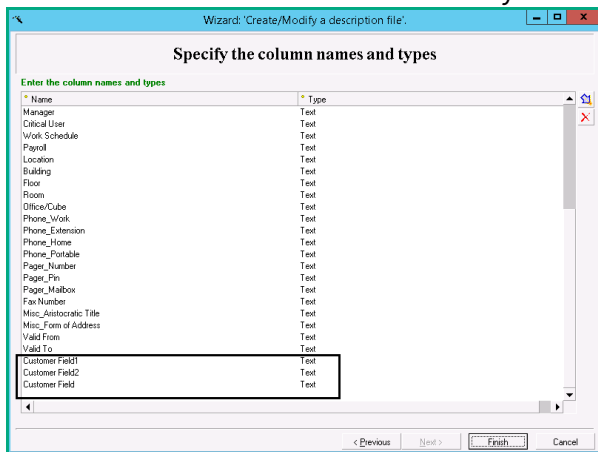
6. Reconfigure the mapping.
   Double-click the mapping to open the following window, and then double-click the highlighted part.
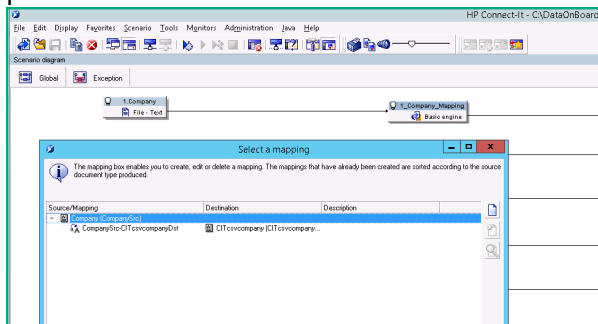
   The field that you added in Excel now appears on the left-side pane. Drag and drop the field to the right-side pane. Click **OK**.

Double-click the Contacts mapping, and then drag and drop the customer fields to the middle pane to map them to their corresponding fields in the Service Manager 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 onboarding

This section provides tips that help you troubleshoot data onboarding issues that you may encounter in Connect-It and the ITSMA suite.

Troubleshoot in Connect-It

The following are some errors that you may encounter in Connect-It.

"Invalid value" error

- *Description*: when running the data onboarding scenario, this error is displayed. See the following figure for an example.

- *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

- Description: when running the data onboarding scenario, this error is displayed.
- *Root cause*: you have added one or more columns in the Excel spreadsheet and exported the data to CSV files, and then run the data onboarding scenario without reconfiguring the source connector and mapping. This is because the newly added data is not reloaded to the scenario.
- *Solution*: if a CSV file is updated, 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

- *Description*: when running the data onboarding scenario, this error is displayed.
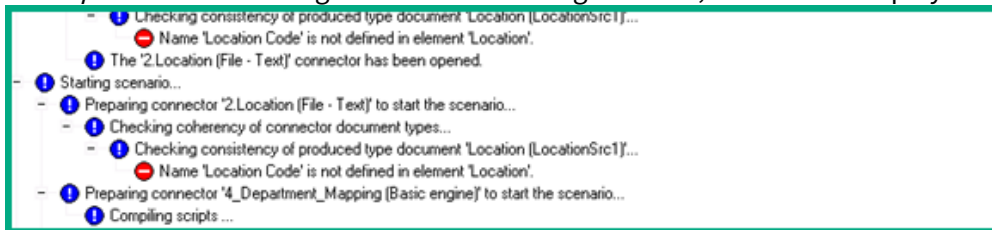
- Root cause: you have update a column header in the Excel spreadsheet and exported the data to CSV files, and then run the data onboarding scenario without reconfiguring the source connector and mapping. This is because the newly added data is not reloaded to the scenario.
- Solution: If the update 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 in the ITSMA suite

Follow these guidelines to troubleshoot data import problems on the ITSMA suite side.

Monitor the eventin queue

Once the data is imported into Service Manager, 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 SM 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**. Click **Search**.

If **eventin** records remain in the queue, do the following depending on their Status value:

- If the Status is empty: this status indicates that the data is not executed.

