



Service Manager

Installation and Deployment Guide

2021.4

Copyright Notice

This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti"), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.ivanti.com.

Copyright © 2021, Ivanti. All rights reserved.

Ivanti and its logos are registered trademarks or trademarks of Ivanti, Inc. and its affiliates in the United States and/or other countries. Other brands and names may be claimed as the property of others.

Protected by patents, see <https://www.ivanti.com/patents>.

Last updated: 2/23/2022

Contents

Copyright Notice	2
About the Installation and Deployment Guide	6
Intended Audience	6
Document Organization	6
Related Documentation	7
How to Contact Us	7
Service and Asset Manager Deployment Overview	8
Hardware Considerations	8
Demonstration or Proof-of-Concept Deployment	8
Minimum Production Deployment	10
Enterprise Production Deployment	13
Hardware Requirements for the Enterprise Production Deployment	14
High Availability and Load Balancing	16
About Installing the Service and Asset Manager for the Enterprise Production Deployment	17
Security Enterprise Production Deployment	17
Database Deployment Options	20
Operations Console Deployment Options	27
Reporting Services Deployment Options	33
Voice Deployment Options	39
Ivanti Service Manager Installation Prerequisites	42
About Roles	42
About the Different Accounts Used in Service and Asset Manager	44
About Passwords Used in Service and Asset Manager	46
About Using a Virtual Machine with Service and Asset Manager	46
Enabling Attachment File Streaming	46
Installing the Service and Asset Manager Reporting Feature	50
Enabling Full-Text Search	52
Verifying Server Roles and Features	54
Installing the Service and Asset Manager System	58
Installation Overview	58
Installing Service and Asset Manager	59
Installing the Reporting Feature	61
Installing Discovery on a Dedicated Server	63
Installing the Knowledge Uploader (Knowledge Import Tool)	64
Initially Configuring the System	74
Using the System Configuration Wizard	80
Configuring Service and Asset Manager	84
Finishing the System Configuration	119
Configuring the Reporting Feature	120
Configuring Discovery	131
Configuring the Deployment on the Service and Asset Manager Operations Console	134
Optional SSL Configuration	139

Optional LDAP Configuration	149
About Configuring with ADFS	149
About Configuring Throttling Settings	149
Setting up Redis	152
Different install and uninstall options and scenarios	152
Option 1 - Install Redis in Linux Container on Windows Server	152
Option 2 - Install Redis on Linux Machine	155
Uninstall Redis	159
Logging into Service and Asset Manager	161
Logging In Using the Standard Login Dialog Box	161
Logging In Using the Standard Login Dialog Box with an Application Menu	162
Adding the Application Menu Option to the Standard Login Dialog Box	162
Adding Features and Changing Settings	163
Adding and Deleting Features	163
Changing Feature Settings by Running the System Configuration Wizard	164
Upgrading Service and Asset Manager from an Earlier Release	166
About Upgrading	166
About Upgrading from Earlier Releases	167
Upgrading from Ivanti Service Management Release 2017.3.x	169
Upgrading from Ivanti Service Management Release 2014.3 or Earlier	172
Upgrading from Ivanti Service Manager 2020.1 Release to 2020.2 Release	173
Using the License Manager	174
About the License Manager	174
Types of Licenses	174
About License Bundles	175
Using the License Manager	177
Chat Configuration	189
Configuring Chat	189
Create Incident Quick Action	191
Known Issues	193
Release Version 2021.3	193
Release Version - 2021.2	193
Issue Details	193
Release Version - 2021.1	194
Issue Details	194
Release Version - 2020.4	195
Issue Details	195
Release Version - 2020.3	195
Issue Details	196
Release Version - 2020.2	196
Issue Details	196
Release Version - 2020.1	200
Issue Details	201
Release Version - 2019.3.1	204
Issue Details	204

Release Version - 2019.3	205
Issue Details	205
	208
Release Version - 2019.2	208
Release Version - 2019.1 and earlier	208
Issue Details	209
Troubleshooting	225
Error Messages	225
Software Problems	233

About the Installation and Deployment Guide

- "Intended Audience" (6)
- "Document Organization" below
- "Related Documentation" on the next page
- "How to Contact Us" on the next page

Intended Audience

This document is intended for system administrators who are migrating from ITSM Release 6.x, ITSM Release 7.x, ITSM Release 8.x and Ivanti Classic to Service and Asset Manager Version 2021.4.

Document Organization

This guide contains the following sections:

- "Service and Asset Manager Deployment Overview" on page 8: Describes recommended and optional deployment architectures, including the Service and Asset Manager reporting feature and Ivanti Voice.
- "Ivanti Service Manager Installation Prerequisites" on page 42: Provides information about confirming your role, the different accounts and passwords used in Service and Asset Manager, using a virtual machine, enabling file streaming and full-text search in Microsoft SQL Server, and verifying server roles and features.
- "Installing the Service and Asset Manager System" on page 58: Describes how to install Service and Asset Manager, including the Service and Asset Manager Operations Console, the reporting feature, ISM Discovery, and ISM Knowledge.
- "Initially Configuring the System" on page 74: Describes how to use the System Configuration Wizard to configure Service and Asset Manager, including its servers and databases; and how to use the Service and Asset Manager Operations Console to configure the deployment.
- "Upgrading Service and Asset Manager from an Earlier Release" on page 166: Contains information and instructions for upgrading Service and Asset Manager from an earlier release to the current release.
- "Using the License Manager" on page 174: Explains how to install and use the Service and Asset Manager License Manager.
- "Troubleshooting" on page 225: Contains solutions to common problems.

Related Documentation

Service and Asset Manager has online help available within the application.

Additional documentation is available through

- The [Ivanti community](#) website. You may need to request user access if you cannot log in.

Or through

- The [IvantiProduct Documentation](#) website. Click the Service and Asset Manager tile to see a list of the documents available.

How to Contact Us

To contact us about the documentation, or if you have any other questions or issues about Service and Asset Manager, contact Ivanti Software Global Support services by logging an incident via Self Service, or at: <https://www.ivanti.com/support/ivanti-support>.

Service and Asset Manager Deployment Overview

- "Hardware Considerations" below
- "Demonstration or Proof-of-Concept Deployment" below
- "Minimum Production Deployment " on page 10
- "Enterprise Production Deployment" on page 13
- "Security Enterprise Production Deployment" on page 17
- "Database Deployment Options" on page 20
- "Operations Console Deployment Options" on page 27
- "Reporting Services Deployment Options" on page 33
- "Voice Deployment Options" on page 39

Hardware Considerations

The following factors drive the hardware requirements for a new Service and Asset Manager deployment:

Service and Asset Manager supports separate landscapes: development (also called staging), test (also called UAT), and production. You can run these landscapes on the same server or isolate them on separate servers.

If you choose to run them on separate servers, you must provide additional hardware. Except for the demonstration or proof-of-concept deployment, we do not recommend putting all of the landscapes on one server.

- You can adjust the amount of hardware used after you deploy your system, after you have collected usage data. The Service and Asset Manager software is horizontally and vertically scalable, allowing you to add more hardware to increase performance without license changes.

Demonstration or Proof-of-Concept Deployment

- "About the Demonstration or Proof-of-Concept Deployment" on the next page
- "Hardware Requirements for the Demonstration or Proof-of-Concept Deployment" on the next page
- "About Installing the Service and Asset Manager Components for the Demonstration or Proof-of-Concept Deployment" on the next page

About the Demonstration or Proof-of-Concept Deployment

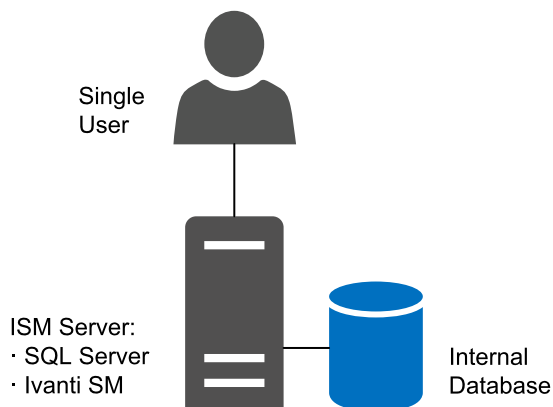


This deployment is only recommended for demonstration purposes. Do not use this deployment for any production environment.

You can run the entire Service and Asset Manager system on a single server for the purpose of a demonstration or a proof-of-concept system.

Install Service and Asset Manager, with all options enabled, onto a single server that has Microsoft SQL Server loaded locally. Most users install this deployment in a virtual environment.

Example of Service and Asset Manager and Databases on a Single Server



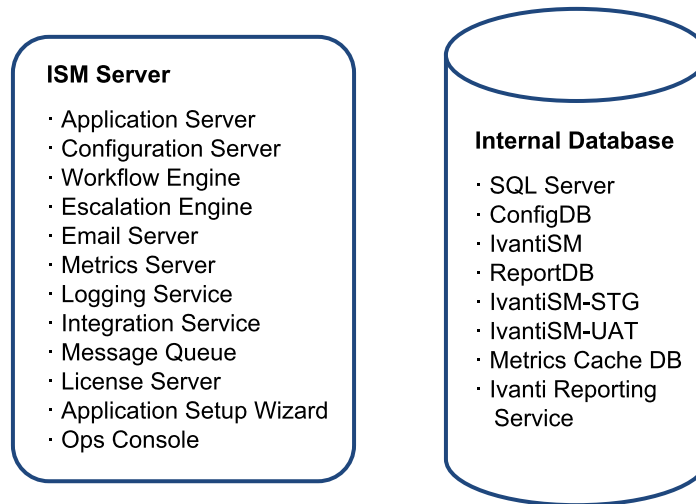
Hardware Requirements for the Demonstration or Proof-of-Concept Deployment

- 1 server, either virtual or physical
- 1 CPU
- 4 GB memory
- 40 GB hard drive

About Installing the Service and Asset Manager Components for the Demonstration or Proof-of-Concept Deployment

"Demonstration or Proof-of-Concept Deployment" on the previous page shows a diagram of the recommended locations of the various Service and Asset Manager software components in this deployment.

Service and Asset Manager Components and Databases on a Single Server



If you plan to include the Service and Asset Manager reporting feature in your deployment, you must install the Microsoft SQL Server Reporting Services (SSRS) component of Microsoft SQL Server. See "Installing the Service and Asset Manager Reporting Feature" on page 50.

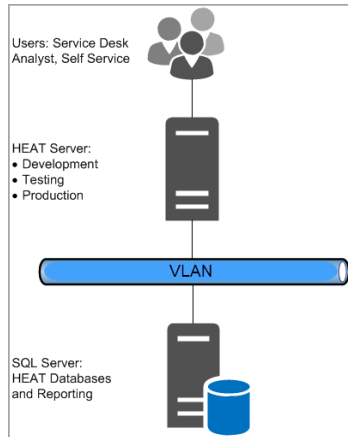
Minimum Production Deployment

- "About the Minimum Production Deployment" below
- "Hardware Requirements for the Minimum Production Deployment" on the next page
- "About Installing the Service and Asset Manager Components for the Minimum Production Deployment" on the next page

About the Minimum Production Deployment

Customers with 10 or fewer users often want to minimize their hardware investment. With the minimum production deployment architecture, you install all Service and Asset Manager components, except for the Service and Asset Manager databases, onto a single server. We recommend that you install the Service and Asset Manager databases onto a separate Microsoft SQL server.

Example of Service and Asset Manager and Databases on Separate Servers



In this deployment, all three landscapes (development [staging], testing [UAT], and production) run on the same server. As a result:

- Any issues created during the development cycle might affect production users.
- You cannot perform preupgrade testing.

Hardware Requirements for the Minimum Production Deployment

The following are the hardware requirements for the Service and Asset Manager server:

- One server, either physical or virtual
- 2 CPU
- 4 GB memory
- 200 GB hard drive

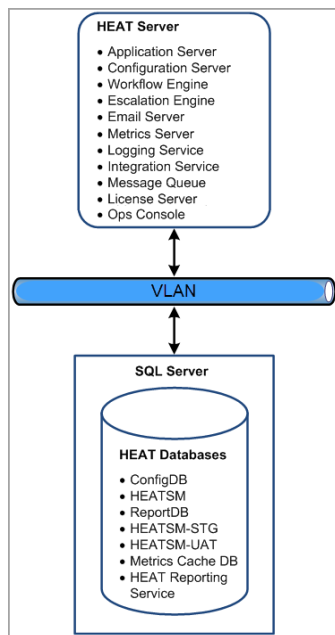
The following are the hardware requirements for the Microsoft SQL server where the databases reside:

- One server (we recommend a physical server)
- 2 CPU
- 8 GB memory
- 1 TB hard drive

About Installing the Service and Asset Manager Components for the Minimum Production Deployment

"Service and Asset Manager Components and Databases on Separate Servers" below shows a diagram of the recommended locations of the various Service and Asset Manager software components in this deployment.

Service and Asset Manager Components and Databases on Separate Servers



Enterprise Production Deployment

Customers supporting large user populations of 100 or more are primarily concerned with availability and load management rather than with minimizing hardware expense. Customers with more than 100 users should use this setup as a baseline and then add the equivalent amount of hardware for each additional 100 users. The enterprise production deployment architecture splits Service and Asset Manager into:

- Front-end web servers
- Back-end processing servers

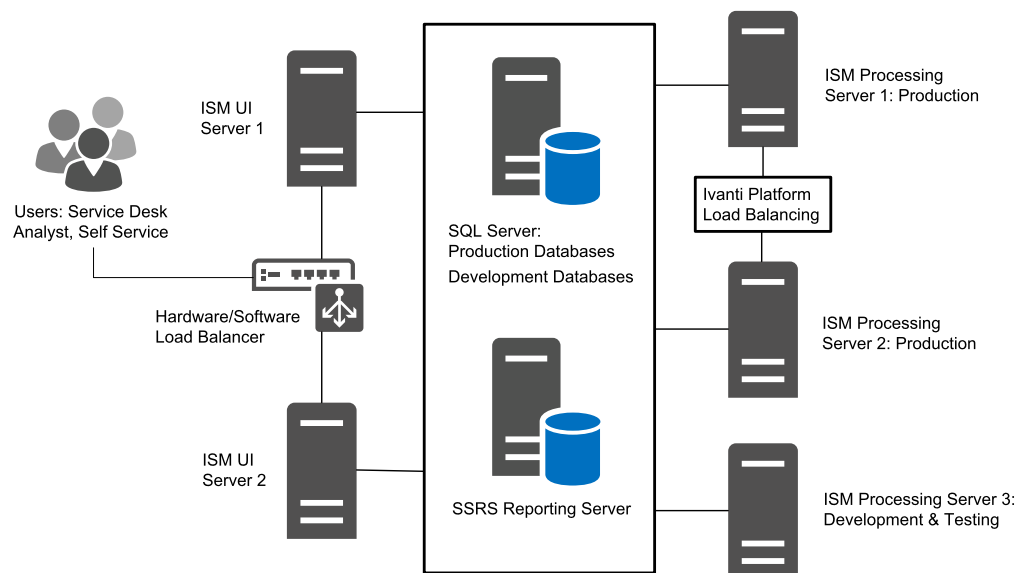
The back-end servers handle workflow, email processing, license allocation, inventory management, and so on. This architecture also separates the production environment from development and testing.

There are two key advantages of separating development and testing from production:

- Any issues created during the development cycle do not affect production users.
- You can perform upgrade testing on the development and testing servers before upgrading the production servers.

Optionally, you can install your development and test landscapes onto separate physical servers.

Example of Service and Asset Manager in an Enterprise Deployment



Hardware Requirements for the Enterprise Production Deployment

Web Servers

The following are the hardware requirements for the Service and Asset Manager web servers:

- Two virtual servers
- Outside the firewall
- Load balanced
- 4 CPU
- 16 GB memory
- 200 GB hard drive

Processing Servers (Production)

The following are the hardware requirements for the Service and Asset Manager processing servers used for the production landscape:

- Two virtual servers
- Inside the firewall
- Load balanced
- 4 CPU
- 16 GB memory
- 200 GB hard drive

Processing Servers (Development and Testing)

The following are the hardware requirements for the Service and Asset Manager processing server used for the development (staging) and testing (UAT) landscapes:

- One physical or virtual server
- 2 CPU
- 4 GB memory
- 200 GB hard drive

Microsoft SQL Server Requirements

Microsoft SQL Server is the database server for the deployment. Depending on your needs, you may have multiple database servers. The following are the requirements for the Microsoft SQL server where the databases reside:

- One physical server
- Microsoft SQL Server Release 2016
- Inside the firewall
- 8 CPU
- 24 GB memory
- 1 TB hard drive



Customers may experience an error when **Always On Availability** is configured on the database server. Ivanti Service Manager currently does not support **Always On Availability**. For more details, see [Ivanti Community](#).

Microsoft SSRS Reporting Server

The reporting feature requires that Microsoft SQL Server Reporting Services (SSRS) be installed and running on the database server that hosts the Service and Asset Manager reporting feature.

Microsoft SSRS can be installed on the Microsoft SQL server or on a separate Microsoft SSRS server, depending on your preference. We recommend a separate installation in the following situations:

- Multi-tenant environments, including managed service providers and enterprises with multiple Ivanti Service Manager tenants.
- The Microsoft SQL database is used also for applications other than Service and Asset Manager.
- Installations where the database server must remain online, because upgrading Microsoft SSRS often requires a reboot.

The following are the requirements for the Microsoft SQL Server Reporting Services (SSRS) reporting server:

- One physical server
- Microsoft SQL Server Release 2016
- Inside the firewall
- 8 CPU
- 24 GB memory
- 1 TB hard drive

Hardware Requirements when Adding Additional Users

For each additional 100 users, add this to architecture:

- Two additional Service and Asset Manager web servers.
- Two additional Service and Asset Manager processing servers.

System load determines the actual number of servers to add. You can add the web and processing servers on demand.

In most cases, you do not need to add more development (staging) or testing (UAT) servers.

High Availability and Load Balancing

You can achieve high availability through physical load balancing or by load balancing handled within Service and Asset Manager. For example, in the configuration shown in "Example of Service and Asset Manager in an Enterprise Deployment" on page 13. The Ivanti Service Manager components are connected to one or more load-balanced servers. In this example:

- The Service and Asset Manager web servers, which contain Service and Asset Manager components that are user-facing, all connect to a physical load-balancing server.
- The Service and Asset Manager process servers, which contain Service and Asset Manager components that are not user-facing, do not connect to a physical load-balancing server, but instead use a built-in load balancer. The escalation engine, workflow engine, and email server have built-in load-balancing mechanisms.
- The Service and Asset Manager web servers and process servers all connect to the same Ivanti Service Manager application database and configuration database. High availability for the Service and Asset Manager databases is achieved through a cluster.

Communication within the system, such as between an Service and Asset Manager process server and an Service and Asset Manager web server, does not require SSL. However, external communication can use SSL.



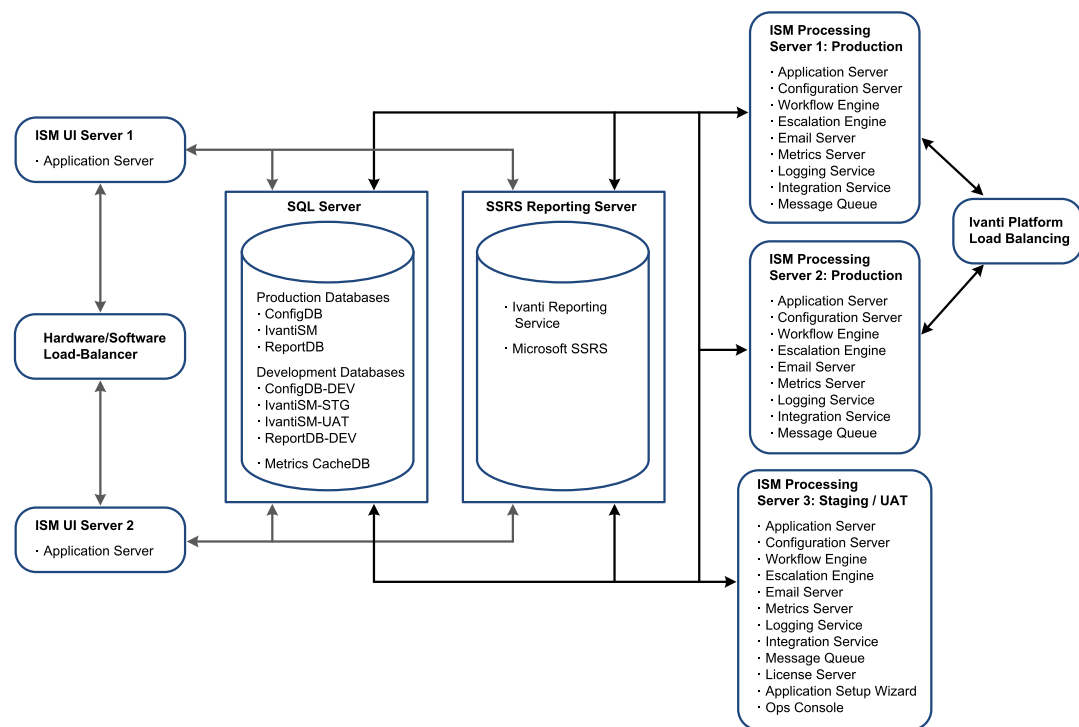
By default, the **Use SSL** checkbox in all instances will be selected for new customers. New customers must provide the fully qualified domain name for the server location in the **SSL certificate** field. However, the **Use SSL** checkbox is not selected by default for the existing customer, and they have to select **Use SSL** if needed and provide the domain name. For more details on the **SSL Certificate**, see "Optional SSL Configuration" on page 139.

When using a hardware load balancer, turn on session persistence so that connections from the web browsers always get directed to the same web server.

About Installing the Service and Asset Manager for the Enterprise Production Deployment

"Service and Asset Manager Components and Databases in an Enterprise Deployment" below shows a diagram of the recommended locations of the various Service and Asset Manager components.

Service and Asset Manager Components and Databases in an Enterprise Deployment



Security Enterprise Production Deployment

- "About the Security Enterprise Production Deployment" on the next page

- "About Using a DMZ with Web Servers" below
- "About Using a DMZ with Reverse Proxy Servers" on the next page

About the Security Enterprise Production Deployment

This deployment is based on the "Enterprise Production Deployment" on page 13 with a DMZ added to provide security where users log in from outside of the company network.

We recommend the following DMZ configurations:

- DMZ with Service and Asset Manager web servers
- DMZ with reverse proxy servers

The DMZ is configured for authenticated access. When web servers are in the DMZ, each user must enter his user name and password to log into Service and Asset Manager. This architecture involves the additional cost of setting up and maintaining two firewalls.

Where you implement reverse proxy servers, you can add another layer of access authentication. This architecture involves the additional cost of setting up and maintaining two reverse proxy servers and a load balancer.

About Using a DMZ with Web Servers

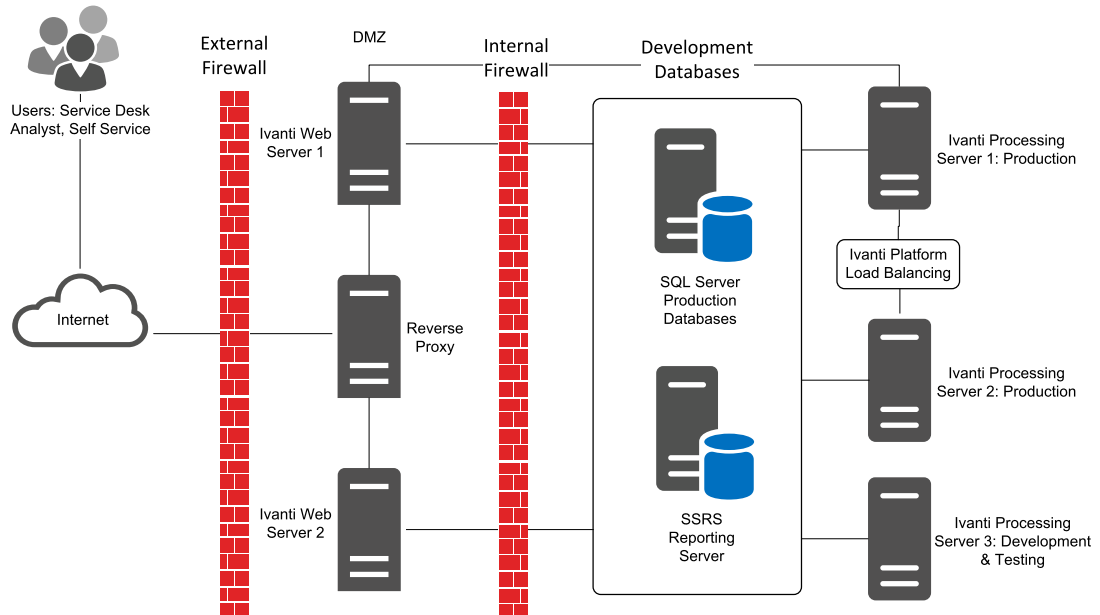
This option offers a greater level of security than placing your Service and Asset Manager web servers outside of a single company firewall. Placing a second firewall between the Internet and the web servers forms a semi-trusted network that prevents external access to your Service and Asset Manager process servers and databases.

We recommend that you harden the Service and Asset Manager web servers by taking the following actions:

- Disabling all unnecessary services
- Running necessary services with the lowest possible privileges
- Requiring strong passwords
- Locking an account after a certain number of login failures
- Deleting or disabling unnecessary user accounts, such as the guest user account
- Renaming or changing the description of the administrator account
- Installing the latest security updates and patches on the server
- Enabling security logging and checking the logs frequently

The same Service and Asset Manager components are installed on the web servers when they are located in the DMZ as when they are located outside of the company firewall. See "About Installing the Service and Asset Manager for the Enterprise Production Deployment" on page 17.

Example of an Enterprise Deployment with Service and Asset Manager Web Servers in the DMZ



About Using a DMZ with Reverse Proxy Servers

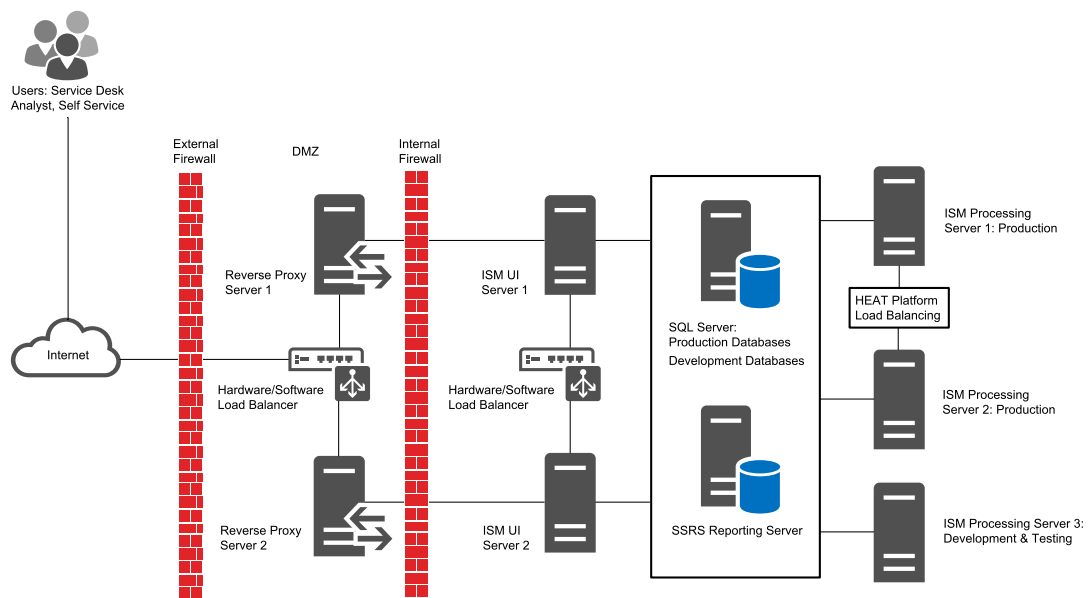
This option offers the greatest level of security by placing your web servers inside the company firewall. By placing reverse proxy servers in the DMZ, you prevent direct user login to the Service and Asset Manager web servers.

In addition, by locating the web servers on the same network as the process servers and databases, you achieve a true three-tier architecture.

The same Service and Asset Manager components are installed on the web servers when they are located inside the firewalls as when the servers are located outside.

This architecture involves the additional costs of servers to host the reverse-proxy service, as well as setting up and maintaining a second firewall. See "About Installing the Service and Asset Manager for the Enterprise Production Deployment" on page 17.

Example of an Enterprise Deployment with Service and Asset Manager Reverse Proxy Servers in the DMZ



Database Deployment Options

This section describes the different options available for the Service and Asset Manager databases.

- "About the Databases Used in Service and Asset Manager" below
- "Diagram Conventions" on page 22
- "Option D1: Separate Database Servers (Recommended and Best Practice)" on page 23
- "Option D2a: Single Database Server (Best Practice)" on page 23
- "Option D2b: Single Database Server" on page 24
- "Option D3: Single Configuration Database on a Single Database Server" on page 25
- "Option D4: Multiple Configuration Databases on a Single Server" on page 25
- "Option D5: Multiple Configuration Databases on Multiple Servers" on page 26
- "Option D6: Single Configuration Database on Separate Database Servers (for MSPs)" on page 27
- "Option D7: Multiple Configuration Databases on Separate Database Servers (for MSPs)" on page 27

About the Databases Used in Service and Asset Manager

The following are the databases used in Service and Asset Manager:

- configuration database (ConfigDB)
- Service and Asset Manager application database (IvantiSM)
- Service and Asset Manager reporting database (ReportDB). This database is used for the reporting feature. See "Reporting Services Deployment Options" on page 33 for more information.
- Metrics cache database (Metrics Cache DB). This database is used to cache the run-time state of the schedule jobs. Only one metrics cache database is needed in each isolated landscape. For example, if the configuration database and the Service and Asset Manager application database are hosted on the same database server, your deployment only needs one metrics cache database.

In addition, there are generally three instances for each tenant:

- Staging
- UAT
- Production

Each tenant instance, Staging (development), UAT (Test) and Production, can have its own database instance or server. These are called:

Database	Description
IvantiSM	Application database for production
IvantiSM-STG	Application database for staging (development)
IvantiSM-UAT	Application database for UAT (testing)
IvantiSM-Dev	Application database for staging (development) and UAT (testing)
ConfigDB	Configuration database for production
ConfigDB-STG	Configuration database for staging (development)
ConfigDB-UAT	Configuration database for UAT (testing)
ConfigDB-Dev	Configuration database for staging (development) and UAT (testing)
ReportServer	Report database for production
ReportServer-STG	Report database for staging (development)
ReportServer-UAT	Report database for UAT (testing)
ReportServer-Dev	Report database for staging (development) and UAT (testing)

The advantage of hosting a database on its own server is that it ensures security by isolating the production landscape. It also enhances performance. When you make multiple changes or upgrades to the staging or UAT landscapes, you do not want that to affect the performance of the production landscape. Separating the different databases makes it easier to upgrade the systems, because when you upgrade the systems you have to shut them down and that affects users in the production landscape.

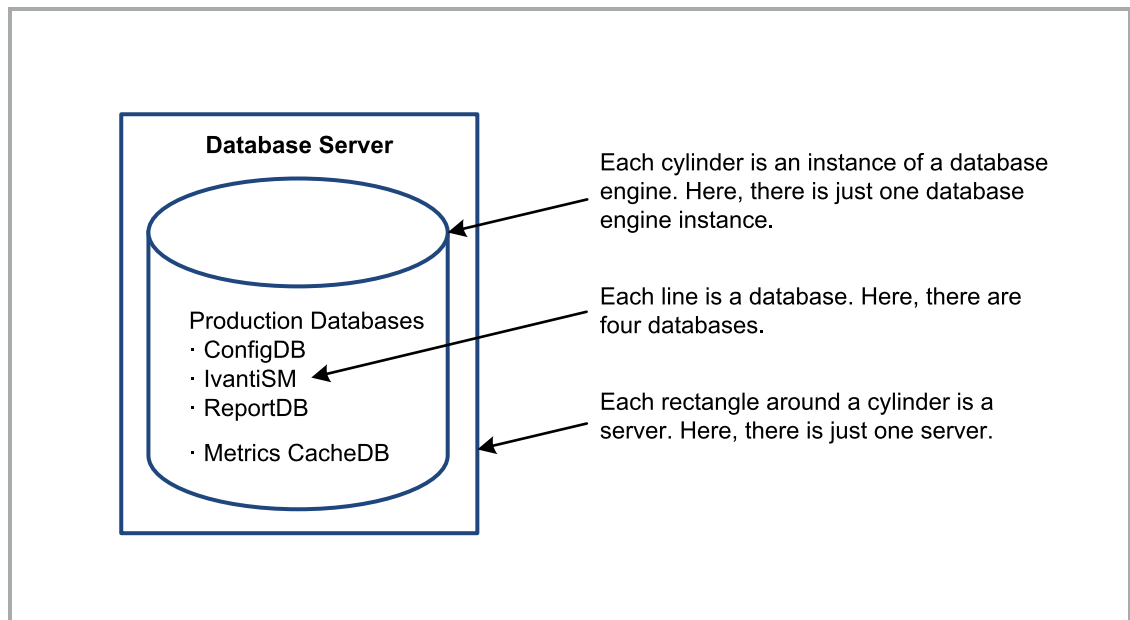
The advantage of hosting everything on one server is that you save money by only having to purchase and administer one server and one Microsoft SQL Server license.

Diagram Conventions

The following conventions are used in the diagrams:

- A line item is considered a database. There can be many databases within one database engine instance.
- A barrel is considered a database engine instance. It can contain multiple database instances.
- A square or rectangle around something means it is on one server (machine). Each server can potentially host multiple database engine instances.

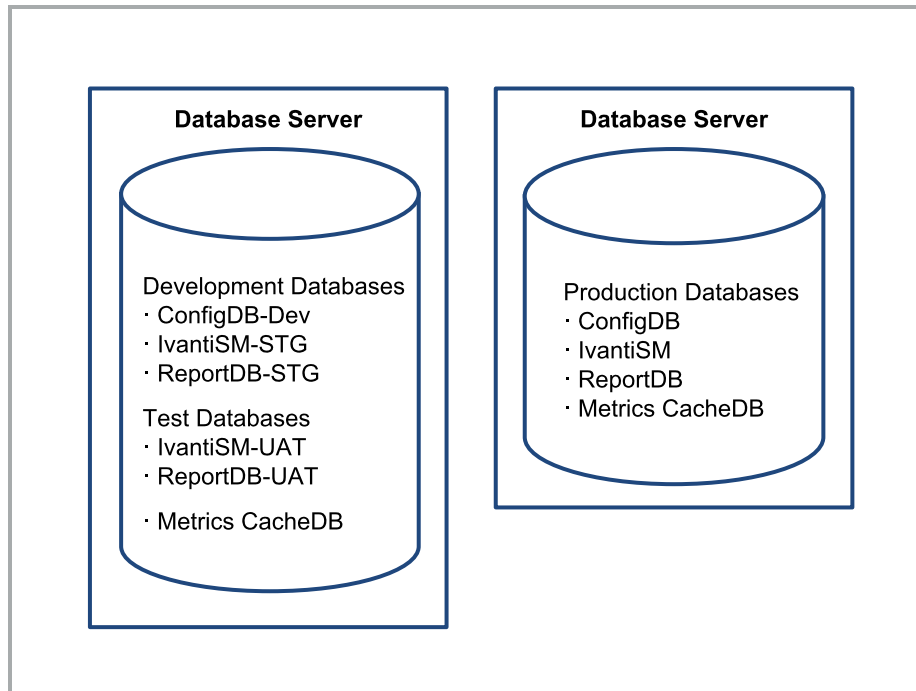
Diagram Conventions



Option D1: Separate Database Servers (Recommended and Best Practice)

In this deployment, there are two separate database servers. One is for the production landscape and the other is for the staging and UAT landscape. The staging and UAT servers share a configuration database.

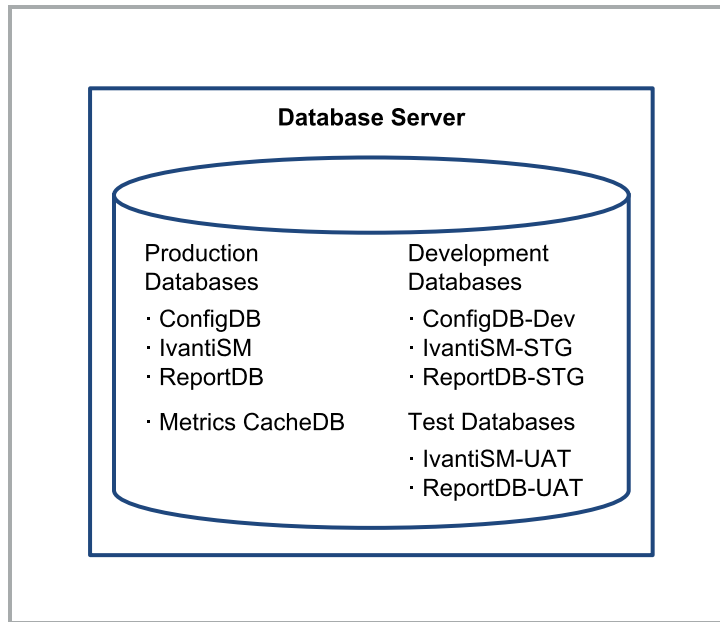
Example of Separate Database Servers



Option D2a: Single Database Server (Best Practice)

In this deployment, there is a single database server and one configuration database (ConfigDB-Dev).

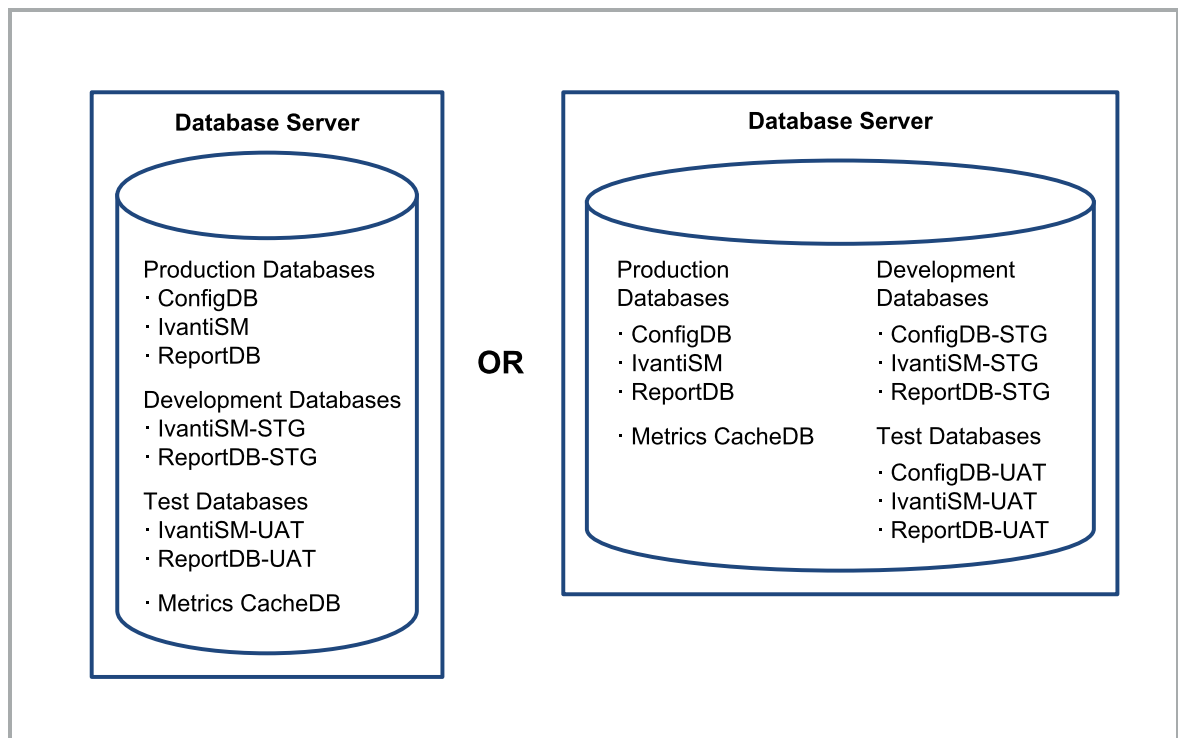
Example of Recommended Single Database Server



Option D2b: Single Database Server

In this deployment, there is a single database server and either no configuration database or two configuration databases (ConfigDB-STG and ConfigDB-UAT).

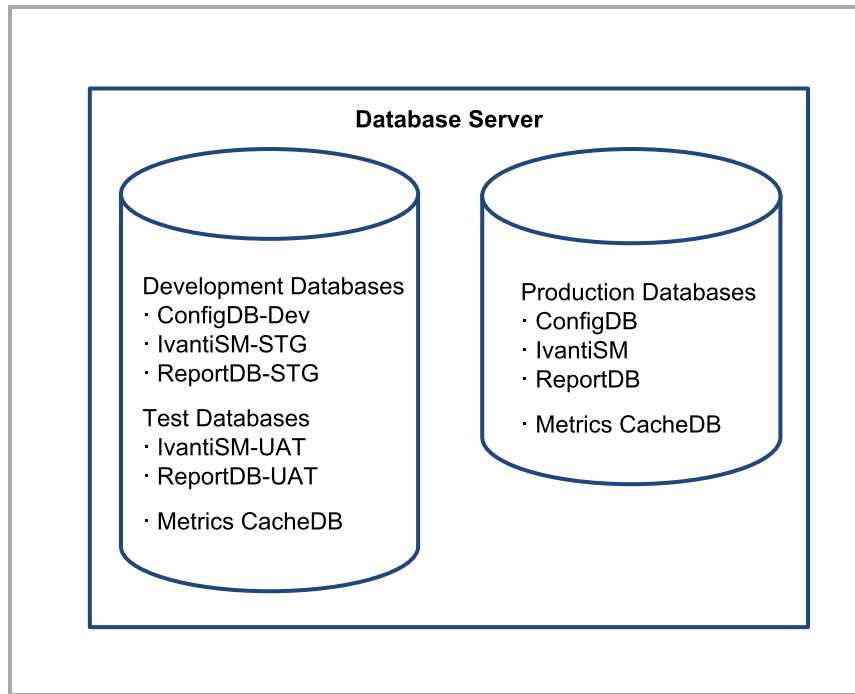
Example of Alternative Single Database Servers



Option D3: Single Configuration Database on a Single Database Server

In this deployment, there is one configuration database for the production landscape and another configuration database shared between the staging and UAT landscapes.

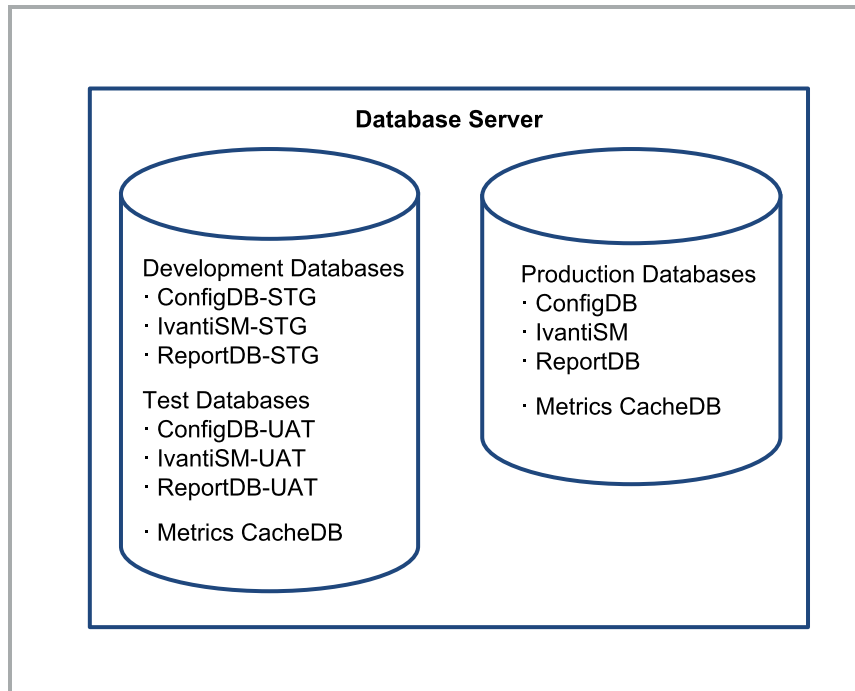
Example of Separate Database Engine Instances on a Single Database Server



Option D4: Multiple Configuration Databases on a Single Server

In this deployment, there are separate configuration databases for the production landscape, the staging landscape, and the UAT landscape.

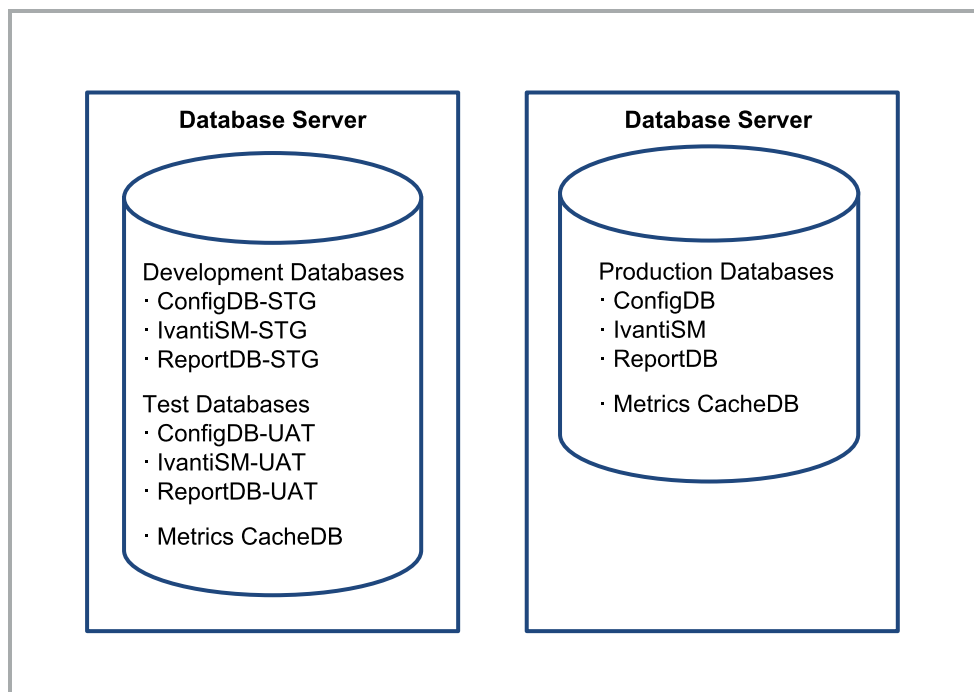
Example of Multiple Configuration Databases on a Single Server



Option D5: Multiple Configuration Databases on Multiple Servers

In this deployment, there are separate configuration databases for the production landscape, the staging landscape, and the UAT landscape and separate instances.