  Solution: go to **System Status** on the navigator to restart the **event** process.
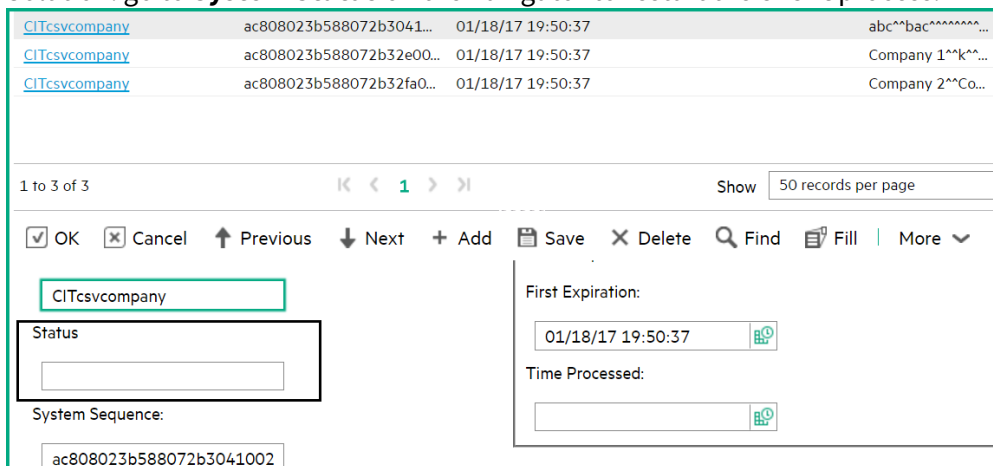
- If the Status is "error": this status indicates errors occurred when the system attempted to insert the data into the database.

  Solution: debug the error according to the error messages. For example, the following figure shows an error caused by an empty primary key value.
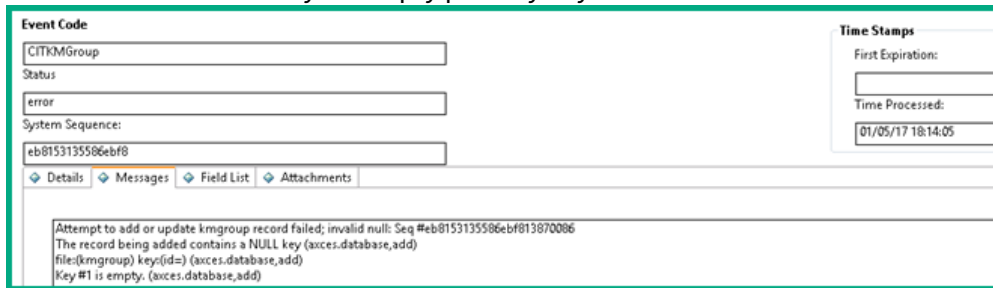
Check the Scheduled Event Types global list

For successful data import, 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 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.

User data onboarding in ITSMA

User data onboarding in 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 tool set 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 tool set to import master data.

> - This tool set supports incremental data import. You can always run the tool set to import new user data.
> - For Service Portal, no user data onboarding is needed. However, manual LDAP configuration is needed before LDAP users can log in to Service Portal. For more information, see Configure an external LDAP server.

User data onboarding in CMDB

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

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

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

> If you are using the internal LDAP server, users from the LDAP server are created in CMDB with a 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.

Configure Email

User role: Suite Administrator

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. On the suite landing page, click **Suite Configuration**.
2. Click **CONFIGURATION** > **Email Service**.
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 of 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.

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. If the system fails to restart some of the services, click **Revert** to revert all changes that you just made.

Configure log level for debugging

User role: Suite Administrator

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

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

Once debugging is enabled, additional logging information is written to the suite logs, which you can download from ITOM Container Deployment Foundation (CDF). For more information, see Manage Suite Export Logs.

> After your confirmation for applying the changes, the system restarts the related services. If the system fails to restart some of the services, click **Revert** to revert all changes that you just made

Configure 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 dropdown list and then click the **Update** button. Or, you can directly modify the parameter values in the text area.

> For information about the description and values for the Service Management server parameters, search for the parameter in the Service Manager Help Center . 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 in the text box.

Parameter name	Default value	Possible values
sqllimit	10	Number of seconds For example: 1,2,3,4,5,10,20,30,60
debugdbquery	5	Number of seconds or 999 for a full query debug. For example: 1,2,3,4,5,10,20, 999
cache_clean_interval	3600	1800; 2700; 3600;
webservices_sessiontimeout	1800	15; 30; 60; 120; 300; 600; 900; 1800; 3600
connectionTimeout	180000	45000; 60000; 90000; 180000
smartemailTimeout	45000	30000; 45000; 60000; 90000; 180000
sqldebug		0 (Disable) ;1 (Enable)
debughttp		0 (Disable) ;1 (Enable)
debugjavascript		1; 2; 3
debugrest		0 (Disable) ;1 (Enable)
logdebuglevel	1	0 = DEBUG; 1 = INFO(default); 2= WARN; 3 = ERROR; 4 = FATAL
debugjni		0 (Disable) ;1 (Enable)
log4jDebug		com.hp.ov.sm.common.oom.LowMemoryHandler
enablecoredump		0 (Disable) ;1 (Enable)

rtm		0, 1, 2, 3, 4, 5
maxlogsize	20 (Size in MB)	5, 10, 20, 40, 60, 80, 100
numberoflogfiles	10	0 to 100

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

> For information about the description and values for the SM web tier parameters, search for the parameter in the Service Manager Help Center .

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

Parameter name	Default value	Possible values
session-timeout	15	Number of minutes
viewrecordlist	true	true; false
querySecurity	true	true; false
jsDebug	false	true; false

6. Click **Apply.**

> - The default folder to store customized branding files and settings is **<ITSMA NFS shared folder>/logs/sm-9.52/webtier**.
> - The default path to store the exported dashboard report is **<ITSMA NFS shared folder>/logs/sm-9.52/report-export**.
>
> **<ITSMA NFS shared folder>** is the directory that you set up for NFS sharing for ITSMA during installation (For example: **/var/vols/itom/itsma/itsma-itsma1**). For more information, see Configure NFS sharing for ITSMA.

Configure 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 add more modules with their log levels specified.
   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 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 these log levels:
   - INFO (default): An event for informational purposes.
   - DEBUG: A general debugging event.
4. Click **Apply**.

Configure 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 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 dropdown 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

- Click **Apply**.

Add Smart Analytics content groups

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

To Smart Analytics content groups, follow these steps:

1. On the suite landing page, click **Suite Configuration**.
2. Click **Operation** > **Smart Analytics.**
3. View the capacity of the current content groups for Service Portal and 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 Service Portal search and Smart Search features stop 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 Service Portal search or Smart Search feature without any downtime.

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

> A fter you add a new content group, you are recommended to redistribute documents to make the new content group active.

Set up Service Portal

When the ITSMA suite is installed, Service Portal is pre-configured with the following settings:

- Creation of mapping of LDAP groups to the IdM consumer group so that LDAP users are consumers
- Creation of a supplier for Service Management
- Creation of service and support aggregation (with automatic publishing of catalog items)

Shared IdM

The ITSMA suite uses HPE Identity Manager (IdM) for user authentication. So does Service Portal. When working as a standalone application, Service Portal uses its own built-in IdM service. In the ITSMA suite, Service Portal and the ITSMA suite share one IdM instance.

Shared Smart Analytics

Service Portal uses Smart Analytics for its search functionality. In the ITSMA suite, Service Portal shares one Smart Analytics instance with the Service Management capability.

Out-of-box organizations

In the out-of-box Service Portal system, there are two organizations.

Organization	Description
Provider	• Has type "PROVIDER", which is different than the "CONSUMER" type organization (ITSMA); designed to be used for cross-organization configuration • Contains integration users for cross-service communication • Allows service-exchange "content-pack" management • Allows configuration of all organizations and creation of new ones in idm-admin
ITSMA	Designed to be used for consumers (end users)

The following are post-installation configurations that are needed for Service Portal to work correctly.

Enable the Hot News application

Normally, your ITSMA is deployed behind a firewall. In this case, you need to perform the following steps to activate the Hot News application in Service Portal. If you fail to do this, users are not able to open the Hot News application.