Example of Multiple Configuration Databases on Multiple Servers

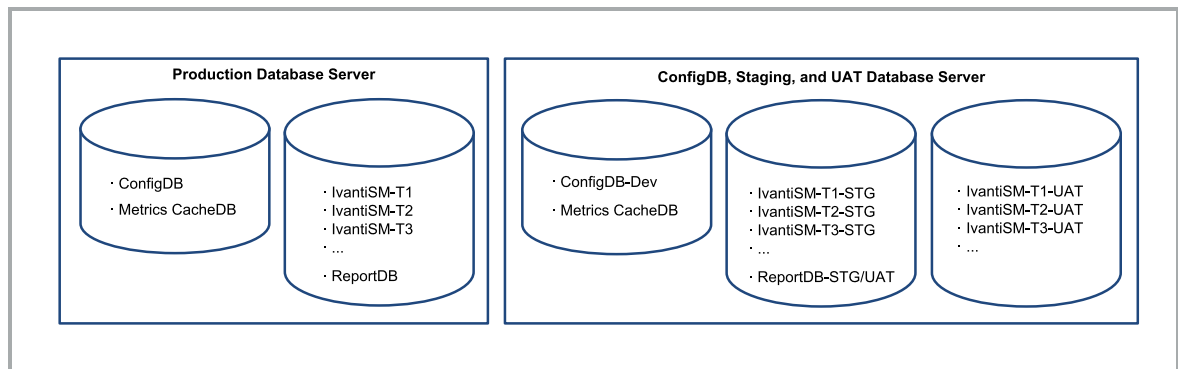


Option D6: Single Configuration Database on Separate Database Servers (for MSPs)

A Managed Service Provider (MSP) is a service partner who provides Service and Asset Manager for multiple tenants or outside customers.

In this deployment, there is a single configuration database shared between landscapes.

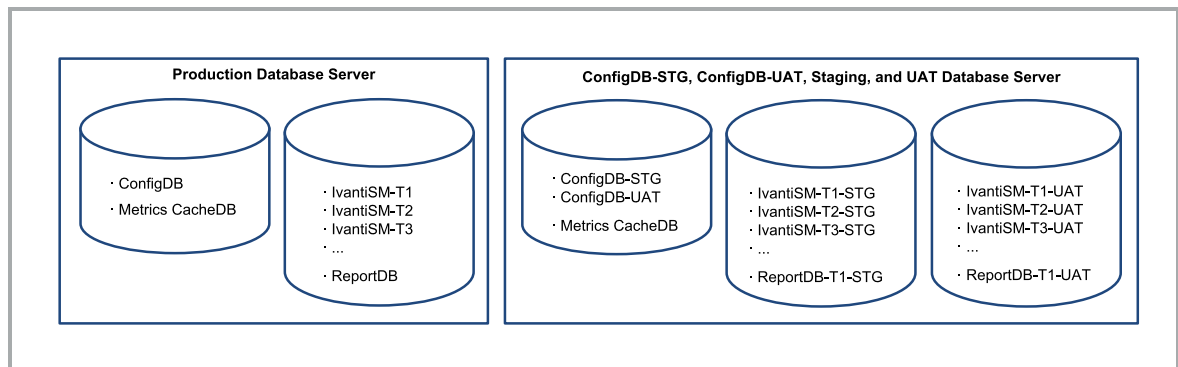
Example of a Single Configuration Database on Separate Database Servers



Option D7: Multiple Configuration Databases on Separate Database Servers (for MSPs)

In this deployment, there are separate configuration databases for the production landscape, the staging landscape, and the UAT landscape and separate instances.

Example of Multiple Configuration Databases on Separate Database Servers



Operations Console Deployment Options

- "About the Service and Asset Manager Operations Console Deployment Options" on the next page
- "Option OC1: Separate Configuration Databases and Application Servers for Production and Development (Best Practice)" on the next page

- "Option OC2: Two Configuration Databases and Separate Application Servers for Each Landscape (Best Practice)" on the next page
- "Option OC3: Separate Configuration Databases for Each Landscape (Best Practice)" on page 30
- "Option OC4: One Configuration Database and One Application Server" on page 31
- "Option OC5: One Configuration Database and Separate Application Servers for Each Landscape" on page 32

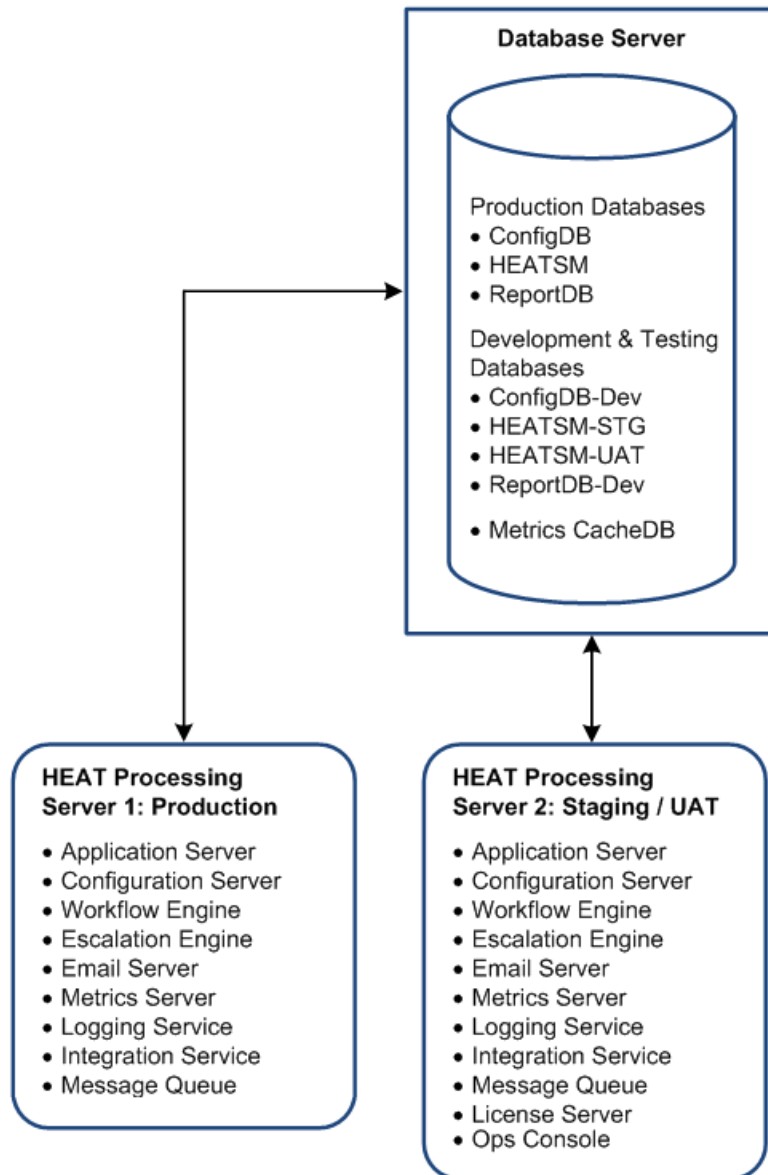
About the Service and Asset Manager Operations Console Deployment Options

- Determine your database deployment options first. In all of the Operations Console deployment options below, you can substitute any of the database deployments described in "Database Deployment Options" on page 20 for the database deployments in the figure. So for the database engine instance shown in Option OC1 below, you could substitute Option D1, Option D2a, Option D2b, Option D3, and so on for that database engine instance.
- To use the Operations Console, the production, staging, and UAT application servers must all use the same version of Service and Asset Manager. When you test new versions of Service and Asset Manager, either install the new version in a separate environment or plan the Operations Console pushes before testing the new version.
- We recommend using a deployment that has either two or three configuration databases, such as Option OC1, Option OC2, or Option OC3.

Option OC1: Separate Configuration Databases and Application Servers for Production and Development (Best Practice)

You only install the Operations Console on the staging/UAT server. Do not install it on any other servers.

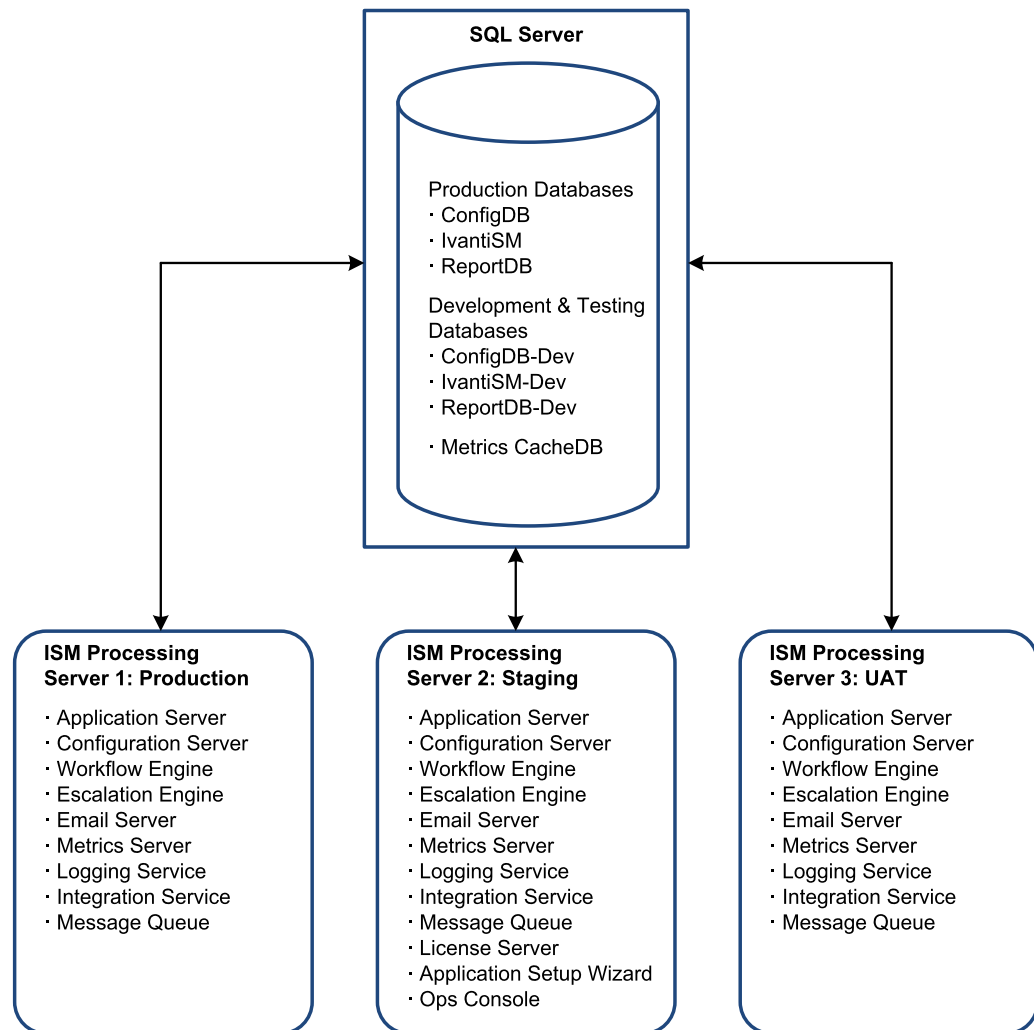
Example of Separate Configuration Databases and Application Servers for Production and Development



Option OC2: Two Configuration Databases and Separate Application Servers for Each Landscape (Best Practice)

You only install the Operations Console on the staging server. Do not install it on any other servers.

Example of Two Configuration Databases and Separate Application Servers for Each Landscape



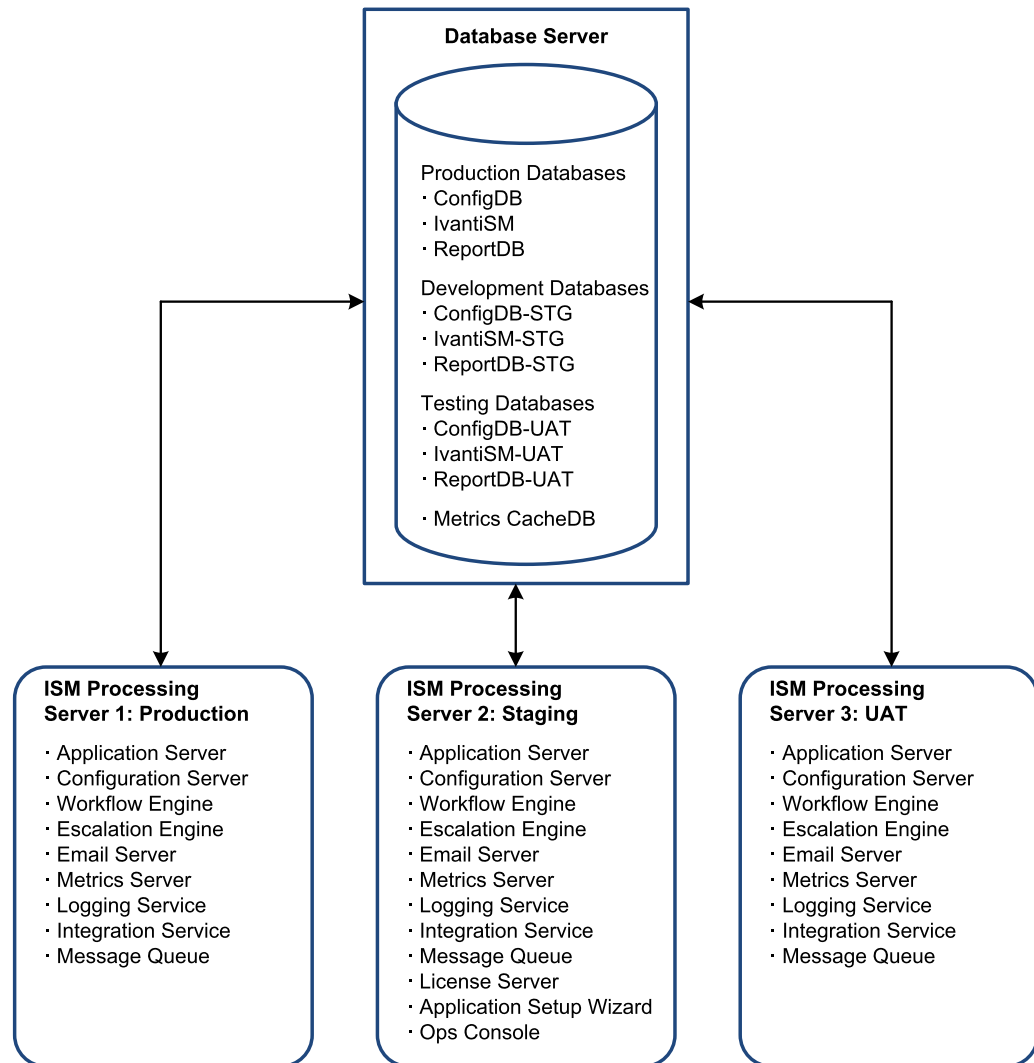
Option OC3: Separate Configuration Databases for Each Landscape (Best Practice)



The only use case for this option is to upgrade the staging or UAT landscape at different times.

You only install the Operations Console on the staging server. Do not install it on any other servers.

Example of Separate Configuration Databases for Each Landscape

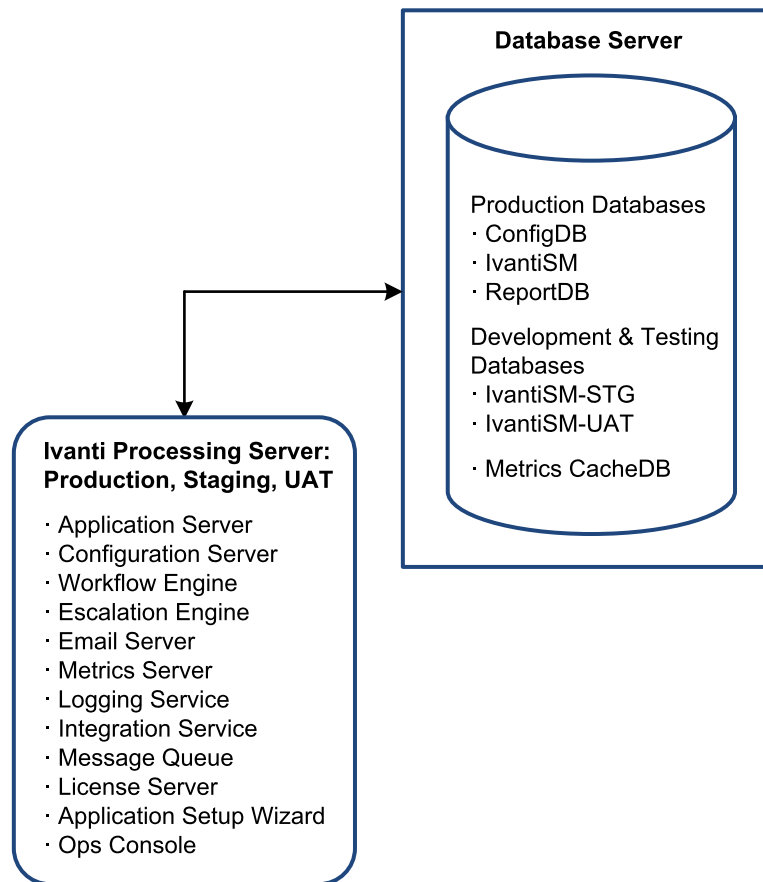


Option OC4: One Configuration Database and One Application Server



We do not recommend using this or any similar deployment that has only one configuration database that is used for IvantiSM, IvantiSM-STG, and IvantiSM-UAT, unless you are setting up a demo environment. The reason for this only being viable for demo environments is that this deployment prevents you from being able to test future upgrades on development tenants without forcing production to upgrade at the same time.

Example of One Configuration Database and One Application Server



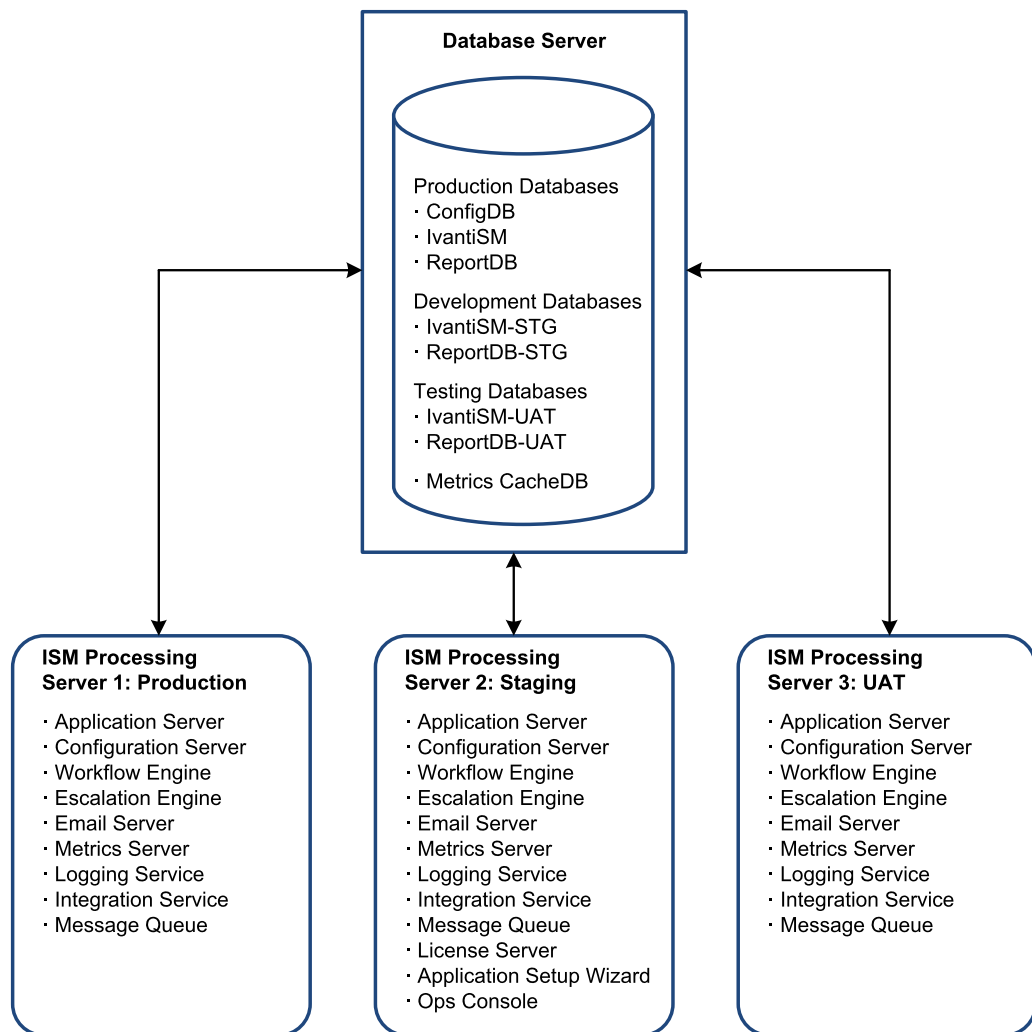
Option OC5: One Configuration Database and Separate Application Servers for Each Landscape



We do not recommend using this or any similar deployment that has only one configuration database that is used for IvantiSM, IvantiSM-STG, and IvantiSM-UAT, unless you are setting up a demo environment. The reason for this only being viable for demo environments is that this deployment prevents you from being able to test future upgrades on development tenants without forcing production to upgrade at the same time.

You only install the Operations Console on the staging server. Do not install it on any other servers.

Example of One Configuration Database and Separate Application Servers for Each Landscape



Reporting Services Deployment Options

- "About the Reporting Services Deployment Options" on the next page
- "Option R1: Multiple Microsoft SSRS Instances on the Same Database Server (Best Practice)" on the next page
- "Option R2: Separate Microsoft SSRS Instances and a Separate Database Server (Best Practice)" on page 35
- "Option R3: Separate Microsoft SSRS Instances" on page 36
- "Option R4: Multiple Microsoft SSRS Instances on a Separate Report Server" on page 37

- "Option R5: Single Microsoft SSRS Instance on One Database Server" on page 38

About the Reporting Services Deployment Options

- Determine your database deployment options first (see "Database Deployment Options" on page 20), and then your Operations Console deployment options (see Service and Asset Manager"Operations Console Deployment Options" on page 27). Then determine your reporting services deployment options.

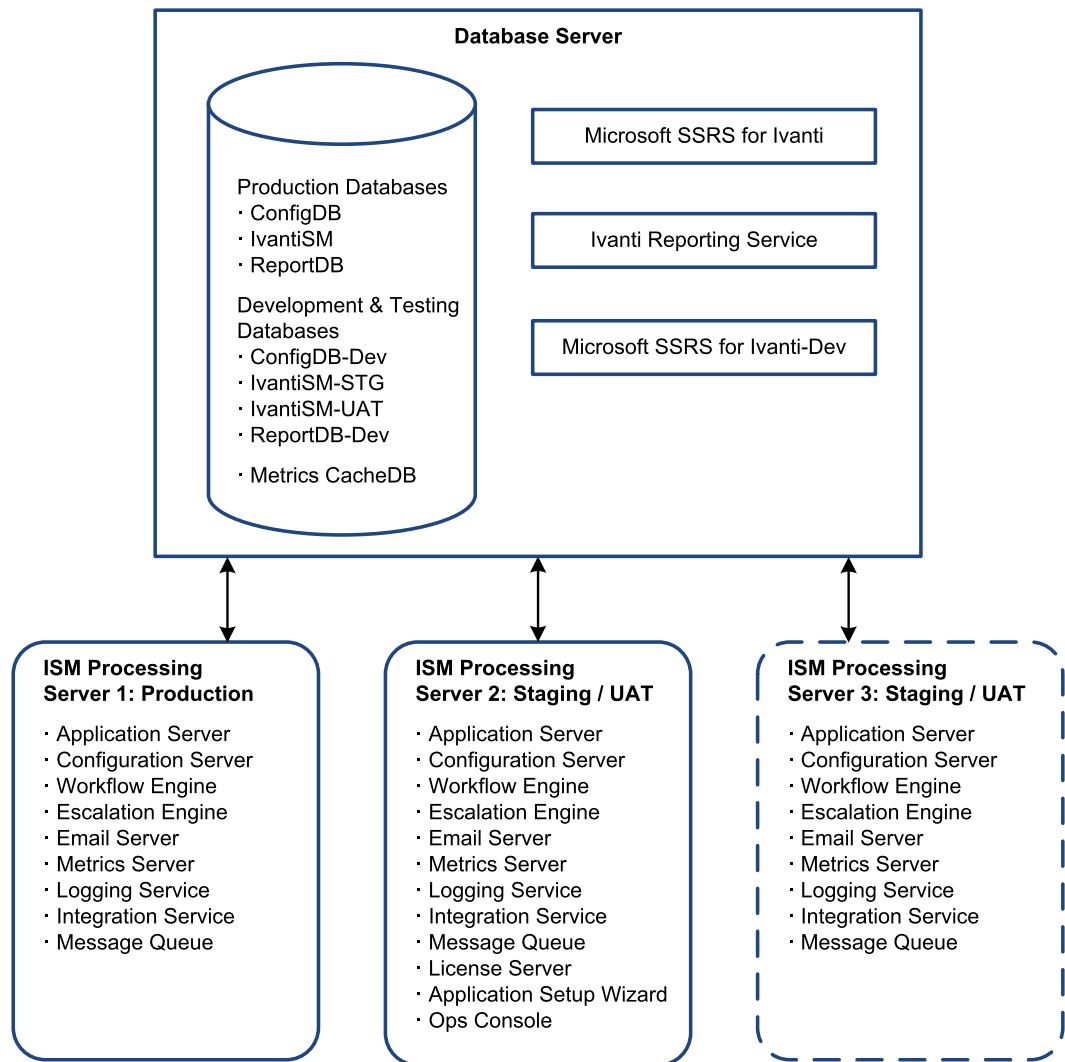
In all of the reporting services deployment options below, note the following:

- You can substitute any of the database deployments described in "Database Deployment Options" on page 20 for the database deployments in the figure. For example, for the database engine instance shown in Option R5 below, you could substitute Option D1, Option D2a/b, Option D3, and so on for that database engine instance.
- You can substitute any of the Operations Console deployments described in Service and Asset Manager"Operations Console Deployment Options" on page 27 for the Operations Console deployments in the figure. For example, for the single application server shown in Option R5 below, you could substitute Option OC3 for that application server.
- The Service and Asset Manager report database can reside on a separate database instance, or on a database instance on a separate server.
- The Microsoft SSRS instance can run on the Service and Asset Manager database server, application server, or on a separate server.
- The reporting feature should be installed on the Microsoft SSRS Server.
- We recommend using either Option R1 or Option R2.

Option R1: Multiple Microsoft SSRS Instances on the Same Database Server (Best Practice)

This deployment is the most common and recommended for simplicity and security. The advantage of this deployment is that you have a reporting feature for production that is separate from the development environments.

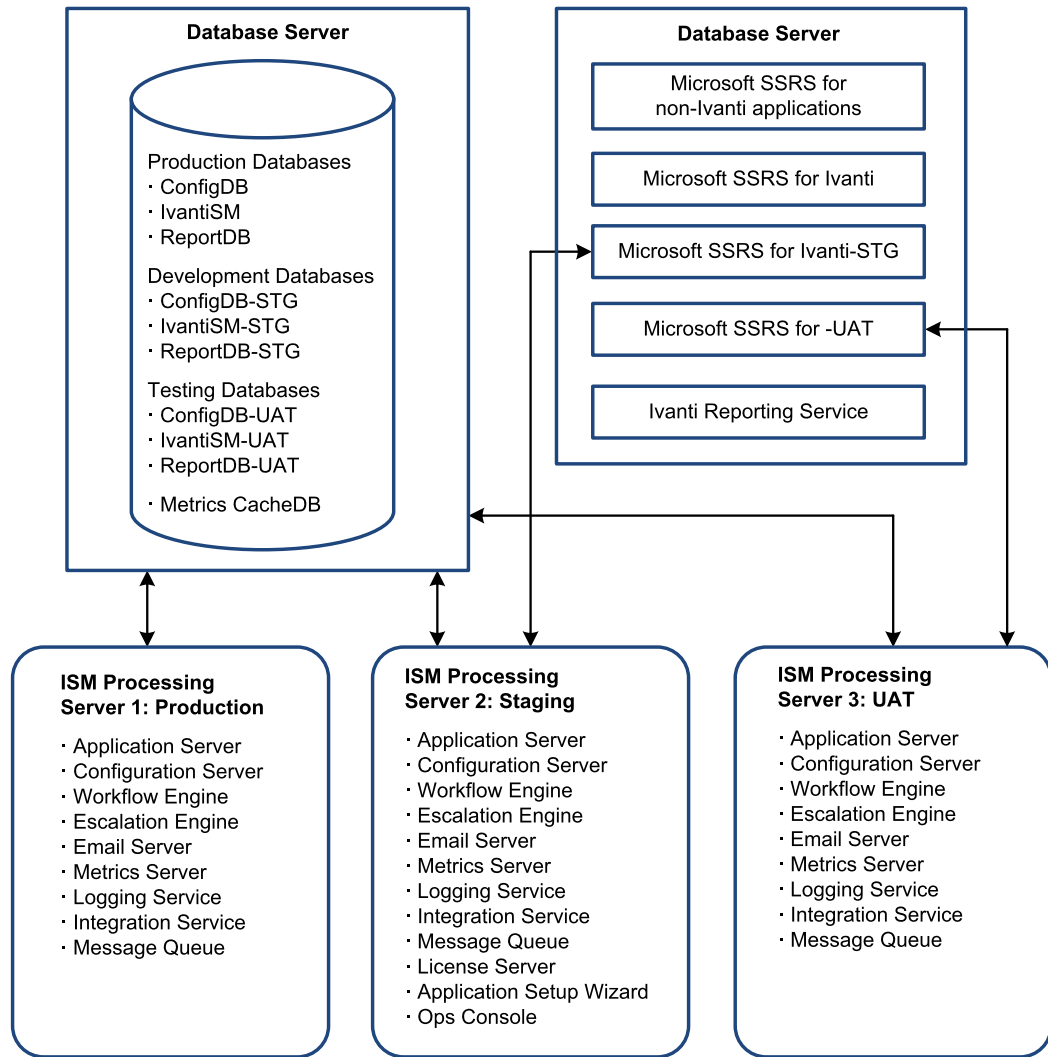
Example of Multiple Microsoft SSRS Instance on One Database Server



Option R2: Separate Microsoft SSRS Instances and a Separate Database Server (Best Practice)

Use this deployment to keep the reporting separate between the production and development environments.

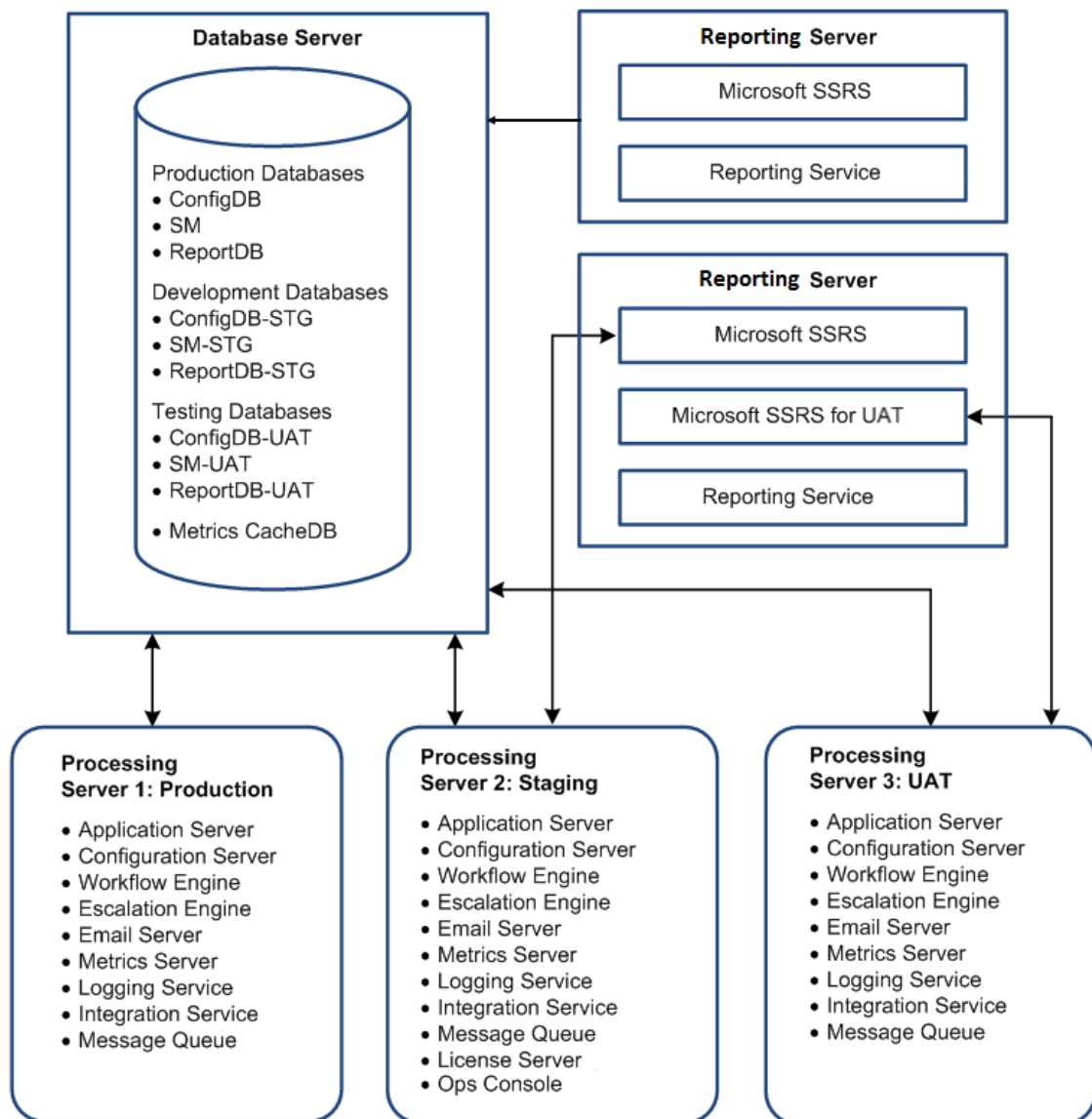
Example of Separate Microsoft SSRS Instances and a Separate Database Server



Option R3: Separate Microsoft SSRS Instances

Use this deployment to keep the reporting separate between the production and staging/UAT environments.

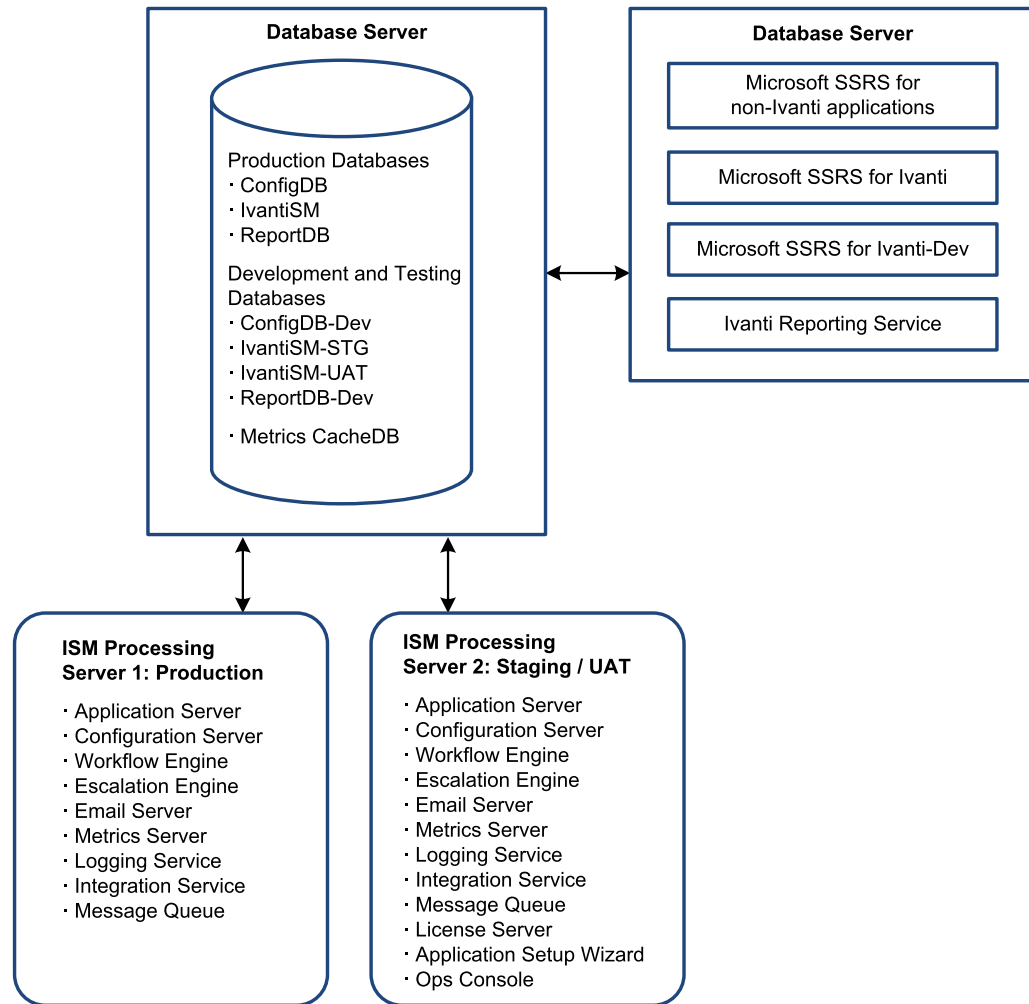
Example of Separate Microsoft SSRS Instances



Option R4: Multiple Microsoft SSRS Instances on a Separate Report Server

This deployment is recommended if you need to maintain your database in a locked down environment and keep it separate from the development environment. We also recommend this deployment if you already have a server with a Microsoft SSRS instance for other applications.

Example of a Multiple Microsoft SSRS Instances on a Separate Report Server

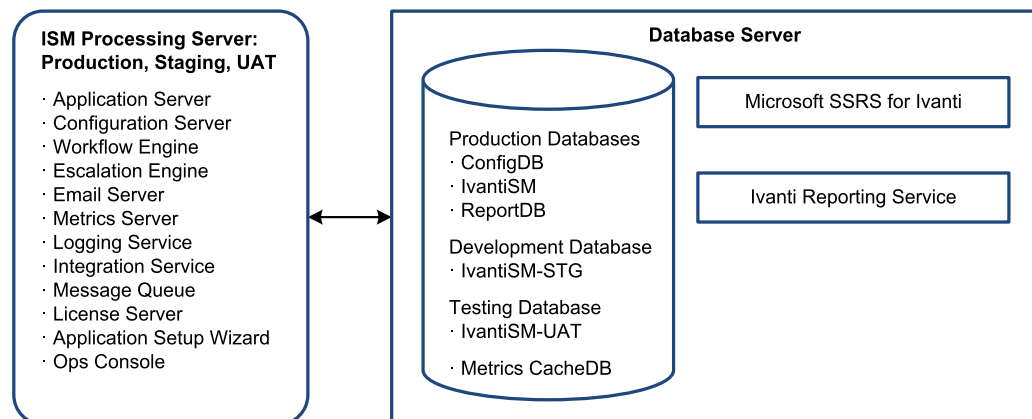


Option R5: Single Microsoft SSRS Instance on One Database Server



We do not recommend using this deployment unless you are setting up a demo environment.

Example of a Single Microsoft SSRS Instance on One Database Server



Voice Deployment Options

- "About Ivanti Voice" below
- "About this Deployment" below
- "Installing and Configuring Ivanti Voice" on page 41
- "Integrating Ivanti Voice with Service and Asset Manager" on page 41

About Ivanti Voice

Ivanti Voice is the telephony application that integrates automated call routing and management and computer telephone integration to Ivanti Software applications such as Service and Asset Manager. Ivanti Voice uses the next-generation, standards-based IP communication transport, called Session Initiation Protocol (SIP). Service and Asset Manager and Voice are typically installed and maintained on separate servers..

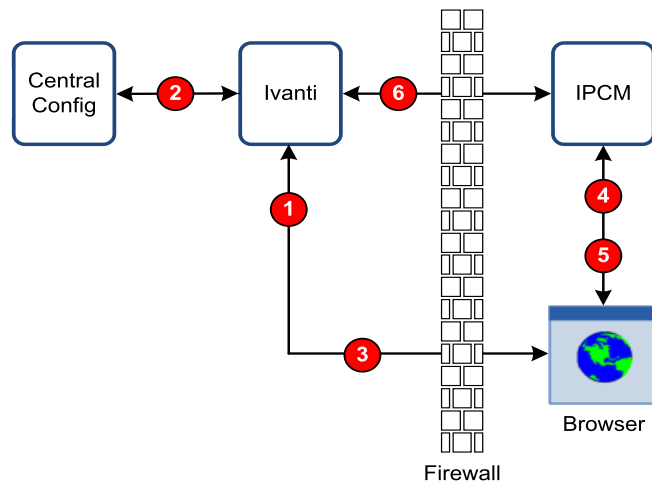
About this Deployment

- "Agent Login Sequence" below
- "Incoming Call Sequence" on the next page

Agent Login Sequence

" Agent Login Sequence" below shows the Voice agent login sequence.

Agent Login Sequence

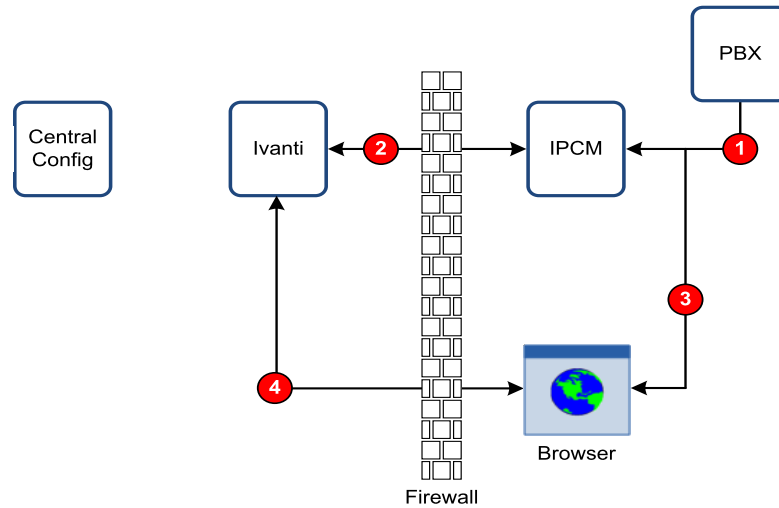


1. The agent logs into a secure (HTTPS) connection.
2. The system verifies the Voice server IP address or domain name.
3. The system obtains the session key from the Ivanti Voice server IP address or domain name.
4. The system verifies the session key (TCP 5743).
5. The system makes the phone connection (SIP UDP 5060).
6. The system validates the session key (HTTPS).

Incoming Call Sequence

"Incoming Call Sequence" below shows the sequence of events for Ivanti Voice incoming calls.

Incoming Call Sequence



1. The system receives a call (SIP UDP 500).
2. The IVR searches and updates the record (HTTPS).
3. The call is forwarded to the agent (SIP UDP 5060, RTP UDP, TCP 5743).
4. The record appears to the agent (HTTPS).

Installing and Configuring Ivanti Voice

For information about installing and configuring Ivanti Voice, see the *IP Communications Management Administrator Guide*.

Integrating Ivanti Voice with Service and Asset Manager

For complete information about integrating Voice with Service and Asset Manager, see *Working with Voice* in the Service and Asset Manager online help.

Ivanti Service Manager Installation Prerequisites

Before you install Service and Asset Manager, do the following:

- Confirm your role. See "About Roles" below.
- Create the needed accounts. See "About the Different Accounts Used in Service and Asset Manager" on page 44.
- Meet the system, hardware, and software prerequisites. This information is contained in the *System Requirements and Compatibility Matrix for Service and Asset Manager*.
- Configure the ports needed for your deployment. This information is contained in the *System Requirements and Compatibility Matrix for Service and Asset Manager*.
- If you are going to deploy Service and Asset Manager as a virtual image, review the requirements at "About Using a Virtual Machine with Service and Asset Manager" on page 46.
- Ensure that the FILESTREAM feature is enabled on the Microsoft SQL Server. See "Enabling Attachment File Streaming" on page 46.
- If you are going to deploy the reporting feature, ensure that Microsoft SQL Server Reporting Services (SSRS) is enabled. See "Installing the Service and Asset Manager Reporting Feature" on page 50.
- Enable full-text search for Microsoft SQL Server. See "Enabling Full-Text Search" on page 52.
- (Optional) Verify the server roles and features described in "Verifying Server Roles and Features" on page 54.
- Determine the directories in which to install the Service and Asset Manager components on the host that you are logged into.

About Roles

- "Administrator Account Permissions" below
- "Database Access Rights Needed for Service and Asset Manager" on the next page
- "Database Access Rights Needed for the Reporting Feature" on the next page

Administrator Account Permissions

Use your account that has local administrator permissions to install Service and Asset Manager, including all optional components. This administrator account must have permission to create and modify folders, files, and registry keys.

Database Access Rights Needed for Service and Asset Manager

The following are the minimum access rights required for the account of the user running the System Configuration Wizard:

Role	Access Right
Server	public
	dbcreator
	securityadmin
	NOTE: This role is only needed temporarily, to assign the db_owner role to the configuration database and the Service and Asset Manager databases.

If you do not want to give this permission to the user running the System Configuration Wizard, you must go into the Microsoft SQL Server Management Studio and manually assign the service account as the db_owner for the configuration database and the Service and Asset Manager databases.

Database Access Rights Needed for the Reporting Feature

The following are the minimum access rights used in Microsoft SQL Server Management Studio for Service and Asset Manager when also using the reporting feature:

Role	Access Right
Server	public
	dbcreator
	securityadmin *
Database	db_owner of master
	db_owner of msdb
<p>* The securityadmin role, and the db_owner of the master Microsoft database, are only needed if you set up Microsoft SSRS and create a new report server database. If you have already configured Microsoft SSRS and do not make any changes to it, you do not need this role.</p> <p>The securityadmin role creates the following Microsoft SSRS-related roles in the master, msdb, report server, and report server temporary databases:</p> <p>RSExecRole</p> <p>SQLAgentOperatorRole</p> <p>SQLAgentReaderRole</p> <p>SQLAgentUserRole</p>	

The service account for Microsoft SSRS requires:

Database	Role
MSDB	RSExecRole
	SQLAgentOperatorRole
	SQLAgentReaderRole
	SQLAgentUserRole
Master	RSExecRole
Report server	RSExecRole
	db_owner
Report server temporary	RSExecRole
	db_owner

About the Different Accounts Used in Service and Asset Manager

Before you install and configure Service and Asset Manager, you must create and know the credentials for the following accounts:

- "IT Account" below
- "Database Account " on the next page
- "Service Account" on the next page

During configuration of Service and Asset Manager, you create the following accounts:

- "Administrator Account for the Configuration Database" on the next page
- "Administrator Account for Service and Asset Manager" on page 46
- "Administrator Account for the Reporting Service" on page 46
- "Administrator Account for the Operations Console" on page 46

IT Account

This is the account that you are logged into when installing Service and Asset Manager and running the System Configuration Wizard.

You must create this account before you start the installation. This account must have administrator privileges on the servers on which you install Service and Asset Manager. Your IT department sets up this account for you.

Database Account

You must create this account before you start the installation.

You enter your credentials for the Service and Asset Manager database account on the following System Configuration Wizard pages:

- **Configuration Application**
- **Ivanti Service Manager Application**
- **Metrics Server**
- **Ivanti Discovery Application Server**

If you plan on installing the reporting feature, you also enter your credentials for the Service and Asset Manager database account on the following System Configuration Wizard pages:

- **Microsoft SSRS Configuration**
- **Reporting Service Configuration**

Service Account

You must create this account before you start the installation and configuration and it must have administrator privileges on the Service and Asset Manager application server.

A Service and Asset Manager service account is only required when you:

- Do not use the local system account for the Microsoft IIS application pool identity and Windows service.
- Install the reporting feature.

You enter your credentials for the Service and Asset Manager service account on the following System Configuration Wizard pages:

- **Ivanti Application Server Settings**
- **Microsoft SSRS Configuration**

Administrator Account for the Configuration Database

This account enables you to log into the configuration database.

You create this account during system configuration on the **Configuration Application** page of the System Configuration Wizard.

There will probably be different accounts used for different tenants.

Administrator Account for Service and Asset Manager

This account enables you to log into Service and Asset Manager, with access to the Service Desk Console and Configuration Console.

You create this account during system configuration on the **Ivanti Service Manager Application** page of the System Configuration Wizard.

There will probably be different accounts used for different tenants.

Administrator Account for the Reporting Service

This account enables you to log into the reporting feature.

You create this account during system configuration on the **Reporting Service Configuration** page of the System Configuration Wizard.

Administrator Account for the Operations Console

This account enables you to log into the Operations Console.

You create this account during system configuration when you check **Use this host for Operations Console** on the **Ivanti Application Server Settings** page of the System Configuration Wizard.

About Passwords Used in Service and Asset Manager

We recommend that you follow industry standards for creating strong passwords.

See <https://msdn.microsoft.com/en-us/library/ms161962.aspx> and <https://msdn.microsoft.com/en-us/library/ms161959.aspx>.

About Using a Virtual Machine with Service and Asset Manager

You can also deploy Service and Asset Manager as a virtual image. If you use a virtual machine, always keep the same universally unique identifier (UUID). See your virtual machine documentation for more information.

Enabling Attachment File Streaming

- "About Enabling Attachment File Streaming" on the next page
- "Task 1: Enabling the FILESTREAM Feature" on the next page
- "Task 2: Setting up Service and Asset Manager" on page 49
- "Task 3: Running the File Stream Attachment Script" on page 50

About Enabling Attachment File Streaming

Microsoft SQL Server 2008 and later versions come with enhanced support for unstructured data in the form of the FILESTREAM data type, which stores unstructured data files in the NTFS file system while storing the metadata about the unstructured data files in the Microsoft SQL Server database. For more information, see [https://technet.microsoft.com/en-us/library/bb933993\(v=sql.105\).aspx](https://technet.microsoft.com/en-us/library/bb933993(v=sql.105).aspx).

Beginning with Release 2016.1.1, Service and Asset Manager supports the FILESTREAM attachment type when you perform the tasks below.



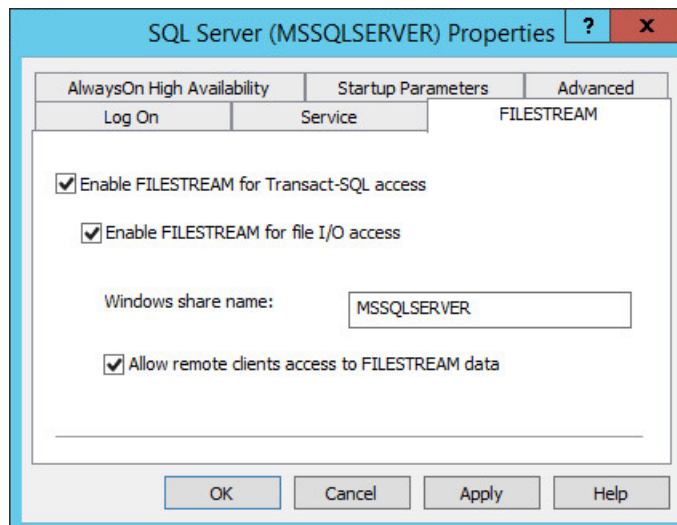
This procedure is only required for deployments that store FILESTREAM attachments.

Task 1: Enabling the FILESTREAM Feature

You must enable the FILESTREAM feature on the Microsoft SQL Server instances where you plan to install the configuration database and the Service and Asset Manager application database. The database administrator normally performs this task.

1. On the database server, go to the Windows apps menu and click **SQL Server Configuration Manager**.
2. Navigate to the **SQL Server Services** node and double-click the Microsoft SQL Server instance to modify. For example, select **SQL Server (MSSQLSERVER)**.

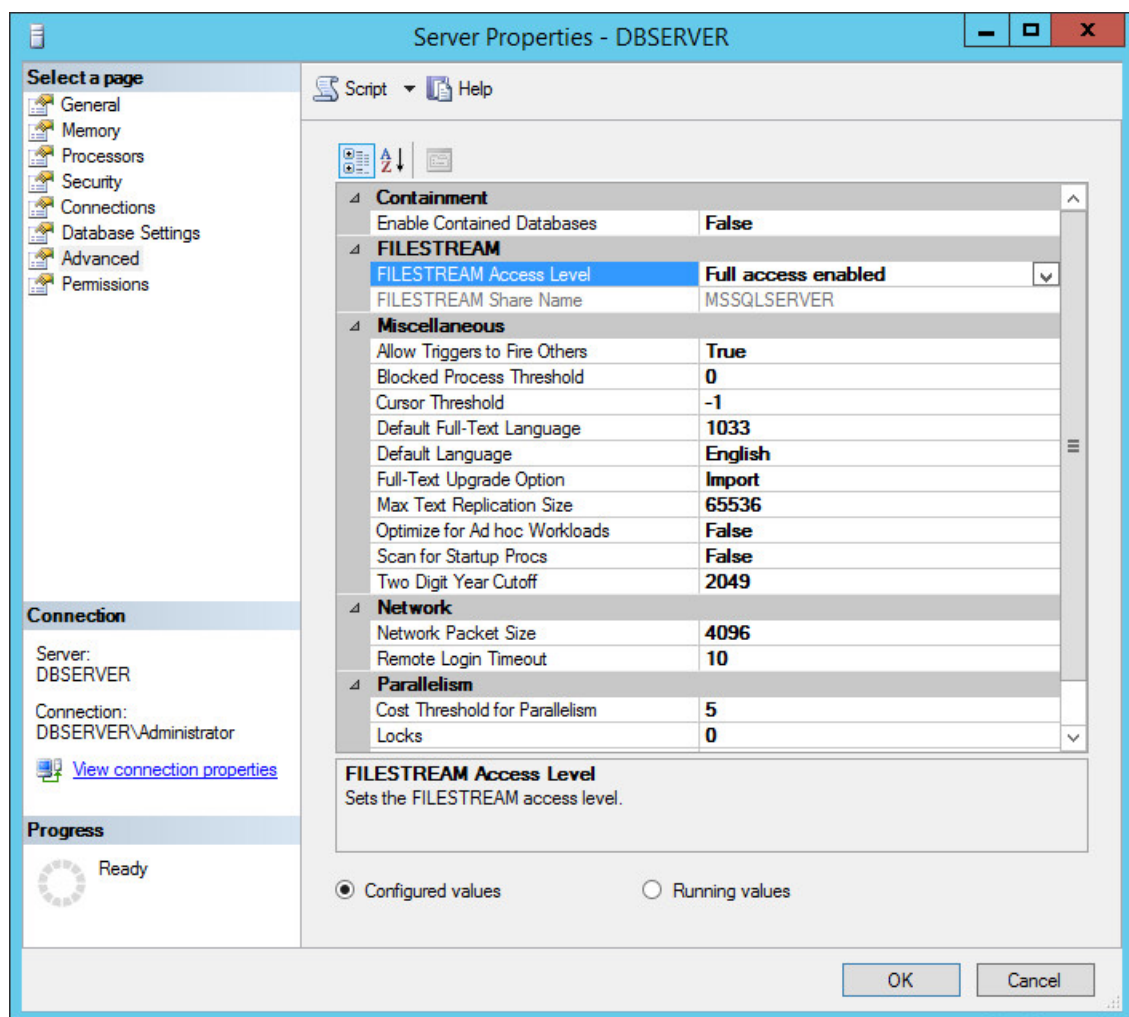
Microsoft SQL Server Properties Dialog Box



3. Click the **FILESTREAM** tab.
4. Check **Enable FILESTREAM for Transact-SQL access** and **Enable FILESTREAM for file I/O access**.
5. Enter a Windows share name for the files.
6. Check **Allow remote clients access to FILESTREAM data**.

7. Click **OK**.
8. On the database server, go to the Windows apps menu and click **SQL Server Management Studio**.
9. In Microsoft SQL Server Management Studio, connect to the database server.
10. Right-click the server and choose **Properties** from the pop-up menu.
11. Under **Select a page**, click **Advanced**.
12. Double-click the entry called **FILESTREAM Access Level** until it displays **Full access enabled**.
13. Click **OK**.
14. (Optional) If you see a restart required message, restart the Microsoft SQL Server.

Microsoft SQL Server Properties



Task 2: Setting up Service and Asset Manager

The Service and Asset Manager application database and the configuration database are Microsoft SQL databases. On Microsoft SQL databases, user accounts with the db_owner fixed database role can perform all configuration and maintenance activities on the database.

These steps are in addition to those described under "Configuring Service and Asset Manager " on page 84.

1. On the database server, go to the Windows apps menu and click **System Configuration Wizard**.
2. On the **Configuration Application** page, specify a configuration database user account that has a db_owner role on Microsoft SQL Server. This is for the **User Name** field. See "Configuring the Configuration Database" on page 85.
3. When you create a new configuration database, specify the directory path to the MDF and LDF database files.

Creating a New Configuration Database

New Database

Configuration Database Name: ConfigDB

Configuration Database Location: C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA

Collation: <Server Default>

Advanced Options

Database files

Logical Name	File Type	Initial Size(MB)	Autogrowth	Path
ConfigDB	Rows Data	100	By 10MB. Unrestricted growth.	C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA
ConfigDB_log	Log	1	By 10%. Unrestricted growth.	C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA

OK Cancel

4. On the **Service and Asset Manager Application** page, specify a Service and Asset Manager application database user account that has a db_owner role on Microsoft SQL Server. This is for the **User Name** field. See "Configuring the Service and Asset Manager Application" on page 90.

5. When you create a new Service and Asset Manager application database, specify an additional path to the server.

Task 3: Running the File Stream Attachment Script

The FileStreamAttachment.sql script is included on the Software product CD. The script creates an attachment filestream database file group and a filestream.

Before you run the script, open it in Microsoft SQL Server Management Studio and read the script notes carefully, so that you understand what the script does.

1. On the Microsoft SQL Server hosting the configuration database, run the FileStreamAttachment.sql script.
2. On the Microsoft SQL Server hosting the Service and Asset Manager application database, run the FileStreamAttachment.sql script.

When you create your Service and Asset Manager application database, you can now specify the FILESTREAM attachment type. See "Configuring the Service and Asset Manager Application" on page 90.

Installing the Service and Asset Manager Reporting Feature

- "About Microsoft SSRS" below
- "Checking if Microsoft SSRS is Installed" below
- "Installing Microsoft SSRS" on the next page

About Microsoft SSRS

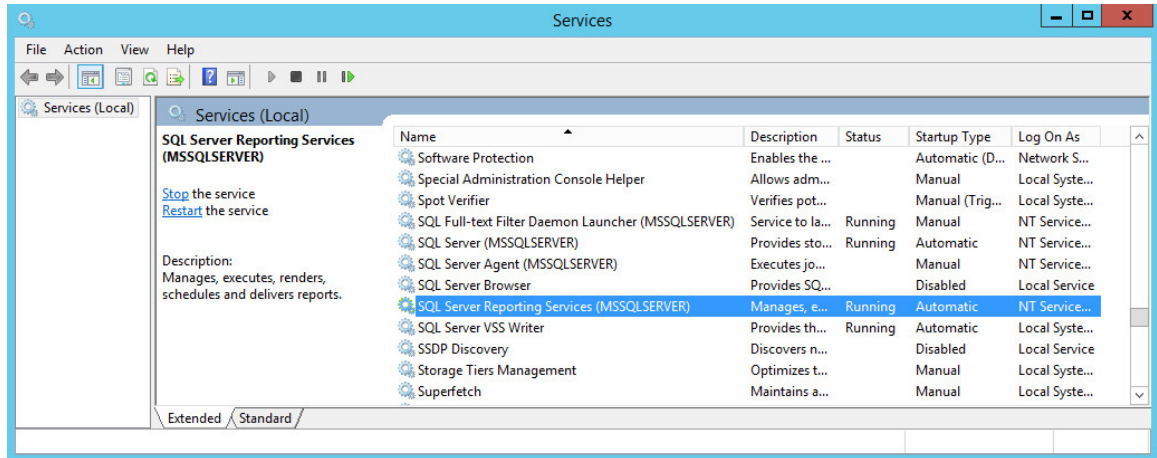
The Service and Asset Manager reporting feature requires that the 64-bit version of Microsoft SQL Server and Microsoft SQL Server Reporting Services (SSRS) are installed and running on the Service and Asset Manager database server. The reporting feature does not support the 32-bit version of Microsoft SQL Server and Microsoft SQL Server Reporting Services (SSRS).

Checking if Microsoft SSRS is Installed

To verify that Microsoft SSRS is installed on your system, do the following:

1. Open the Microsoft Windows **Services** dialog box and look for an entry called SQL Server Reporting Services.

Windows Services Dialog Box



The name in parentheses is the Microsoft SSRS instance name. See "Windows Services Dialog Box" on the previous page. During the reporting feature configuration, you must enter this instance name.

The instance name cannot contain any special characters, such as \, , ; ... and so on. The instance names can contain \$ and _ . See <https://support.microsoft.com/en-us/help/2282743/fix-the-special-characters-are-displayed-incorrectly-in-a-textbox-cont>.



If the names of the current Microsoft SSRS instances have special characters, you must install an additional Microsoft SSRS instance with an instance name free of special characters.

2. Choose the appropriate action:

- If Microsoft SSRS is already installed and the instance name (the name in parentheses) has no special characters (-, _ #, and so on), make sure that:
 - The value in the **Status** column is set to **Running**.
 - The value in the **Startup Type** column is set to either **Automatic** or **Automatic (Delayed Start)**.
- If Microsoft SSRS is already installed but the instance name has special characters (-, _ #, and so on), use the Microsoft SQL Server Installation Center to add a new Microsoft SSRS instance with an instance name free of special characters.
- If Microsoft SSRS is not installed, use the Microsoft SQL Server Installation Center to add a Microsoft SSRS component to an existing Microsoft SQL installation.

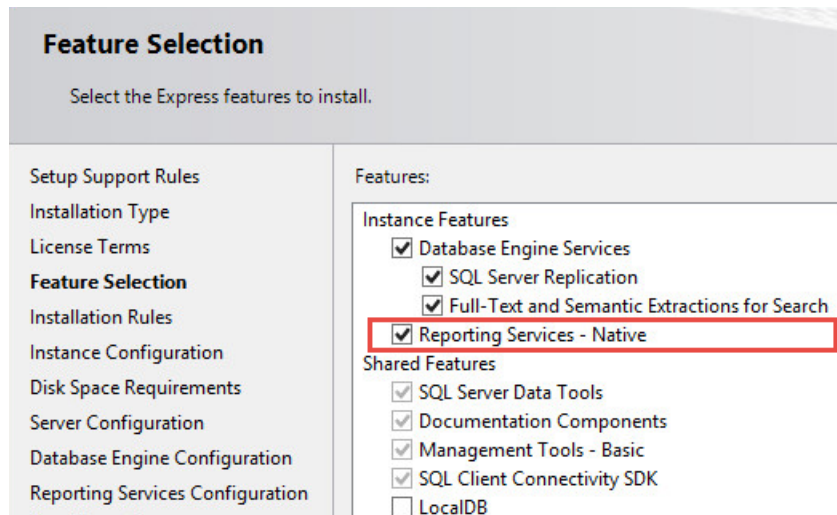
Installing Microsoft SSRS

Microsoft SQL Server Reporting Services (SSRS) is an optional installation feature of Microsoft SQL Server. It is a server-based, report-generating software system.

The Microsoft SSRS feature is disabled by default. This section describes how to enable and configure the Microsoft SSRS feature of Microsoft SQL Server.

1. During Microsoft SQL Server installation, in the **Feature Selection** page of the Microsoft SQL Server setup wizard, check **Reporting Services - Native**.

Checking Reporting Services - Native



2. As you work your way through the Microsoft SQL Server setup wizard, verify that **Reporting Services - Native** is part of the server configuration.
3. When the installation is complete, go back to Windows Services and verify that Microsoft SQL Server Reporting Services is present. See "Checking Reporting Services - Native" above.

With Microsoft SSRS present and running, the database server is ready for you to install and configure Service and Asset Manager.

Enabling Full-Text Search

- "About Full-Text Search" below
- "Enabling the Full-Text Search Feature" on the next page

About Full-Text Search

The full-text search feature of Microsoft SQL Server is a specialized indexing and querying service for character-based data in Microsoft SQL Server database tables.

By default, the application database is configured to index these incident fields:

- Owner
- ProfileFullName
- Resolution

- Subject
- Symptom

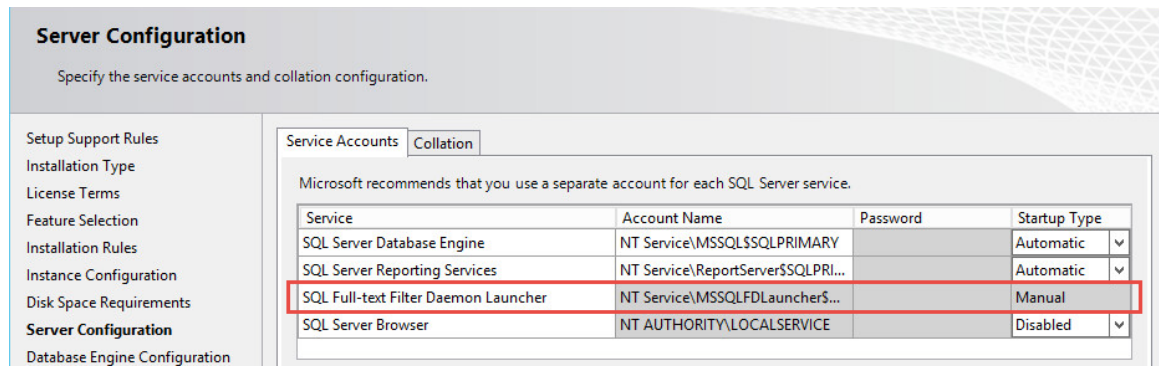
The full-text search feature is disabled by default.

Enabling the Full-Text Search Feature

This section describes how to enable and configure the full-text search feature of Microsoft SQL Server.

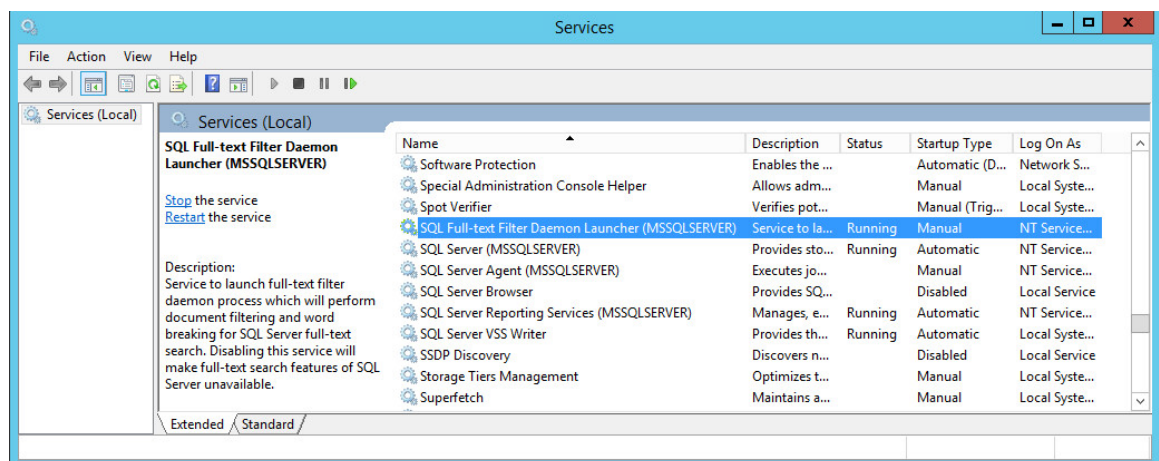
1. During Microsoft SQL Server installation, in the **Feature Selection** page of the Microsoft SQL Server setup wizard, check **Full-Text and Semantic Extractions for Search**.
2. In the **Server Configuration** page of the Microsoft SQL Server setup wizard, ensure that the **Microsoft SQL Full-text Filter Daemon Launcher** is configured with the local service account.

Server Configuration



3. In the **Services** panel for the system, ensure that the status for **SQL Full-text Filter Daemon Launcher** says Running.

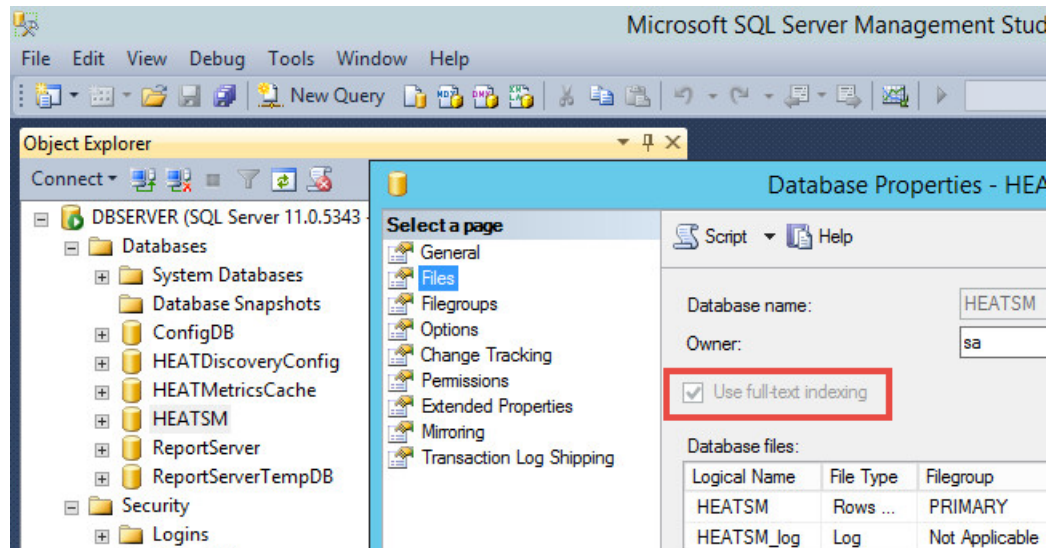
Services Dialog Box



4. Verify that full-text search is configured in Microsoft SQL Server Management Studio by doing the following:

- a. Open the **Files** page from the **Database Properties** dialog box.
- b. Ensure that **Use full-text indexing** is checked.
- c. If it is not checked, verify that the full-text search services are running as described in "In the Services panel for the system, ensure that the status for SQL Full-text Filter Daemon Launcher says Running." on the previous page

Checking the Use Full-Text Indexing Option



Verifying Server Roles and Features

You can optionally verify which server roles and features are installed by the Service and Asset Manager installer.

- If you install Service and Asset Manager on Windows Server 2008 R2, verify the Microsoft IIS Release 7.5 configuration. See "Verifying Server Roles and Feature for Windows 2008 R2 " below.
- If you install Service and Asset Manager on Windows Server 2012 or Windows Server 2016, verify the Microsoft IIS Release 8.0 configuration. See "Verifying Roles and Features for Windows Server 2012 and 2016" on page 56.

Verifying Server Roles and Feature for Windows 2008 R2

1. Go to the **Start** menu and click **Administrative Tools > Server Manager**.
2. In the **Navigation** pane, expand **Roles > Web Server (IIS)**.
3. Verify that these role services are installed under the **Web Server** section:
 - Common HTTP features
 - Static Content

- Default Document
- Directory Browsing
- HTTP Errors
- Application Development
 - ASP.NET
 - .NET Extensibility
 - ISAPI Extensions
 - ISAPI Filters
- Health and Diagnostics
 - HTTP Logging
- Security
 - Request Filtering
- Performance
 - Static Content Compression
 - Dynamic Content Compression
- Management Tools
 - IIS Management Console

Check the box of any listed server role that is not installed.

4. In the **Navigation** pane, expand **Features > Add Features**.
5. Verify that these items are selected for .NET Framework features:
 - ASP.NET 4.5
 - WCF Services
 - HTTP Activation
 - Windows Process Activation Service
 - Process Model
 - Configuration APIs

Check the box of any listed feature that is not installed.

6. Click **Next** and then click **Install**.

Verifying Roles and Features for Windows Server 2012 and 2016

1. Go to the Windows apps menu and click **Server Manager**.
2. Under configure this local server, click **Add roles and features**.
3. On the **Roles** page, verify that these server roles are installed under **Web Server (IIS) > Web Server**:
 - Common HTTP features
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - Static Content
 - Health and Diagnostics
 - HTTP Logging
 - Performance
 - Static Content Compression
 - Dynamic Content Compression
 - Security
 - Request Filtering
 - Application Development
 - .NET Extensibility
 - ASP.NET
 - ISAPI Extensions
 - ISAPI Filters

Under Web Server (IIS) > Management Tools:

- IIS Management Console

Check the box of any listed server role that is not installed.

4. On the **Features** page, verify that these features are selected:
 - NET Framework 4.5
 - ASP.NET 4.5

- WCF Services > HTTP Activation
- Windows Process Activation Service
 - Process Model
 - Configuration APIs

Check the box of any listed feature that is not installed.

5. Click **Next** and then click **Install**.

Installing the Service and Asset Manager System

- "Installation Overview" below
- "Installing Service and Asset Manager" on the next page
- "Installing the Reporting Feature" on page 61
- "Installing Discovery on a Dedicated Server" on page 63

Installation Overview

This section describes how to install Service and Asset Manager for a new, complete system using the recommended deployment as described in "Service and Asset Manager Deployment Overview" on page 8.

- "Installing Service and Asset Manager in the Production Environment" below
- "Installing Service and Asset Manager in the Staging and UAT Environments" below
- "Installing the Reporting Feature" on the next page
- "Installing the Service and Asset Manager Operations Console" on the next page

Installing Service and Asset Manager in the Production Environment

To install Service and Asset Manager in the production environment, do the following:

- Install all Service and Asset Manager features except for the Operations Console. See "Installing Service and Asset Manager" on the next page.
- Use the System Configuration Wizard to configure your production environment. See "Configuring Service and Asset Manager " on page 84.

Installing Service and Asset Manager in the Staging and UAT Environments

- If you are hosting the staging and UAT environments on one server, follow the steps below.
- If you are hosting the staging and UAT environments on separate servers, follow the steps below once for the staging environment and once for the UAT environment.

To install Service and Asset Manager in the staging and UAT environments, do the following:

- Install all Service and Asset Manager features including the Operations Console. See "Installing Service and Asset Manager" below.



If you are hosting the staging and UAT environments on separate servers, we recommend only installing the Operations Console on the staging server and not on both.

- Use the System Configuration Wizard to configure your staging and UAT environments. See "Configuring Service and Asset Manager " on page 84.

Installing the Reporting Feature

To install the reporting feature, do the following:

- Install the reporting feature on the Service and Asset Manager database server. See "Installing the Reporting Feature" on page 61.
- Use the System Configuration Wizard to configure the reporting feature. See "Configuring the Reporting Feature" on page 120.

Installing the Service and Asset Manager Operations Console

You use the Service and Asset Manager Operations Console to create the staging and UAT instances of the tenant. (The system automatically created the production instance of the tenant.)

If you have any problems with the installation, you can review the installation log file that resides with the other system temporary files in the system temporary folder at %tmp%.

See "Configuring the Deployment on the Service and Asset Manager Operations Console" on page 134.

Installing Service and Asset Manager

- "Where to Install Service and Asset Manager" below
- "Installing Service and Asset Manager" on the next page

Where to Install Service and Asset Manager

Before you begin installation, be clear on your deployment plan for Service and Asset Manager. See Service and Asset Manager"Service and Asset Manager Deployment Overview" on page 8.

- For the "Demonstration or Proof-of-Concept Deployment" on page 8, you install Service and Asset Manager onto the Service and Asset Manager server. With this deployment, you must install Microsoft SQL Server and Microsoft SQL Server Reporting Services (SSRS) on your server before you install Service and Asset Manager.

- For the "Minimum Production Deployment " on page 10, you install Service and Asset Manager onto the Service and Asset Manager server.
- For the "Enterprise Production Deployment" on page 13, you install Service and Asset Manager onto each of your Service and Asset Manager processing servers and web servers, as described below.

Installing Service and Asset Manager

Installation is basically the same for all hosts in your deployment, except for the features to be installed, which happens in "Your selection of features from the Setup Type dialog box depends on the role of the individual host in your deployment plan." below

Do the following on each production server in your deployment:

1. Access the installation folder on the Software product CD or zip file and run IvantiServiceManager.exe. Right-click and select **Run as Administrator** to ensure proper installation.

The installer checks for the prerequisite software components. If any of those components is not installed, the system prompts you to install them now.
2. Click **Install** at the prompt. Installation of the prerequisite software can take several minutes. If you are prompted to restart the system, click **Yes**. The system displays the **Welcome** dialog box. The installer checks for space and other requirements before displaying the **Next** button.
3. Click **Next**. The system displays the **License Agreement** dialog box.
4. Choose **I accept the terms in the license agreement** and click **Next**. The system displays the **Destination Folder** dialog box.
5. Click **Next** to accept the default installation folder, or click **Change** and select a different folder. The system displays the **Setup Type** dialog box.
6. Your selection of features from the **Setup Type** dialog box depends on the role of the individual host in your deployment plan.
 - For the "Demonstration or Proof-of-Concept Deployment" on page 8, choose **Complete**, click **Next**, and install all components.
 - For the "Minimum Production Deployment " on page 10, choose **Complete**, click **Next**, and install all components.
 - For the "Enterprise Production Deployment" on page 13, your choice depends on the role of the host:
 - **Production processing server:** Choose **Custom**, click **Next**, and install all components except for the Service and Asset Manager Operations Console. You must install this server first before you install the staging, UAT, or web servers.

- **Staging or UAT processing servers:** Choose **Complete**, click **Next**, and install all components.
- **Web servers:** Choose **Custom**, click **Next**, and only install the Service and Asset Manager application server.

For the "Enterprise Production Deployment" on page 13, note the following:

- If your deployment includes different processing servers for production, staging, and UAT, you must install the License Manager in every one of those landscapes.
- You can choose **Complete** and install all Service and Asset Manager features on all of your servers, but doing that takes up more disk space than necessary.

When installing components, note the following:

- To not install a component, click the down arrow next to the server icon next to the category name, highlight the component, right click, and select **This feature will not be available**.
 - If your deployment includes DSM, you do not need to install the DSM Integration service because that component has been incorporated into Service and Asset Manager since Release 2015.2.
7. Click **Next**. The system displays the **Ready to Install the Program** dialog box.
 8. Click **Install**. The system begins installing Service and Asset Manager and displays a status dialog box, showing the installation progress of each module over the next few minutes.
 9. Click **OK** if the system displays a dialog box saying that reboot is required after installation.
 10. If the system displays a dialog box saying that some of the files that need to be updated are currently in use, choose **Automatically close and attempt to restart applications** and click **OK**.

When the installation is completed, the system displays the System Configuration Wizard.

11. Go to "Configuring Service and Asset Manager " on page 84 for instructions about using the System Configuration Wizard.

Installing the Reporting Feature

- "About Installing the Reporting Feature" on the next page
- "Where to Install the Reporting Feature" on the next page
- "Installing the Reporting Feature" on the next page

About Installing the Reporting Feature

Service and Asset Manager deployments can have multiple reporting tenant instances. To use the reporting feature in a multi-tenant environment, we highly recommend that you install a separate Microsoft SSRS instance for the reporting feature only. For example, a deployment may have one reporting server for the production instance of the tenant and another reporting server for the staging and UAT instances of the tenant. See "Enterprise Production Deployment" on page 13.

Where to Install the Reporting Feature

Where you install the reporting feature depends on which deployment you have chosen. See Service and Asset Manager "Service and Asset Manager Deployment Overview" on page 8.

- For the "Demonstration or Proof-of-Concept Deployment" on page 8, you install the reporting feature onto the Service and Asset Manager database server, after you have installed Service and Asset Manager.
- For the "Minimum Production Deployment " on page 10, you install the reporting feature on the Service and Asset Manager database server.
- For the "Enterprise Production Deployment" on page 13, you can install the reporting feature on the Service and Asset Manager database servers or on a dedicated reporting server. See "Reporting Services Deployment Options" on page 33.

Installing the Reporting Feature

Before you begin, ensure that you have met all of the prerequisites for installing the Service and Asset Manager reporting feature. See "Installing the Service and Asset Manager Reporting Feature" on page 50. In particular, be sure that Microsoft SSRS is installed and running. See "Checking if Microsoft SSRS is Installed" on page 50.



If you are using SQL 2016 or higher, ensure that you install Microsoft Report Builder manually.

To install the reporting feature, do the following:

1. Access the installation folder on the Software product CD or zip file and run ReportingServices.exe. Right-click and select **Run as Administrator** to ensure proper installation.

The installer checks for the prerequisite software components. If any of those components is not installed, the system prompts you to install them now.
2. Select **Install** at the prompt. Installation of the prerequisite software can take several minutes. If you are prompted to restart the system, click **Yes**. The system displays the **Welcome** dialog box. The installer checks for space and other requirements before displaying the **Next** button.
3. Click **Next**. The system displays the **License Agreement** dialog box.

4. Select **I accept the terms in the license agreement** and click **Next**. The system displays the **Destination Folder** dialog box.
5. Click **Next** to accept the default installation folder, or click **Change...** and select a different folder.
6. Click **Next**. The system displays the **Ready to Install the Program** dialog box.
7. Click **Install**. The system begins installing the Service and Asset Manager reporting feature and displays a status dialog box showing the installation progress over the next few minutes.

When the components are installed, the system automatically launches the System Configuration Wizard.

8. Go to "Configuring the Reporting Feature" on page 120 for instructions about using the System Configuration Wizard.

Installing Discovery on a Dedicated Server

In small deployments, you install Discovery with the other Service and Asset Manager components on the Service and Asset Manager production servers. For an "Enterprise Production Deployment" on page 13, you can either install Discovery on the production servers or, to reduce the load on the production servers, you can configure a dedicated Discovery server. If you install Discovery on your production servers and then experience a significant load increase, we recommend configuring a dedicated Discovery server.

This topic describes how to install Discovery on a dedicated server.

1. Install Service and Asset Manager on your production servers. See "Installing Service and Asset Manager" on page 59.
2. On the server dedicated to Discovery, access the installation folder on the Software product CD or zip file and run IvantiServiceManager.exe. Right-click and select **Run as Administrator** to ensure proper installation.

The installer checks for the prerequisite software components. If any of those components is not installed, the system prompts you to install them now.
3. Click **Install** at the prompt. Installation of the prerequisite software can take several minutes. If you are prompted to restart the system, click **Yes**. The system displays the **Welcome** dialog box. The installer checks for space and other requirements before displaying the **Next** button.
4. Click **Next**. The system displays the **License Agreement** dialog box.
5. Select **I accept the terms in the license agreement** and click **Next**. The system displays the **Destination Folder** dialog box.
6. Click **Next** to accept the default installation folder or click **Change...** and select a different folder. The system displays the **Setup Type** dialog box.
7. Select the following components for the **Custom Setup** dialog box. Under Discovery, choose:
 - Web Application Components

- Discovery Web Server
8. Click **Next**. The system displays the **Ready to Install the Program** dialog box.
 9. Click **Install**. The system begins installing Discovery and displays a status dialog box showing the installation progress of each component over the next few minutes.

When the components are installed, the system automatically displays the System Configuration Wizard.
 10. Go to "Configuring the Discovery Application Server" on page 110 for instructions about using the System Configuration Wizard.

Installing the Knowledge Uploader (Knowledge Import Tool)

- "About the Knowledge Uploader (Knowledge Import Tool)" below
- "Installing the Knowledge Uploader (Knowledge Import Tool)" below
- "Initially Configuring and Logging Into the NXT Knowledge Import Tool" on page 66
- "Using the NXT Knowledge Import Tool" on page 68
- "Initially Configuring and Logging Into the Knowledge Import Tool" on page 70
- "Using the Knowledge Import Tool" on page 71

About the Knowledge Uploader (Knowledge Import Tool)

You can import knowledge articles from HEAT Classic, ITSM, or a local or networked file system into Service and Asset Manager. Service and Asset Manager currently has two knowledge import tools: the NXT Knowledge Server Tool (for NXT formats such as ITSM or HEAT Classic) and the Knowledge Server Tool (to use with file systems). These tools are collectively called the Knowledge Uploader and are also called the Knowledge Import Tool.

For information about using these tools after you have installed and configured them, see **Using the Knowledge Uploader** in the Service and Asset Manager online help.

Installing the Knowledge Uploader (Knowledge Import Tool)

Most installations of Service and Asset Manager automatically include the Knowledge Uploader (also called the Knowledge Import Tool).

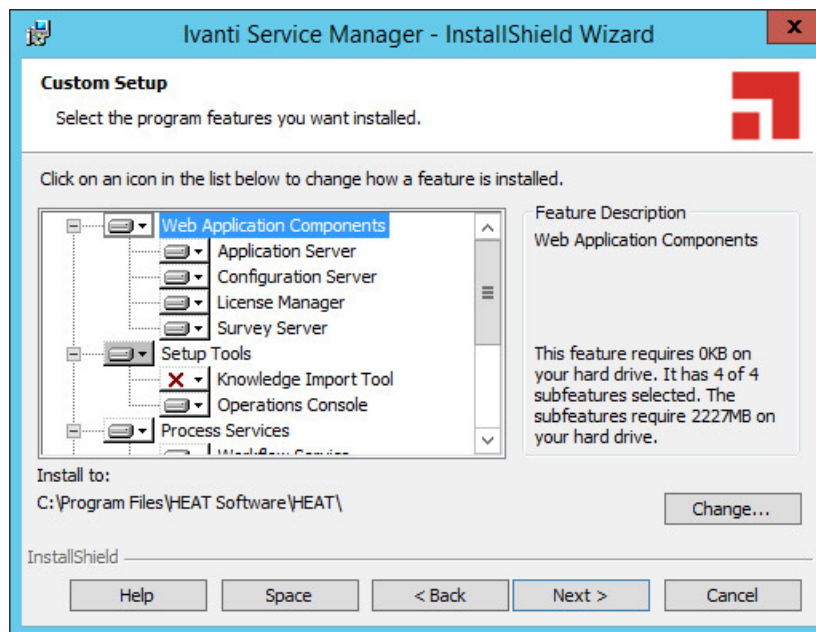
The following procedure is necessary only if you did not install the Knowledge Uploader when you installed Service and Asset Manager.

On the server or servers that you are going to use as the production environment, do the following:

1. Access the installation folder on the Software product CD or zip file and run IvantiServiceManager.exe. Right-click and select **Run as Administrator** to ensure proper installation.

The installer checks for the prerequisite software components. If any of those components is not installed, the system prompts you to install them now.
2. Click **Install** at the prompt. Installation of the prerequisite software can take several minutes. If you are prompted to restart the system, click **Yes**. The system displays the **Welcome** dialog box. The installer checks for space and other requirements before displaying the **Next** button.
3. Click **Next**. The system displays the **License Agreement** dialog box.
4. Choose **I accept the terms in the license agreement** and click **Next**. The system displays the **Destination Folder** dialog box.
5. Click **Next** to accept the default installation folder or click **Change...** and select a different folder. The system displays the **Setup Type** dialog box.
6. Select **Custom** in the **Setup Type** dialog box and click the **Knowledge Import Tool** under Setup Tools. See "Custom Setup and the Knowledge Import Tool" below.

Custom Setup and the Knowledge Import Tool



7. Click **Next**. The system displays the **Ready to Install the Program** dialog box.
8. Click **Install**. The system begins installing Service and Asset Manager and displays a status dialog box showing the installation progress of each component over the next few minutes.

When the installation is finished, the system displays the **InstallShield Wizard Completed** dialog box.

9. Click **Finish**. When the file installation is finished, the system displays the System Configuration Wizard.
10. Close the System Configuration Wizard, as there is no specific configuration for the Knowledge Uploader in the System Configuration Wizard.

The system now has two new applications on it. They are called Knowledge Import Tool and Knowledge Import Tool (NXT).

Initially Configuring and Logging Into the NXT Knowledge Import Tool



There are two knowledge tools. This topic is about the NXT Knowledge Import Tool and NOT the Knowledge Import Tool.

After you have installed Service and Asset Manager, including the Knowledge Uploader (also called the Knowledge Import Tool), do the following to initially configure and log into the NXT Knowledge Import Tool:

1. On the system where you installed Service and Asset Manager, open the application called **Knowledge Import Tool NXT**. The system displays the **NXT Knowledge Server Configuration** dialog box. See "NXT Knowledge Server Configuration Dialog Box" below.

NXT Knowledge Server Configuration Dialog Box

2. Enter information into the fields.

Parameter	Description
Server Version	The version of the NXT server that you are taking the knowledge articles from. To determine the server version, open the program and find the server information.

Parameter	Description
	<p>You can choose from any of the following:</p> <p>Knowledge Service V5.0.4003.3</p> <p>Knowledge Service Plus V9.6.1.13</p> <p>Knowledge Service Plus V9.6.1.14</p>
Server Address	<p>Enter the following:</p> <p>The protocol type (uses TCP by default)</p> <p>The server path of the NXT server that you are taking the knowledge articles from</p> <p>The port (uses 2242 by default)</p>
User Name	The user name of a person who can access the NXT server that you are taking the knowledge articles from.
Password	The password associated with the user name.
Save password	Saves the password.



To change these settings after the initial configuration, from the menu bar select **Configuration > Configure NXT server**.

- Click **Continue**.
- The system displays the **Login** dialog box. See "Knowledge Server Tool Login" below.

Knowledge Server Tool Login

- Enter information into the fields.

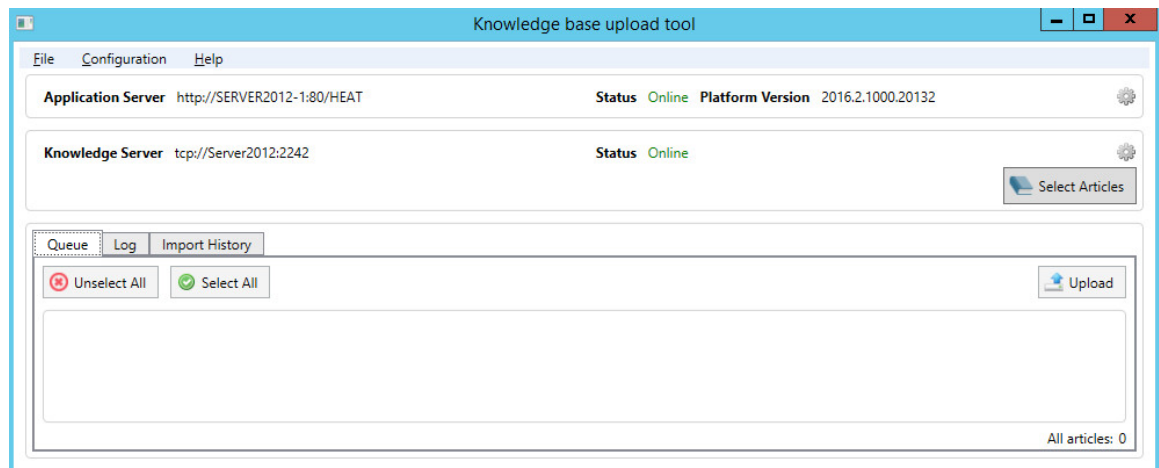
Parameter	Description
User Name	The user name of a person who can access Service and Asset Manager.

Parameter	Description
Password	The password associated with the user.
Tenant	The tenant to log into. You can select either ConfigDB to log into the configuration database or IvantiSM to log into Service and Asset Manager.
Save password	Saves the password.

i To change these settings after the initial configuration, from the menu bar select **Configuration > Configure application server**.

- Click **Continue**. The system displays the **Select role** dialog box.
- Select the role to log in as and click **Continue**. The system displays the **Knowledge base upload tool** page.

Knowledge Base Upload Tool



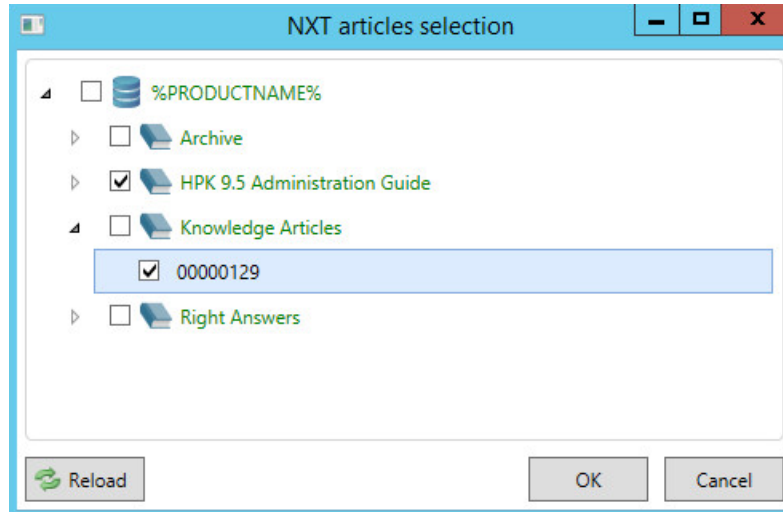
Using the NXT Knowledge Import Tool

i There are two knowledge tools. This topic is about the NXT Knowledge Import Tool and NOT the Knowledge Import Tool.

Follow these steps to import knowledge into Service and Asset Manager.

- Click **Select Articles** to select the knowledge articles to import. The system displays the **NXT articles selection** dialog box.
- Expand the list to see where knowledge articles are located, and then highlight one or more articles.

Select the Knowledge Articles to Import



3. Click **OK**. The system lists the selected articles on the bottom part of the page.
4. Select the articles to upload and click **Upload** to launch the **Article Creation** wizard and start the upload process.

The **Article Creation wizard** page contains two main areas: a **Selected Documents** area on the left containing the list of files to import, and a **Document Properties** area on the right that contains two tabs. One tab is called **Default Values** and the other is called **Selected Documents**.

5. To remove a document from the **Selected Documents** section, check it and click **Remove selected**. By default, the knowledge uploader imports all of the documents in the **Selected Documents**, even if you do not select them.
6. Optionally, use the **Document Properties** section to specify the properties that the knowledge uploader displays together with the files in Service and Asset Manager. You can specify properties for all files (using the **Default values** tab) or for individual files (using the **Selected Document** tab after highlighting the file in the **Selected Documents** section).

You can specify these properties:

- **Article Type:** The article type. Select from Document, Error Message, Issue Resolution, Patch, Q&A, or Reference.
- **Article Status:** The status of the article. Select from Approved, Draft, Expired, Failed Review, Pending Review, Published, or Submitted.
- **Target collection:** The target. Select from Company Policy & Procedure, Customer Knowledge, Internal Knowledge, IT Knowledge, or Service Desk.
- **Category:** The category for this knowledge article.
- **Subject:** The subject of the article.
- **Resolution:** The resolution details if the knowledge article contains this information.