1. Log in to the master node.
2. Add your proxy setting to the configmap file:
   a. Run the following commands:
      cd /var/vols/itom/core/suite-install/itsma/output/
      vi configmap.yaml
   b. Configure your proxy in this file:
      http_proxy=http://<your proxy>:<port>
      https_proxy=https://<your proxy>:<port>

3. Run the following commands to restart configmap:
   kubectl delete -f configmap.yaml
   kubectl create -f configmap.yaml
4. Run the following commands to restart the launchpad service:
   kubectl delete -f propel-launchpad.yaml
   kubectl create -f propel-launchpad.yaml
5. Verify that the Hot News application is working correctly.
   a. Log in to ITSMA**.** For details, see Log in to ITSMA.
   b. Click **Service Portal**, and then click **Hot News**.

Bind the internal PostgreSQL database to a dedicated worker node

Some applications such as the DB and analytics applications are I/O sensitive, and need to be bound to dedicated worker nodes to ensure their stability in a production environment. This is required only if you are using the internal PostgreSQL database for the ITSMA suite. You need to bind the three internal PostgreSQL instances for Service Management, Service Portal, and CMDB to three dedicated worker nodes. For this reason, three additional worker nodes are required for using the internal PostgreSQL database (see Sizing recommendations).

To do this, follow these steps:

1. Add a new label to the dedicated worker node (VM).
   a. Log in to the Management Portal as **admin**: https://<master node FQDN>:5443.
   b. Navigate to **ADMINISTRATION** > **Nodes**.
   c. In the Predefined Labels section, enter a desired label name (for example, enter SMDB for the Service Management DB) and then click the **+** button.

   Predefined Labels

   Worker Database DB [-] SMDB SMDB   [+]
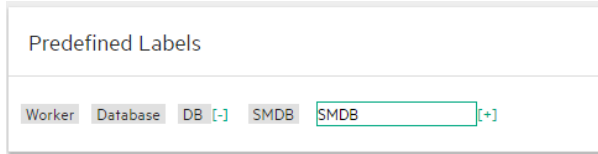
   d. Drag the newly created label to a desired worker node.

   Nodes + ADD   REFRESH

   Status   Name   Labels filter label
   ✓   Worker [-]
   ✓   Worker [-]
   ✓   Worker [-]
   ✓   Worker [-]
   ✓   SMDB [-]
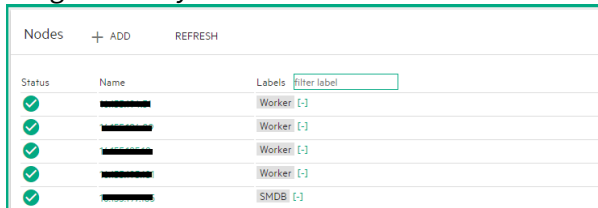
2. Change the label from **Worker** to **SMDB** in the sm-db-rc.yaml file:
   sm-db-rc.yaml

```
template:
  metadata:
    labels:
        name: sm-postgres
        role: master
  spec:
    nodeSelector:
        #Worker: label
        SMDB: label
```

   - If your NFS server is on the master node, this yaml file is located in the following path: /var/vols/itom/core/suite-install/itsma/output.
   - If your NFS server is on a dedicated host, this yaml file is located in the following path: /var/lib/kubelet/pods/xxxxxxxxxx-xxxxxx-xxxxxxx/volumes/kubernetes.io~nfs/itom-vol/suite-install/itsma/output/.
   The path can be found by running the following command:
   `mount| grepitom | head-1`

3. Restart the service:

   - Change to the directory of the yaml file: **cd <yaml file location>**.

   > See the previous step for the yaml file location.

   a. Delete and create the service again by running the following commands:
   kubectl delete -f sm-db-rc.yaml
   kubectl create -f sm-db-rc.yaml

4. Repeat the previous steps for the PostgreSQL instances for Service Portal and CMDB to bind the instances to another two dedicated worker nodes.

> The yaml files that you need to update for Service Portal and CMDB are: propel-postgres.yaml and ucmdb-suite.yaml.