- **Description:** A description for the knowledge article.
7. Click **Import**. The system starts importing the selected knowledge articles.
If you select a file that has already been imported into the knowledge base, the system displays the **Collision warning** dialog box.
 8. Depending on what you want to do with the file that has already been imported, click one of the following:
 - **Apply for all:** Applies your choice to all previously imported files that are found during the import process.
 - **Update:** Overwrites the file that already exists in the Knowledge Base with the file that is being imported.
 - **Create New:** Does not overwrite the file being imported with the file that already exists in the Knowledge Base. After importing, there are two knowledge articles with the same name in the Knowledge Base.
 - **Cancel:** Cancels the import process.The system displays a dialog box with the status of the import.
 9. Click **OK**.
 10. Optionally, do the following:
 - Review the import logs by clicking the **Log** tab. You can clear or save the log.
 - Review the import history by clicking the **Import History** tab. Click a number in the **Imported** column to display more information about an import session.

Initially Configuring and Logging Into the Knowledge Import Tool

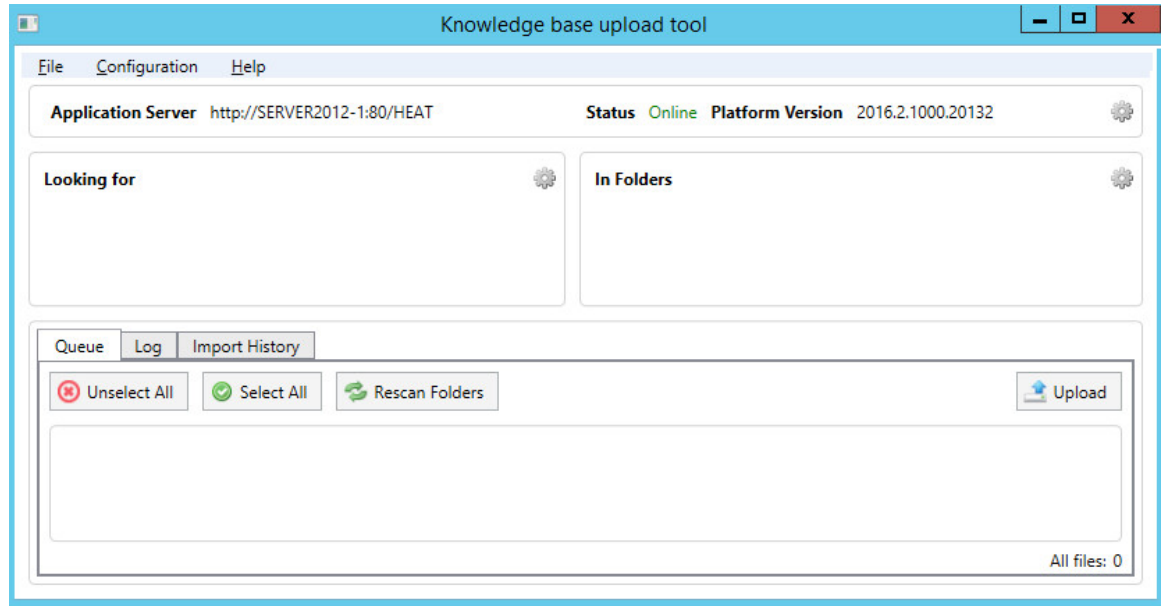


There are two knowledge tools. This topic is about the Knowledge Import Tool and NOT the NXT Knowledge Import Tool.

After you have installed Service and Asset Manager, including the Knowledge Uploader, do the following to initially configure and log into the Knowledge Import Tool:

1. On the system where you installed Service and Asset Manager, open the application called **Knowledge Import Tool**. The system displays the **Select role** dialog box.
2. Select the role to log in as and click **Continue**. The system displays the **Knowledge base upload tool** page.

Knowledge Base Upload Tool





Using the Knowledge Import Tool



There are two knowledge tools. This topic is about the Knowledge Import Tool and NOT the NXT Knowledge Import Tool.

Follow these steps to import knowledge into Service and Asset Manager.

1. Specify the article file type to search for, by doing the following:
 - a. Click the **Settings** icon  in the **Looking for** section. The system displays the **File search filters** dialog box.
 - b. In the **Add New** drop-down list, select one or more file types:
 - **Microsoft office documents**: Files that have .doc, .docx, .xls, and .xlsx extensions.
 - **PDF files**: Files that have a .pdf extension.
 - **Images**: Files that have .bmp, .jpg, and .gif extensions.
 - c. Optionally, you can add more file types by clicking **Custom**. The system adds a line item to the filter list called Custom. Click the line item to open it for editing. You can change the filter name and specify one or more extensions. Click **OK**. The system adds the file types that you specified to the **Looking for** section.
2. Specify which local or network folders to search for knowledge articles and then perform the search:

- a. Click the **Settings** icon  in the **In Folders** section. The system displays the **Import folders** dialog box.
- b. Click **Add New**. The system displays the **Browse For Folder navigation** dialog box.
- c. Navigate to a folder and highlight it. (To optionally add a new subfolder to the folder, click **Make New Folder**.)
- d. Click **OK**. The system adds the folder to the list of folders to search. If you created a new folder, the system adds it to the file system as an empty folder.
- e. Optionally, check **Recursive** for a folder to specify that the system should search the subfolders within the folder.
- f. Optionally, check **Monitor for changes** to configure the knowledge uploader to monitor all of the folders on the list for changes to the file types that you specified in step 1b.
- g. Repeat steps b-f to continue to add folders to the list as necessary.
- h. Click **OK**.

The knowledge uploader performs the search and displays all of the files that meet the search criteria.

3. Select the files to upload:

- a. If you think the contents of the scanned folders might have changed, click **Rescan Folders** to regenerate the file list.
- b. In the file list, check the files to upload, or click **Select All** to upload all of the files.
- c. Click **Upload** to launch the **Article Creation** wizard and start the upload process.

The **Article Creation wizard** page contains two main areas: a **Selected Documents** area on the left containing the list of files to import, and a **Document Properties** area on the right that contains two tabs. One tab is called **Default Values** and the other is called **Selected Documents**.

4. To remove a document from the **Selected Documents** section, check it and click **Remove selected**. By default, the knowledge uploader imports all of the documents in the **Selected Documents**, even if you do not select them.
5. Optionally, use the **Document Properties** section to specify the properties that the knowledge uploader displays together with the files in Service and Asset Manager. You can specify properties for all files (using the **Default values** tab) or for individual files (using the **Selected Document** tab after highlighting the file in the **Selected Documents** section).

You can specify these properties:

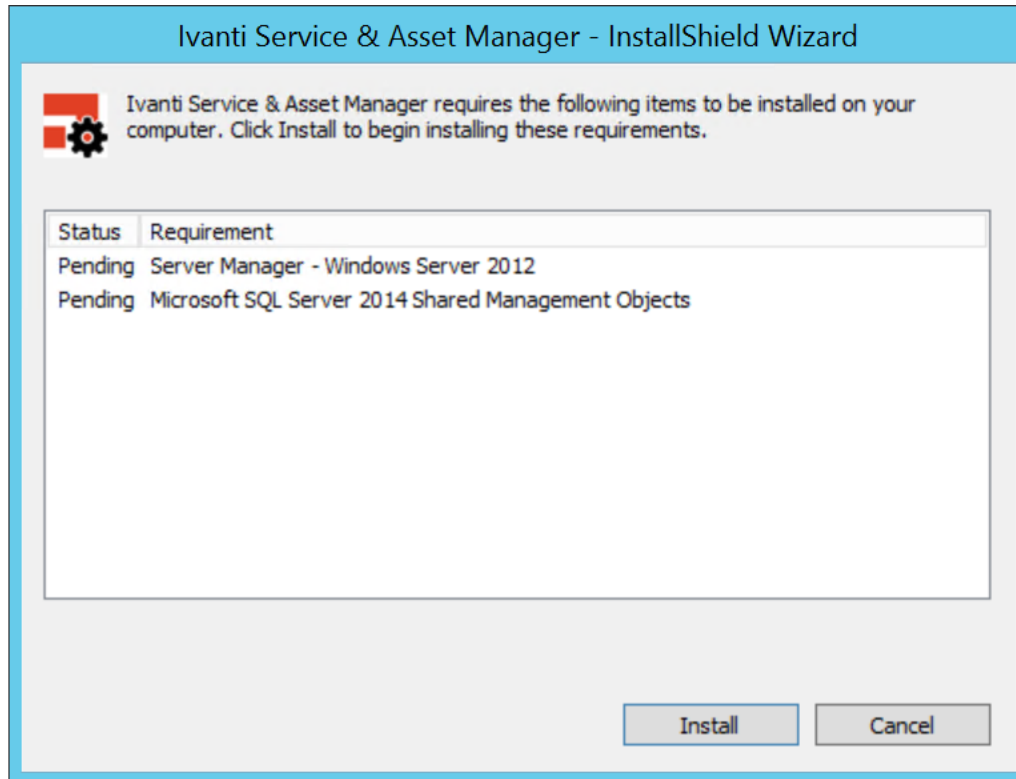
- **Article Type:** The article type. Select from Document, Error Message, Issue Resolution, Patch, Q&A, or Reference.
 - **Article Status:** The status of the article. Select from Approved, Draft, Expired, Failed Review, Pending Review, Published, or Submitted.
 - **Target collection:** The target. Select from Company Policy & Procedure, Customer Knowledge, Internal Knowledge, IT Knowledge, or Service Desk.
 - **Category:** The category for this knowledge article.
 - **Use file name as Subject:** Check to use the article file name to fill in the **Subject** field.
 - **Subject:** Only use this field if you did not check **Use file name as Subject**. Enter a subject for the article.
 - **Resolution:** Enter the resolution if the knowledge article contains one.
 - **Description:** Enter a description for the knowledge article.
6. Click **Import**. The import process begins.
- If you select a file that has already been imported into the knowledge base, the system displays the **Collision warning** dialog box.
7. Depending on what you want to do with the file that has already been imported, click one of the following:
- **Apply for all:** Applies your choice to all previously imported files that are found during the import process.
 - **Update:** Overwrites the file that already exists in the knowledge base with the file that is being imported.
 - **Create New:** Does not overwrite the file being imported with the file that already exists in the knowledge base. After importing, there are two knowledge articles with the same name in the knowledge base.
 - **Cancel:** Cancels the import process.
- The system displays an Import dialog box with the status of the import.
8. Click **OK**.
9. Optionally, do the following:
- Review the import logs by clicking the **Log** tab. You can clear or save the log.
 - Review the import history by clicking the **Import History** tab. Click a number in the **Imported** column to display more information about an import session.

Initially Configuring the System

As part of the Service and Asset Manager installation, you must configure the system using the System Configuration Wizard.

The wizard walks you through the first-time set up and configuration as shown in the screenshots below.

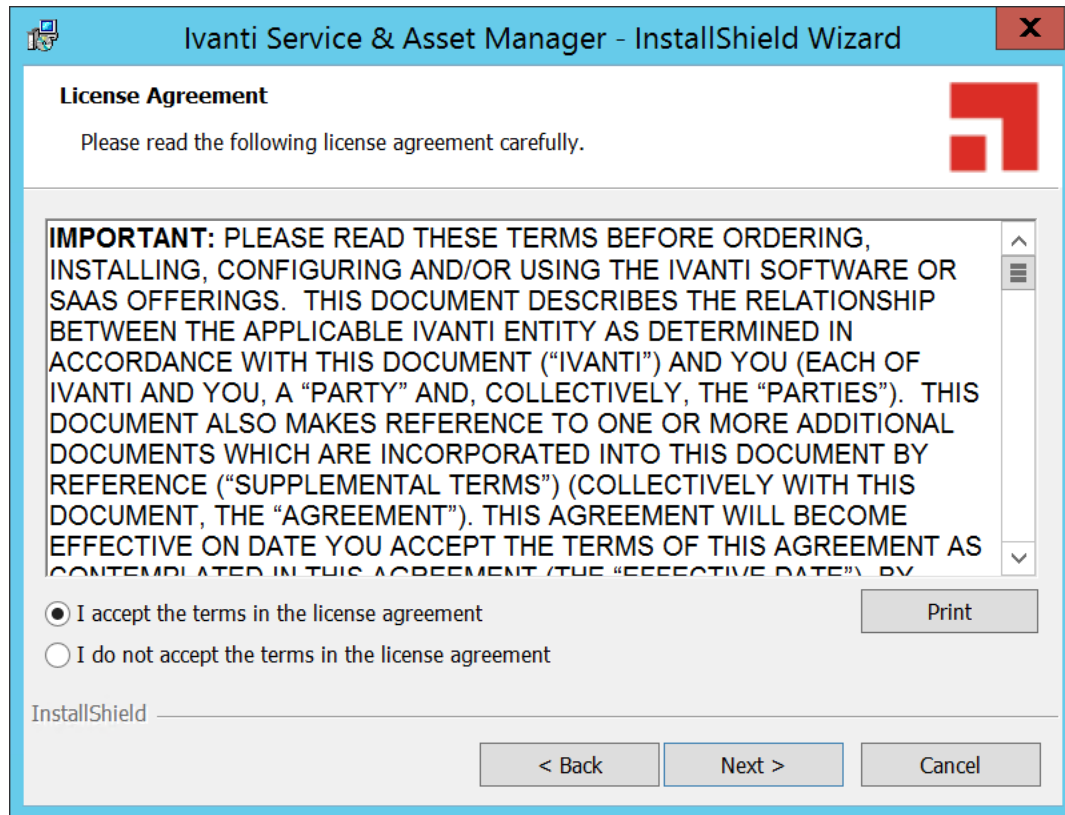
1. Click **Install** to begin the installation.



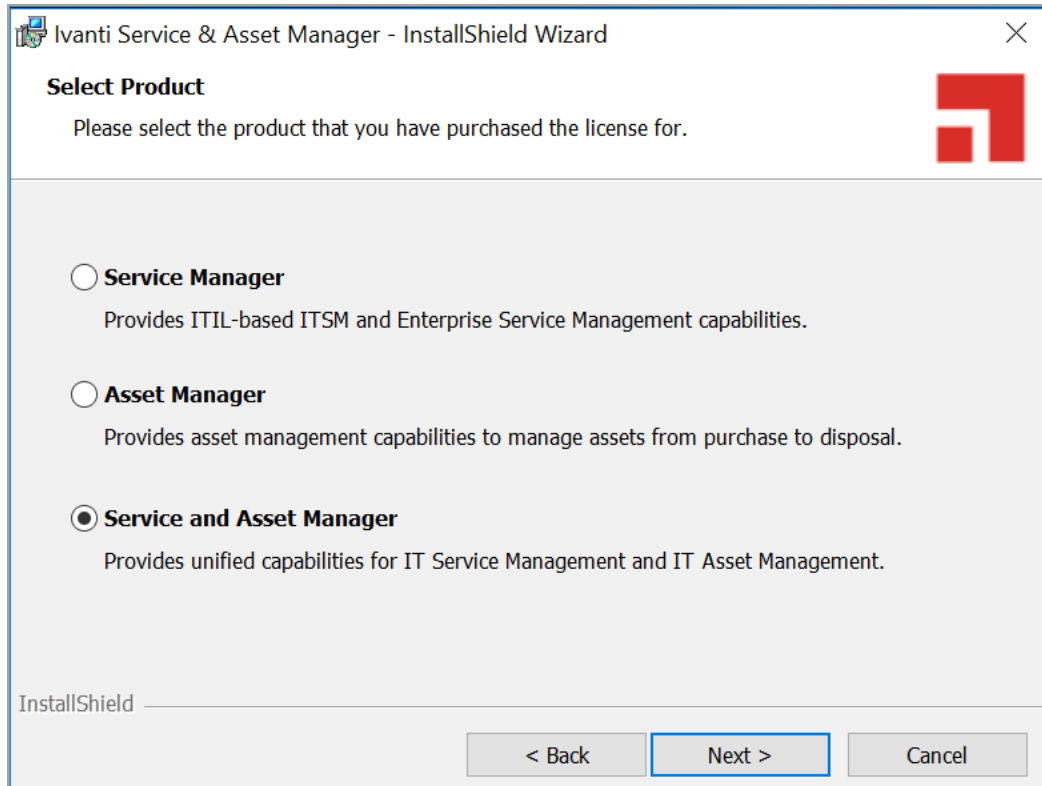
2. Click **Next**.



3. Click **Next** to continue the installation process.



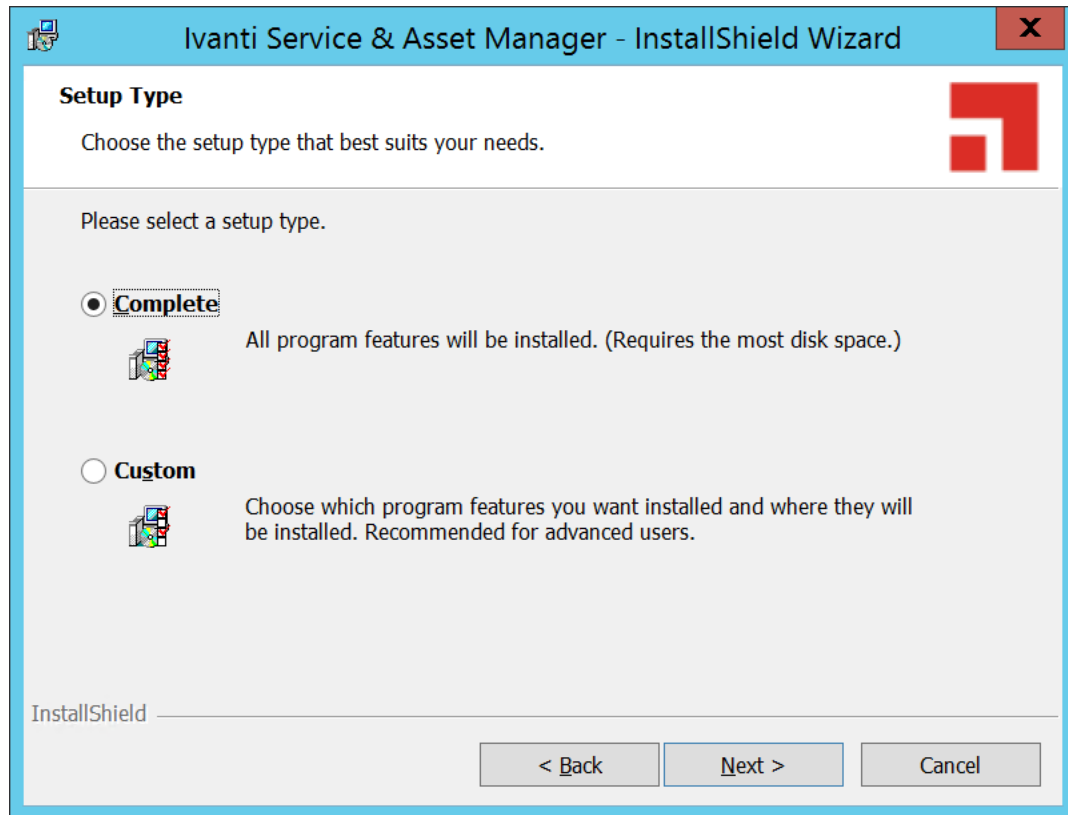
4. Select one of the options, **Service Manager**, **Asset Manager**, or **Service and Asset Manager**.



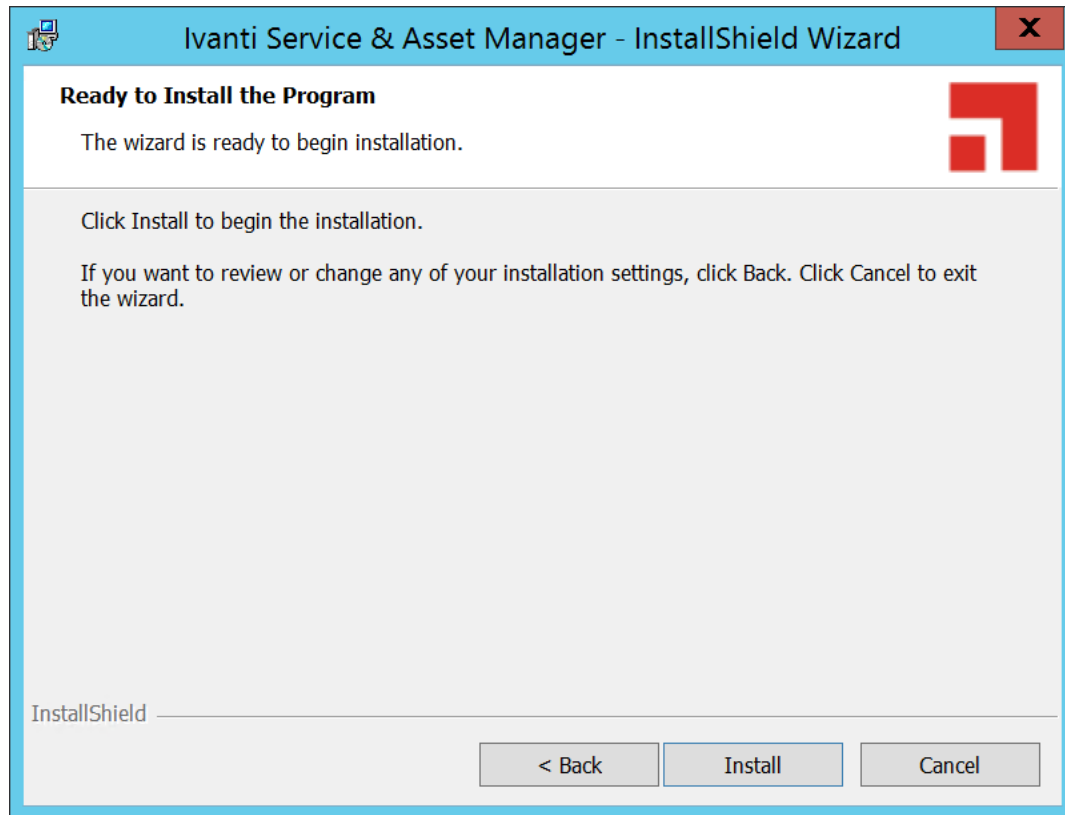
For more information on Asset Manager, access the following URL:

https://help.ivanti.com/docs/help/en_US/IAM/2018/LandingPage.htm

5. Select the **Custom** or **Complete** options.



6. Click **Next**.



The tabs that you see in the wizard depend on which components that you installed. You may see all of the tabs or you may just see a subset of them.

See the following sections:

- "Using the System Configuration Wizard" on the next page
- "Configuring Service and Asset Manager " on page 84
- "Configuring the Reporting Feature" on page 120
- "Configuring Discovery" on page 131
- "Configuring the Deployment on the Service and Asset Manager Operations Console" on page 134
- "Optional SSL Configuration" on page 139
- "Optional LDAP Configuration" on page 149
- "About Configuring with ADFS" on page 149
- "About Configuring Throttling Settings" on page 149

Using the System Configuration Wizard

The System Configuration Wizard provides an interface in which you can perform various configuration tasks for the initial setup of Service and Asset Manager.

- "Starting the System Configuration Wizard Manually" below
- "Navigating the System Configuration Wizard" below
- "Actions to Perform in Each Page" on page 82

Starting the System Configuration Wizard Manually

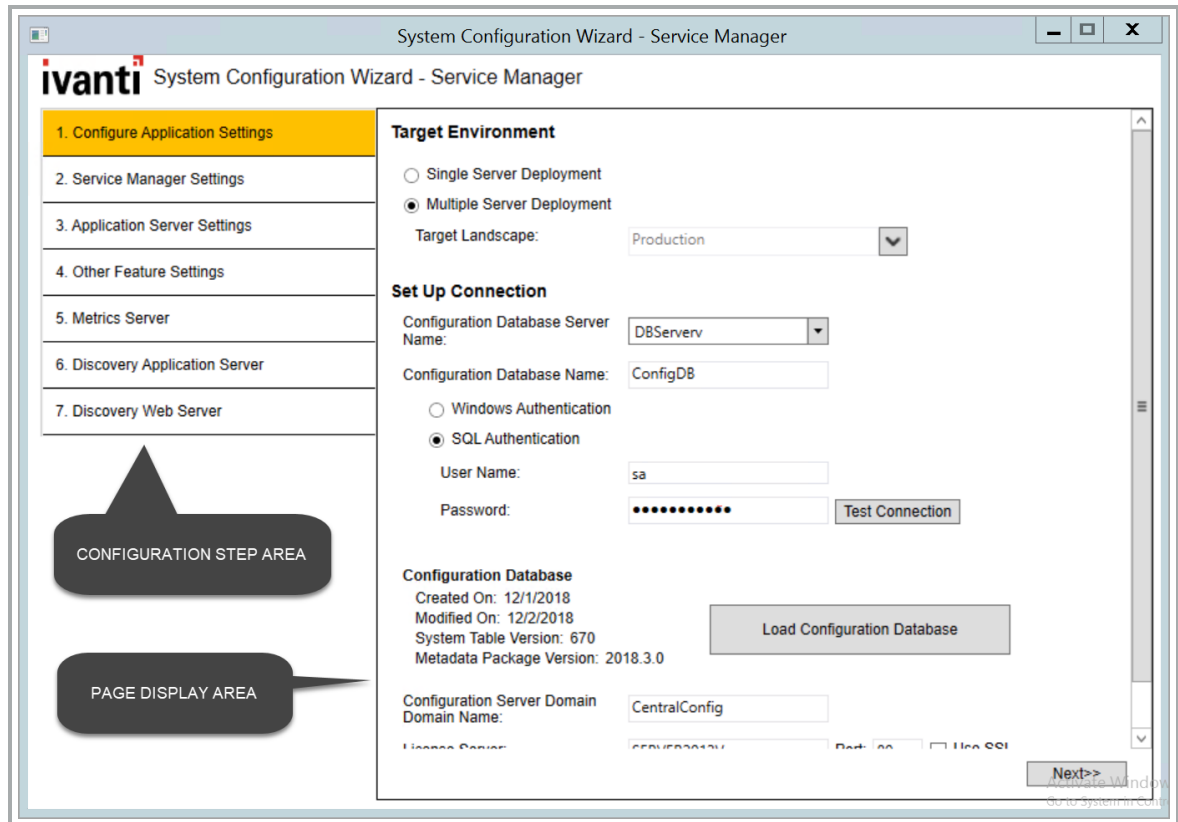
The System Configuration Wizard starts automatically after you finish installing Service and Asset Manager.

You can also start the System Configuration Wizard manually after your system is configured. See "Changing Feature Settings by Running the System Configuration Wizard" on page 164.

Navigating the System Configuration Wizard

The System Configuration Wizard contains the areas shown in "System Configuration Wizard Areas" below.

System Configuration Wizard Areas



- In the configuration step area, the page that you are currently working on is highlighted in yellow.
- After you complete a page and click **Next**, the system places a green check mark next to the completed page name to show that it has been completed.



The configuration step area is not a navigation pane. You cannot go to a page by clicking it in the configuration step area. Instead, click the **Next** and **Previous** buttons to move through the pages sequentially.

- The page display area shows the wizard page itself, including the fields and controls that you set the various parameters.



- Chat Configuration installs Redis version 6.2 re-distributable which requires internet access while configuring the System Configuration Wizard.
 - The default behavior of the System Configuration Wizard with respect to **SSL** check boxes have changed from **non-SSL** to **SSL**. For non-SSL based installation these check boxes need to be cleared.
 - As part of the security fix, the System Configuration Wizard requires host name with domain (Fully Qualified Domain Name). For more information, refer to the [Configuring the Application Server Settings section](#) in the Installation and Deployment guide.
-

Actions to Perform in Each Page

The System Configuration Wizard page numbers can change depending on the features you choose to install.

Unless otherwise noted, the settings that you specify in each wizard page are stored in the Configuration Database.

Configuration Application Settings page:

- Specify the name of the configuration database and the authentication method that is used by all supported web applications when connecting to the configuration database.
- Create or recreate the configuration database.
- If you use Windows Integrated Security for the configuration database, specify the Windows domain credentials for the service account.

See "Configuring the Configuration Database" on page 85.

Service Manager Settings page:

- Specify the name and authentication method for the server where the Service and Asset Manager application database resides.
- Load the demo database on a server other than the server where the Service and Asset Manager application database resides. This option allows you to review the demo database while the Service and Asset Manager application database continues to run in its current configuration.
- Specify the application name, attachment location, client authorization key, and the type of name to use when accessing the application.

See "Configuring the Service and Asset Manager Application" on page 90.

Application Server Settings page:

- Specify the location of the configuration server and the host name.

- Specify if you will use this server for surveys or the reporting feature.
- If you use Windows Integrated Security for the Service and Asset Manager application server, specify the Windows domain credentials for the service account.

See "Configuring the Application Server Settings" on page 97.

Other Feature Settings page:

- Specify the log file and temporary file locations on the configuration server.
- Specify different server hosts and whether to use SSL for the Service and Asset Manager application server.
- Specify the inbound web server information.

See "Configuring Other Feature Settings" on page 101.

Metrics Server page:

- Specify the locations for the log file and the Service and Asset Manager configuration server.
- Map applications to the metrics server.

See "Configuring the Metrics Server" on page 105.

Microsoft SSRS Configuration page:

- Appears when you install the reporting feature.
- Specify information about the Microsoft SQL Server database for the reporting feature.

See "Configuring the Reporting Feature" on page 120.

Reporting Service Configuration page:

- Appears when you install the reporting feature.
- Specify information about the Service and Asset Manager report database for the reporting feature.

See "Configuring the Reporting Feature" on page 120.

Discovery Application Server page:

- Specify information about the configuration of the Discovery application server.

See "Configuring the Discovery Application Server" on page 110.

Discovery Web Server page:

- Specify information about the configuration of the Discovery web server.
- Upgrade the configuration database and the Service and Asset Manager application database.

See "Configuring the Discovery Web Server" on page 116.

Upgrade System page:

- Appears when you upgrade to a newer release of Service and Asset Manager.
- Upgrade the configuration database and the Service and Asset Manager application database.

See "Upgrading Service and Asset Manager from an Earlier Release" on page 166.

Configuring Service and Asset Manager

The following sections contain step-by-step instructions for the procedures that you can perform through the System Configuration Wizard.

- "About Entering Server Location Names in the System Configuration Wizard" below
- "Configuring the Configuration Database" on the next page
- "Configuring the Service and Asset Manager Application" on page 90
- "Configuring the Application Server Settings" on page 97
- "Configuring Other Feature Settings" on page 101
- "Configuring the Metrics Server" on page 105
- "Configuring the Discovery Application Server" on page 110
- "Configuring the Discovery Web Server" on page 116
- "Finishing the System Configuration" on page 119
- "Installing the Demo Data Package" on page 119

About Entering Server Location Names in the System Configuration Wizard

For all of the fields in the System Configuration Wizard that ask for a server location, unless noted otherwise, you can enter one of three things:

- An IP address
- A machine name
- A fully-qualified domain name

We recommend that you use the same naming format in all server location fields, if possible.

If you are using SSL, you must enter a fully-qualified domain name.

If you have a load-balanced system, we recommend using a fully-qualified domain name.

Configuring the Configuration Database

After you have installed Service and Asset Manager, the System Configuration Wizard starts automatically and displays the **Configuration Application** page.

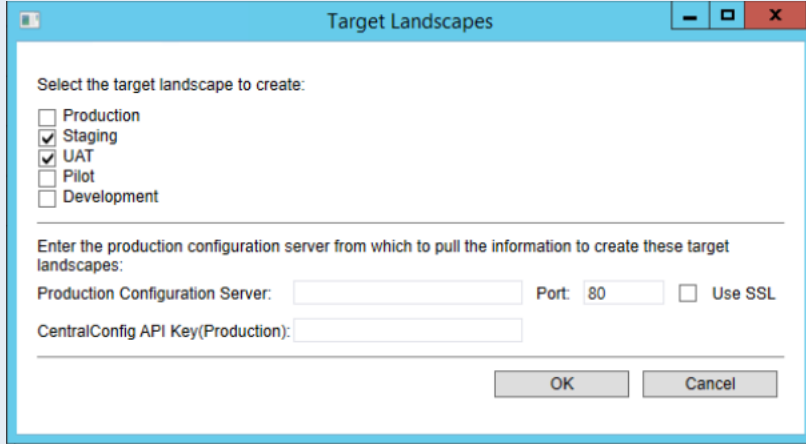
On this page, you will do the following:

- Specify the name of the configuration database and the authentication method that is used by all supported web applications when connecting to the configuration database.
- Create or recreate the configuration database.
- If you use Windows Integrated Security for the configuration database, specify the Windows domain credentials for the service account.

Configuration Application Page

1. Enter values into the fields:

Parameter	Description
Target Environment	
Deployment	<p>Choose one of the following:</p> <p>Single Server Deployment: If you are setting up the "Minimum Production Deployment" on page 10.</p>

Parameter	Description
	Multiple Server Deployment: If you are setting up the "Enterprise Production Deployment" on page 13.
Target Landscape	<p>(Only if you selected Multiple Server Deployment) Click the down arrow. The system displays the Target Landscapes dialog box.</p> <p>On the first server that you configure, check Production and click OK.</p> <p>On subsequent servers, check any combination of landscapes other than production and enter values in the subsequent fields. See below.</p> <p><i>Target Landscapes Dialog Box</i></p> 
Production Configuration Server	<p>(Only if you selected Multiple Server Deployment and selected anything other than Production in the Target Landscape field)</p> <p>The host or domain name of the configuration server for the production instance. Do not enter the information for any other instance; you must enter the information for the production instance.</p>
Port	<p>(Only if you selected Multiple Server Deployment and selected anything other than Production in the Target Landscape field)</p> <p>The port number of the production server. The default is 80, or 443 if you check Use SSL.</p>
Use SSL	<p>(Only if you selected Multiple Server Deployment and selected anything other than Production in the Target Landscape field)</p> <p>Check to enable SSL encryption to the server.</p>
CentralConfig API Key (Production)	<p>CentralConfig API key of the production environment.</p> <p>To retrieve the CentralConfig API Key, - navigate to the Configuration console > Configure > Security Controls > API Keys > CentralConfigApiKey (Key groups) > CentralConfigApiKey.</p>

- Click **OK** to close the **Target Landscapes** dialog box.
- Enter values into the fields:

Parameter	Description
Configuration Database Server Name	<p>The server where the configuration database is located.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name of the server of the configuration database.</p> <p>Browse for a server name by clicking the down arrow and selecting <Browse for more...>. The system displays any Microsoft SQL Server instances in your network. Choose a server and click OK.</p> <p>NOTE: Do not choose localhost unless you are setting up a "Demonstration or Proof-of-Concept Deployment" on page 8.</p>
Configuration Database Name	The name of the configuration database. The default name is ConfigDB and you cannot change the name.
Authentication Method	<p>Select one of the following:</p> <p>Windows Authentication: Uses Microsoft Windows authentication.</p> <p>SQL Authentication: Uses Microsoft SQL authentication. If you select this option, enter the user name and password below.</p>
User Name	<p>(Only if you selected SQL Authentication) The user name associated with the Microsoft SQL authentication.</p> <p>NOTE: If your deployment store FILESTREAM attachments, specify a configuration database user account that has a db_owner role on Microsoft SQL Server. See "Task 2: Setting up Service and Asset Manager" on page 49.</p>
Password	(Only if you selected SQL Authentication) The password associated with the user name for the Microsoft SQL authentication.

- Click **Test Connection** to test the connection to the configuration database server. The system displays *Connection successful!* if the connection is good. You must have a working connection to create a database. You cannot continue with the configuration if this connection does not work.
- Depending if there is already a configuration database, click **Load Configuration Database** or **Re-Create & Load Configuration DB**. If the configuration database already exists, the system asks if you want to recreate the database. Click **Yes**. The system displays the **New Database** dialog box.

New Database Dialog Box

New Database

Configuration Database Name: ConfigDB

Configuration Database Location: C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA

Collation: <Server Default>

Advanced Options

Database files

Logical Name	File Type	Initial Size(MB)	Autogrowth	Path
ConfigDB	Rows Data	100	By 10MB. Unrestricted growth.	C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA
ConfigDB_log	Log	1	By 10%. Unrestricted growth.	C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA

OK Cancel

6. Enter values into the fields:

Parameter	Description
Configuration Database Name	The name of the configuration database. The default name is ConfigDB and cannot be changed.
Configuration Database Location	The location for the configuration database. NOTE: If you have customized the existing configuration database, specify a different location; otherwise, the system overwrites your customization when you load the recreated database.
Collation	The set of rules that describe how to compare and sort strings, such as the order in which letters are sorted and whether case matters. NOTE: ISM application does not support case sensitive SQL Collation.
Advanced Options	
Logical Name	The logical name of the configuration database. This name is stored as a file name, and is a separate entity from the read-only database name that is displayed in Microsoft SQL Server Management Studio.
File Type	The file type, either database records or database logs. These values are read-only.

Parameter	Description
Initial Size (MB)	The initial file size, in MB, when creating the configuration database.
Autogrowth	Specifies how the database will expand when it reaches its maximum file size. We recommend having at least 1 GB or 10% to start with. Click ... to update the values.
Path	The location of the file. Click ... to update the location.
File Name	The name of the file.

- Click **OK**. The system creates the configuration database and installs it on the configuration database server that you specified. Several progress dialog boxes appear as various Microsoft SQL scripts execute to create and load the configuration database. After the system loads the configuration database, the **Configuration Application** page displays *Configuration database loaded*.
- Click **Next**. The system refreshes the **Configuration Application** page. (If you end up on the next page of the System Configuration Wizard, click **Previous** to return to the **Configuration Application** page.)
- Enter values into the fields:

Parameter	Description
Configuration Server Domain Name	The fully-qualified domain name of the configuration server in this format: config.servername.com.
License Server	The name of the license server. We recommend using a fully-qualified domain name.
Port	The port number of the license server. The default is 80, or 443 if you check Use SSL .
Use SSL	Check if the license server uses SSL.
IvantiSM License File-Production	<p>The name of the license file for the Service and Asset Manager production instance. Click Browse..., navigate to the license file, and click Open. License files have a .lic suffix.</p> <p>NOTE: The system displays either one or both of the license fields, depending on your landscape environment. At this point, you only need to enter one license, which allows the License Manager to start and run Service and Asset Manager. You can import additional licenses, if needed, at a later time from within the License Manager. See "Using the License Manager" on page 174.</p>
IvantiSM License File-Non-Production	<p>The name of the license file for the Service and Asset Manager non- production instance. Click Browse..., navigate to the license file, and click Open. License files have a .lic suffix.</p> <p>NOTE: The system displays either one or both of the license fields, depending on your landscape environment. At this point, you only need to enter one license, which allows the License Manager to start and run Service and Asset Manager. You can import additional licenses, if needed, at a later time from within the License Manager. See "Using the License Manager" on page 174.</p>

10. Create the administrator account for the configuration database. You only need to create this account once. If you return to this page in the System Configuration Wizard later, these fields are not displayed.

Enter values into the fields:

Parameter	Description
Login ID	The system automatically displays the login ID of HSWAdmin. You cannot change this.
Password	The password associated with the administrator. Record this password for future reference. If you lose the password, you must recreate and load the configuration database.
Confirm Password	Re-enter the password associated with the administrator.
First Name	The first name of the administrator.
Last Name	The last name of the administrator.
Email Address	The email address of the administrator.

11. Do one of the following:

- If you chose **Single Server Deployment**, click **Next**. The system displays the **Service and Asset Manager Application** page.
- If you chose **Multiple Server Deployment**, repeat all of the steps in this procedure to create a configuration database for each of your tenants. Then click **Next**. The system displays the **Service and Asset Manager Application** page.

Configuring the Service and Asset Manager Application

On this page you will do the following:

- Specify the name and authentication method for the server where the application database resides.
- Load the demo database on a server other than the server where the application database resides. This option allows you to review the demo database while the application database continues to run in its current configuration.
- Specify the application name, attachment location, client authorization key, and the type of name to use when accessing the application.

The first time that you see this page, there is no application database, as shown in "Service Manager Application Page: No Database" below.

Service Manager Application Page: No Database

1. Enter values into the fields:

Parameter	Description
Application Database Server	<p>The server where the application database is located. Usually this is the same server where the configuration database is located (specified earlier on the Configuration Application page).</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name of the server of the application database.</p> <p>Browse for a server name by clicking the down arrow and selecting <Browse for more...>. The system displays any Microsoft SQL Server instances in your network. Choose a server and click OK.</p> <p>NOTE: Do not choose localhost unless you are setting up a "Demonstration or Proof-of-Concept Deployment" on page 8.</p>
Application Database Name	<p>The name of the application database. The default name is IvantiSM. The name that you specify here is used when the application database is created, and later, recreated.</p>
Authentication Method	<p>Select one of the following:</p>

Parameter	Description
	<p>Windows Authentication: Uses Microsoft Windows authentication.</p> <p>SQL Authentication: Uses Microsoft SQL authentication. If you select this option, enter the user name and password below.</p> <p>See "Configuring the Reporting Feature" on page 120 for information on the appropriate database authentication type.</p>
User Name	(Only if you selected SQL Authentication) Enter the user name associated with the Microsoft SQL authentication.
Password	(Only if you selected SQL Authentication) Enter the password associated with the user name for the Microsoft SQL authentication.

- Click **Test Connection** to test the connection to the application database server. The system displays *Connection successful!* if the connection is good. You must have a working connection to create a database. You cannot continue with the configuration if this connection does not work.
- Depending if there is already an application database, click **Load Application Database** or **Re-Create & Load Application DB**. If the application database already exists, the system asks if you want to recreate the database. Click **Yes**. The system displays the **New Database** dialog box.

New Database Dialog Box

New Database

Application Database Name:

Application Database Location: ...

Collation:

^ **Advanced Options**

Database files

Logical Name	File Type	Initial Size(MB)	Autogrowth	Path
IvantiSM	Rows Data	2000	By 200MB. Unrestricted growth. ...	C:\Program Files\Microsoft SQL Server\MSSQL12
IvantiSM_log	Log	1	By 10%. Unrestricted growth. ...	C:\Program Files\Microsoft SQL Server\MSSQL12

OK Cancel

4. Enter values into the fields:

Parameter	Description
Application Database Name	The name of the application database. The default name is IvantiSM and cannot be changed.
Application Database Location	The location for the application database. NOTE: If you have customized the existing application database, specify a different location; otherwise, the system overwrites your customization when you load the recreated database.
Collation	The set of rules that describe how to compare and sort strings, such as the order in which letters are sorted and whether case matters. NOTE: ISM application does not support case sensitive SQL Collation.
Advanced Options	
Logical Name	The logical name of the application database. This name is stored as a file name, and is a separate entity from the read-only database name that is displayed in Microsoft SQL Server Management Studio.
File Type	The file type, either database records or database logs. These values are read-only.

Parameter	Description
Initial Size (MB)	The initial file size, in MB, when creating the application database.
Autogrowth	Specifies how the database will expand when it reaches its maximum file size. We recommend having at least 1 GB or 10% to start with. Click ... to update the values.
Path	The location of the file. Click ... to update the location.
File Name	The name of the file.

- Click **OK**.

The system creates the application database and installs it on the application database server that you specified. The system displays several progress dialog boxes as the system executes various Microsoft SQL scripts that create and load the application database. After the system loads the application database, the system displays *Application Database loaded*.

- (Optional) Click **Advanced Options** to open the **Landscape Advanced Options** dialog box. See the "Adding a Landscape" topic in the *Operations Console User Guide for Service and Asset Manager* for more information about these patterns.

Landscape Advanced Options Dialog Box

Landscape Advanced Options

1. Database Name Pattern

Production: {dbName}

2. Application Name Pattern

Production: {tenantName}

OK Cancel

- Click **Next**. The system refreshes the **Application** page. See "Application Page: Newly Created Database" below. (If you end up on the next page of the System Configuration Wizard, click **Previous** to return to the **Application** page.)

Application Page: Newly Created Database

8. Service and Asset Manager comes with optional transaction data that you can use to test and view the analytic metrics, financial, ITFM, and other features.

To include demo data, ensure that **Don't include Demo data** is unchecked. You must install the demo data manually after the System Configuration Wizard finishes. See "Installing the Demo Data Package" on page 119.

9. Enter values into the fields:

Parameter	Description
Application Name	The name of the application.
Attachment Type	<p>The location of the folder on the application database server where any Service and Asset Manager attachments reside.</p> <p>Select one of the following:</p> <p>Database</p> <p>FILESTREAM</p> <p>File System</p>
Client Auth Key	The authentication key that is used when the web services API accesses Service and Asset Manager.

Parameter	Description
Import Remote Control License File	<p>(Optional) If you are going to use the remote control feature, you must have a remote control license.</p> <p>Contact Ivanti Software to get the license. See "How to Contact Us" on page 7.</p> <p>To import the remote control license file, click Browse... next to the Import Remote Control License File field.</p> <p>Browse to the location of the license file and click OK to select it.</p>
To access the application	<p>Select whether to use the application database server machine name or the fully-qualified domain name for access to the application database server:</p> <p>Use machine name to access Ivanti application: When other Service and Asset Manager components log into the application server, they use the machine name of the server. For example, they use SERVER-01. If you choose this option, the system detects the current machine name and uses it automatically; you do not need to specify the machine name.</p> <p>Use domain name to access Ivantiapplication: When other Service and Asset Manager components log into the application server, they use the fully-qualified domain name of the server. For example, they use SERVER-01.company.com. If you plan on using SSL for connecting to the application server (configured later on the Other Feature Settings page), you must enter a fully-qualified domain name here, either for an individual machine or for a load-balanced instance.</p>
Application server domain name	<p>(Only if you selected Use domain name to access Ivantiapplication) The domain name of the application server.</p>

- Click **Next** to refresh the **Application** page. (If you end up on the next page of the System Configuration Wizard, click **Previous** to return to the **Application** page.)
- Create the administrator account for the application database. This login ID and password allows you to access the Service and Asset Manager Service Desk Console and Configuration Console. See "Logging into Service and Asset Manager" on page 161. You only need to create this account once. If you return to this page in the System Configuration Wizard later, these fields are not displayed.

Enter values into the fields:

Parameter	Description
Login ID	The system automatically displays the login ID of IvantiAdmin. You cannot change this.
Password	<p>The password associated with the administrator.</p> <p>Record this password for future reference. If you lose the password, you must recreate and load the application database.</p>
Confirm Password	Re-enter the password associated with the administrator.
First Name	The first name of the administrator.

Parameter	Description
Last Name	The last name of the administrator.
Email Address	The email address of the administrator.

12. If you chose **Multiple Server Deployment** on the **Configuration Application** page, your system has multiple tenants. Each tenant must have an administrator account, so that the administrator can access the Service and Asset Manager Service Desk Console and Configuration Console.

To create a new administrator account for another tenant instance, do the following:

- a. In the **Application Database Name** field at the top of this page, enter the next tenant to get an account.

For example, if you named your production tenant IvantiSM, your staging tenant IvantiSM-STG, and your UAT tenant IvantiSM-UAT, then the first time that you are on this page, enter **IvantiSM** in the **Application Database Name** field. The second time that you are on this page, enter **IvantiSM-STG** in the **Application Database Name** field. The third time that you are on this page, enter **IvantiSM-UAT** in the **Application Database Name** field.

- b. Create the administrator account for the application database for the tenant. See step 11 above.
 - c. Click **Next**. The system displays the **Application Server Settings** page.
 - d. Click **Previous** to return to the **Service and Asset Manager Application** page.
 - e. Repeat steps a. through d. for the next tenant.
13. After all of your tenants have an administrator account, click **Next** to advance to the **Application Server Settings** page.

Configuring the Application Server Settings

You set connections to other databases in Service and Asset Manager on the **Application Server Settings** page. You will do the following:

- Specify the location of the configuration server and the host name.
- Specify if you will use this server for surveys or the reporting feature.
- If you use Windows Integrated Security for the Application Server, specify the Windows domain credentials for the service account.