Apply PostgreSQL parameter updates in ITSMA

The internal PostgreSQL database in ITSMA is recommended for test environments only. However, if you use it in a production environment, you may need to update certain PostgreSQL parameters. The major reasons to do this include the following:
- Performance tuning (for example, by default, the internal PostgreSQL database in this release supports only up to 50 connections)
- Maintenance (autovacuum) rule setting
- Other requirements

Once you have updated parameters of the internal PostgreSQL database, you need to apply these updates. To do this, follow these steps:

1. Stop the postgres pod:
   a. Log in to the Management Portal as **admin**.
   b. Navigate to **RESOURCES**, and then select the namespace for ITSMA.
   c. Navigate to **Workloads** > **Replication Controllers**.
   d. Find your postgres service (for example: sm-postgres), and then click the action icon (three dots).
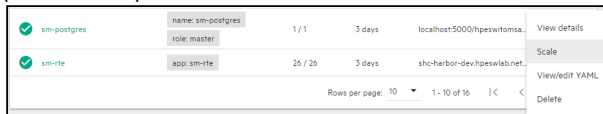
   e. Set the number of pods to 0.
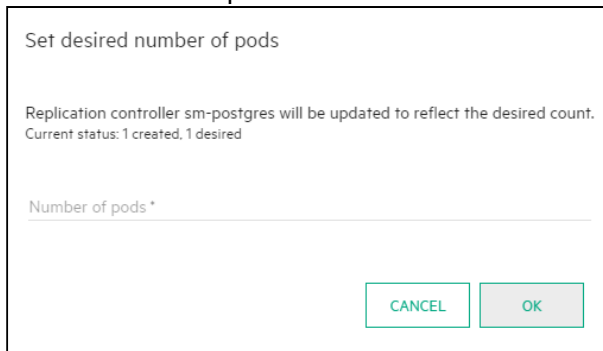
2. Update postgresql.conf file.
   The file is located in the following path (taking sm-postgres for example):
   /var/vols/itom/itsma/itsma-<your namespace>/db/sm
   Update it with the attached postgresql.conf file . Make sure the owner of the file is still 'itsma'.
3. Start the postgres pod:
   a. Log in to the Management Portal as **admin**.
   b. Navigate to **RESOURCES**, and then select your namespace.

c. Navigate to **Workloads** > **Replication Controllers**.
d. Find your postgres service, for example, **sm-postgres**, and then click the action icon.
e. Set the number of pods to 1.

ITSMA node ports

The ITSMA suite uses the following ports for connections and communications.

Item	Value
SM RTE port	31181
SM PostgreSQL port	31132
SM Integration port	31190
SM-CIT integration port	31191
SM Openfire port	31199
Smart search DIH	31370
Smart search DIH index port	31371
Internal LDAP port	31389
UCMDB ports	31400, 31401
UCMDB PostgreSQL port	31402

Customize the ITSMA login page

You can change the text on the out-of-box ITSMA login page to suite your business needs.

The text you can change is highlighted in the following screenshot:
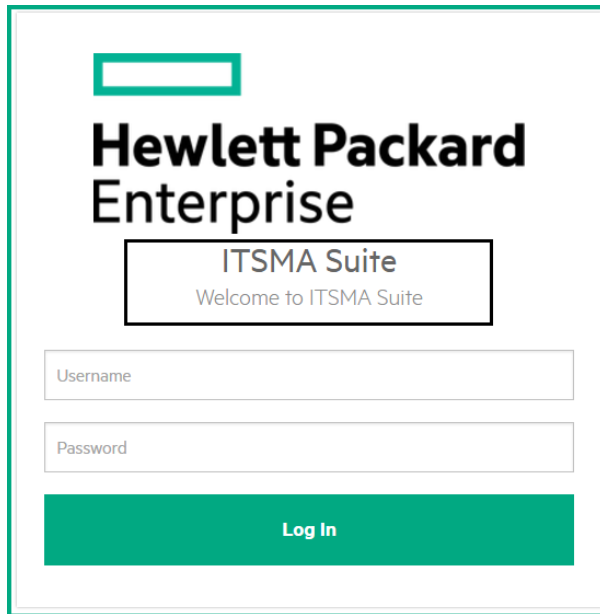
To change the text, follow these steps:

1. Log in to ITSMA as **sysadmin:**
   https://<master node FQDN>/main
2. Click **Service Portal**.
3. On the Launchpad, open the **Identity** application.
4. Click **ITSMA**.
5. On the **Customization** tab, change the values for the following parameters:
   - **portalTitle** (default value: **ITSMA Suite**)
   - **portalWelcomeMsg** (default value: **Welcome to ITSMA Suite**)

Configure users for the internal LDAP server

In the out-of-box system, the internal LDAP server has only five sample users configured. You can configure more users if needed.