Application Server Settings Page

System Configuration Wizard - Service Manager

ivanti System Configuration Wizard - Service Manager

1. Configure Application Settings

2. Service Manager Settings

3. Application Server Settings

4. Other Feature Settings

5. Metrics Server

6. Microsoft SSRS Configuration

7. Reporting Service Configuration

8. Discovery Application Server

9. Discovery Web Server

Application Server Settings

Configuration Server Location: Port: ☐ Use SSL

Host Name:

Use this host for Operations Console: ☐

Use this host for Survey: ☐

Use these settings for Reporting Service: ☐

Local system account will be used for IIS Application Pool Identity and Windows Service.
Use a different account: ☐

<<Previous

1. Enter values into the fields:

Parameter	Description
Configuration Server Location	<p>The host name or domain name of the configuration server. The default value is the name of the server that you are logged into now.</p> <p>If the host that you are logged into now is <i>not</i> the configuration server, enter the machine name or fully-qualified domain name of your Configuration Server.</p> <p>If you check Use SSL below, you must enter the host name of the configuration server.</p>
Port	<p>The port number of the configuration server. The default is 80, or 443 if you check Use SSL.</p>
Use SSL	<p>Check to use SSL for connections to the configuration server.</p> <p>NOTE: We do not recommend enabling SSL on the configuration server until you have fully tested Service and Asset Manager to ensure that it works with SSL. For information on configuring Service and Asset Manager with SSL, see "Optional SSL Configuration" on page 139.</p>

2. Click **Test Connection** to test the connection to the configuration server. The system displays a success or failure message. Click **OK** to close the message.
3. Enter values in the fields:

Parameter	Description
Host Name	<p>The location of the system that hosts the Application Server. The default value is the server that you are logged into now.</p> <p>Do one of the following:</p> <p>If you are installing all Service and Asset Manager components on the same host, accept the default value.</p> <p>If you enter a different location, it must be a machine name. Do <i>not</i> enter a fully-qualified domain name.</p>
Use this host for Ivanti Operations Console	<p>Uses this server for the Ivanti Service Manager Operations Console.</p> <p>NOTE: If you have an "Enterprise Production Deployment" on page 13, we recommend that you only install and use the Service and Asset Manager Operations Console on the staging (STG) instance of the tenant.</p>
Landscape Type	<p>(Only if you checked Use this host for Ivanti Operations Console) Displays the landscape type and cannot be changed.</p>
Database Server	<p>(Only if you checked Use this host for Ivanti Operations Console) Displays the database server and cannot be changed.</p>
Operations Console Backup Location	<p>(Only if you checked Use this host for Ivanti Operations Console) The backup location for the Service and Asset Manager Operations Console. The backup location can either be on a database server or on a network folder.</p> <p>Do one of the following:</p> <p>Accept the default location.</p> <p>Enter a new location.</p> <p>Click Browse... and navigate to a new location.</p>
Test Backup & Restore	<p>(Only if you checked Use this host for Ivanti Operations Console) The database to test to ensure you can back up and restore it. Select one from the drop-down list. We recommend that you select the configuration database since it is small.</p> <p>Click test to test the connection. The system displays a message with the results of the test. Click OK to close the message.</p>
Use this host for Survey	<p>Uses this server for the Service and Asset Manager survey component.</p> <p>If you use Windows Authentication for the configuration server, the system prompts you for the Windows domain account and credentials. See "Configuring the Configuration Database" on page 85. This setting is already configured if all Service and Asset Manager components are installed on one server.</p>
Use these settings for Reporting Service	<p>Uses this server for the Service and Asset Manager reporting feature.</p>

Parameter	Description
	Usually, you configure the reporting feature on the Microsoft SSRS Configuration and Ivanti Reporting Service Configuration pages. However, if you have two different domains and the reporting feature server cannot reach the web server, you can configure these settings to enable the servers to communicate.
Use SSL for Reports	(Only if you checked Use these settings for Reporting Service) Uses SSL for reports.
Use Windows Authentication for SSRS	(Only if you checked Use these settings for Reporting Service) Uses Windows authentication for reports. If you plan on sharing the same Microsoft SSRS instance with other applications besides the reporting feature, you must use Windows authentication.
Web Service Virtual Directory	(Only if you checked Use these settings for Reporting Service) The name of the web service virtual directory.
Ivanti Web Application Pool Identity Account	<p>(Only if you checked Use these settings for Reporting Service) The application pool identity for the Service and Asset Manager web application pool. Select one of the following:</p> <p>Keep existing account</p> <p>Specify new account</p> <p>If you select Specify new account, click Set to enter the credentials.</p>
User Name	<p>(Only if you checked Use these settings for Reporting Service and selected Specify new account for the Ivanti Web Application Pool Identity Account field)</p> <p>The user name for the application pool identity for the Service and Asset Manager web application pool.</p>
Password	<p>(Only if you checked Use these settings for Reporting Service and selected Specify new account for the Ivanti Web Application Pool Identity Account field)</p> <p>The password associated with the user above. Click OK.</p>

4. If you are using Microsoft SQL authentication for the configuration server, the system displays this message: "Local system account will be used for IIS Application Pool Identity and Windows Service". See "Service Account" on page 45 for more information about this account.

To use a different account, do the following:

- a. Check **Use a different account**.
- b. Click **Set**.
- c. Enter the user name for the service account.
- d. Enter the password associated with the service account.
- e. Click **OK**.

- Each tenant in a multiple server deployment must have an administrator account. If you selected **Multiple Server Deployment** on the **Configuration Application** page, click **Previous** to return to the Service and Asset Manager application page and create additional tenant accounts.

Configuring Other Feature Settings

On this page you will do the following:

- Specify the log file and temporary file locations on the configuration server.
- Specify different servers and ports and whether to use SSL for the other Service and Asset Manager servers.
- Specify the inbound web server information.

Other Feature Settings Page

System Configuration Wizard - Service Manager

ivanti System Configuration Wizard - Service Manager

1. Configure Application Settings ☒

2. Service Manager Settings ☒

3. Application Server Settings ☒

4. Other Feature Settings

5. Metrics Server

6. Microsoft SSRS Configuration

7. Reporting Service Configuration

8. Discovery Application Server

9. Discovery Web Server

Configuration Settings

Log File Location: C:\Logs

Temp Folder Location: C:\Temp

Cache Location: C:\HEATCache

Customize Server

Application Server: SERVER2012-034 Port: 80 ☐ Use SSL

Message Queue Server: SERVER2012-034 Port: 7200 ☐ Use SSL

Integration Service Server: SERVER2012-034 Port: 80 ☐ Use SSL

Discovery Application Server: SERVER2012-034 Port: 8382 ☐ Use SSL

Inbound Web Service Settings

Inbound Web Service Server: SERVER2012-034 Port: 80 ☐ Use SSL

Trusted Host & Remote Host Blocked List:

☒ Restart services after setting configuration files.

- Enter values into the fields:

Parameter	Description
Configuration Settings	
Log File Location	The folder on the server that you are logged into now where the log files are located.

Parameter	Description
	<p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name of the folder where the log files are located.</p> <p>Browse for a different folder by clicking Browse.... Select a new folder and click OK.</p>
Temp Folder Location	<p>The folder on the server that you are logged into now where the temporary files are located. The temporary folder is used to cache JavaScript files and to enable integration server and Service and Asset Manager Operations Console features.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name of the folder where the temporary files are located.</p> <p>Browse for a different folder by clicking Browse.... Select a new folder and click OK.</p>
Cache Location	<p>The folder on the server that you are logged into now where the cached files are located.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name of the folder where the cached files are located.</p> <p>Browse for a different folder by clicking Browse.... Select a new folder and click OK.</p>
Customize Server	
Application Server	<p>Where the application server is located. The default value is the server that you are logged into now.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name where the application server is located.</p> <p>If you use SSL, you must enter a fully-qualified domain name.</p> <p>NOTE: If you choose a different server for the application server and check Use SSL, SSL is only enabled for the application server. It does not enable SSL for the configuration server.</p>
Port	<p>The port number of the application server. The default is 80, or 443 if you check Use SSL.</p>

Parameter	Description
Use SSL	Enables SSL encryption to the application server.
Message Queue Server	<p>Where the message queue server is located. The default value is the server that you are logged into now.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name where the Service and Asset Manager message queue server is located.</p> <p>If you use SSL, you must enter a fully-qualified domain name.</p>
Port	The port number of the message queue server. The default is 7200.
Use SSL	Enables SSL encryption to the message queue server.
Integration Server	<p>Where the integration server is located. The default value is the server that you are logged into now.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the server where the Service and Asset Manager integration server is located.</p> <p>If you use SSL, you must enter a fully-qualified domain name.</p>
Port	The port number of the Service and Asset Manager integration server. The default is 80, or 443 if you check Use SSL .
Use SSL	Enables SSL encryption to the Service and Asset Manager integration server.
Discovery Application Server	<p>Where the Discovery application server is located. The default value is the server that you are logged into now.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the server where the Discovery application server is located.</p> <p>If you use SSL, you must enter a fully-qualified domain name.</p>
Port	The port number of the Discovery application server. The default is 8382, or 443 if you check Use SSL .

Parameter	Description
Use SSL	Enables SSL encryption to the Discovery application server.
Inbound Web Service Settings	
Inbound Web Server	Where the inbound web server is located. The default value is the server that you are logged into now. Do one of the following: Accept the default value. Enter the server where the Service and Asset Manager inbound web server is located. If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the Service and Asset Manager inbound web server. The default is 80, or 443 if you check Use SSL .
Use SSL	Enables SSL encryption to the Service and Asset Manager inbound web server.

You can set a list of remote hosts to block and a list of remote hosts to trust. By default, the list is empty.

2. To designate a list of blocked servers, do the following:
 - a. Next to the **Trusted Host & Remote Host Blocked List** field, click **Set**.
 - b. In the **Remote Host Blocked List** area, click the plus icon.
 - c. Enter the starting IP address and the ending IP address for the blocked servers.
 - d. If you are blocking web scripts, check **Is Web Script**.
 - e. Click **OK**.
3. To designate a list of trusted servers, do the following:
 - a. Next to the **Trusted Host & Remote Host Blocked List** field, click **Set**.
 - b. In the **Integration Trusted Host List** area, click the plus icon.
 - c. Enter a name for the trusted host list.
 - d. Enter the starting IP address and the ending IP address for the trusted servers.
 - e. Click **OK**.

Edit Integration Trusted Host and Remote Host Blocked List Dialog Box



To update the list at a later time, run the System Configuration Wizard, advance to the **Other Feature Settings** page, click **Set**, and make your changes. When you are done, click **OK**.

4. To restart the Service and Asset Manager services after you exit the System Configuration Wizard, check **Restart services after setting configuration files**.
5. Verify that the Service and Asset Manager services restart after the wizard closes.
6. If you did not check **Restart services after setting configuration files**, restart the Service and Asset Manager services manually.
7. Click **Next**. The system displays the **Metrics Server** page.

Configuring the Metrics Server

Perform these steps to configure one or more Metrics Server databases, which you can use to analyze data. Your deployment can have multiple Metrics Server databases to improve performance.

On this page, you will do the following:

- Specify the locations for the log file and the configuration server.
- Map applications to the Metrics Server.

Metrics Server Page

System Configuration Wizard - Service Manager

ivanti System Configuration Wizard - Service Manager

1. Configure Application Settings

2. Service Manager Settings

3. Application Server Settings

4. Other Feature Settings

5. Metrics Server

6. Microsoft SSRS Configuration

7. Reporting Service Configuration

8. Discovery Application Server

9. Discovery Web Server

Metrics Server

Metrics Cache Database Connection

Database Server Name: DbServer-034

Database Name: HEATMetricsCache

☐ Windows Authentication

☒ SQL Authentication

User Name: sa

Password:

Test Connection

A Metrics Server Database is detected.

Created On: 12/20/2018

Modified On: 12/20/2018

Re-Create & Load Metrics Server DB

Configuration Server Location: SERVER2012-034 Port: 80 ☐ Use SSL Test Connection

This server is registered in Metrics Server. You may map this server to each application.

Name: Metrics Server

Description:

Server Name: SERVER2012-034

Use SSL ☐

Enabled ☒

Remove

Select checkbox which application you want to use this Metrics Server

<<Previous

Next>>

1. Enter values into the fields:

Parameter	Description
Metrics Cache Database Connection	
Database Server Name	<p>Where the metrics cache database server is located. The default value is the server where the application server is located.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name of the server of the metrics cache database.</p> <p>Browse for a server name by clicking the down arrow and selecting <Browse for more...>. The system displays all available database servers in the network for your connection. Choose a server and click OK.</p> <p>NOTE: Do not choose localhost unless you are setting up a "Demonstration or Proof-of-Concept Deployment" on page 8.</p>
Database Name	<p>The name of the metrics cache database.</p> <p>Do one of the following:</p>

Parameter	Description
	Accept the default value. Enter the name of the metrics cache database.
Authentication Method	Select one of the following: Windows Authentication: Uses Microsoft Windows authentication. SQL Authentication: Uses Microsoft SQL authentication. If you select this option, enter the user name and password below. NOTE: The metrics cache database server is not compatible with SSL if your system has Windows authentication set up.
User Name	(Only if you selected SQL Authentication) The user name associated with the Microsoft SQL authentication.
Password	(Only if you selected SQL Authentication) The password associated with the user name for the Microsoft SQL authentication.

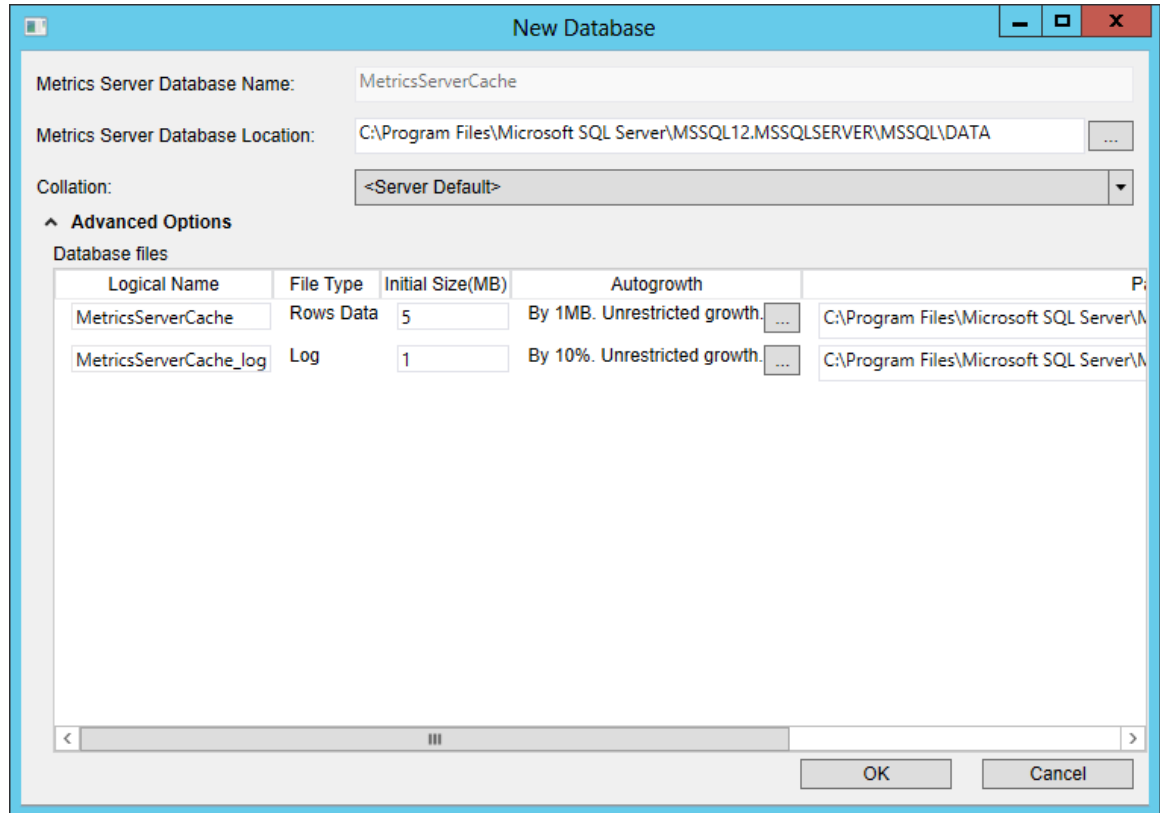
- Click **Test Connection** to test the connection to the metrics cache database server. The system displays a success or failure message below the **Test Connection** button. You must have a working connection to create a database. You cannot continue with the configuration if this connection does not work.
- Do one of the following:
 - If this is the initial setup, go to "Creating a New Metrics Server Database" below.
 - If your system already has a metrics server database, go to "Recreating the Metrics Server Database" on page 110.

Creating a New Metrics Server Database

An initial installation does not have a metrics server database. Follow these steps to create one.

- Click **Create & Load Metrics Server DB**. The system displays the **New Database** dialog box.

New Database Dialog Box



2. In the **Location** field, select a location for the metrics server database.
3. Click **Advanced Options** to view and reconfigure these metrics server database settings:
 - **Logical name:** The logical name of the metrics database. This name is stored as a file name, and is a separate entity from the read-only database name that is displayed in Microsoft SQL Server Management Studio.
 - **File type:** The file type, either database records or database logs. These values are read-only.
 - **Initial size in MB:** The initial file size, in MB, when creating the metrics database.
 - **Autogrowth size:** Specifies how the database will expand when it reaches its maximum file size. We recommend having at least 1 GB or 10% to start with. Click ... to update the values.
 - **The location of the database:** The location of the file. Click ... to update the location.
 - **File name:** The name of the file.
4. Click **OK** in the **New Database** dialog box.

The **Configuration Server Location** field indicates the location of the system that hosts the configuration server. The default value is the name of the host that you are logged into now.

5. If this is the system that hosts the configuration server, accept the default value.

If the host that you are logged into now is not the configuration server, enter the machine name or fully-qualified domain name of your configuration server.

If you use SSL, you enter the fully-qualified domain name of the configuration server.
6. Enter the port number in the **Port** field. The default value is 80. If you click **Use SSL**, it changes to 443.
7. Select whether to use SSL for connections to the configuration server.

If you use SSL, you must provide a fully-qualified domain name in the **Configuration Server Location** field.
8. Click **Test Connection** to test the connection to the configuration server. A pop-up message notifies you of success or failure.



We do not recommend enabling SSL on the configuration server until you have fully tested Service and Asset Manager to ensure that it works with SSL.

For information on configuring Service and Asset Manager with SSL, see "Optional SSL Configuration" on page 139.

9. Enter the following information to register a server in a multi-server deployment to the metrics server database:
 - Accept the default server name or enter a different name.
 - Optional. Enter a description of the server.
 - The default server name value is the name of the host that you are logged into now. You must use this name or localhost.
 - Check the box to use SSL encryption.
 - Check the box to enable this metrics server.
10. Click **Save**.
11. To map an application to the new metrics server to an application, check **Map**. You can reference the same metrics server to multiple Service and Asset Manager applications.



To change this server at a later time, run the System Configuration Wizard, advance to the **Metrics Server** page, and click **Remove**.

12. Click **Next**. The system displays the **Discovery Application Server** page.

Recreating the Metrics Server Database

If you are upgrading or repairing Service and Asset Manager, you already have a metrics server database, and the **Metrics Server** page looks like "Metrics Server Page" below.

Metrics Server Page

1. To recreate the metrics server database, click **Re-Create & Load Metrics Server DB**. The system displays the **New Database** dialog box.
2. Perform steps 2 through 12 in "Creating a New Metrics Server Database" on page 107.



If you have customized the existing metrics server database, specify a different location in the **Metrics Server Database Location** field in the **New Database** dialog box. Otherwise, the system overwrites your customization when you load the recreated database.

Configuring the Discovery Application Server

On this page you will specify information about the configuration of the Discovery application server and the Discovery configuration database. Follow these steps:

- "Starting the Configuration for the Discovery Application Server" on the next page

- "Configuring a System without a Discovery Configuration Database (Creating a New One)" on page 114
- "Configuring a System with a Discovery Configuration Database (Editing One that Already Exists)" on page 115

Starting the Configuration for the Discovery Application Server

The first time that you see this page, there is no Discovery configuration database, as shown in "Discovery Application Server Page: No Database" below.

Discovery Application Server Page: No Database

System Configuration Wizard - Service Manager

ivanti System Configuration Wizard - Service Manager

1. Configure Application Settings ✓
 2. Service Manager Settings ✓
 3. Application Server Settings ✓
 4. Other Feature Settings ✓
 5. Upgrade System ✓
 6. Metrics Server ✓
 7. Discovery Application Server
 8. Discovery Web Server

Discovery Application Server Configuration

Configuration Server: DBSERVER-021 Port: 80 ☐ Use SSL **Test Connection**

Log File Location: C:\Logs **Browse...**

Message Queue Server: DBSERVER-021 Port: 7200 ☐ Use SSL

Discovery Application Server: DBSERVER-021 Port: 8382 ☐ Use SSL

Discovery Database Setup

Database Server: DBSERVER-021

Database Name: HEATDiscoveryConfig

☐ Windows Authentication
☒ SQL Authentication

User Name: sa

Password: **Test Connection**

Discovery Database
 Created On: 12/16/2018 **Re-Create & Load Discovery DB**

☒ Restart services after setting configuration files.

<<Previous **Next>>**

1. Enter values into the fields:

Parameter	Description
Configuration Server	<p>The host name or fully-qualified domain name of the configuration server. The default value is the name of the host that you are logged into now.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name of the server of the configuration server.</p>

Parameter	Description
	If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the configuration server. The default is 80, or 443 if you check Use SSL .
Use SSL	Enables SSL encryption to the configuration server.

- Click **Test Connection** to test the connection to the configuration server. The system displays a success or failure message. Click **OK** to close the message. You must have a working connection to the server. You cannot continue with the configuration if this connection does not work.
- Enter values into the fields:

Parameter	Description
Log File Location	<p>The folder on the server that you are logged into now where the log files are located. The default location for the log files is C:\Logs.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name of the folder where the log files are located.</p> <p>Browse for a different folder by clicking Browse.... Select a new folder and click OK.</p>
Message Queue Server	<p>Where the Service and Asset Manager message queue server is located. The default value is the server that you are logged into now.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name where the Service and Asset Manager message queue server is located.</p> <p>If you use SSL, you must enter a fully-qualified domain name.</p>
Port	The port number of the Service and Asset Manager message queue server. The default is 7200.
Use SSL	Enables SSL encryption to the Service and Asset Manager message queue server.
Discovery Application Server	<p>Where the Discovery application server is located. The default value is the server that you are logged into now.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name where the Discovery application server is located.</p>

Parameter	Description
	If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the Discovery application server. The default is 80, or 443 if you check Use SSL .
Use SSL	Enables SSL encryption to the Discovery application server.
Discovery Database Setup	
Database Server	<p>The name of the system proposed for the Discovery configuration database. The default value is the server that you are logged into now.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name of the Discovery configuration database server.</p> <p>Browse for a server name by clicking the down arrow and selecting <Browse for more...>. The system displays any Microsoft SQL Server instances in your network. Choose a server and click OK.</p>
Database Name	The name of the Discovery configuration database. The default name is HEATDiscoveryConfig and you cannot change the name.
Authentication Method	<p>There are two authentication methods for the Discovery configuration database, one for creation and one for access.</p> <p>Select the authentication method for creating the Discovery configuration database:</p> <p>Windows Authentication: Uses Microsoft Windows authentication.</p> <p>SQL Authentication: Uses Microsoft SQL authentication. If you select this option, enter the user name and password below.</p>
User Name	(Only if you selected SQL Authentication) The user name associated with the Microsoft SQL authentication.
Password	(Only if you selected SQL Authentication) The password associated with the user name for the Microsoft SQL authentication.

4. Click **Test Connection** to test the connection to the Discovery configuration database server. The system displays a success or failure message. Click **OK** to close the message. You must have a working connection to create a database. You cannot continue with the configuration if this connection does not work.
5. Do one of the following:
 - If this is the initial setup, go to "Configuring a System without a Discovery Configuration Database (Creating a New One)" on the next page.

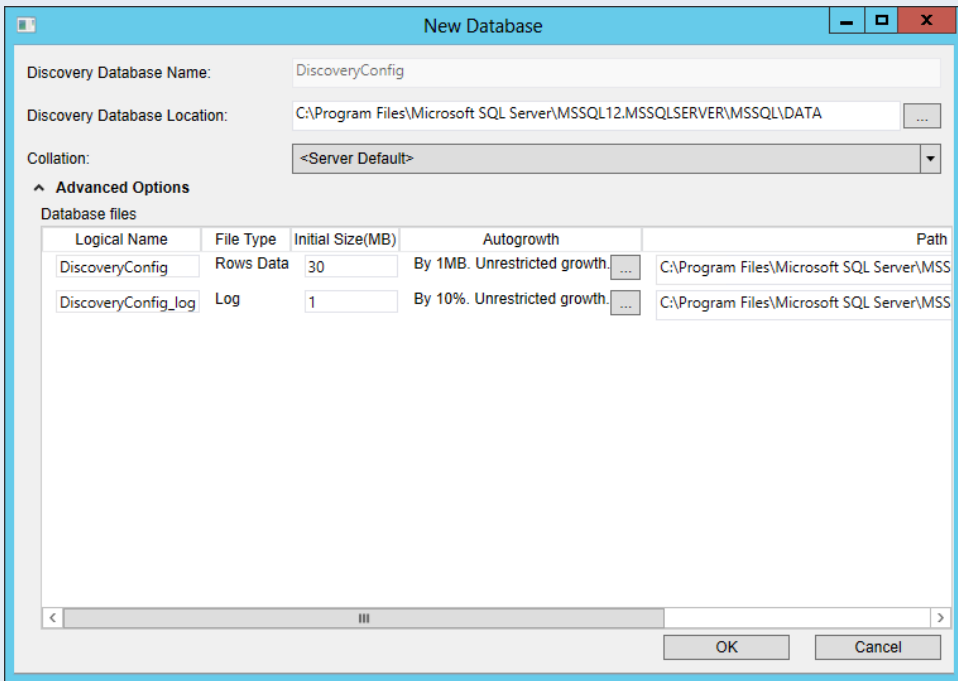
- If your system already has a Discovery configuration database, go to "Configuring a System with a Discovery Configuration Database (Editing One that Already Exists)" on the next page.

Configuring a System without a Discovery Configuration Database (Creating a New One)

An initial installation does not have a Discovery configuration database. The system displays this: "No Discovery (HEATDiscoveryConfig) Database is detected."

Follow these steps to create one.

1. Enter values into the fields:

Parameter	Description
Create & Load Discovery DB	<p>Click to create and load a new Discovery configuration database. The system displays the New Database dialog box.</p> <p><i>New Database Dialog Box</i></p> <div></div>
Discovery Database Name	The name of the Discovery configuration database. The default name is HEATDiscoveryConfig and you cannot change the name.
Discovery Database Location	The location for the Discovery configuration database.

Parameter	Description
Collation	The set of rules that describe how to compare and sort strings, such as the order in which letters are sorted and whether case matters. NOTE: ISM application does not support case sensitive SQL Collation.
Advanced Options	
Logical Name	The logical name of the Discovery configuration database. This name is stored as a file name, and is a separate entity from the read-only database name that is displayed in Microsoft SQL Server Management Studio.
File Type	The file type, either database records or database logs. These values are read-only.
Initial Size (MB)	The initial file size, in MB, when creating the Discovery configuration database.
Autogrowth	Specifies how the database will expand when it reaches its maximum file size. We recommend having at least 1 GB or 10% to start with. Click ... to update the values.
Path	The location of the file. Click ... to update the location.
File Name	The name of the file.

- Click **OK** in the **New Database** dialog box. The system creates the Discovery configuration database.
- To restart the Service and Asset Manager services after you finish the installation, check **Restart services after setting configuration files..**
- Click **Next**. The system displays the **Discovery Web Server** page.

Configuring a System with a Discovery Configuration Database (Editing One that Already Exists)

If you are upgrading or repairing Service and Asset Manager you already have a Discovery configuration database.

- To recreate the Discovery configuration database, click **Re-Create & Load Discovery DB**. The system displays a confirmation message.



If you have customized the existing Discovery configuration database, specify a different location in the **Discovery Database Location** dialog box. Otherwise, the system overwrites your customization when you recreate the database.

- Click **OK** at the confirmation message.
- To restart the Service and Asset Manager services after you finish the installation, check **Restart services after setting configuration files..**
- Click **Next**. The system displays the **Discovery Web Server** page.

Configuring the Discovery Web Server

Configure the relationship between Service and Asset Manager, the Discovery web server, and the Discovery application server from the **Discovery Web Server** page of the System Configuration Wizard.

The system displays the **Discovery Web Server** page. See "Discovery Web Server Page" below.

Discovery Web Server Page

System Configuration Wizard - Service Manager

Discovery Web Server Configuration

Configuration Server:	DBSERVER-021	Port: 80	<input type="checkbox"/> Use SSL	Test Connection
Application Server:	DBSERVER-021	Port: 80	<input type="checkbox"/> Use SSL	
Discovery Application Server:	DBSERVER-021	Port: 8382	<input type="checkbox"/> Use SSL	
Discovery Web Server:	DBSERVER-021	Port: 80	<input type="checkbox"/> Use SSL	
MDI Server:	DBSERVER-021	Port: 8734		
Message Queue Server:	DBSERVER-021	Port: 7200	<input type="checkbox"/> Use SSL	
Log File Location:	C:\Logs Browse...			

☒ Restart services after setting configuration files.

[<<Previous](#) [Finish](#)

1. Enter values into the fields:

Parameter	Description
Configuration Server	<p>The host name or fully-qualified domain name of the configuration server. The default value is the name of the host that you are logged into now.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name of the server of the configuration server.</p> <p>If you use SSL, you must enter a fully-qualified domain name.</p>

Parameter	Description
Port	The port number of the configuration server. The default is 80, or 443 if you check Use SSL .
Use SSL	Enables SSL encryption to the configuration server.

2. Click **Test Connection** to verify the connection to the configuration server.
3. Enter values into the fields:

Parameter	Description
Application Server	<p>Where the application server is located. The default value is the server that you are logged into now.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name where the application server is located.</p> <p>If you use SSL, you must enter a fully-qualified domain name.</p>
Port	The port number of the application server. The default is 80, or 443 if you check Use SSL .
Use SSL	Enables SSL encryption to the application server.
Discovery Application Server	<p>Where the Discovery application server is located. The default value is the server that you are logged into now.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name where the Discovery application server is located.</p> <p>If you use SSL, you must enter a fully-qualified domain name.</p>
Port	The port number of the Discovery application server. The default is 8382, or 443 if you check Use SSL .
Use SSL	Enables SSL encryption to the Discovery application server.
Discovery Web Server	<p>Where the Discovery web server is located. The default value is the server that you are logged into now.</p> <p>Do one of the following:</p> <p>Accept the default value.</p> <p>Enter the name where the Discovery web server is located.</p>

Parameter	Description
	If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the Discovery web server. The default is 80, or 443 if you check Use SSL .
Use SSL	Enables SSL encryption to the Discovery web server.
MDI Server	Where the MDI server is located. (The Mobile Device Inventory [MDI] service is bundled with Discovery.) The default value is the server that you are logged into now. Do one of the following: Accept the default value. Enter the name where the MDI server is located.
Port	The port number of the MDI server. The default is 8734.
Message Queue Server	Where the message queue server is located. The default value is the server that you are logged into now. Do one of the following: Accept the default value. Enter the name where the Service and Asset Manager message queue server is located. If you use SSL, you must enter a fully-qualified domain name.
Port	The port number of the Service and Asset Manager message queue server. The default is 7200.
Use SSL	Enables SSL encryption to the Service and Asset Manager message queue server.
Log File Location	The folder on the server that you are logged into now where the log files are located. The default location for the log files is C:\Logs on the Discovery web server. Do one of the following: Accept the default value. Enter the name of the folder where the log files are located. Browse for a different folder by clicking Browse.... Select a new folder and click OK .

- To restart the Service and Asset Manager services after you exit the System Configuration Wizard, check **Restart services after setting configuration files**.
- Verify that the Service and Asset Manager services restart after the wizard closes.
- If you did not check **Restart services after setting configuration files**, restart the Service and Asset Manager services manually.

Finishing the System Configuration

When you have finished configuring the ISM Discovery web server, do the following:

1. Click **Finish**. The System Configuration Wizard closes and the system displays the **Completed** page of the install wizard.
2. Click **Finish**.
3. Restart the host server that you just configured.
4. Verify that you can access Service and Asset Manager by navigating to `http://server_name/HEAT`.

Installing the Demo Data Package



Only perform this procedure if you did NOT check **Don't include Demo data** on the **Service and Asset Manager Application** page of the System Configuration Wizard. See "Configuring the Service and Asset Manager Application" on page 90 for information about the **Service and Asset Manager application** page.

Service and Asset Manager comes with additional transaction database that you can use to test and view the analytic metrics, financial, IT Financial Management, and other Service and Asset Manager features.

Follow these steps to install the demo data package:

1. Navigate to: C:\Program Files\HEAT\Software\HEAT\SystemConfigurationWizard\DB\AppServer\SQL\DemoData.
2. Extract the Demo Data Pkg.rar file.
3. Use Microsoft SQL Management Studio to restore the file called DemoData_Database.bak. This file was created based on Microsoft SQL Release 2008 R2.
4. Back up the current Service and Asset Manager database.
5. Use Microsoft SQL Management Studio to open the script called Demo Data Transfer Script.sql. The script updates the names of the source and target databases, based on your environment.
6. Use Microsoft SQL Management Studio to run the script called Demo Data Transfer Script.sql.
7. Use Microsoft SQL Management Studio to open the script called ITFM Demo Data Update.sql. The script updates the IT Financial Management dates in the database.
8. Use Microsoft SQL Management Studio to run the script called ITFM Demo Data Update.sql.

Configuring the Reporting Feature

If your Service and Asset Manager deployment includes the reporting feature, you need to set up authentication. Authentication is only needed for the reporting feature, and not for deployments that do not use the reporting feature.

- "Authenticating the Application Database" below
- "Configuring Microsoft SSRS" on page 124
- "Configuring the Reporting Feature" on page 128

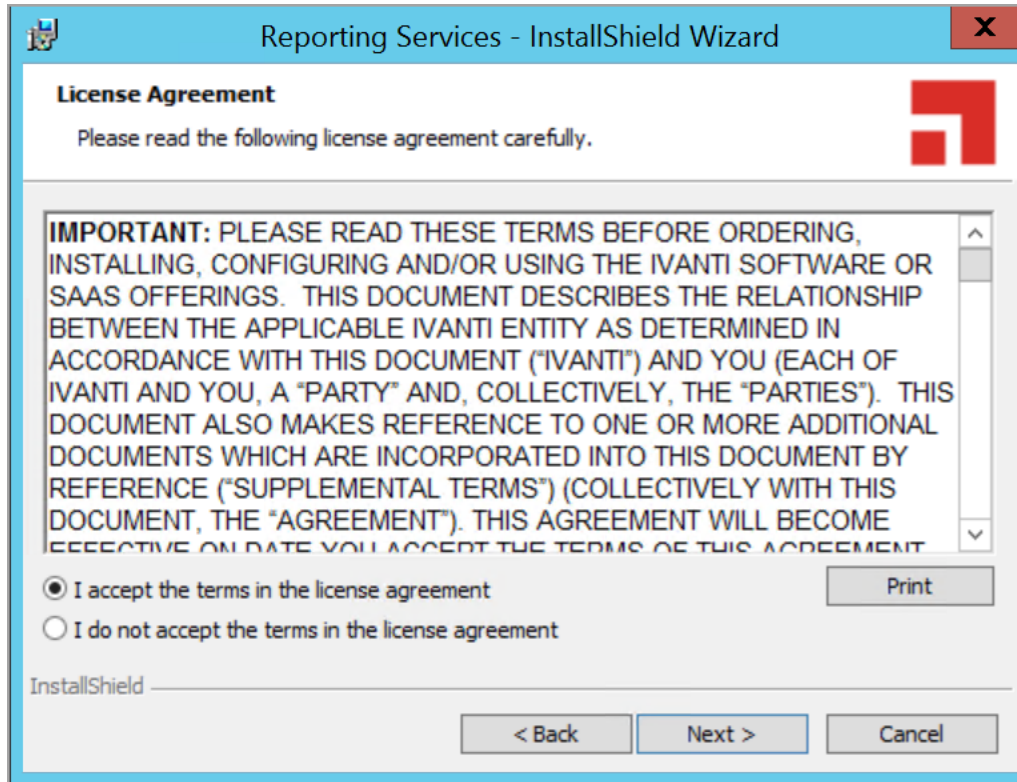
Authenticating the Application Database

The wizard walks you through the first-time set up and configuration as shown in the screenshots below.

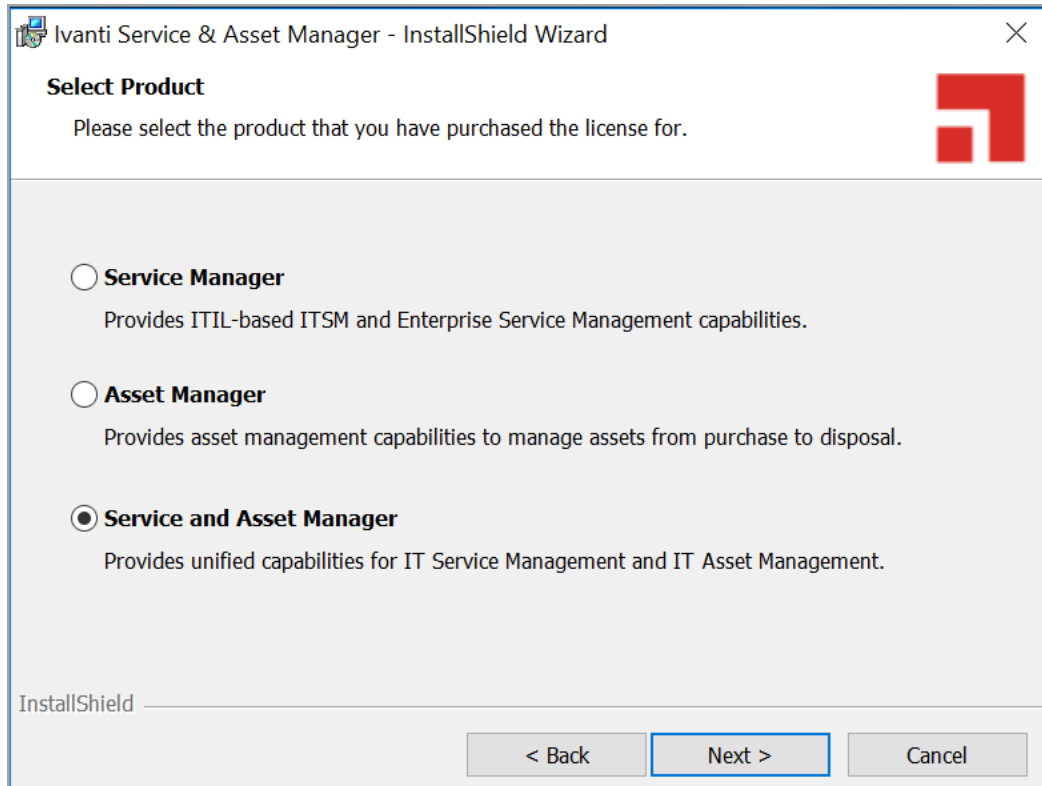
1. Click **Next**.



2. Click **Next** to continue the installation process.

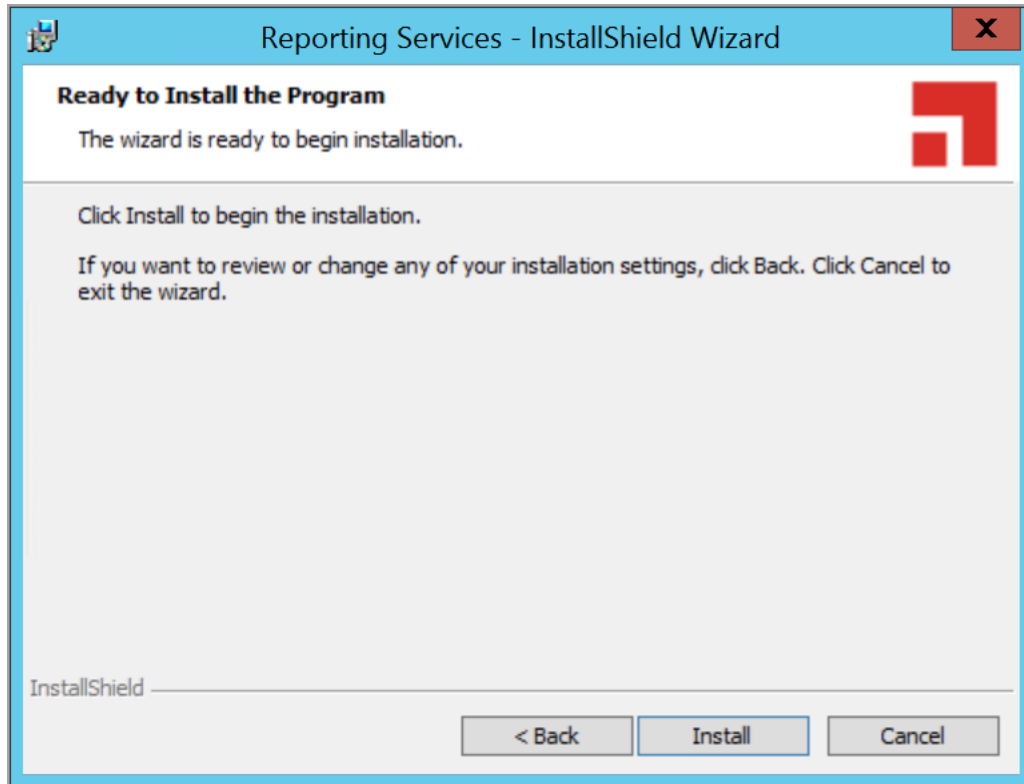


3. Select one of the options, **Service Manager**, **Asset Manager**, or **Service and Asset Manager**.



For more information on Asset Manager, access the following URL:
https://help.ivanti.com/docs/help/en_US/IAM/2018/LandingPage.htm

4. Click **Next**.



When you configure Service and Asset Manager, you set the authentication for the application database on the **Service and Asset Manager Application** page of the System Configuration Wizard, as shown in "Ivanti Service Manager Application Settings" below.

Ivanti Service Manager Application Settings

Application Settings

Application Database Server:

Application Database Name:

☒ Windows Authentication
☐ SQL Authentication

User Name:

Password:

Connection successful!

You can select either **Windows Authentication** or **SQL Authentication**. (When you configure the reporting feature, you have an opportunity to review and change the authentication method, if necessary, on the **Microsoft SSRS Configuration** page. See "Configuring the Reporting Feature" on page 128.)

- If you select **Windows Authentication**, you can use the Microsoft SSRS service account, the Microsoft IIS app pool identity account, or any other account, but they must have permission to access the application database and the Microsoft SSRS database.
- If you select **SQL Authentication**, you can use a different system account.

We recommend having separate authentication for Microsoft SSRS, the application database, and the Microsoft SSRS database.

Configuring Microsoft SSRS

Microsoft SSRS Configuration Page

1. Enter values into the fields:

Parameter	Description
Report Server Host	The name of the Service and Asset Manager reporting feature server. The default name is the name of the server that you are currently logged into. You cannot change this value.
Microsoft SSRS Instance	The instance of Microsoft SSRS to use for the Reporting feature. Select a value from the drop-down list.

2. (Recommended) Click **Backup** to back up your Microsoft SSRS configuration. (If prompted, enter a password to unlock the backup file, and then click **OK**.) The system displays the **New SSRS Configuration Backup** dialog box with information about the backup.

New SSRS Configuration Backup Dialog Box

New SSRS Configuration Backup

Current SSRS Information

SQL Server Instance: MSSQLSERVER

Report Server Service Account:

Password: *****

Web Service Virtual Directory: ReportServer

Report Manager Virtual Directory: Reports

SQL Server Name: DBSERVER

Database Name: ReportServer

Credential: Service Account

Login:

Password: *****

SMTPServer:

SenderAddress:

Backup Path:

C:\SSRSBackup\20170109125606 **Browse...**

Description:

[Manually] Description of this backup.

OK **Cancel**

3. To change the location of the backup, click **Browse...**, select a new location, and click **OK**.
4. Click **OK** to close the dialog box. The system displays the **Backup Encryption Key** dialog box. (If you do not see this dialog box immediately, the system displays it after you click **Next** at the bottom of the page when you are done with the configuration on this page of the System Configuration Wizard.)
5. Do the following:
 - (Optional) Enter a new file location.
 - Enter a password.
 - Confirm the password.
 - Click **OK**.
6. Select a Microsoft SSRS authentication type:
 - **Windows Authentication:** Shares the Microsoft SSRS instance with multiple applications, including Service and Asset Manager.

- **Custom Authentication:** Does not share the Microsoft SSRS instance with any other applications. The Microsoft SSRS instance is used for Service and Asset Manager only. With custom authentication, you can have a multi-tenant environment.

If you have multiple instances of Microsoft SSRS, choose each instance carefully before choosing the authentication method to use with that instance.

- If you plan to share the same Microsoft SSRS instance with other applications besides the reporting feature, you must use Windows authentication.
- If you plan to create a multiple-tenant environment, you must use custom authentication.
- If you plan to use a dedicated Microsoft SSRS instance only for the reporting feature, you can use either Microsoft SSRS authentication type.

If you select a Microsoft SSRS instance and select **Custom Authentication**, the System Configuration Wizard overwrites the existing Microsoft SSRS configuration.



If the Microsoft SSRS instance that you selected is shared with another application, the Service and Asset Manager installer deletes the configuration for that application. Before proceeding, be sure that the Microsoft SSRS instance is not in use by another application.

7. Enter values into the fields:

Parameter	Description
Service Account	<p>Select the service account to use. This can be the same account that is used for the IIS application pool identity and the Windows service, that you entered on the Application Server Settings page. You can select one of the following:</p> <p>Use built-in account (NOTE: You cannot select this option if you selected Windows Authentication for the Microsoft SSRS authentication type in step 5.)</p> <p>Use another account</p>
Use built-in account	<p>(Only if you selected Use built-in account) Select the built-in account to use. This can be the same account that is used for the IIS application pool identity and the Windows service, that you entered on the Application Server Settings page. You can select one of the following:</p> <p>Local System: This account has the most permissions.</p> <p>Network Service: We recommend that you use this account.</p> <p>Local Service</p>
Account	<p>(Only if you selected Use another account) The name of the service account. Use the format domain/name.</p>
Password	<p>(Only if you selected Use another account) The password associated with the service account.</p>

Parameter	Description
Web Service Virtual Directory	<p>The name of the web service virtual directory. The system automatically fills in this field with the value that you entered in the Web Service Virtual Directory field on the Application Server Settings page. See "Configuring the Application Server Settings" on page 97.</p> <p>The default value for the web service virtual directory is ReportServer + _SSRS_instance_name.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> Accept the default value. Enter a new value. <p>Click Advanced... to configure multiple identities for the reporting feature web service.</p>
Report Manager Virtual Directory	<p>The name of the report manager virtual directory. The default value is Reports + _SSRS_instance_name.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> Accept the default value. Enter a new value. <p>Click Advanced... to configure multiple identities for the report manager.</p>
Database Server	<p>The name of the database server. The system automatically displays the default Microsoft SQL server name.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> Accept the default value. Enter the name of the server of the configuration database in this format: <code>machinename\instance</code>. Browse for a server name by clicking the down arrow and selecting <Browse for more...>. The system displays any Microsoft SQL Server instances in your network. Choose a server and click OK. <p>NOTES:</p> <p>Do not choose localhost unless you are setting up a "Demonstration or Proof-of-Concept Deployment" on page 8.</p> <p>To restore the Microsoft SQL server name if you changed the name previously, open Microsoft SQL Server Management Studio. The system displays the Microsoft SQL server name in the Connect to Server dialog box.</p>

Parameter	Description
Database Name	The name of the reporting database. The default name is ReportServer + \$SSRS instance name .
Credentials	The credentials to use with the reporting feature. Select one of the following: SQL Server Credentials Windows Credentials Service Credentials
User Name	The user name for the credential used with the reporting feature.
Password	The password associated with the credential used with the reporting feature.

8. Click **Test Connection**. The system displays *Connection successful!* if the connection is good.
9. Enter values into the fields:

Parameter	Description
SMTP Server	The server that sends out the reports. The system automatically verifies the SMTP server name that you enter. If the name is not valid, the system displays an error message.
Sender Address	The email address for the account that sends out the reports.

10. Click **Next**. The system displays the **Ivanti Reporting Service Configuration** page. See "Configuring the Reporting Feature" below. (If the system displays the Backup Encryption Key dialog box, see step 5.)

Configuring the Reporting Feature

You configure the reporting feature on the **Reporting Service Configuration** page. See "Reporting Service Configuration Page" below.

Reporting Service Configuration Page

ivanti System Configuration Wizard - Service Manager

1. Configure Application Settings ✓
 2. Service Manager Settings ✓
 3. Application Server Settings ✓
 4. Other Feature Settings ✓
 5. Metrics Server ✓
 6. Microsoft SSRS Configuration ✓
7. Reporting Service Configuration
 8. Discovery Application Server
 9. Discovery Web Server

Reporting Configuration

Configuration Server: SERVER2012-034 Port: 80 ☐ Use SSL

The service account must be able to reach the Application Database with read-only access. Enter a database account.

Account Type: SQL Server Credentials
 User Name: sa
 Password: ••••••••

Application Server(s) list for Reporting Service:

Report server name and credentials are not populated in Configuration database and will be added

OOB Reports (not provisioned yet)

<<Previous

1. Enter values into the fields:

Parameter	Description
Configuration Server	<p>The host name of the configuration server. The default value is the name of the server that you are logged into now.</p> <p>If the host that you are logged into now is <i>not</i> the configuration server, enter the machine name or fully-qualified domain name of your configuration server.</p> <p>If you check Use SSL below, you must enter the fully-qualified domain name of the configuration server.</p>
Port	The port number of the configuration server. The default is 80, or 443 if you check Use SSL .
Use SSL	<p>Check to use SSL for connections to the configuration server.</p> <p>NOTE: We do not recommend enabling SSL on the configuration server until you have fully tested Service and Asset Manager to ensure that it works with SSL. For information on configuring Service and Asset Manager with SSL, see "Optional SSL Configuration" on page 139.</p>

2. Click **Test Connection** to test the connection to the configuration server. The system displays a success or failure message. Click **OK** to close the message.
3. Enter values into the fields:

Parameter	Description
Account Type	<p>The database account type. Select from one of the following:</p> <p>SQL Server Credentials</p> <p>Windows Credentials</p> <p>NOTE: If you selected Custom Authentication in step 6 of "Configuring Microsoft SSRS" on page 124, this option automatically displays as SQL Server Credentials and you cannot change it.</p>
User Name	The user name for the Service and Asset Manager database read-only account.
Password	The password associated with the user name.

4. Click **Test Connection** to test the connection to the configuration server. The system displays *Connection successful!* if the connection is good.
5. Click **Modify** to add servers to or remove servers from the list of Service and Asset Manager application servers that are used with the reporting feature.



If you have multiple domains in your deployment, the reporting server may not be able to connect to the web server. In this case, remove the server from the list and configure reporting manually.

6. Enter values into the fields:

Parameter	Description
Report User Name	(Only if you selected Custom Authentication in step 6 of "Configuring Microsoft SSRS" on page 124) The user name for the user who configures the reporting feature.
Report User Password	(Only if you selected Custom Authentication in step 6 of "Configuring Microsoft SSRS" on page 124) The password associated with the user name.

7. To verify that the configuration settings work, do the following:
 - a. Click **Reprovision Report Now** to update the sample report data to the application. See "Reporting Service Configuration Page" on page 128. If the system returns an exception such as "Cannot Decrypt the Symmetric Key", see "Troubleshooting" on page 225.
 - b. Log into Service and Asset Manager as a Report Manager.
 - c. Ensure that you can see the sample reports and create one.

8. When you see confirmation that the out-of-the-box reports have been provisioned, that is, the last line of this step changes from *OOB Reports (not provisioned yet)* to *OOB Reports (provisioned on date)*, click **Finish** to close the System Configuration Wizard.

The system displays the **Completed** page of the System Configuration Wizard.



If the system displays an error message that the system failed to configure reporting for an Service and Asset Manager application server, ensure that you checked **Use these settings for Reporting Service** on the **Application Server Settings** page.

9. Restart your system (the host server that you just configured).
10. After the system restarts, ensure that you can access Service and Asset Manager. Go to `http://server_name/HEAT` and ensure that the reporting feature is functional.

Configuring Discovery

This topic describes how to configure Discovery.

- "Configuring Discovery on a Dedicated Server" below
- "Configuring Discovery on the Production Servers" on page 133

Configuring Discovery on a Dedicated Server

After you have installed the Discovery components, the System Configuration Wizard automatically starts and displays the **Configuration Application** page.

1. On the **Configuration Application** page, do the following:
 - a. Under **Target Environment**, choose **Single Server Deployment**.
 - b. Under **Setup Connection**, verify that the configuration matches the settings that you configured for the Service and Asset Manager production servers. See "Configuring the Configuration Database" on page 85.
 - c. Click **Next**.
2. On the **Service Manager Application** page, do the following:
 - a. Verify that the configuration matches the settings that you configured for the Service and Asset Manager production servers. See "Configuring the Service and Asset Manager Application" on page 90.
 - b. Check **Discovery Stand alone**.
 - c. Click **Next**.
3. On the **Application Server Settings** page, do the following:

- a. Verify that the configuration matches the settings that you configured for the Service and Asset Manager production servers.
 - b. Click **Next**.
4. On the **Other Features Settings** page, do the following:
 - a. Under **Customize Server**, in the **Discovery Application Server** field, enter the name of the Discovery dedicated server.
 - If you are not using SSL, enter the host name.
 - If you are using SSL, enter the fully-qualified domain name.
 - b. Verify that the rest of the configuration matches the settings that you configured for the Service and Asset Manager production servers. See "Configuring Other Feature Settings" on page 101.
 - c. Click **Next**.
5. On the **Metrics Server** page, do the following:
 - a. Verify that the configuration matches the settings that you configured for the Service and Asset Manager production servers. See "Configuring the Metrics Server" on page 105.
 - b. Click **Next**.
6. On the **Discovery Application Server** page, do the following:
 - a. In the **Discovery Application Server** field, enter the name of the Discovery dedicated server.
 - If you are not using SSL, enter the host name.
 - If you are using SSL, enter the fully-qualified domain name.
 - b. Verify that the rest of the configuration matches the settings that you configured for the Service and Asset Manager production servers. See "Configuring the Discovery Application Server" on page 110.
 - c. Click **Next**.
7. On the **Discovery Web Server** page, do the following:
 - a. In the **Discovery Application Server** field, enter the name of the Discovery dedicated server.
 - If you are not using SSL, enter the host name.
 - If you are using SSL, enter the fully-qualified domain name.

- b. Verify that the rest of the configuration matches the settings that you configured for the Service and Asset Manager production servers. See "Configuring the Discovery Web Server" on page 116.
- c. Click **Finish**.

The system displays the **Completed** page of the System Configuration Wizard.

8. Restart your system (the host server you just configured).
9. After the system restarts, ensure that you can access Service and Asset Manager. Go to `http://server_name/HEAT` and ensure that the system is functional.

Configuring Discovery on the Production Servers

Now that there is a dedicated Discovery server in your deployment, you must configure your production servers to recognize it.

On each production server in your deployment, do the following:

1. Go to the Windows apps menu and click **System Configuration Wizard**. The system opens the System Configuration Wizard and displays the **Configuration Application** page.
2. On the **Configuration Application** page, click **Next**.
3. On the Service and Asset Manager application page, click **Next**.
4. On the **Application Server Settings** page, click **Next**.
5. On the **Other Features Settings** page, do the following:
 - a. In the **Discovery Application Server** field, enter the name of the Discovery dedicated server.
 - If you are not using SSL, enter the host name.
 - If you are using SSL, enter the fully-qualified domain name.
 - b. Click **Next**.
6. On the **Metrics Server** page, click **Next**.
7. On the **Discovery Application Server** page, do the following:
 - a. In the **Discovery Application Server** field, enter the name of the Discovery dedicated server.
 - If you are not using SSL, enter the host name.
 - If you are using SSL, enter the fully-qualified domain name.
 - b. Click **Next**.
8. On the the **Discovery Web Server** page:

- a. In the **Discovery Application Server** field, enter the name of the Discovery dedicated server.
- If you are not using SSL, enter the host name.
- If you are using SSL, enter the fully-qualified domain name.
- b. Click **Finish**.

Configuring the Deployment on the Service and Asset Manager Operations Console

- "Configuring the Service and Asset Manager Operations Console" below
- "Creating the Staging and UAT Instances of the Tenants" on page 137
- "Making Configuration Changes to Tenants" on page 138

Perform these steps from the Operations Console, which you installed in the staging/UAT environment.

This section only contains brief, high-level instructions.



For complete information about using the Operations Console, including how to log in, see the *Operations Console User Guide for Service and Asset Manager*.

Configuring the Service and Asset Manager Operations Console

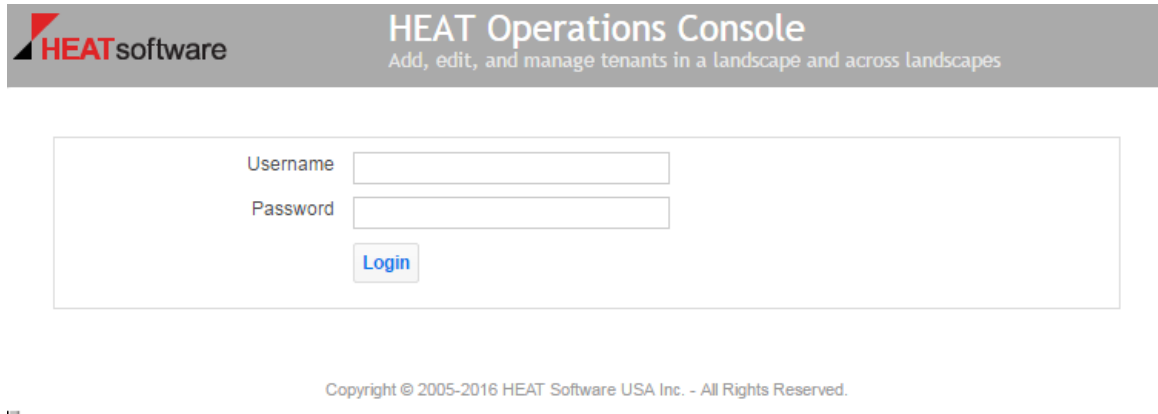
To log into the Operations Consoles, do the following:

1. In the **Start** menu, click the down arrow to see the **Apps** menu, and then click **HEAT Operations Console**.
2. Enter your user name and password and then click **Login**.



The default user name is admin and the default password is manage.

Operations Console Log In Screen



HEAT software

HEAT Operations Console

Add, edit, and manage tenants in a landscape and across landscapes

Username

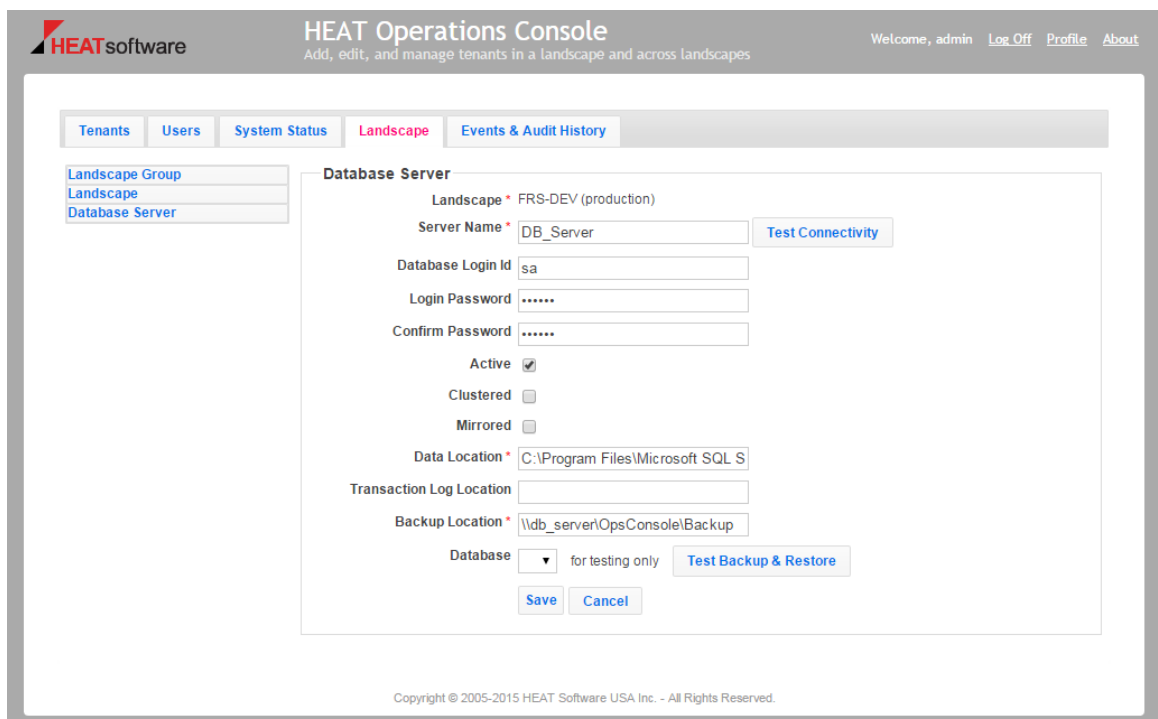
Password

[Login](#)

Copyright © 2005-2016 HEAT Software USA Inc. - All Rights Reserved.

3. Use the Operations Console to update the values for the Service and Asset Manager application database by doing the following:
 - a. Click the **Landscape** tab.
 - b. Click **Database Server** on the left.
 - c. Click **Add Database Server**.
 - d. Enter a database login ID and password and set the data and backup locations. See the example values in "Adding a Database Server" below.

Adding a Database Server



HEAT software

HEAT Operations Console

Add, edit, and manage tenants in a landscape and across landscapes

Welcome, admin [Log Off](#) [Profile](#) [About](#)

[Tenants](#) [Users](#) [System Status](#) [Landscape](#) [Events & Audit History](#)

[Landscape Group](#)
[Landscape](#)
[Database Server](#)

Database Server

Landscape * FRS-DEV (production)

Server Name [Test Connectivity](#)

Database Login Id

Login Password

Confirm Password

Active ☒

Clustered ☐

Mirrored ☐

Data Location *

Transaction Log Location

Backup Location *

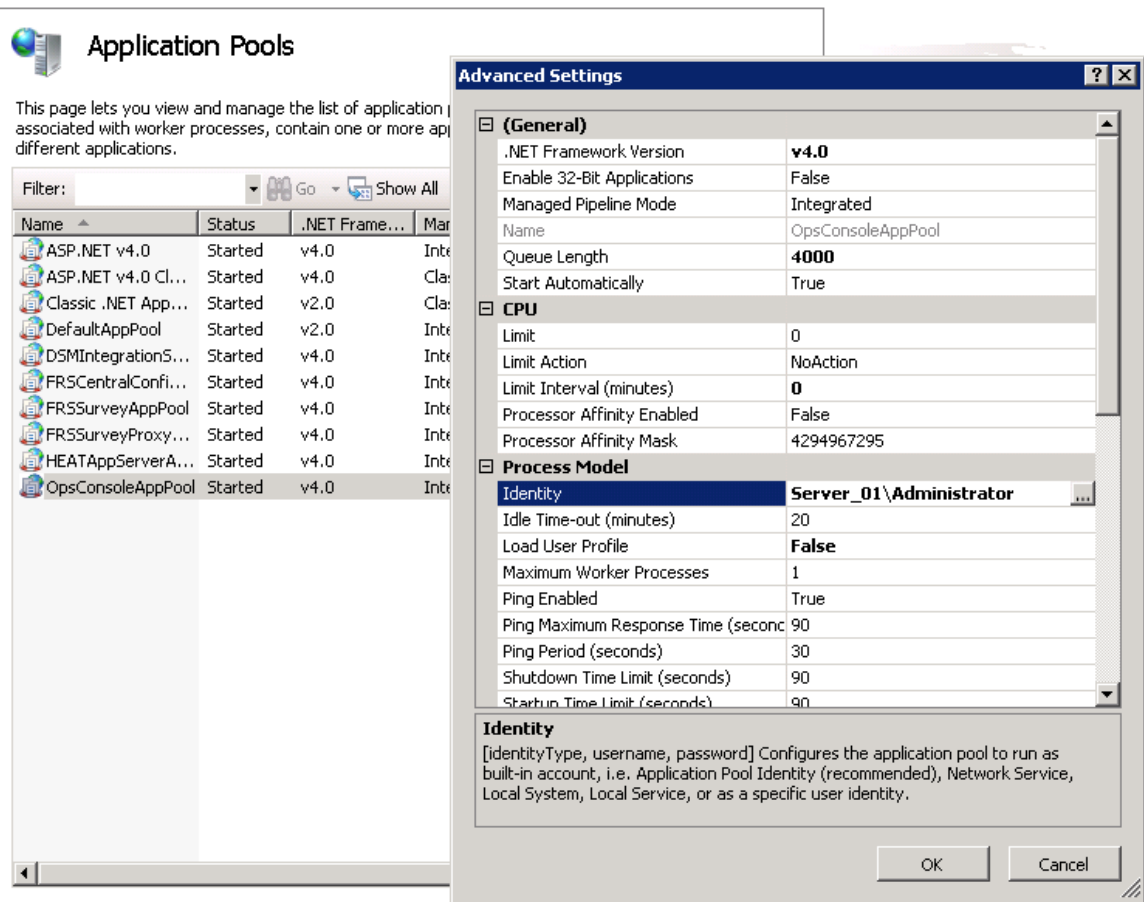
Database [Test Backup & Restore](#)

[Save](#) [Cancel](#)

Copyright © 2005-2015 HEAT Software USA Inc. - All Rights Reserved.

- e. For the data and backup locations, change the application pool identity so that it has read access. See "Changing the Application Pool Identity" on the next page.

Changing the Application Pool Identity



See the *Working with Database Servers* section of the *Operations Console User Guide for Service and Asset Manager* for complete details about editing a database server.

4. Delete the Service and Asset Manager application databases on the staging and UAT instances of the tenant, by doing the following:
 - a. Click the **Tenants** tab.
 - b. Click **Expanded View** to view all the details about the tenants.
 - c. Find the staging instance of the tenant and click **Deactivate**.
 - d. Click **Deactivate** at the confirmation prompt.
 - e. For the staging instance of the tenant, click **Delete**.
 - f. Check **Skip Backup** and click **Delete** at the confirmation prompt.
 - g. Repeat steps c. through f. for the UAT instance of the tenant.

You now have three instances of the configuration database and a production instance of the tenant.

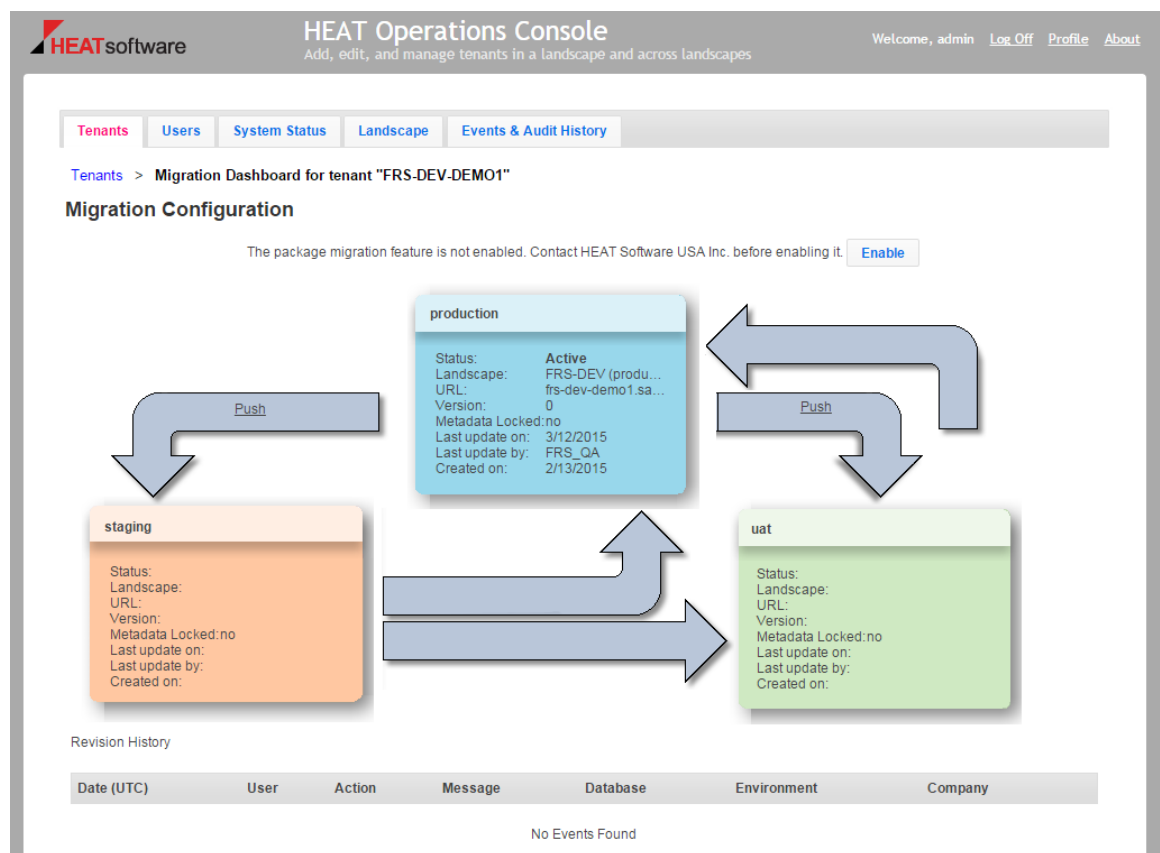
See the *Editing a Tenant* section of the *Operations Console User Guide for Service and Asset Manager* for complete details about deleting tenants and tenant instances.

Creating the Staging and UAT Instances of the Tenants

To create the staging and UAT instances of the tenant, based on the production instance, do the following:

1. Log into the Operations Console.
2. Click the **Tenants** tab.
3. Navigate to the production instance of the tenant and click **Manage Migration**.
4. Create the staging instance of the tenant, by doing the following:
 - a. In the migration dashboard, click **Push** which is located inside the arrow going from the production instance of the tenant to the staging instance of the tenant. See "Creating a Staging Instance of the Tenant" below.

Creating a Staging Instance of the Tenant



The system displays the **Copy Production to Staging** dialog box.

- b. In the **Target DB Option** field, select **From live MSSQL backup**. See "Copy Production Instance of the Tenant to the Staging Instance of the Tenant" on the next page.

Copy Production Instance of the Tenant to the Staging Instance of the Tenant

- c. Click **Execute**.
5. Create the UAT instance of the tenant:
 - a. In the migration dashboard, click **Push** which is located inside the arrow going from the production instance of the tenant to the UAT instance of the tenant. See "Creating a Staging Instance of the Tenant" on the previous page. The system displays the **Copy Production to UAT** dialog box.
 - b. In the **Target DB Option** field, select **From live MSSQL backup**. See "Copy Production Instance of the Tenant to the Staging Instance of the Tenant" above.
 - c. Click **Execute**.

You can now customize Service and Asset Manager and use the Operations Console to push those customizations to the other instances of the tenant.

Making Configuration Changes to Tenants

1. Log into the Operations Console.
2. Click the **Tenants** tab.
3. Make configuration changes in the staging instance of the tenant.

4. Push the configuration changes that you made in the staging instance of the tenant to the UAT instance of the tenant by doing the following:
 - a. Click **Push** which is located inside the arrow going from the staging instance of the tenant to the UAT instance of the tenant. See "Creating a Staging Instance of the Tenant" on page 137. The system displays the **Copy Staging to UAT** dialog box.
 - b. You can use simple mode by leaving **Advanced Mode** unchecked, or you can use advanced mode by checking **Advanced Mode**. If you use advanced mode, select **Copy Configuration** in the **Operation** field and check your options. See "Copy Production Instance of the Tenant to the Staging Instance of the Tenant" on the previous page.
 - c. Click **Execute**.
5. Verify that the configuration changes that you made to the staging instance of the tenant (in step 3) were successfully migrated to the UAT instance of the tenant.
6. Make additional configuration changes in the staging instance of the tenant as needed.
7. After you have finished making configuration changes and have verified them, push the configuration changes from the UAT instance of the tenant to the production instance of the tenant.

Optional SSL Configuration



The Metrics Server is not compatible with SSL if your Service and Asset Manager system has Windows authentication set up.

- "About the SSL Configuration" below
- "Configuring SSL for the Configuration and Application Databases" on the next page
- "Configuring SSL for the Application Database Only" on page 145

About the SSL Configuration



For all fields in the System Configuration Wizard that ask for a server location, when using SSL, you must enter a fully-qualified domain name (FQDN). This is because SSL needs a certificate and the certificate authority requires an FQDN.

You can configure Service and Asset Manager for SSL. This configuration is optional. There are three scenarios:

- The Service and Asset Manager application database and the configuration database both use SSL. See "Configuring SSL for the Configuration and Application Databases" on the next page.

- The Service and Asset Manager application database uses SSL but the configuration database does not use SSL. See "Configuring SSL for the Application Database Only" on page 145.
- Neither the Service and Asset Manager application database nor the configuration database uses SSL. In this scenario, do not check SSL on any of the pages of the System Configuration Wizard.

Configuring SSL for the Configuration and Application Databases

To configure both your Service and Asset Manager application database and the configuration database to use SSL, follow all of the steps in all of these sections:

- "Before You Begin" below
- "Configuring SSL in Microsoft IIS Manager" below
- "Configuring SSL in the System Configuration Wizard" on the next page

Before You Begin

- Ensure that https://localhost:443 displays the Microsoft IIS Manager welcome page.
- Ensure that your system has a valid certificate.

Configuring SSL in Microsoft IIS Manager

1. In Microsoft IIS Manager, navigate to **Sites > Default Web Site** and select **SSL Settings**.
2. On the **SSL Settings** page, check **Require SSL** and under client certificates, select **Ignore**.
3. Navigate to **Sites > HEAT** and select **SSL Settings**.
4. On the **SSL Settings** page, check **Require SSL** and under client certificates, select **Ignore**.
5. Navigate to **Sites > CentralConfig** and select **SSL Settings**.
6. On the **SSL Settings** page, check **Require SSL** and under client certificates, select **Ignore**.
7. Navigate to **Sites > FRSSurveyProxy** and select **SSL Settings**.
8. On the **SSL Settings** page, check **Require SSL** and under client certificates, select **Ignore**.
9. Add an SSL port by doing the following:
 - a. Navigate to **Sites > Default Web Site**, right click, and select **Edit Bindings....**
 - b. Click **Add....**
 - c. In the **Add Site Binding** dialog box, for the **Type** field, select **HTTPS** and in the **SSL certificate** field, select the certificate that you received from the certificate authority. The system automatically enters 443 for the port.
 - d. In the **IP Address** field, enter a fully-qualified domain name.
 - e. Click **OK**.

10. Verify that you can access https://fully_qualified_domain_name.

Configuring SSL in the System Configuration Wizard

1. In the System Configuration Wizard, on the **Configuration Application** page, ensure that the value in the **Configuration Server Domain Name** field uses a fully-qualified domain name. Do not use a machine name.

Configuration Application Page

System Configuration Wizard

1. Configuration Application

2. Service Manager Application

3. Application Server Settings

4. Other Feature Settings

5. Metrics Server

6. Discovery Application Server

7. Discovery Web Server

Configuration Database Name: ConfigDB

☒ Windows Authentication
☐ SQL Authentication

User Name: administrator

Password: Test Connection

Connection successful!

Configuration Database
 Created On: 7/31/2017
 Modified On: 7/31/2017
 System Table Version: 657
 Metadata Package Version: 2016.2.0

Re-Create & Load Configuration DB

Configuration Server Domain Name: **AZ-TP-WIN2012-1.ivanti.com**

License Server: AZ-TP-WIN2012-1 Port: 80 ☐ Use SSL

License File for Production: C:\Users\Administrator\Desktop\USA-Service Browse...

Administrator Account for Ivanti Service Manager Configuration Application

Login ID: HSWAdmin

Password:

Confirm Password:

First Name: HSW

Last Name: Admin

Email Address: HSWAdmin@ivanti.com

Next>>

2. On the bottom of the **Service and Asset Manager Application** page, ensure that you check **Use domain name to access Application** and enter a fully-qualified domain name for the Service and Asset Manager application server. Do not use a machine name.

Service and Asset Manager Application Page

System Configuration Wizard - Service Manager

ivanti System Configuration Wizard - Service Manager

1. Configure Application Settings

2. Service Manager Settings

3. Application Server Settings

4. Other Feature Settings

5. Metrics Server

6. Discovery Application Server

7. Discovery Web Server

Application Database Server: DBSERVER-021

Application Database Name: HEATSM

☐ Windows Authentication

☒ SQL Authentication

User Name: sa

Password: Test Connection

Application Database

Created On: 12/16/2018

Modified On: 12/16/2018

System Table Version: 664

Metadata Package Version: 2018.1.0

☐ Don't include Demo data.

Load Application Database

Application Name: Ivanti Service Manager

Attachment Type: Database

Client Auth Key: efe5c2f77290454f91a561dd03

Import Remote Control License File: Browse...

☐ Use machine name to access application

☒ Use domain name to access application

Application server domain name: SERVER2012-021

Advanced Options

<<Previous

Next>>

3. On the **Application Server Settings** page, do the following:
- Ensure that you enter the fully-qualified domain name in the **Configuration Server Location** field.
 - Check **Use SSL**.
 - Enter the fully-qualified domain name in the **Host Name** field.

Application Server Settings Page.

System Configuration Wizard - Service Manager

ivanti System Configuration Wizard - Service Manager

1. Configure Application Settings ✓
2. Service Manager Settings ✓
3. Application Server Settings
4. Other Feature Settings
5. Upgrade System
6. Metrics Server
7. Discovery Application Server
8. Discovery Web Server

Application Server Settings

Configuration Server Location: DBSERVER-021 Port: 80 ☐ Use SSL **Test Connection**

Host Name: DBSERVER-021

Host (DBSERVER-021) is not detected and will be added to Configuration Database.

Use this host for Operations Console: ☐
Use this host for Survey: ☐
Use these settings for Reporting Service: ☐

Local system account will be used for IIS Application Pool Identity and Windows Service.
Use a different account: ☐

<<Previous Next>>

4. On the **Other Feature Settings** page, for the Service and Asset Manager application server, check **Use SSL**.

Other Feature Settings Page

System Configuration Wizard - Service Manager

ivanti System Configuration Wizard - Service Manager

1. Configure Application Settings ✓
2. Service Manager Settings ✓
3. Application Server Settings ✓
4. Other Feature Settings
5. Upgrade System
6. Metrics Server
7. Discovery Application Server
8. Discovery Web Server

Configuration Settings

Log File Location: C:\Logs
Temp Folder Location: C:\Temp
Cache Location: C:\HEATCache

Customize Server

Application Server: DBSERVER-021 Port: 80 ☐ Use SSL
Message Queue Server: DBSERVER-021 Port: 7200
Integration Service Server: DBSERVER-021 Port: 80 ☐ Use SSL
Discovery Application Server: DBSERVER-021 Port: 8382 ☐ Use SSL

Inbound Web Service Settings

Inbound Web Service Server: DBSERVER-021 Port: 80 ☐ Use SSL
Trusted Host & Remote Host Blocked List:
☒ Restart services after setting configuration files.

<<Previous

5. On the **Metrics Server** page, check **Use SSL**.

Metrics Server Page

System Configuration Wizard

1. Configuration Application
2. Service Manager Application
3. Application Server Settings
4. Other Feature Settings
5. Metrics Server
6. Discovery Application Server
7. Discovery Web Server

Password: **Test Connection**

A Metrics Server Database is detected.
Created On: 8/1/2017
Modified On: 8/1/2017
Re-Create & Load Configuration DB

Configuration Server Location: Port: ☒ Use SSL **Test Connection**

This server is not registered as a Metrics Server. Click Save to register it with Ivanti Service Manager.

Name:
Description:
Server Name:
Use SSL ☐
Enabled ☒ **Save**

Select checkbox which application you want to use this Metrics Server

Application Name	Metrics Server	Map
Ivanti Service Manager	<input type="checkbox"/>	<input type="checkbox"/>

<<Previous **Next>>**

Configuring SSL for the Application Database Only

To configure your Service and Asset Manager application database to use SSL but not the configuration database, follow all of the steps in all three sections:

- "Before You Begin" below
- "Configuring SSL in Microsoft IIS Manager" below
- "Configuring SSL in the System Configuration Wizard" on the next page

Before You Begin

- Ensure that `https://localhost:443` displays the Microsoft IIS Manager welcome page.
- Ensure that your system has a valid certificate.

Configuring SSL in Microsoft IIS Manager

1. In Microsoft IIS Manager, navigate to **Sites > Default Web Site** and select **SSL Settings**
2. On the **SSL Settings** page, ensure that **Require SSL** is not checked. Under client certificates, select **Ignore**.

3. Navigate to **Sites > HEAT** and select **SSL Settings**.
4. On the **SSL Settings** page, check **Require SSL** and under client certificates, select **Ignore**.
5. Navigate to **Sites > CentralConfig** and select **SSL Settings**.
6. On the **SSL Settings** page, ensure that **Require SSL** is not checked. Under client certificates, select **Ignore**.
7. Navigate to **Sites > FRSSurveyProxy** and select **SSL Settings**.
8. On the **SSL Settings** page, check **Require SSL** and under client certificates, select **Ignore**.
9. Add an **SSL** port by doing the following:
 - a. Navigate to **Sites > Default Web Site**, right click, and select **Edit Bindings....**
 - b. Click **Add...**
 - c. In the **Add Site Binding** dialog box, for the **Type** field, select **HTTPS** and in the **SSL certificate** field, select the certificate that you received from the certificate authority. The system automatically enters 443 for the port.
 - d. In the SSL certificate field, enter a fully-qualified domain name.
 - e. Click **OK**.
10. Verify that you can access `https://local_host`.

Configuring SSL in the System Configuration Wizard

1. In the System Configuration Wizard, on the **Service and Asset Manager Application** page, ensure that the Service and Asset Manager application database uses a fully-qualified domain name and not a machine name.

Service and Asset Manager Application Page

System Configuration Wizard - Service Manager

ivanti System Configuration Wizard - Service Manager

1. Configure Application Settings

2. Service Manager Settings

3. Application Server Settings

4. Other Feature Settings

5. Metrics Server

6. Discovery Application Server

7. Discovery Web Server

Application Database Server: DBSERVER-021

Application Database Name: HEATSM

☐ Windows Authentication

☒ SQL Authentication

User Name: sa

Password: •••••••• **Test Connection**

Application Database

Created On: 12/16/2018

Modified On: 12/16/2018

System Table Version: 664

Metadata Package Version: 2018.1.0

☐ Don't include Demo data.

Load Application Database

Application Name: Ivanti Service Manager

Attachment Type: Database

Client Auth Key: efe5c2f77290454f91a561dd03

Import Remote Control License File: **Browse...**

☐ Use machine name to access application

☒ Use domain name to access application

Application server domain name: SERVER2012-021

Advanced Options

<<Previous **Next>>**

2. On the **Application Server Settings** page, do the following:
 - Ensure that **Use SSL** is not checked.
 - Ensure that you enter the fully-qualified domain name in the **Configuration Server Location** field.
 - Ensure that you enter the host name, and not the fully-qualified domain name, in the **Host Name** field.

Application Server Settings Page

System Configuration Wizard - Service Manager

ivanti System Configuration Wizard - Service Manager

1. Configure Application Settings ✓

2. Service Manager Settings ✓

3. Application Server Settings

4. Other Feature Settings

5. Upgrade System

6. Metrics Server

7. Discovery Application Server

8. Discovery Web Server

Application Server Settings

Configuration Server Location: DBSERVER-021 Port: 80 ☐ Use SSL **Test Connection**

Host Name: DBSERVER-021

Host (DBSERVER-021) is not detected and will be added to Configuration Database.

Use this host for Operations Console: ☐

Use this host for Survey: ☐

Use these settings for Reporting Service: ☐

Local system account will be used for IIS Application Pool Identity and Windows Service.

Use a different account: ☐

<<Previous Next>>

3. On the **Other Feature Settings** page, check **Use SSL**.



This is the *only* place in the System Configuration Wizard where you check **Use SSL**. Do *not* check **Use SSL** on any other page.

Other Feature Settings Page

System Configuration Wizard - Service Manager

ivanti System Configuration Wizard - Service Manager

1. Configure Application Settings ✓
 2. Service Manager Settings ✓
 3. Application Server Settings ✓
 4. Other Feature Settings
 5. Upgrade System
 6. Metrics Server
 7. Discovery Application Server
 8. Discovery Web Server

Configuration Settings

Log File Location: C:\Logs Browse...
 Temp Folder Location: C:\Temp Browse...
 Cache Location: C:\HEATCache Browse...

Customize Server

Application Server: DBSERVER-021 Port: 80 ☐ Use SSL
 Message Queue Server: DBSERVER-021 Port: 7200
 Integration Service Server: DBSERVER-021 Port: 80 ☐ Use SSL
 Discovery Application Server: DBSERVER-021 Port: 8382 ☐ Use SSL

Inbound Web Service Settings

Inbound Web Service Server: DBSERVER-021 Port: 80 ☐ Use SSL
 Trusted Host & Remote Host Blocked List: Set
☒ Restart services after setting configuration files.

<<Previous Next>>

Optional LDAP Configuration

Service and Asset Manager supports LDAP. LDAP is configured from the Configuration Console.

After installation, go to the online help and view the topic called *Configuring LDAP Settings*.

About Configuring with ADFS

Service and Asset Manager supports ADFS. ADFS is configured from the Configuration Console.

After installing the system, go to the online help and view the topic called *Working with ADFS/SAML*.

About Configuring Throttling Settings

- "About Throttling" on the next page
- "Checking the Throttling Status" on the next page
- "Configuring Outbound Throttling Settings" on the next page

About Throttling

In Service and Asset Manager, throttling is when the system intentionally slows the speed of web services. We use this process to regulate the network traffic and to minimize bandwidth congestion. When using web services, Service and Asset Manager may limit the message rate, based on overall load. If you exceed the rate of 100,000 API calls per day, you may find your responses slowed to an appropriate rate. This helps ensure that you get a fair share of resources, and Ivanti Software can prevent unintended performance degradation from runaway integrations and denial of service attempts.

For more information about using the Service and Asset Manager integration web services, go to the online help and view the topic called *Working with the Integration Web Service*.

Checking the Throttling Status

Configuring Outbound Throttling Settings

In on-premise implementations, your web service use only affects your environment. If you exceed the recommended rate, you may see performance implications. You can adjust your outbound throttling thresholds to maximize performance. The hardware capacity of your system also affects the values that you set these parameters to.

The following are the outbound throttling parameters:

Parameter	Description
ResetRuntimeCacheExpectedTimeout	The amount of time, in ms, that the system allocates to reset the runtime cache operation. If it takes longer than this, the system moves the operation to the pending actions and marks the server as unhealthy.
ResetRuntimeCacheUnhealthyDelayTime	If the server is considered unhealthy, this is the amount of time, in ms, to delay things. After this amount of time has passed, the system executes the action.
PendingActionCleanupPeriod	How often, in ms, to clean up the pending actions that are stored in memory.
PendingActionsThreshold	The amount of memory, in bytes, used to store all of the pending actions. Whenever a pending action exceeds the timeout value, the system adds the action to the pending action collection in memory.
ThrottlingEnable	Turns on or off outbound throttling.

Change the throttling parameters as follows:

1. Navigate to the AppServer folder and open the web.config file using a text editor such as Notepad.
2. Search for and find the following strings:

```
<!--Expected timeout on executing reset runtime cache action
during throttling (value in milliseconds)-->
<add key="ResetRuntimeCacheExpectedTimeout" value="1000" />

<!--Expected delaying on executing reset runtime cache before
executing action in during throttling (value in milliseconds)-->
<add key="ResetRuntimeCacheUnhealthyDelayTime" value="5000" />

<!--Expected period to clean up the pending actions (value
in milliseconds)-->
<add key="PendingActionCleanupPeriod" value="300000" />

<!--Expected size threshold of pending actions collection -->
<add key="PendingActionsThreshold" value="15728640" />

<add key="ThrottlingEnable" value="true" />
```

3. Change the values as needed.
4. Save the file.
5. Perform a Microsoft IIS reset.

Setting up Redis

You will have to setup Redis if you want to use the Chat service in Neurons for ITSM. All the different setup scenarios are explained below.



If you have installed Redis but not using the Chat service, you might consider uninstalling it. To uninstall refer to the section [Uninstall Redis](#).

Different install and uninstall options and scenarios

- Upgrading/Installing Redis for existing/New customer:
 - [Installing Redis in Linux Container on Windows](#)
 - [Installing Linux container on Windows Server with Docker](#)
 - [Installing Redis 6.2.5 in Docker](#)
 - [Installing Redis on Linux Machine](#)
 - [Installing Redis on Linux Machine \(Ubuntu\)](#)
 - [Establish the remote Redis Connection](#)
- [Uninstalling Redis from Windows Server \(existing customer\)](#)
 - [Remote Redis Connection - using redis.bat script](#)
 - [Remote Redis Connection from Windows UI](#)
 - [Remote Redis Connection using redis-server.exe](#)
- [Uninstalling from Linux Container](#)
- [Uninstall from Linux Machine](#)

Option 1 - Install Redis in Linux Container on Windows Server

Prerequisite:

- Windows server - version 2019 or above with Hyper – V enabled.

For more information on Linux Container requirements check out <https://docs.microsoft.com/enus/virtualization/requirements>

For upgrading your Windows Servers, check out the following links:

- Upgrade from Windows Server 2012r2 - <https://docs.microsoft.com/en-us/windows-server/upgrade/upgrade-2012r2-to-2019>
- Upgrade from Windows Server 2016 - <https://docs.microsoft.com/en-us/windows-server/upgrade/upgrade-2016-to-2019>

Installation steps:

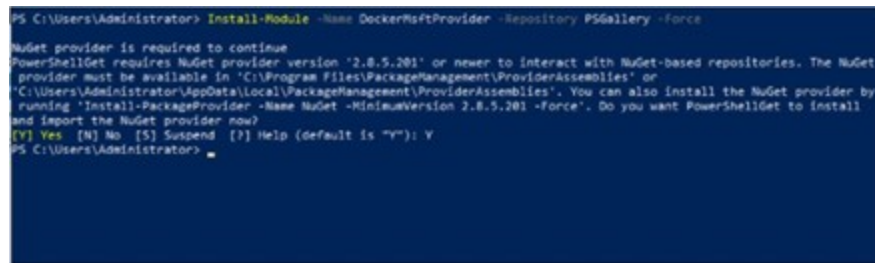
Installing Linux container with docker on Windows Server

1. Open PowerShell as Administrator and run the following command:

```
Install-Module -Name DockerMsftProvider -Repository PSGallery -Force
```

This will install Docker-Microsoft PackageManagement provider.

Sample Output



```
PS C:\Users\Administrator> Install-Module -Name DockerMsftProvider -Repository PSGallery -Force
NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\Administrator\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
PS C:\Users\Administrator>
```

2. Install the preview build of Docker EE using the following commands:

```
Install-Module DockerProvider
Install-Package Docker -ProviderName DockerProvider -
RequiredVersion preview
```

3. Agree to installing using "Yes" or "Y" or "A" to Agree to all.
4. When the installation is complete, reboot the system.
5. Enable LinuxKit system for running Linux containers using the following :

```
[Environment]::SetEnvironmentVariable("LCOW_SUPPORTED", "1", "Machine")
```

6. Restart the system/Docker service after the change using the following command:

```
Restart-Service docker
```

Linux Container should now successful run on your Windows Server.

For more information, refer - [How to run Docker Containers on Windows Server 2019](#)

Installing Redis 6.2.5 in Docker

1. Open PowerShell as Administrator and run the following command:

```
docker run -d -p 6379:6379 --name redis-con redis:6.2.5
```

2. Check if it has successfully installed by executing the command - `docker ps`

Best Practices

- Run the command - `docker update --restart always redis-con` to always restart Redis Container whenever the docker/machine is restarted. If this is not enabled you have to enable Redis container manually everytime the docker/machine is restarted.
- Enable Authentication for Redis. Refer, Add Authentication to Redis.

Setting up Redis Authentication

Add Auth to Redis server

1. Open Powershell and run the command - `docker exec -it redis-con sh`.
This will give you Redis console.
2. Run **Redis-cli** to set password to Redis server.
3. Run this command to set Redis password - `redis-cli Config Set requirepass <your-password>`.
Your password is successfully set now.
4. To test run the command - `redis-cli Auth <your-password>` it should return "Ok."

Set the password through SCW for the application to authenticate through Redis password.

- In step 2 of SCW configuration (Service and Asset Manager settings) in the field **Redis Auth Password**, enter the same password that is set in the **redis-cli**, and save it.



Once docker/Redis server/machine is restarted , the auth will be set back to noAuth, ensure to remember and update the password to redis server every time restarted.

ivanti System Configuration Wizard - Service and Asset Manager

1. Configure Application Settings

2. Service and Asset Manager Settings

3. Application Server Settings

4. Other Feature Settings

5. Upgrade System

6. Metrics Server

7. Discovery Application Server

8. Discovery Web Server

Application Settings

Application Database Server: localhost

Application Database Name: HEATSM

☐ Windows Authentication

☒ SQL Authentication

User Name: sa

Password: **Test Connection**

Application Database

Created On: 5/13/2021

Modified On: 9/27/2021

System Table Version: 678

Metadata Package Version: 2021.2.0

☐ Don't include Demo data.