> The ITSMA suite uses the following port and user to connect Service Manger and UCMDB to the internal LDAP server:
>
> - Port: 31389
> - LDAP DN: cn=falcon,ou=people,dc=itsma,dc=com (password: 123456)

To do this, follow these steps:

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

   > The following 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 **Apache Directory LDAP Client API** is selected.

   See the following figure for an example.
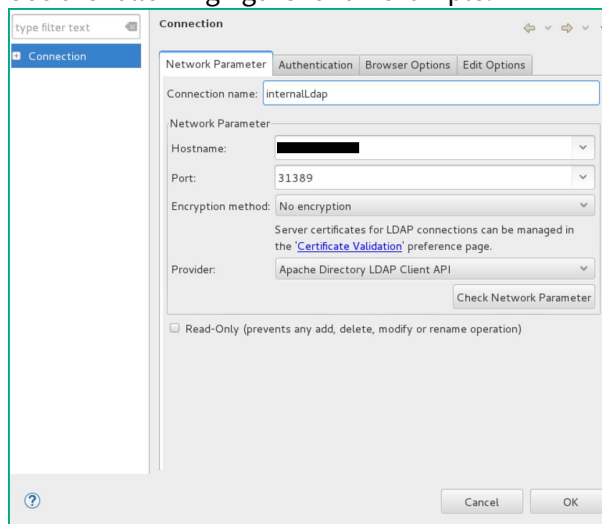
   On the **Authentication** tab, provide the following information:
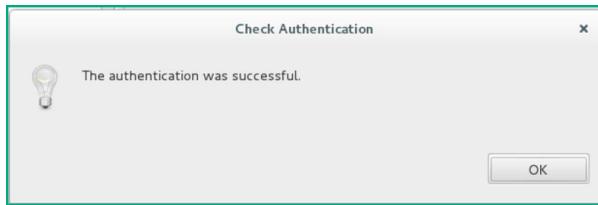   - **Authentication Method**: Make sure **Simple Authentication** is selected.
   - **Bind DN or user**: Enter **cn=admin,dc=itsma,dc=com**.
   - **Bind password**: Enter **secret**. This is the LDAP server administrator password.

   See the following figure for an example.
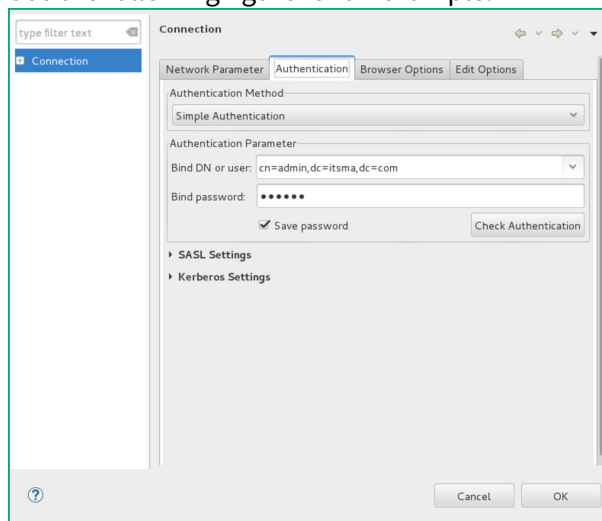
   Click **Check Authentication** to make sure the connection information is correct:

Click **OK**.

3. Add users for the LDAP server. For details, see the OpenLDAP documentation.

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on ITSMA documents (ITSMA 201704)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to ovdoc-ITSM@hpe.com.

We appreciate your feedback!