Load Application Database

Application Name: SAAM

Attachment Type: Database

Client Auth Key: d788204cd0484939832059f2f

Redis Auth Password:

Import Remote Control License File: **Browse...**

☒ Use machine name to access application

☐ Use domain name to access application

<<Previous **Next>>**

Option 2 - Install Redis on Linux Machine

Prerequisite:

- Ubuntu 16.04 or above

Steps to install:

1. Execute the following commands:
 - `Sudo apt update`
 - `Sudo apt install redis-server`
2. Check if Redis is set up using the following command:
 - `sudo systemctl status redis`

If the result displays as `Active: active (running)` then Redis is successfully setup.

```

santosh@santosh-Virtual-Machine:~$ sudo systemctl status redis
● redis-server.service - Advanced key-value store
   Loaded: loaded (/lib/systemd/system/redis-server.service; enabled; vendor pre
   Active: active (running) since Mon 2021-12-06 12:59:52 GMT; 17min ago
     Docs: http://redis.io/documentation,
           man:redis-server(1)
   Process: 4763 ExecStopPost=/bin/run-parts --verbose /etc/redis/redis-server.po
   Process: 4758 ExecStop=/bin/kill -s TERM $MAINPID (code=exited, status=0/SUCCE
   Process: 4756 ExecStop=/bin/run-parts --verbose /etc/redis/redis-server.pre-do
   Process: 4776 ExecStartPost=/bin/run-parts --verbose /etc/redis/redis-server.p
   Process: 4773 ExecStart=/usr/bin/redis-server /etc/redis/redis.conf (code=exit
   Process: 4768 ExecStartPre=/bin/run-parts --verbose /etc/redis/redis-server.pr
   Main PID: 4775 (redis-server)
   CGroup: /system.slice/redis-server.service
           └─4775 /usr/bin/redis-server *:6379

Dec 06 12:59:52 santosh-Virtual-Machine systemd[1]: Starting Advanced key-value
Dec 06 12:59:52 santosh-Virtual-Machine run-parts[4768]: run-parts: executing /e
Dec 06 12:59:52 santosh-Virtual-Machine run-parts[4776]: run-parts: executing /e
Dec 06 12:59:52 santosh-Virtual-Machine systemd[1]: Started Advanced key-value s
lines 1-19/19 (END)

```

3. Edit the **redis.conf** file to make Redis port available to other servers (by default, the Redis port is on :6379) "*sudo gedit /etc/redis/redis.conf*" or "*sudo nano /etc/redis/redis.conf*"
4. Check for the line "**bind 127.0.0.1**" comment this line by prepending '#'
Since you have removed binding, it is highly recommended to add authentication to Redis Server.
5. Edit **redis.conf** "*sudo gedit /etc/redis/redis.conf*"
6. Search for requirepass foobared, replace foobared with your_password.
7. Restart the Redis Server to apply changes.
"*sudo systemctl restart redis.service*"
8. Then follow "Remote Redis Connection" and "Set password through SCW for the application to authenticate through Redis password"

Establish the remote Redis Connection

1. Edit the **.env** file in the path "<install-Path>\Heat\Appserver\chat\.env"
2. Edit the attribute **REDIS_HOST=localhost** to **REDIS_HOST=<remote-server-ip>**
3. Save the file.
4. This will install redis successfully.
5. Check if Redis is up by using the command *sudo systemctl status redis* - you should see the active (running status)

Uninstall Redis for Windows Server (Existing Customer)

This is a mandatory step for existing customers who have already installed Redis and are upgrading to the new version. Uninstall the obsolete Redis version from your machine by following the below server details and uninstall steps.

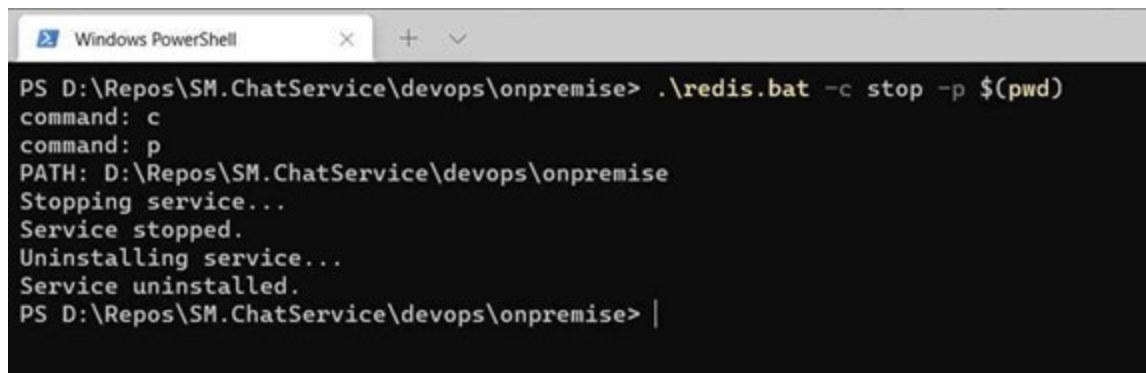
Redis server details:

Version	3.0.503
Path	<install_path>\HEAT\Appserver\AppServer.Main\redis
Project	https://github.com/microsoftarchive/redis
License	https://raw.githubusercontent.com/microsoftarchive/redis/3.0/license.txt

Option 1 - Uninstall using redis.bat script

1. Run the following in Powershell with administrator privileges.

```
cd <install_path>\HEAT\Appserver\AppServer.Main\redis; .\redis.bat -p $(pwd) -c stop
```



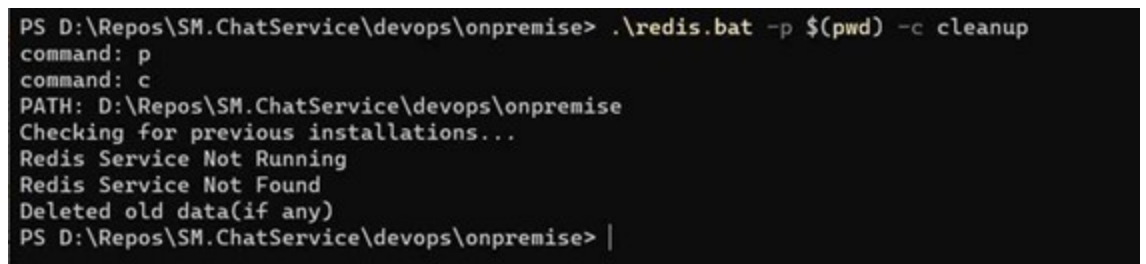
```

Windows PowerShell
PS D:\Repos\SM.ChatService\devops\onpremise> .\redis.bat -c stop -p $(pwd)
command: c
command: p
PATH: D:\Repos\SM.ChatService\devops\onpremise
Stopping service...
Service stopped.
Uninstalling service...
Service uninstalled.
PS D:\Repos\SM.ChatService\devops\onpremise> |

```

2. Optional Step: Cleanup Redis installation files by using the below command:

```
.\redis.bat -p $(pwd) -c cleanup
```



```

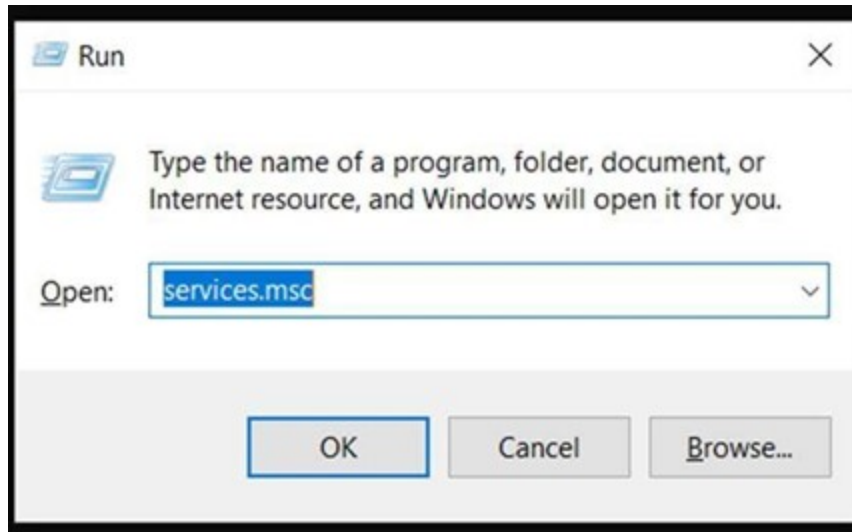
PS D:\Repos\SM.ChatService\devops\onpremise> .\redis.bat -p $(pwd) -c cleanup
command: p
command: c
PATH: D:\Repos\SM.ChatService\devops\onpremise
Checking for previous installations...
Redis Service Not Running
Redis Service Not Found
Deleted old data(if any)
PS D:\Repos\SM.ChatService\devops\onpremise> |

```

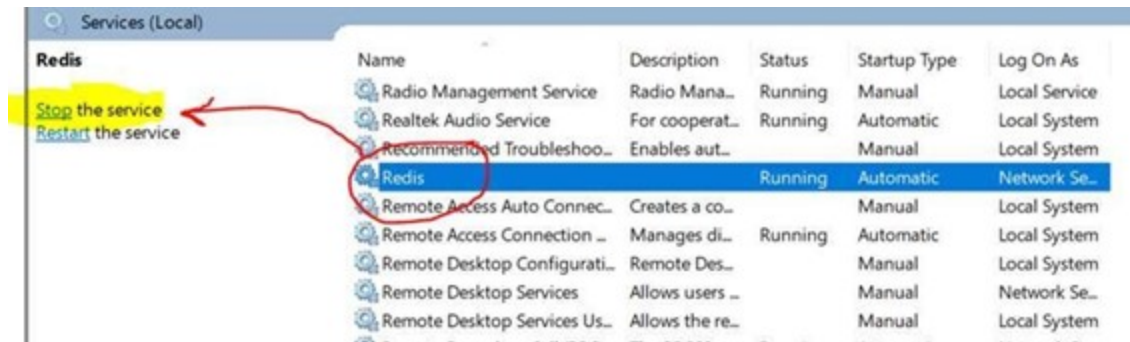
Option 2 - Uninstall from Windows UI

1. Run the following in Powershell with administrator privileges:

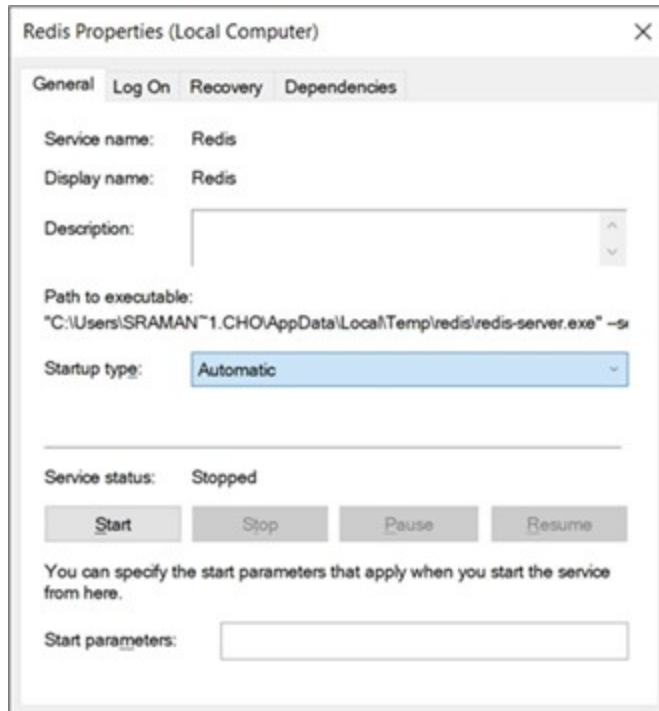
```
Run services.msc
```



2. Locate Redis in the list and stop the service.



3. Right click > **Properties**, Change **Startup type** to **Disabled**.



Option 3 - Uninstall using redis-server.exe

Stop the service

- Run the following in Powershell with administrator privileges.

```
.\redis-server.exe --service-stop
PS D:\Repos\SM.ChatService\devops\onpremise\redis> .\redis-server.exe --service-stop
[16956] 15 Sep 16:49:03.174 # Redis service successfully stopped.
PS D:\Repos\SM.ChatService\devops\onpremise\redis> |
```

Uninstall service

- Run the following in Powershell with administrator privileges.

```
.\redis-server.exe --service-uninstall redis.windows.conf
```

Uninstall Redis

If you do not want to use the Chat service, you may uninstall Redis by the following the below steps:

Option 1 - Uninstall Redis in container

- Execute the following command:

```
Docker rm /redis-con
```

Option 2 - Uninstall Redis in Linux Machine

For ubuntu distributions

```
# if you use apt-get to install redis then use
sudo apt-get purge --auto-remove redis-server
# if you compiled redis manually then follow the
# steps below to remove it completely from linux/ubuntu
sudo service redis_version stop
# Now delete everything related to Redis server from /usr/local/bin/
sudo rm /usr/local/bin/redis-*
# Now delete Redis Configuration files directory and it's content.
sudo rm -r /etc/redis/
# Delete existing Redis log files.
sudo rm /var/log/redis_*
# Delete existing Redis data directory and it's content.
sudo rm -r /var/lib/redis/
# Delete existing Redis server init scripts
sudo rm /etc/init.d/redis_*
# Remove existing Redis PID files (Only if exists)
sudo rm /var/run/redis_*
```

Logging into Service and Asset Manager

- "Logging In Using the Standard Login Dialog Box" below
- "Logging In Using the Standard Login Dialog Box with an Application Menu" on the next page
- "Adding the Application Menu Option to the Standard Login Dialog Box" on the next page

Logging In Using the Standard Login Dialog Box

The standard login dialog box enables you to access Service and Asset Manager on the host that you are logged into now. You see this dialog box when you click the any of the following:

- The Service and Asset Manager desktop shortcut
- The Windows apps menu shortcut

In the dialog box, enter your user name and password, and then click **Login**.

Standard Login Dialog Box

Ivanti. Copyright © 2005-2017 Ivanti. All rights reserved. [Privacy Policy](#) - [Legal Terms and Notices](#)'." data-bbox="245 531 830 664"/>

The default user name for Service and Asset Manager is HEATAdmin. You created the password when you configured the application database. See "Configuring the Service and Asset Manager Application" on page 90.

Logging In Using the Standard Login Dialog Box with an Application Menu

This login dialog box enables you to access the following:

- The Service and Asset Manager system on the host that you are logged into now.
- Individual tenants, such as staging or UAT, if you have more than one.
- The configuration database (ConfigDB).

In the dialog box, enter your user name and password, select an application, and click **Login**.



The default user name for the configuration database (ConfigDB) is HSWAdmin. You chose the password when you created the database. See "Configuring the Configuration Database" on page 85.

The default user name for Service and Asset Manager is HEATAdmin. You chose the password when you created the application database. See "Configuring the Service and Asset Manager Application" on page 90.

Adding the Application Menu Option to the Standard Login Dialog Box

To see the login dialog box with the application menu option (only for server-side login), do the following:

1. Go to C:\Program Files\HEAT Software\HEAT\AppServer\.
2. Right-click the HEAT.url file, and choose **Properties**.
3. Change the host name and port number to **localhost**. For example, change http://SERVER2012:80/HEAT to http://localhost/HEAT.
4. Click **OK**.
5. Open a directory window or a browser window and enter either **localhost/HEAT** or **http://localhost/HEAT**.

Adding Features and Changing Settings

- "Adding and Deleting Features" below
- "Changing Feature Settings by Running the System Configuration Wizard" on the next page

Adding and Deleting Features

Adding features to or deleting features from an existing Service and Asset Manager system is much easier than upgrading the system.

If you have an "Enterprise Production Deployment" on page 13, your action might apply to just one, some, or all of the servers, depending on the features that you are adding or deleting.



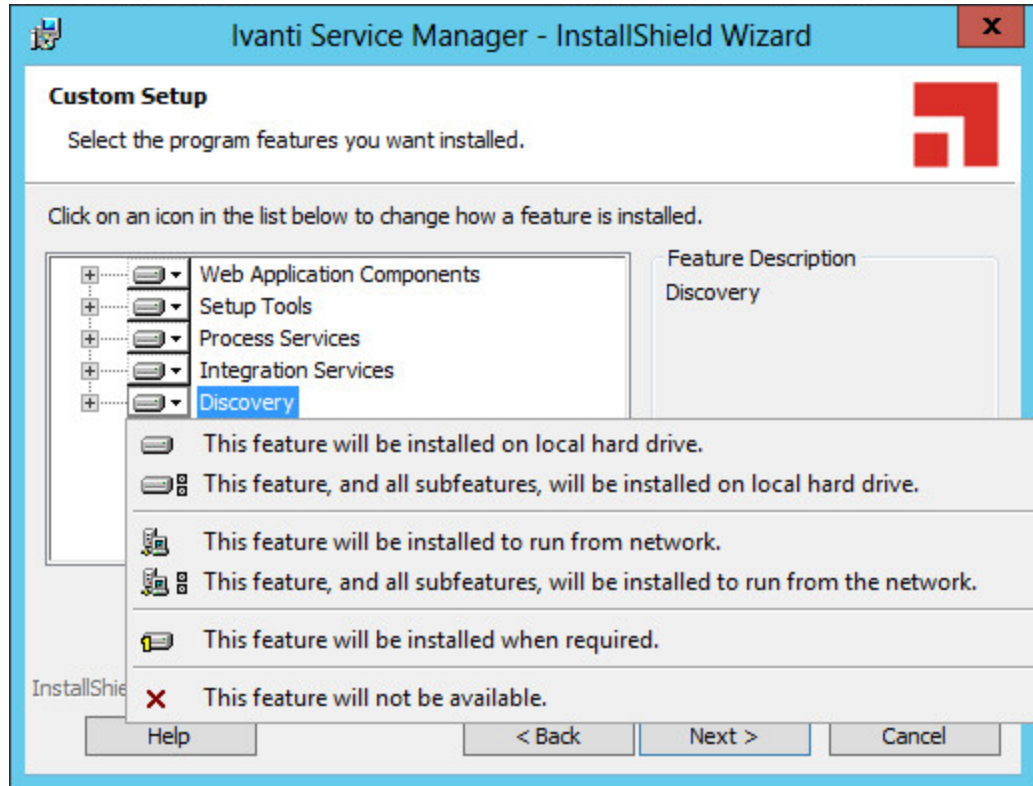
To add servers to your deployment, follow the instructions under "Installing the Service and Asset Manager System" on page 58

To add features or delete features, do the following:

1. Access the installation folder on the Ivanti Software product CD or zip file and run IvantiServiceManager.exe. Right-click and select **Run as Administrator** to ensure proper installation.

The installer checks for the prerequisite software components. If any of those components is not installed, the system prompts you to install them now.
2. Select **Install** at prompt. Installation of the prerequisite software can take several minutes.
3. If you are prompted to restart the system, select **Yes**. The system displays the **Welcome** dialog box.
4. Click **Next**. The system displays the **Program Maintenance** dialog box.
5. Choose **Modify** and click **Next**. The system displays the **Custom Setup** dialog box.

Custom Setup Dialog Box



6. Click the down arrow on each feature and make your selection.



Adding features requires more hard-drive space. If there is not enough space on your hard drive, the installer displays a message.

7. Click **Next** and then click **Install**.

The Service and Asset Manager installation begins. The system displays a status dialog box showing the installation progress of each component over the next few minutes.

8. If you cancel the installation at any time, click **Finish** to close the installer.

When the components are installed, the system automatically launches the System Configuration Wizard.

9. Go to "Configuring Service and Asset Manager " on page 84 for instructions about using the System Configuration Wizard.

Changing Feature Settings by Running the System Configuration Wizard

To change settings without adding or deleting features, you do not need the Ivanti Software product CD or zip file.

1. In the **Start** menu, click the down arrow to see the **Apps** menu, and then click **System Configuration Wizard**.



You must click **Run as administrator** when you start the System Configuration Wizard manually.

2. Go to "Configuring Service and Asset Manager " on page 84 for instructions about using the System Configuration Wizard.

Upgrading Service and Asset Manager from an Earlier Release

- "About Upgrading" below
- "About Upgrading from Earlier Releases" on the next page
- "Upgrading from Ivanti Service Management Release 2017.3.x" on page 169
- "Upgrading from Ivanti Service Management Release 2014.3 or Earlier" on page 172
- [Upgrading from Ivanti Service Manager 2020.1 to 2020.2](#)

About Upgrading

Landscapes

During an Service and Asset Manager upgrade, you can upgrade the development (staging) or testing (UAT) landscapes and test them without affecting the production landscape. After you have verified that the development (staging) or testing (UAT) landscape upgrade was successful, go ahead with production landscape upgrade.

Reporting Feature

You must upgrade both Service and Asset Manager and the reporting feature at the same time. The versions of the software for both Service and Asset Manager and the reporting feature must be the same.

Licenses

Versions of Ivanti Service Management before Release 2015.1 used a different licensing structure. When you upgrade to Service and Asset Manager Release 2021.4, the system automatically uses the licenses that you used in the previous release.

In the System Configuration Wizard, on the **Configuration Application** page, there are fields to enter the license files. The system populates these fields automatically based on your previous license file. See "Configuring the Configuration Database" on page 85.

DSM Integration

If your Service and Asset Manager deployment includes a DSM integration, you must configure and verify your DSM integration for the new release.



Although there is a DSM integration service component in the Service and Asset Manager installer, it is only used for DSM integrations prior to Ivanti Service Management Release 2015.2.

For DSM integrations after Ivanti Service Management Release 2015.2, you must use the package from the Ivanti App Store.

After you have upgraded Service and Asset Manager, access the Ivanti Software App Store and the DSM integration by doing the following:

1. Log into <https://support.heatsoftware.com/>.
2. Go to the Ivanti Software App Store by selecting **App Store** from the top menu.
3. From within the Ivanti Software App Store, open the DSM integration package.
4. Download the DSM integration package for Release 2019.1 and the accompanying instructions.
5. Follow the instructions to configure and verify your DSM integration.

For more information about DSM, see *Working with DSM* in the online help.

About Upgrading from Earlier Releases



- The upgrade to the N version of Ivanti Service and Asset Manager should be always performed from N-1 version. For example, upgrade of on-premise version 2018.1.1 to 2019.1.0 should be done only after the upgrade path of 2018.3.1. Skipping of any of the released version of the application during an upgrade might fail the application upgrade or the application might stop working post the upgrade.
- 2019.2 is a cloud-only release and has no updates for on-premise customers.
- The system upgrade log file name under `c:\Logs\ReleaseTool` will be `"ApplyPatchConfigDB2019.3.1.log"` for config database which is expected for 2020.1 release.

To upgrade to Service and Asset Manager Release 2021.4, you must upgrade your system to every Service Management release between your currently installed release and Service and Asset Manager Release 2020.3 in sequential order. See the table below.

Upgrade From Release	Uninstall	Install Release
2013.1.x	The current Ivanti Service Management version and the Inventory Management component, if present. See "Uninstalling the Inventory Management Component" on page 172.	2013.2.2
2013.2.x		2014.1.1
2014.1.x		2014.2.1
2014.2.x		2014.3.1
2014.3.x		2015.1
2015.1.x	Nothing.	2015.2
2015.2.x		2016.1
2016.1.x		2016.2
2016.2.x		2017.2
2017.2.x		2017.3.x
2017.3.x		2018.1.x
2018.1.x		2018.3.x
2018.3.x		2019.1.x
2019.1.x		2019.3.x
2019.3.x		2020.1.x
2020.1.x	Important steps to be performed. Click here to view the steps.	2020.2.x
2020.2.x	Nothing	2020.3.x
2020.3.x		2020.4.x
2020.4x		2021.1x
2021.1x		2021.2x
2021.2x		2021.3x
2021.3x		2021.4x

For example, if you are currently on Ivanti Service Management Release 2014.1.x and you want to upgrade to Ivanti Service Management Release 2018.3, you must do the following:

1. Uninstall Ivanti Service Management Release 2014.1.x and the Inventory Management component, if present. See "Uninstalling the Inventory Management Component" on page 172.
2. Install Ivanti Service Management Release 2014.2.x.
3. Uninstall Ivanti Service Management Release 2014.2.x.
4. Install Ivanti Service Management Release 2014.3.x.
5. Uninstall Ivanti Service Management Release 2014.3.x.

6. Install Ivanti Service Management Release 2015.1.x.
7. Install Ivanti Service Management Release 2015.2.x.
8. Install Ivanti Service Management Release 2016.1.x.
9. Install Ivanti Service Management Release 2016.2.x.
10. Install Ivanti Service Manager Release 2017.3.1
11. Install Ivanti Service Manager Release 2018.1.x
12. Install Ivanti Service Manager Release 2018.3.x
13. Install Ivanti Service Manager Release 2019.1.x
14. Install Ivanti Service Manager Release 2019.3.x
15. Install Ivanti Service Manager Release 2020.1.x
16. Install Ivanti Service Manager Release 2020.2.x - Important steps to be performed. [Click here](#) to view the steps.
17. Install Ivanti Service Manager Release 2020.3.x
18. Install IvantiService Manager 2020.4.x

Upgrading from Ivanti Service Management Release 2017.3.x

If you are upgrading to Service and Asset Manager Version 2018.3, you must first upgrade to Service and Asset Manager Version 2018.1.1. You do not have to uninstall Ivanti Service Management Release 2017.3.x.

If you have a multiple server environment, you must shut off the notifications to the web servers before you upgrade the system. This is because when you make metadata changes as part of the upgrade, the system tries to synchronize them, but because the versions are different, the system hangs or takes a lot of time. See step 2 below.

Perform these steps on the system that hosts the Service and Asset Manager components:

1. Back up the following items:
 - Service and Asset Manager Configuration Database (ConfigDB)
 - Service and Asset Manager Application Database
 - Attachment folder (if used)
2. (Optional, if your system uses multiple servers) Deactivate the web servers by doing the following:
 - a. Log into the Configuration Database. See the *Configuration Database Guide for Service and Asset Manager* for information about using the configuration database.
 - b. Open the **Web Servers** workspace. The system displays a list of web servers.

- c. Open a web server record.
 - d. Clear the **Server is Active** check box.
 - e. Click **Save**.
 - f. Repeat for all of the web servers.
3. Access the installation folder on the Ivanti product CD or zip file and run IvantiServiceManager.exe. Right-click and select **Run as Administrator** to ensure proper installation.

The installer checks for the prerequisite software components. If any of those components is not installed, the system prompts you to install them now.
4. Click **Install** at the prompt. Installation of the prerequisite software can take several minutes. If you are prompted to restart the system, click **Yes**.
5. In the **Upgrade Confirmation** dialog box, click **Yes**. The system displays the **Welcome** dialog box. The installer checks for space and other requirements before displaying the **Next** button.
6. In the **Welcome** dialog box, click **Next**. The system displays the **License Agreement** dialog box.
7. Choose **I accept the terms in the license agreement** and click **Next**. The system displays the **Destination Folder** dialog box.
8. Click **Next** to accept the default installation folder, or click **Change** and select a different folder. The system displays the **Setup Type** dialog box.
9. Your selection of features from the **Setup Type** dialog box depends on the role of the individual host in your deployment plan.
 - For the "Demonstration or Proof-of-Concept Deployment" on page 8, choose **Complete**, click **Next**, and install all components.
 - For the "Minimum Production Deployment " on page 10, choose **Complete**, click **Next**, and install all components.
 - For the "Enterprise Production Deployment" on page 13, your choice depends on the role of the host:
 - **Production processing server**: Choose **Custom**, click **Next**, and install all components except for the Operations Console.
 - **Staging or UAT processing servers**: Choose **Complete**, click **Next**, and install all components.
 - **Web servers**: Choose **Custom**, click **Next**, and only install the Ivanti Service Manager application server.

For the "Enterprise Production Deployment" on page 13, note the following:

- If your deployment includes different processing servers for production, staging, and UAT, you must install the License Manager in every one of those landscapes.
- You can choose **Complete** and install all Service and Asset Manager features on all of your servers, but doing that takes up more disk space than necessary.

When installing components, note the following:

- To not install a component, click the down arrow next to the server icon next to the category name, highlight the component, right click, and select **This feature will not be available**.
- If your deployment includes DSM, you do not need to install the DSM integration service because that component has been incorporated into Ivanti Service Management since Release 2015.2.

10. Click **Next**. The system displays the **Ready to Install the Program** dialog box.
11. Click **Install**. The system begins installing Service and Asset Manager and displays a status dialog box, showing the installation progress of each module over the next few minutes.
12. Click **OK** if the system displays a dialog box saying that reboot is required after installation.
13. If the system displays a dialog box saying that some of the files that need to be updated are currently in use, choose **Automatically close and attempt to restart applications** and click **OK**.

When the installation is completed, the system displays the System Configuration Wizard.

14. Go through the pages in the wizard making any changes that might be necessary.



If you already have an existing administrator account, you do not need to create a new account. Just enter the information for your existing administrator account.

15. Notice that the system table version and metadata package version for the configuration database are not the latest versions.
16. Click **Finish**.
17. Restart the host server.
18. (Optional) If you also installed the Service and Asset Manager reporting feature, you must upgrade it to match the release number of your Service and Asset Manager system. Access the installation folder on the Ivanti Software product CD or download folder and run ReportingService.exe to upgrade Service and Asset Manager reporting feature.
19. Log in to the configuration database and activate the web servers that you deactivated in step 2.

Upgrading from Ivanti Service Management Release 2014.3 or Earlier

- "About Upgrading From Ivanti Service Management Release 2014.3 or Earlier" below
- "Uninstalling the Inventory Management Component" below

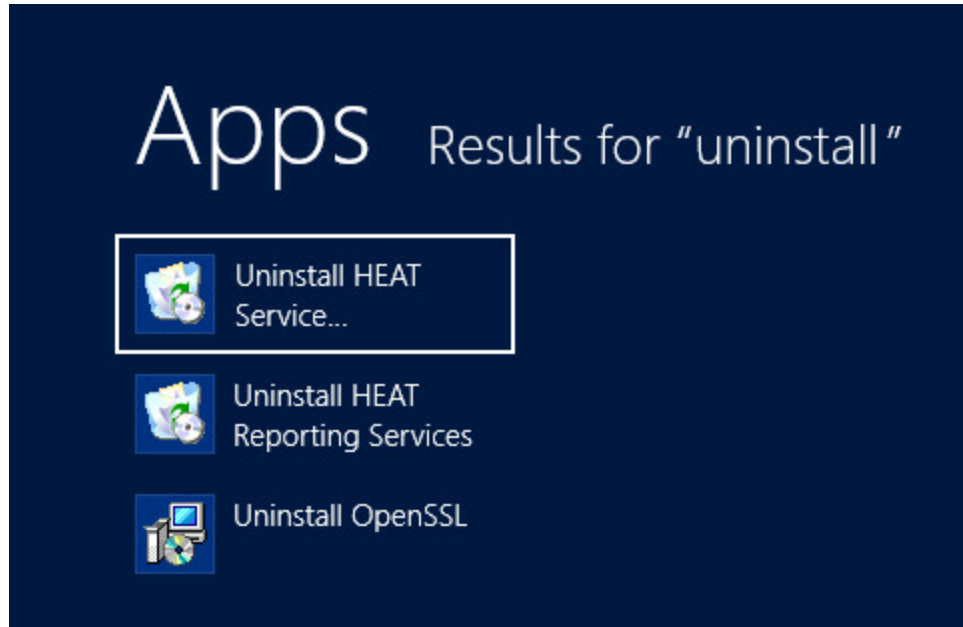
About Upgrading From Ivanti Service Management Release 2014.3 or Earlier

Beginning with Ivanti Service Management Release 2015.1, the Inventory Management component is known as Ivanti HEAT Discovery. As a result, before you can upgrade to the current version of Service and Asset Manager, if you are upgrading from Release 2014.3 or earlier, you must first uninstall the Inventory Management component.

Uninstalling the Inventory Management Component

Perform these steps on the system that hosts Service and Asset Manager:

1. Click the arrow at the bottom of the **Start** menu to view the **Apps** menu.
2. Mouse-over the **Uninstall Ivanti Service Management** icons to find the one for the Inventory Management component.



3. Click **Uninstall Ivanti Service Management**.
4. In the confirmation dialog box, click **Yes**.

Upgrading from Ivanti Service Manager 2020.1 Release to 2020.2 Release

The following steps should be performed before installing 2020.2 from 2020.1 release.

1. Log in to Service Manager with the Administrator role.
2. Open the Configuration console.
3. Under Security Controls, select Security and Sessions.
4. Under Concurrent Session, change the value of Named User, Privileged User, and Non Privileged User to 0.
5. Save the changes and refresh the page and re-validate the values are changed.
6. Now you can install 2020.2 Service Manager.
7. After installation is complete, you can change the concurrent users values as it was earlier.

Using the License Manager

- "About the License Manager" below
- "Types of Licenses" below
- "About License Bundles" on the next page
- "Using the License Manager" on page 177

About the License Manager

Use the License Manager to track your license usage.

For the "Demonstration or Proof-of-Concept Deployment" on page 8 and "Minimum Production Deployment" on page 10, the License Manager is installed on the Service and Asset Manager server along with the other Service and Asset Manager components.

For the "Enterprise Production Deployment" on page 13, the License Manager is installed on the Service and Asset Manager processing servers along with the other Service and Asset Manager components.

During installation, the System Configuration Wizard enabled you to import one production license, one non-production license, or both, depending on your landscape environment. You can import additional licenses, if needed. See "Importing Licenses" on page 179.

Types of Licenses

Service and Asset Manager mainly uses production and non-production licenses:

License Type	Description	Expiration
Production	Used to access the production landscape of a tenant.	Does not expire unless the MAC address is unspecified. In that instance, the license expires after 30 days. If you move the license to a new server with a different MAC address, then you must acquire a new license tied to the new MAC address.
Development	A non-production license used to access the staging and UAT landscapes.	Expires according to the maintenance agreement between your organization and Service and Asset Manager.
Not For Resale	A non-production license, mainly used by Ivanti Service Manager partners. It can also be used for staging, UAT, or testing if you already have development licenses.	Expires after 30 days if you do not specify the MAC address. After you set the MAC address, it expires according to the maintenance agreement between your organization and Service and Asset Manager.
Evaluation	A non-production license used by potential customers. Has the maximum number of named and concurrent user licenses.	Expires after 30 days. Is not associated with a MAC address.

There are two types of user licenses, for both production and non-production licenses:

- **Concurrent licenses:** For any user who is currently logged into the system. This is a shared pool of licenses. The concurrent license that is used is specified by the bundle that is specified for each role.
- **Named user licenses:** Specific to a certain user. The user can log in to the system from many places at one time and it is counted as only one license. You specify which users are named users in the employee record, and you can change which employees get a named user license at any time.

About License Bundles

- "List of License Bundles and Components" below
- "Assigning a Bundled License to a Role" on page 177
- "License Tracking in Service and Asset Manager" on page 177

Service and Asset Manager has defined several license bundles, which are sets of modules, or user interfaces. Each role is associated with a license bundle.

List of License Bundles and Components

License Bundle	Components
Help Desk	Dashboards and Reporting Incident Management Knowledge Management Mobile Self Service Service Catalog Survey Voice Automation (optional add-on) Workflow Automation
Service Desk	Dashboards and Reporting Incident Management Knowledge Management Mobile Self Service Service Catalog Survey

License Bundle	Components
	Voice Automation (optional add-on) Workflow Automation Change Management CMDB Configuration Management Problem Management Service Level Management
Service Management	Dashboards and Reporting Incident Management Knowledge Management Mobile Self Service Service Catalog Survey Voice Automation (optional add-on) Workflow Automation Change Management CMDB Configuration Management Problem Management Service Level Management Availability Management Event Management Financial Management Portfolio and Project Management Release Management

The following are considered license add-on modules:

Add-on Module	Components
Discovery	Discovery
Voice	Voice
Mobile	Mobile

Assigning a Bundled License to a Role

To assign a bundled license to a role, follow the procedure in the "Assigning a Bundled License to a Role" topic in the Service and Asset Manager online help. By default, roles do not have a license bundle associated with them, so you must assign a license bundle to each role manually. If you do not, you may get license violation errors logged in your system even though you have the correct licenses.



If you have imported licenses but do not see the correct license bundles displayed in the Configuration Console, clear the validation cache.

Go to **Configure > Cache Management** and then click **Reset cached validation lists only**.

See the Service and Asset Manager online help for more information.

License Tracking in Service and Asset Manager

You cannot use Service and Asset Manager unless you have a license. When you purchased Service and Asset Manager, you also purchased a set number of licenses. If needed, you can purchase additional licenses.

If you consume more seats than you have licenses for, the system does not log you out. It does, however, log an event into a log file. For example, if you have 10 concurrent licenses and try to log in 11 times, the system allows it.

Due to the way that web browsers work, it is very possible for one user to consume more than one license. For example, if a user logs in to Service and Asset Manager using Microsoft Internet Explorer and then opens Google Chrome and logs in again, another license is consumed. If this happens, the system logs a license violation error that you can view in the License Manager in the **System Audit Information** workspace.

Using the License Manager

- "Logging Into the License Manager" on the next page
- "Configuring Landscape Information" on the next page
- "Importing Licenses" on page 179
- "Viewing the Discovery Node Count" on page 181
- "Viewing the Active Licenses" on page 182
- "Configuring the Email Address for Notifications" on page 182
- "Configuring the SMTP Settings" on page 183
- "Working with Scheduled Jobs" on page 184
- "Viewing Reports" on page 186

Logging Into the License Manager

The License Manager uses the same credentials that are used to access the configuration database.

To log into the License Manager, follow these steps:

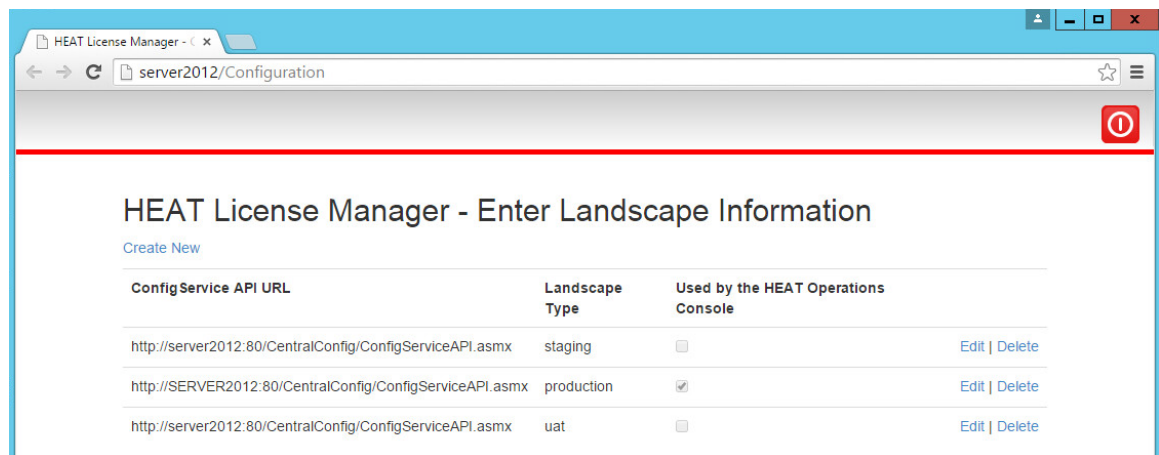
1. In the **Start** menu, click the down arrow to see the **Apps** menu, and then click **License Server**.
2. Select a landscape.
3. Enter your user ID and password. This is the same user ID and password that you use for the configuration database.
4. Click **Continue**.

Configuring Landscape Information

You can create, edit, and delete information about the landscapes to which the License Manager is associated.

1. Log into the License Manager.
2. Click either **Configure Landscapes** in the top right corner of the login page or click **Configure Landscape Information** from any page in the License Manager. The system opens a new browser window and displays the **Enter Landscape Information** page.

Enter Landscape Information Page



3. To allow the Operations Console to use this landscape, check **Used by the Operations Console** on the line associated with the landscape.

The Operations Console can only use one landscape at a time.

4. To edit the information for an existing landscape, do the following:
 - a. Click **Edit** on the line associated with the landscape. The system displays the **Edit Landscape** page.
 - b. Make changes as needed.

- c. Click **Save**.
5. To delete the landscape information, do the following:
 - a. Click **Delete** on the line associated with the landscape.
 - b. Click **Delete** at the confirmation message.
6. When you configured Service and Asset Manager using the System Configuration Wizard, the system automatically created a link to the landscape.

Therefore, in general, you do not need to add a link to a landscape. However, if you do need to add a new link to a landscape, follow these steps:

- a. Click **Create New**. The system displays the **Create Landscape** page.
- b. In the **ConfigService API URL** field, enter the URL of the configuration server.
- c. Check **Used by the Operations Console** if the system should use this link to connect with the Operations Console. The Operations Console can only connect to one landscape.
- d. Click **Load Landscape Types** and then select a landscape from the drop-down list.
- e. Click **Create**.

Importing Licenses

When you initially configured the License Manager in the System Configuration Wizard, you imported either one production license file, one non-production license file, or both. (See "Configuring Service and Asset Manager " on page 84.)

If your deployment has multiple License Managers, when you import a license, ensure that you are importing it on the server that has the same MAC address as the license file.

For example, say you installed License Managers on the following:

- Application Server 1 with a MAC address of AA:10:23:10:00
- Application Server 2 with a MAC address of BB:10:23:10:00

Then you ask for and receive a production license for MAC address AA:10:23:10:00. You import the license from the License Manager that is installed on Application Server 1. After you have imported the license, the License Managers on both Service and Asset Manager application servers respect the license. You do not need a second license for the second Application Server.

To import additional license files, follow these steps:

1. Log into the License Manager.
2. Click **Licensing > Import License Files**. The system displays the **Licensing - Import License Files** page.

Import License Files Page

Refresh

Import License File

List of imported license files

File Name	Expiration Date	MAC Address	Help Desk		
			Concurrent	Named	
USA-ServiceManagement-TC54-42651-54-UNSPECIFIED-732e0ad7...	12/31/2025, 12:00:00 AM	UNSPECIFIED	10	7	7
Total			10	7	7

License distribution per tenant

Tenant	Help Desk		
	Concurrent	Named	
HEAT Service Management	10	7	7
	0	0	0

- Click **Upload License File....**
- Navigate to and select a license file and click **Open**.

The system adds the license to the system. This page shows the following information:

Field	Description
File Name	The name of the license file that you uploaded.
Expiration Date	The expiration date of the license file.
MAC Address	The MAC address associated with the license file.
Self Service	Self Service is the bundle name. The number of Self Service licenses contained in the license file. Broken into concurrent and named licenses.
Service Catalog	Service Catalog is the bundle name. The number of Service Catalog licenses contained in the license file. Broken into concurrent and named licenses.
Service Management	Service Management is the bundle name. The number of Service Management licenses contained in the license file. Broken into concurrent and named licenses.

- Click the **delete** icon to remove the license file and its associated licenses from the License Manager.
- Click the **show details** icon to display the details. The details contain the following information:

Field	Description
Bundle	The name of the bundle.
Name	The name of the module.
Named Licenses	The number of named licenses contained in the license file.
Concurrent Licenses	The number of concurrent licenses contained in the license file.
Expiration Date	The date when the license expires.

If your deployment only has one tenant, the information displayed here is the same as in the **List of imported license files** section.

If your deployment has more than one tenant, this table displays the license distribution across the tenants.

Field	Description
Tenant	The name of the tenant.
Self Service	The number of Self Service licenses allocated per tenant. Broken into concurrent and named licenses.
Service Catalog	The number of Service Catalog licenses allocated per tenant. Broken into concurrent and named licenses.
Service Management	The number of Service Management licenses allocated per tenant. Broken into concurrent and named licenses.

- To distribute licenses among multiple tenants, click in a cell and change the number of licenses to allocate to a tenant. The total number of licenses across the tenants cannot exceed the total number of licenses. See "Allocating Licenses Across Tenants" below.

Allocating Licenses Across Tenants

License distribution per tenant

	Help Desk		Service Desk		Service Management	
	Concurrent	Named	Concurrent	Named	Concurrent	Named
	10	7	7	0	3	3
	0	0	0	0	0	0

Viewing the Discovery Node Count

This information tracks the trend associated with the Discovery licenses and is based on the **Discovery Count** scheduled job.

- Log in to the License Manager.
- Click **Licensing > Discovery**. The system displays the **Licensing - Discovery** page.

This page shows the following information:


Field	Description
Tenant Name	The name of the tenant.
Last Scan Date	The date and time when the job was run.
Nodes Count	The number of configuration items found during the job.

Viewing the Active Licenses

This page displays the active sessions on Service and Asset Manager. It does not show active sessions on the configuration database.

1. Log in to the License Manager.
2. Click **Licensing > Active Licenses**. The system displays the **Licensing - Active Licenses** page.

Active Licenses Page

 Refresh						
Select Tenant:	HEAT Service Management					
Session ID	User	Role	Bundle Name	Add-On Modules	License Taken Time	License Type
541ED76B4DA54FE0860CFD438997E463	HEATAdmin	Admin			10/9/2015, 10:40:51 AM	Concurrent
7A33BE700879437BB9EE6F805388B16C	HEATAdmin	Admin			10/9/2015, 10:21:29 AM	Concurrent

3. Select a tenant from the drop-down list. This page shows the following information:

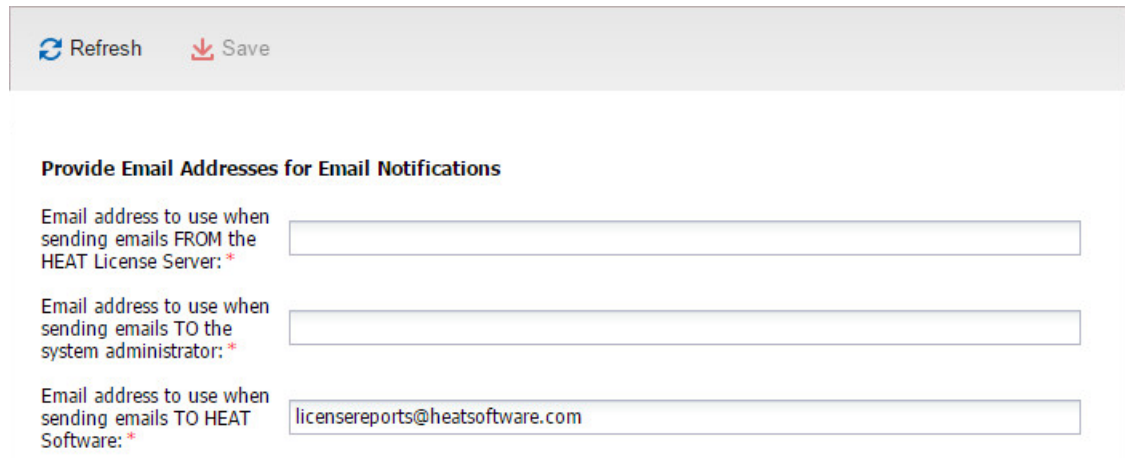
Field	Description
Session ID	The session ID associated with the logged-in user.
User	The user name of a logged-in user.
Role	The role with which the user is logged in.
Bundle Name	The bundle associated with the license associated with the user. See "About License Bundles" on page 175.
Add-On Modules	Any add-on modules associated with the bundle. See "About License Bundles" on page 175.
License Taken Time	The time when the system used the license.
License Type	The license type. Can be named or concurrent.

Configuring the Email Address for Notifications

1. Log in to the License Manager.

- Click **Configuration > Email Address**. The system displays the **Configuration - Email Address** page.

Email Address Page



Provide Email Addresses for Email Notifications

Email address to use when sending emails FROM the HEAT License Server: *

Email address to use when sending emails TO the system administrator: *

Email address to use when sending emails TO HEAT Software: *

- Enter the following information:

Field	Description
Email address to use when sending emails from the License Server	The email address to use as the FROM email address for emails sent from the License Manager.
Email address to use when sending emails to Ivanti Software	The email address to use as the TO email address for emails sent from the License Manager to Ivanti Software. The system sends license usage information based on the License Violation Notification to Frs scheduled job.
Email address to use when sending emails to the system administrator	The email address to use as the TO email address for emails sent from the License Manager to the system administrator of your organization. The system sends license usage information based on the License Violation Notification to Admin scheduled job.



- Click **Save**.

Configuring the SMTP Settings

Use this page to view and edit the SMTP settings used to send emails. The information on this page comes from the System Configuration Wizard.

- Log into the License Manager.
- Click **Configuration > SMTP Setting**. The system displays the **Configuration - SMTP Setting** page.

SMTP Setting Page

 Refresh
  Save

Select a tenant to see the SMTP settings that the tenant uses to send emails. These settings are from the Configuration Database.

Tenant: HEAT Service Management

Use this setting for Email Notifications: ☒

Host: barracuda.datamasters.com

Port: 25

Account: admin@datamasters.com

Domain: ms2.datamasters.com

Use SSL: Yes

The system displays the following information:

Field	Description
Host	The email server host.
Port	The port associated with the email server.
Account	The account associated with this tenant. This is the same as the value in the Username field on the Email Configuration workspace in the Service Desk Console.
Domain	The domain associated with the account.
Use SSL	Specifies if this account should use SSL.

3. Select a tenant from the **Tenant** drop-down list.
4. Check **Use this setting for Email Notifications** to use these SMTP settings for emails.
5. Click **Save**.

Working with Scheduled Jobs

The License Manager has several predefined scheduled jobs. These are used to send information to the administrator on a regular basis instead of sending an email every single time there is an event. All violations are listed on the **System Audit Information** page.

The following are the predefined scheduled jobs that cannot be changed:

- **License Capacity Allocation Notification Job:** Determines if your licenses are valid and that you actually have the licenses that you are allocating.
- **Named License Violation:** Determines if you have more users listed as named users than you have named user licenses.
- **Data Integrity Verification:** Determines if the licenses have been modified.




- **Discovery Count:** Determines if the licenses for your configuration items are valid.

The following are the predefined scheduled jobs that you can edit:

- **License Violation Notification to FRS:** Sends an email to Ivanti Software with information about license violations. By default, this job is disabled.
- **License Violation Notification to Admin:** Sends an email to your system administrator with information about license violations.

1. Log in to the License Manager.
2. Click **System Jobs**. The system displays the **System Jobs - Scheduled Jobs** page.

Scheduled Jobs Page

 Refresh								
Dates and times are displayed in Server Time: (UTC-08:00) Pacific Time (US & Canada)								
Module	Job	Enabled	Start Date	Start Time	Next Run Date Time	Recur Every	Interval	
LicenseCore	Set Data Integrity References	<input checked="" type="checkbox"/>	8/26/2015	12:00 AM	10/9/2015 12:50 PM	Minute	10	
LicenseCore	License Violation Notification To Hsw	<input type="checkbox"/>	8/26/2015	12:00 AM		Day	1	
HeatModule	Discovery Count	<input checked="" type="checkbox"/>	8/26/2015	12:00 AM	10/10/2015 12:00 AM	Day	1	
HeatModule	License Capacity Allocation Notification Job	<input checked="" type="checkbox"/>	8/26/2015	12:00 AM	10/10/2015 12:00 AM	Day	1	
HeatModule	Named License Violation	<input checked="" type="checkbox"/>	8/26/2015	12:00 AM	10/10/2015 12:00 AM	Day	1	
LicenseCore	Data Integrity Verification	<input checked="" type="checkbox"/>	8/26/2015	1:00 AM	10/10/2015 1:00 AM	Day	1	
LicenseCore	License Violation Notification To Admin	<input checked="" type="checkbox"/>	8/26/2015	12:00 AM	10/10/2015 12:00 AM	Day	1	

This page contains the following information:

Field	Description
Module	The name of the module. Can be either LicenseCore or HeatModule.
Job	The name of the job.
Enabled	Specifies if the scheduled job is enabled.
Start Date	The start date of this scheduled job.
Start Time	The start time of this scheduled job.
Next Run Date and Time	The next date and time when the scheduled job runs.
Recur Every	The time period for the recurrence. Can be day, hour, or minute.
Interval	The interval for the recurrence.

For each entry, the system displays additional information at the bottom of the page:

Field	Description
Module	The name of the module. Can be either LicenseCore or HeatModule.

Field	Description
Job	The name of the job.
Run Time	The date and time when the scheduled job was run.
Details	Details of the job. If the job is not successful, contains detailed information.

- To see the job details in a larger format, click the **show details** icon at the end of the row.
- You can edit the details associated with the **License Violation Notification To Frs** and the **License Violation Notification to Admin** scheduled jobs.

To edit a scheduled job, do the following:

- Click the **Edit** icon at the end of the row. The system displays a dialog box.
- Enter or change any of the following information:

Field	Description
Job	The name of the scheduled job. You cannot change this name.
Description	A description of the scheduled job.
Start Date	The start date and time.
Enabled	Specifies if the scheduled job is enabled.
Next Run Date Time	The next date and time when the scheduled job runs.
Recur Every	Specifies the recurrence for this job.

- Click **Save**.

Viewing Reports

You can view two types of reports in the License Manager:






- System audit information
- Logs

Follow these steps to view the reports.

- Log in to the License Manager.
- Click **Reports**.
- To view the system audit information, click **System Audit Information**. The system displays the **Reports - System Audit Information** page. See "System Audit Information Page" on the next page. Examples of the information on this page include license upgrades and license violations.

We recommend that you review the information on this page if you have any problems and then review the information on the **Log** page. See "Log Page " below.

System Audit Information Page

Refresh							
Tenant Name	Event Log Date and Time	Subsystem	Class	Title	Details	Operation Result	
SERVER2012	10/9/2015, 10:40:51 AM	License Violation	Warning	License Violation	Empty Bundle for LoginHEATAdmin Role: Admin and Tenant: SERVER2012	Success	
SERVER2012	10/9/2015, 10:21:29 AM	License Violation	Warning	License Violation	Empty Bundle for LoginHEATAdmin Role: Admin and Tenant: SERVER2012	Success	
SERVER2012	8/26/2015, 8:09:10 AM	License Violation	Warning	License Violation	Empty Bundle for LoginHEATAdmin Role: Admin and Tenant: SERVER2012	Success	
	8/26/2015, 7:07:43 AM	Data Integrity Service	Warning	Data Integrity Violation	Data integrity is corrupted for entity: TenantLicense	Success	
	8/26/2015, 7:06:55 AM	License Upgrade	Info	Not a one-to-one upgrade. License file: upgrade	Original License File Module: FRS ITSM Availability Management Module Named: 0 Concurrent: 10 Module: FRS ITSM Change Management Module Named: 3 Concurrent: 3 Module: FRS ITSM Configuration Management Module Named: 0 Concurrent: 0 Module: FRS ITSM Incident Management Module Named: 10	Success	



















This page contains the following information:

Field	Description
Tenant Name	The name of the tenant.
Event Log Date and Time	The date and time of the log event.
Subsystem	The specific area. Can be license violation, license upgrade, or data integrity service.
Class	The type of information. Can be warning, info, debug, fatal, or error.
Title	A short description of the event.
Details	A longer description of the event.
Operation Result	The result of the operation. Can be success or failure.

If you cannot see all of the columns, resize the columns that you can see so that the remaining columns are displayed.

- Click the **show details** icon at the end of the row to see the details. If you cannot see the **Show Details** icon, resize the columns until it is displayed.
- To view log information, click **Log**. The system displays the **Reports - Log** page. Use this information for troubleshooting.

Log Page

Refresh 				
Subsystem	Event log time	Details		Log type
Named License Violation	10/9/2015, 10:08:14 AM	System.InvalidOperationException: Collection was modified; enumeration op...		Error
Import License	10/9/2015, 10:06:29 AM	Updating Named Bundles in the Tenant:SERVER2012 database.		Info
Import License	10/8/2015, 5:25:20 PM	Updating Named Bundles in the Tenant:SERVER2012 database.		Info
Import License	10/8/2015, 2:22:04 PM	Updating Named Bundles in the Tenant:SERVER2012 database.		Info
Named License Violation	10/8/2015, 12:19:44 PM	System.InvalidOperationException: Collection was modified; enumeration op...		Error
Import License	10/8/2015, 11:05:43 AM	Updating Named Bundles in the Tenant:SERVER2012 database.		Info
Email Notification	10/8/2015, 11:05:42 AM	Unable to send email with Subject: production - HEAT Service Management - ...		Info
Import License	8/26/2015, 7:51:54 AM	Updating Named Bundles in the Tenant:SERVER2012 database.		Info
Import License	8/26/2015, 7:47:31 AM	Updating Named Bundles in the Tenant:SERVER2012 database.		Info
Named License Violation	8/26/2015, 7:41:29 AM	System.ArgumentNullException: Value cannot be null. Parameter name: url a...		Error
Import License	8/26/2015, 7:10:26 AM	Updating Named Bundles in the Tenant:SERVER2012 database.		Info
Import License	8/26/2015, 7:07:44 AM	Updating Named Bundles in the Tenant:SERVER2012 database.		Info
Import License	8/26/2015, 7:07:00 AM	Updating total license counts in ConfigDB for the Tenant:SERVER2012 with n...		Info
License Upgrade	8/26/2015, 7:06:55 AM	End Upgrade file:		Info
License Upgrade	8/26/2015, 7:06:55 AM	Start Upgrade file:		Info
Import License	8/26/2015, 7:06:54 AM	Importing License file:USA-ServiceManagement-TC54-42651-54-UNSPECIFIE...		Info
Configuration Service	8/26/2015, 6:22:00 AM	System.NullReferenceException: Object reference not set to an instance of a...		Error


This page contains the following information:

Field	Description
Subsystem	The name of the subsystem. Can be email notification, import license, license upgrade, named license violation, or configuration service.
Event Log Time	The time and date of this log event.
Details	Information about this log event.
Log Type	The type of log. Can be info, error, or warning.

6. To see the log details in a larger format, click the **show details** icon  at the end of the row.

Chat Configuration

The administrator has to configure the following settings for the chat feature to work.

- **Global Constant** - In the Configuration module, under **Global Constants**, set the **ChatEnabled** field as **True**.
- **User role** - To make the chat icon  available for a user, the administrator should enable chat for the user role.

To enable the chat feature for a user role:

- Log in to Service and Asset Manager with the Administrator user role.
- From the Configuration console, select **Configure > Roles and Permissions**.
- Select the role for which you want to enable the chat feature.
- Ensure the **Overwrite default branding options with the options listed below** check box is selected.
- Select the **Enable Chat as Analyst** check box.



- If you select the **Overwrite default branding options with the options listed below** check box, all check boxes under **Branding Options** will be disabled. Ensure to select them as needed.
- Chat requests to the Service Desk console team get routed using the Round Robin algorithm based on the Service Desk Analyst's login state.

Configuring Chat

The chat configuration settings are pre-defined, however, you can change the settings as need be.

Session Configuration Settings:

- **Concurrent Chat Sessions per Analyst:** Number of chat requests that can be assigned to the Service Desk Analyst at a time.
- **View User Chat History for last Created Incident(s):** Number of previous chat sessions' history that should be stored. History is stored only when an Incident is created in the chat session.
- **First Inactivity Timeout:** Timeout limit when a first warning message is sent to the Self Service Mobile portal user when inactive on a chat session.
- **Second Inactivity Timeout:** Timeout limit when a second warning message is sent to the Self Service Mobile user when inactive on a chat session.

- **Session Expiration Timeout:** Timeout limit when the Self Service Mobile portal user is logged out when inactive on a chat session.
- **Analyst Session Timeout:** Timeout limit when a Service Desk Analyst's status is turned **Offline** when no chat session is assigned.
- **User Timeout:** Timeout limit when a Self Service Mobile portal user is logged off from a chat session when unable to assign the chat session with the Service Desk Analyst.

Details:

- **Online Message Header:** Header displayed to the Self Service Mobile portal user when the Service Desk Analyst staff is online and ready to pick up chat sessions.
- **Offline Header:** Header displayed to the Self Service Mobile portal when the Service Desk Analyst is offline and not available to pick up chat sessions.
- **Hop Header:** Header displayed to the Self Service Mobile portal when the Service Desk Analyst staff is offline during non-hours-of-operation.
- **Join Header:** Header displayed to the to the Self Service Mobile portal when a Service Desk Analyst joins the chat session.
- **Fail Join Header:** Header text displayed to the to the Service Desk Analyst when unable to assign a Service Desk Analyst to the chat session.
- **Knowledge Message:** Link to knowledge base displayed to the Service Desk Analyst user when unable to assign a Service Desk Analyst to the chat session.
- **Warning Header:** First warning header displayed to the Self Service Mobile portal user when inactive on the chat for the set time.
- **Second Warning Header:** Second warning header displayed to the Self Service Mobile portal user when inactive on the chat for the set time.
- **Typing:** Typing indicator displayed in the chat window text box.
- **Send Message Place Holder:** Message displayed in the chat window text box.
- **Incident Created text:** Message displayed in the chat window when an incident is created from the chat session.
- **User Disconnected:** Message displayed to the Service Desk Analyst and the Self Service Mobile portal user when the chat session gets disconnected.
- **Online Message:** Message displayed to the Self Service Mobile portal user when the Service Desk Analyst staff is online.
- **Offline Message:** Message displayed to the Self Service Mobile portal user when the Service Desk Analyst staff is offline during hours-of-operation.

- **Hop Message:** Message displayed to the Self Service Mobile portal user when the Service Desk Analyst staff is offline during non-hours-of-operation.
- **Joining Message:** Message to the Self Service Mobile portal user when trying to assign a Service Desk Analyst to the chat session.
- **Join Message:** Message displayed to the Self Service Mobile portal user when a Service Desk Analyst joins the chat session.
- **Fail Join Message:** Message to the Self Service Mobile portal user when unable to assign a Service Desk Analyst to the chat session.
- **Knowledge Button:** Second line of the knowledge base link message when unable to patch a Service Desk Analyst to the chat session.
- **First Warning text:** First warning message displayed to the Self Service Mobile portal user when inactive on the chat for the set time.
- **Second Warning Text:** Second warning message displayed to the Self Service Mobile portal user when inactive on the chat for the set time.
- **Expired Warning Text:** Message displayed to the Self Service Mobile portal user just before logging off the chat session when the user is inactive on the chat for the set time.
- **Session Expired Text:** Message displayed to the Self Service Mobile portal user after logging off the chat session when the user was inactive on the chat for the set time.
- **User Wait Expired Text:** Message displayed to the Self Service Mobile portal user when unable to assign a Service Desk Analyst to the chat session.



When you make changes to the Chat Configuration, it is recommended that you clear cache for the changes to be effective. To do it, open the Configuration console > **Cache Management** > **Reset Chat Objects**.

Create Incident Quick Action

Service Desk Analyst can create an Incident from the chat session which is based on the **Create Incident** Quick Action added to the **ivnt_Chat Business Object**. This Quick Action can be customized as needed.

Customizing the Create Incident Quick Action

1. Log in to Service and Asset Manager with the Administrator user role.
2. Open the Configuration console.
3. Under **Build**, click **Business Objects** > search and open **ivnt_Chat Business Object**.
4. Click **Create Incident**.

5. Edit the data as needed and click **Save**.

Known Issues

Release Version 2021.3

No known issues in this release.

Release Version - 2021.2

Following known issue is in Ivanti Service Manager 2021.2 release:

1. [Bug 845546](#): When upgrading from 2021.1 to 2021.2, the application throws an error.
2. [Bug 811955](#): Request Offerings do not display in alphabetical order when the Global Constant **EnableUKEnglishLocalization** is set to **True**.

Issue Details

1. **Bug: 845546:**

Issue	When upgrading from 2021.1 to 2021.2, the application throws an error.
Details	The upgrade from 2021.1 to 2021.2 is not successful. The new items introduced in the Configuration Item (CI) Business Object are not imported automatically.
Expected Result	The upgrade should be successful without an errors.
Workaround	<p>The latest ITAM delta upgrade package introduces the CI.ivnt_MedicalDevice new member objects in CI.</p> <p>After applying the delta upgrade package, the new fields introduced in the CI base business object are not automatically inherited in the new member objects.</p> <p>To force the field synchronization, so that missing fields are copied from the CI base object, you need to perform the following steps:</p> <ol style="list-style-type: none"> 1. Go to one of the Existing Business object for example CI.ivnt_infrastructure create a boolean field. <ul style="list-style-type: none"> To create a Boolean field: <ol style="list-style-type: none"> a. From the Configuration console > Business Object > open the respective Business Object > Fields.

	<ol style="list-style-type: none"> b. Click Add new Field, select the Field Type as Boolean. c. Enter a name and click Save. <ol style="list-style-type: none"> 2. Go to the new member object - CI.ivnt_MedicalDevice and create a boolean field with same name created for the CI.ivnt_infrastructure business object. 3. Remove the field that you just added. First remove from CI.ivnt_infrastructure and then from CI.ivnt_MedicalDevice. <p>This workaround will fix the link between all the CI Group and the base business object.</p>
--	---

2. Bug: 811955:

Issue	Request Offerings do not display in alphabetical order when the Global Constant EnableUKEnglishLocalization is set to True .
Details	<ol style="list-style-type: none"> 1. Log in to Neurons for ITSM 2. Open the Configuration console > Global Constants > set the EnableUKEnglishLocalization option as True. 3. Open Languages and add English UK Culture. If it is already added, remove and re-add. 4. Open the Service Desk console > Request Offerings. The list of Request Offerings are in alphabetical order. 5. Edit one of the offering except the first one from list, save and exit the page.
Actual Result	The recently edited offering is on the top of the list.
Expected Result	The Request Offerings should still be displayed in alphabetical order.

Release Version - 2021.1

Following known issue is in Ivanti Service Manager 2021.1 release:

1. [Bug 822605](#): - Provisioning report on SSRS 2019 for custom authentication throws a 401 unauthorized error.

Issue Details

1. **Bug: 822605:**

Issue	Provisioning report on SSRS 2019 for custom authentication throws a 401 unauthorized error.
Details	<p>Steps:</p> <ol style="list-style-type: none"> 1. Install 2021.1 on windows 2019 and sql 2019. 2. Provision report on SSRS 2019. 3. Select Custom Authentication for Microsoft SSRS Authentication Type. 4. Under Service Account, select Use built-in account and Network Service from the drop down list. 5. Click Next and provide the necessary information and click Provision Report Now.
Actual Result	The application throws a 401 error.
Expected Result	Report provision should be successful.
Workaround	Stop and start the Report Server Configuration Manager (SSRS) and provision the report again.

Release Version - 2020.4

Following known issue is in IvantiService Manager 2020.4 release:

1. [Bug 774221](#): - Enabling chat fails.

Issue Details

1. **Bug: 774221:**

Issue	Enabling chat fails.
Details	Enabling chat fails with the error message - "Unable to register in chat" or "Login prompted".
Expected Result	Chat feature should be enabled without any errors.
Workaround	Review the Redis configuration inside AppServer directory of the installation and restart the Redis service.

Release Version - 2020.3

Following known issue is in IvantiService Manager 2020.3 release:

1. [Bug 739326](#) - When trying to install Ivanti Service and Asset Manager, the installer automatically closes without installing upon clicking the **Install** button.

Issue Details

1. Bug: 739326

Issue	When trying to install Ivanti Service and Asset Manager, the installer automatically closes without installing upon clicking the Install button.
Details	<ol style="list-style-type: none"> 1. Setup a machine with Window authentication. 2. Download the Ivanti Service and Asset Manager installer and run as Administrator. 3. Select the product you want to install, that is ISM, ITAM, or ITxM. 4. Follow the next steps and finally click the Install button.
Actual Result	The installer closes automatically.
Expected Result	The product should be installed.
Workaround	Run the installer again.

Release Version - 2020.2

Following is the list of known issues in IvantiService Manager 2020.2 release:

1. [Bug 697328](#) - After session timeout clicking on received notification it redirects to Home page of SSM user in Android and iOS device.
2. [Bug 700504](#) - Enable Biometric Authentication checkbox is not displaying in Android device which has Face ID.
3. [Bug 701732](#) - While renewing session using password, it throws time stamp exception in Android device.
4. [Bug 702094](#) - Navigating to Ivanti Cloud Workspace throws an error.
5. [Bug 703679](#) - TRANSLATION-Japanese-Administrator-Chat Configuration-"Seconds" is mistranslated as "2nd".
6. [Bug 711161](#) - While upgrading from 2020.1, SCW throws an error if the value for Privileged User is set as 1 under Concurrent User section.

Issue Details

1. Bug: 697328

Issue	After session timeout clicking on received notification it redirects to Home page of SSM user in Android and iOS device.
Details	Prerequisite: <ul style="list-style-type: none"> Ensure ISM application is configured to receive push notifications on your device. <ol style="list-style-type: none"> 1. Login to ISM mobile app as SSM role in Android or IOS device 2. Wait for session timeout (configure session time out in Admin UI) 3. In desktop create an incident to get notification in the mobile device 4. Click on the newly received notification 5. It redirects to Login page, enter valid credential to login.
Actual Result	After successful login it redirects to Home page of SSM user.
Expected Result	After successful login it should redirect to Notification Corner.
Workaround	After landing on the home page, user can click on the bell icon on top right to navigate to notification corner to view notification.

2. Bug: 700504

Issue	Enable Biometric Authentication checkbox is not displaying in Android device which has Face ID.
Actual Result	Prerequisite: <ul style="list-style-type: none"> Ensure Biometric authentication is enabled on your device. <ol style="list-style-type: none"> 1. Install latest ISM app in Android device which has Face ID enabled in the device. 2. Launch the App and access the url. 3. In the login page observe for Enable Biometric Authentication check box.
Expected Result	Enable Biometric Authentication checkbox is not displayed to the user.
Actual Result	Enable Biometric Authentication checkbox should be displayed to the user.
Workaround	Use Phone PIN to login or enable fingerprint authentication on your mobile device.

3. **Bug: 701732**

Issue	While renewing session using password, it throws time stamp exception in Android device.
Actual Result	Prerequisite: <ul style="list-style-type: none"> Session timeout value should be set in the Admin UI. e.g – set the value to 1 minute. <ol style="list-style-type: none"> Login to ISM using password in Android device. Wait for session timeout. Click on any workspace. In the "You were logged out. Would you like to continue working?" pop up click the Yes button. In the login page enter password and click the login button.
Expected Result	It throws time stamp exception.
Actual Result	It should login successfully to ISM mobile app.
Workaround	Close the app, relaunch and login again.

4. **Bug: 702094**

Issue	Navigating to Ivanti Cloud Workspace throws an error.
Actual Result	<p>Note: This workspace newly added in 2020.2 and was not present in previous releases.</p> <ol style="list-style-type: none"> Login to ISM as Administrator. Open Ivanti Cloud workspace. In the login page enter password and click the login button.
Expected Result	Workspace doesn't load and displays error.
Actual Result	Workspace should load without any error.
Workaround	No workaround available.

5. **Bug: 703679**

Issue	TRANSLATION-Japanese-Administrator-Chat Configuration-"Seconds" is mistranslated as "2nd".
Actual Result	<ol style="list-style-type: none"> Login to the tenant as Administrator.

	<ol style="list-style-type: none"> Go to the Chat Configuration workspace. Click UI under Session Configuration Settings.
Expected Result	"Seconds" is translated as 2nd in time.
Actual Result	Seconds should be properly translated.
Workaround	No workaround available.

6. Bug: 711161

Issue	While upgrading from 2020.1, SCW throws an error if the value for Privileged User is set as 1 under Concurrent User section.
Workaround	<ol style="list-style-type: none"> Log in to Service Manager with the Administrator role. Open the Configuration console. Under Security Controls, select Security and Sessions. Under Concurrent Session, change the value of Named User, Privileged User, and Non Privileged User to 0. Save the changes and refresh the page and re-validate the values are changed. Now you can install 2020.2 Service Manager. After installation is complete, you can change the concurrent users values as it was earlier. <p>Note: The user session information is stored in Frs_system_settings in case of sql update.</p>

Configure :: Security Controls :: Security and Session

Security and Session Settings

Account Locking

Manages the account locking configuration for the current tenant.

☐ Enabled Enable account locking.

Soft Lock Attempts: Number of login attempts before account softly locked.

Soft Lock Period: Soft lock period in minutes.

Hard Lock Attempts: Number of login attempts before account permanently locked.

Account lock service requires a separate API key with administrator permissions.

API Key: [Account Locking API key](#)

Save

Concurrent Session

Manage allowed concurrent session for different type of users.

Named User:

Privileged User:

Non Privileged User:

Save

Release Version - 2020.1

Following is the list of known issues in IvantiService Manager 2020.1 release:

1. [Bug 670687](#) - ISM SSO: Session renew fails for OpenID and SAML OKTA for Android device.
2. [Bug 670665](#) - ISM SSO: After session timeout user is redirected to different browser while default authentication is activated if user don't want to work in Android device.
3. [Bug 670661](#) - ISM SSO: After session timeout while renewing the session, application opens default external authentication login page in different browser in iOS device.
4. [Bug 636223](#) - Ivanti cloud transfer: Blank record is getting created in Hardware workspace for device.
5. [Bug 648276](#) - Software Asset creation has intermittent issues.
6. [Bug 671029](#) - Username and roles are not visible as the text is in white color by default.
7. [Bug 431449](#) - On-premise : Installation of Metric server for the first time fails.
8. [Bug 678308](#) - On-premise: Unable to Login to Tenant once SCW completed for ITAM/IxM/ISM clean windows authentication.

9. [Bug 676494](#) - Default value of Request Offering text field set to Current User Function (Primary Phone) is not reflecting in Service Catalog.

Issue Details

1. Bug: 670687

Issue	ISM SSO: Session renew fails for OpenID and SAML OKTA for Android device.
Details	Prerequisite: <ul style="list-style-type: none"> Set any one of the external authentication as default. And set timeout session as 1 minute in Admin UI for validation purpose. <ol style="list-style-type: none"> ISM Android Mobile App using OpenID or SAML OKTA as external authentication provider. Wait for more than 1 minute. Click on any one of the workspace. The message "<i>You were logged out. Would you like to continue working?</i>" is displayed. Click Yes.
Actual Result	The same message " <i>You were logged out. Would you like to continue working?</i> " is displayed.
Expected Result	The session should renew without any error.
Workaround	No workaround available.

2. Bug: 670665

Issue	ISM SSO: After session timeout user is redirected to different browser while default authentication is activated if user don't want to work in Android device.
Actual Result	On timeout of your session, if you select No button for the " <i>You were logged out. Would you like to continue working?</i> " the application redirects to different browser and opens default authentication login page in different browser and application continues loading in Android Mobile App.
Expected Result	The application should logout the user session from the Android app.
Workaround	No workaround available.

3. Bug: 670661

Issue	ISM SSO: After session timeout while renewing the session, application opens default external authentication login page in different browser in iOS device.
Actual Result	<p>Scenario 1: When Yes button is clicked for the timeout session message, default authentication provider login page opens in different browser and in mobile app ISM keeps loading.</p> <p>Scenario 2: On clicking the external authentication hyperlink, the external authentication login page is opened in different browser instead of opening within the mobile app.</p>
Expected Result	The application should open in the ISM app.
Workaround	No workaround available.

4. Bug: 636223

Issue	Ivanti cloud transfer: Blank record is getting created in Hardware workspace for device.
Workaround	No workaround is available.

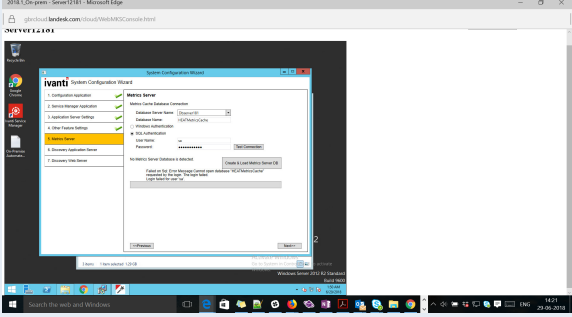
5. Bug: 648276

Issue	<p>Software Asset creation has intermittent issues.</p> <p>For example, when a software is installed on different system, after sometime the same software asset is created twice.</p>
Workaround	No workaround is available.

6. Bug: 671029

Issue	Username and roles are not visible as the text is in white color by default.
Details	<ol style="list-style-type: none"> 1. Login to ISM with Admin role. 2. Verify the logged in username and role.
Actual Result	The username and role are not visible as the text is in white color.
Expected Result	The logged in username and role should be visible.
Workaround	Navigate to the Configuration console > Style Editor and change the role text's color to black.

7. Bug: 431449

Issue	<p>On-premise - Installation of Metric server for the first time fails with db connection error.</p>  <p>Steps:</p> <ol style="list-style-type: none"> 1. Install the latest 2020.1 build on Windows 2014 R2 or any OS. 2. Select the Metric Server configuration in SCW.
Actual Results	The application fails to create the Metric Server database after the "Create" action though the db test connection is successful.
Expected Results	The application should create the Metrix Server database.
Workaround	Recreate works fine.

8. Bug: 678308

Issue	<p>On-premise: Unable to Login to Tenant once SCW completed for ITAM/IxM/ISM clean windows authentication.</p> <p>Steps:</p> <ol style="list-style-type: none"> 1. Set up ITAM clean windows authentication. 2. Once SCW completed open tenant enter valid credentials to login to tenant.
Actual Results	The application throws an error.
Workaround	Re-run the SCW and try to login.

9. Bug: 676494

Issue	<p>Default value of Request Offering text field set to Current User Function (Primary Phone) is not reflecting in Service Catalog.</p> <p>Prerequisite:</p>
--------------	--

	<ul style="list-style-type: none"> Add Phone number to the current user. <p>Steps:</p> <ol style="list-style-type: none"> Login to the application as Admin or Service Owner. Create a new Request Offering. Go to Design Request form and add a text field. Edit the field and set the default value to Function and select Current User: Primary Phone from the drop down list. Publish the Request Offering and save. Open the created Request Offering in Service Catalog and verify the current user phone number is populated.
Actual Results	Current User Phone number is not displayed in the service catalog.
Workaround	This is specific to 2019.1.0 OOTB onwards. No workaround available.

Release Version - 2019.3.1

Following is the list of known issues in IvantiService Manager 2019.3 release:

- [Bug 636223](#) - Ivanti cloud transfer: Blank record is getting created in Hardware workspace for device.
- [Bug 648276](#) - Software Asset creation has intermittent issues.

Issue Details

1. Bug: 636223

Issue	Ivanti cloud transfer: Blank record is getting created in Hardware workspace for device.
Workaround	No workaround is available.

Bug: 648276

Issue	Software Asset creation has intermittent issues. For example, when a software is installed on different system, after some time the same software asset is created twice.
Workaround	No workaround is available.

Release Version - 2019.3

Following is the list of known issues in Ivanti Service Manager 2019.3 release:

1. [Bug 616198](#) - Heat Mobile app may crash when iOS is upgraded from version 12.3.1 to 13.1.
2. [Bug 610706](#) - Post 2019.2 upgrade, Audit History is not updated based on the relationship link for FRS_Approval business object.
3. [Bug 615685](#) - Ivanti Cloud (UNO) Login App V1 & V2 integration does not work on ISM tenant which has Pre-MCT database.
4. [Bug 620323](#) - Duplicate entries for workflow and task on creating a service request from a backup database.
5. [Bug 635269](#) - IP Whitelisting shows "Invalid IP" for all FRSHeat integration API requests when session key from "Authenticate User" is used.
6. [Bug 644185](#) - The application throws an error when trying to link new and edit existing records in Telemetry Logging Configuration tab in config db tenant.
7. [Bug 70551](#) - Embedding content using iFrame in HTML UI Control is not working as expected.
8. [Bug 518404](#) - Request Offering is not getting created in the tenant, when imported via the Release Tool patch file.
9. [Bug 632194](#) - IP whitelisting - Integration trusted host is not allowing any IP to send/receive request, when the load balancer IP is configured.

Issue Details

1. Bug: 616198

Issue	After upgrading iOS version from 12.3.1 to 13.1, some users may experience crashing of the Heat Mobile app.
Workaround	Un-install and re-install the Heat Mobile app.

2. Bug: 610706

Issue	Post 2019.2 upgrade, Audit History is not updated based on the relationship link for FRS_Approval business object.
Actual Results	<ol style="list-style-type: none"> 1. Upgrade Service Manager to version 2019.2. 2. Log in to Service Manager with Admin user role. 3. Open the Configuration console.

	<ol style="list-style-type: none"> 4. Navigate to Business Objects > Service Request > Relationships > ServiceReqAssociatedFRS_Approval. 5. Select the Relationship is Audited check box. 6. Save and exit. 7. Create a Service Request that generates an approval, for example, Mailbox Quota Request. 8. Save the Service Request and exit. 9. Re-open the Service Request and click the Audit History tab. 10. No link to the Approval record is added in the Audit History.
Expected Results	A link to the Approval record should be added in the Audit History.

3. **Bug: 615685**

Issue	Ivanti Cloud (UNO) Login App V1 & V2 integration does not work on ISM tenant which has Pre-MCT database.
Workaround	Upgrade the pre-MCT tenant using MCT migration tool before performing IvantiCloud (UNO) Integration.

4. **Bug: 620323**

Issue	Duplicate entries for workflow and task on creating a service request from a backup database.
Workaround	<p>Note: The issue is re-producible when you restore the 2019.3 OOTB database from any existing tenant.</p> <p>You need to run a clean up script to remove the unwanted entries from specific table so that no duplicate workflow is triggered.</p> <p>Run the below query in the restored tenant database and "isvisible=0" condition is mandatory. Make sure the workflow service is stopped before running this script and start after running.</p> <pre>"select * from Frs_def_businessrules where isvisible = 0"</pre>

5. **Bug: 635269**

Issue	IP Whitelisting shows "Invalid IP" for all FRSHeat integration API requests when session key from "Authenticate User" is used.
Workaround	Use the SID (from ISM application > Developer Tools) to authenticate API requests.

6. **Bug: 644185**

Issue	The application throws an error when trying to link new and edit existing records in Telemetry Logging Configuration tab in config db tenant.
Actual Results	<ol style="list-style-type: none"> 1. Log in to a config db tenant of Service Manager with Admin user role. 2. Open a tenant record and navigate to Telemetry Logging Configuration tab. 3. Click Link > select a service record to link > Add or Edit button. <p>The application displays an error message.</p>
Expected Results	The selected service record should be linked to the Telemetry Logging Configuration.
Workaround	Go to the Telemetry Logging Configuration workspace, add new service records or existing records here. The updated services will be visible in the Telemetry Logging Configuration tab of the tenant page which you can now link.

7. **Bug: 70551**

Issue	Embedding content using iFrame in HTML UI Control is not working as expected.
--------------	---

8. **Bug: 518404**

Issue	Request Offering is not getting created in the tenant, when imported via the Release Tool patch file.
--------------	---

9. **Bug: 632194**

Issue	IP whitelisting - Integration trusted host is not allowing any IP to send/receive request, when the load balancer IP is configured.
--------------	---

Release Version - 2019.2

There are no known issues in Ivanti Service Manager 2019.2 release.

Release Version - 2019.1 and earlier


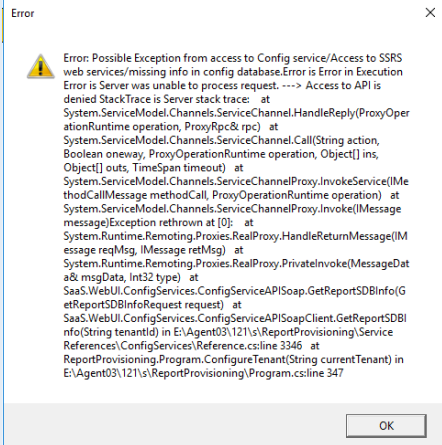
Given below is the list of known issues in Ivanti Service Manager 2019.1 and earlier releases.

1. [Bug 476581](#) - Configuration fails if the App server cache does not have trusted host information of database server.
2. [Bug 492307](#) - On-premise - Re-branding is pending in the ITAM application as it still refers to "Ivanti Service Manager".
3. [Bug 492520](#) - SSRS configuration with custom authentication and domain credentials may throw the 1326 error sometimes.
4. [Bug 492643](#) - Ops console is not re-branded for Ivanti, it still shows HEAT brand names.
5. [Bug 333924](#) - Configure OpenIDConnect Auth Provider for MS Azure AD.
6. [Bug 341934](#) - [Request for Information] Report: Distribution option "Download".
7. [Bug 505677](#) - Multiple records are displayed on the home page search for a single request.
8. [Bug 502699](#) - SSRS configuration fails while trying to add the provision report in SCW.
9. [Bug 504840](#) - There is a browser compatibility issue for Self Service Mobile, in the UI price list/ Cost panel showing Zero(0).
10. [Bug 383101](#) - Japanese characters are shown as ? in the FRS_SurveyAnswer.
11. [Bug 359153](#) - Logout from the Self Service Mobile UI takes users to the ISM login instead of the Auth provider login.
12. [Bug 508376](#) - "FrontRange Solution" installer certificate is not trusted by Microsoft anymore.
13. [Bug 519086](#) - Upgrading 2019.1 directly from 2018.1.1 does not work.
14. [Bug 522220](#) - Unable to create new CI due to the Asset Processor Configuration.
15. [Bug 525479](#) - Login page not loading by throwing Timestamp Error while Internal Services user is disabled.
16. [Bug 522214](#) - Config db/tenant db metadata version field left blank during upgrade/install.
17. [Bug 431449](#) - On-premise : Installation of Metric server for the first time fails.
18. [Bug 526262](#) - Upgraded ISM 2018.3.1 to 2019.1 and post upgrade accessing the below workspaces as LicenseManager role throws exception.
19. [Bug 485595](#) - The Sting "Self" is UNLOC shown under Self Service User - My Items > Benefits Package Claim.
20. [Bug 235039](#) - The Service Request Review and Submit page displays the incorrect employee details if the login IDs are similar.

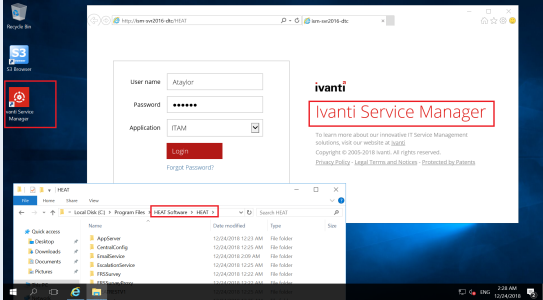
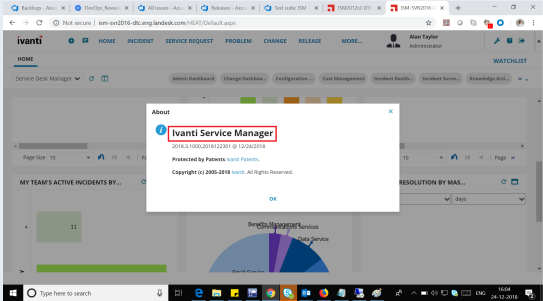
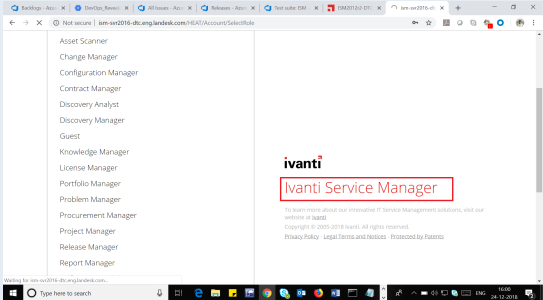
21. [Bug 533210](#) - 2019.1 premise installer seems to silently exit or crash after installing one of the pre-req modules.
22. [Bug 576301](#) - Errors on Form and Grid for BO AuthenticationPrincipal when upgrading from 2018.3.1 to 2019.1.0 premise.

Issue Details

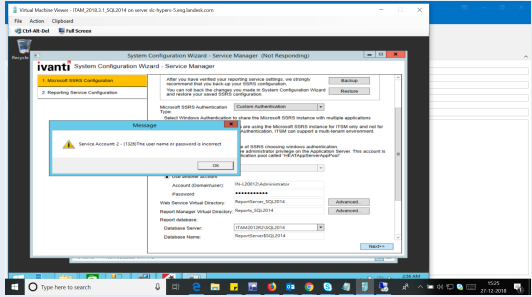
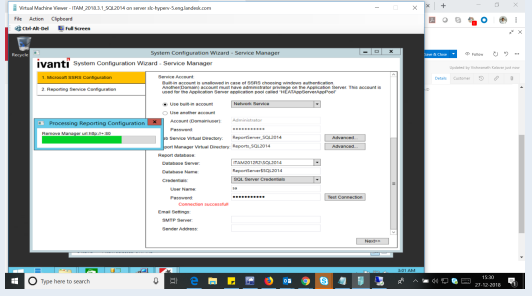
1. Bug: 476581

<p>Issue</p>	<p>Configuration fails if App server cache does not have trusted host information of database server</p> <ol style="list-style-type: none"> 1. Install or upgrade ISM application to latest build version of 2018.1.1 2. Install or upgrade the reporting service 3. Provision the report as part of configuration <hr/> <p> Use Custom Authentication method for SSRS configuration and SQL authentication for database connection type.</p> <hr/> 
<p>Workaround</p>	<p>There is a timing issue on provisioning. If the application cache is not rebuilt after updating the Trusted Host Entry in the config database (central config webapp), then provisioning of reports will fail as post config calls fails (Exception to access config service). Hence, it is advised to make sure Trusted Host Address are already added in the config database and IIS is reset (or wait for 15 mins to rebuild cache).</p>

2. Bug 492307

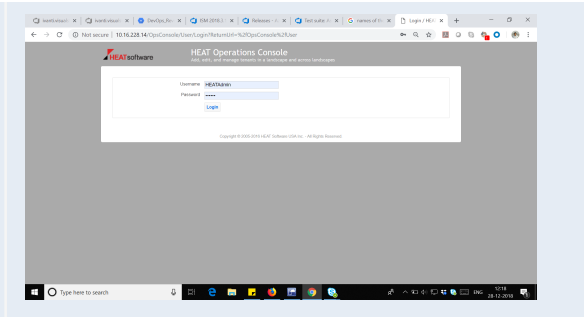
<p>Issue</p>	<p>On-premise - Re-branding is pending in the ITAM application as it still refers to "Ivanti Service Manager".</p> <p>Steps to reproduce</p> <p>Install ITAM application and check the product version and other branding-related information.</p>
<p>Actual Results</p>	  
<p>Expected Results</p>	<p>Currently, the 2018.3.1 on-premise version is built on top of the ISM platform and continues to refer ISM in many places. This needs to be fixed.</p>
<p>Workaround</p>	<p>No application functionality should be lost.</p>

3. Bug 492520

Issue	<p>SSRS configuration with Custom Authentication may fail sometimes if the domain user credentials provided is working. You will see the 1326 error.</p> <p>Steps to reproduce</p> <p>Configure SSRS with Custom Authentication with Domain credentials.</p>
Actual Results	<p>SSRS configuration with Custom Authentication is shown below:</p> 
Expected Results	<p>Provided domain credentials should work and users should be able to proceed.</p>
Workaround	<p>Use Custom authentication with the User in-built account type "Network Service" to proceed.</p> 

4. Bug 492643

Issue	<p>2018.3.1 ops console is not re-branded for Ivanti, it still shows HEAT brand names.</p> <p>Steps to reproduce</p> <p>Login to ops console by accessing the following path: http://10.16.228.14/OpsConsole/User</p>
--------------	--

Actual Results**5. Bug 333924****Issue**

When configuring OpenIDConnect Authentication Provider for MS Azure AD and making "Test Authentication", the following message appears: "Use Sub as external login as e-mail is not available at this step."

Azure AD does not return "email" claim in response and there is no "email" in "Extracted JWT token".

Instead of returning email in "email" claim, Azure returns an email in "upn" claim:

```
{ "typ": "JWT",
  "alg": "RS256",
  "x5t": "z44wMdHu8wKsumrbfaK98qxs5YI",
  "kid": "z44wMdHu8wKsumrbfaK98qxs5YI" }. { "aud": "022c4d20-1d56-4a73-a421-86b2b423f344",
  "iss": "https://sts.windows.net/23afecaf-6440-44aa-a6f2-b6e38bd02ba9/",
  "iat": 1517385849,
  "nbf": 1517385849,
  "exp": 1517389749,
  "aio": "Y2NgYGt+6xjp02/t1/erTNy+LKVPa8dC4+/TP3xennmSm1+8+z4A",
  "amr": [ "pwd" ],
  "family_name": "Sandyrov",
  "given_name": "Andrej",
  "ipaddr": "88.119.194.198",
  "name": "Andrej Sandyrov",
  "oid": "83f1b61f-1e77-4ce5-85ad-c76bed5a1247",
  "onprem_sid": "S-1-5-21-1293440551-2949271503-1314497110-1132",
  "sub": "qX_OE8OkmVyYRXyI7chX4qqSWPyCQLVRI8CU_YtYOY8",
  "tid": "23afecaf-6440-44aa-a6f2-b6e38bd02ba9",
  "unique_name": "andrejs@synergy.lt",
  "upn": "andrejs@synergy.lt",
  "uti": "ZmsLjPCsLEqe3Kbp8qkDAA",
  "ver": "1.0" }
```

The following errors occur:

User not found for external login qX_OE8OkmVyYRXyI7chX4qqSWPyCQLVRI8CU_YtYOY8. Try to use auto-provisioning

...

Value is missing for 'email'










System.ArgumentException: Value is missing for 'email'

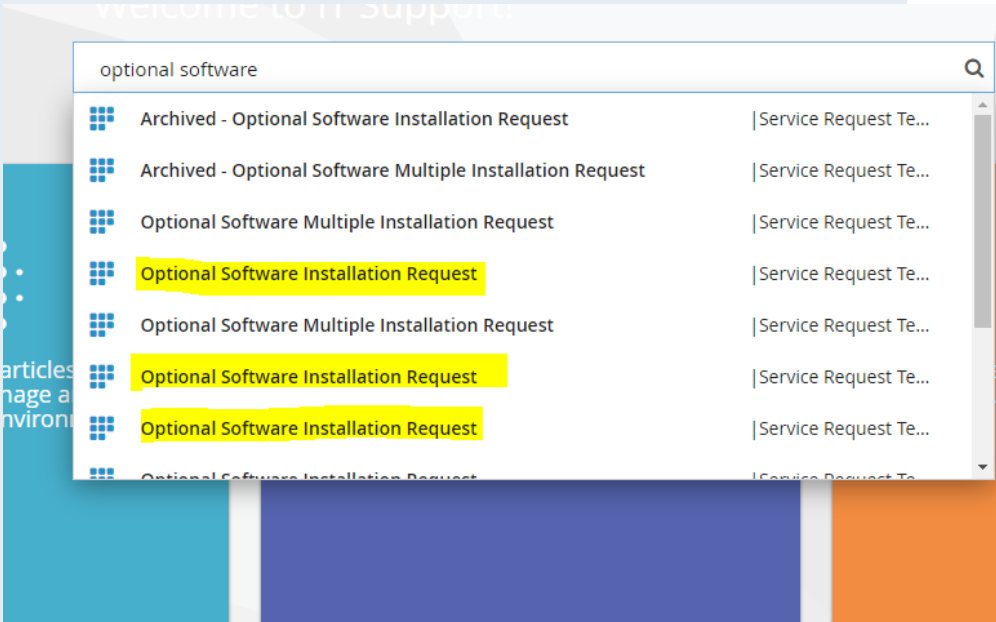
	?? at HEAT.Authentication.Sso.Oidc.OidcResultHandler.GetDictStringValue (IDictionary`2 dict, String ... Authentication failed unexpected error
Actual Results	Configuration to install Ivanti SM handler to use "upn" instead of "email."

6. Bug 341934

Issue	When choosing the "Download" option in Distribution Information of the report from the homepage dashboard or report list, download is not happening.
Expected Results	Reports should be downloaded from homepage dashboard or report list.

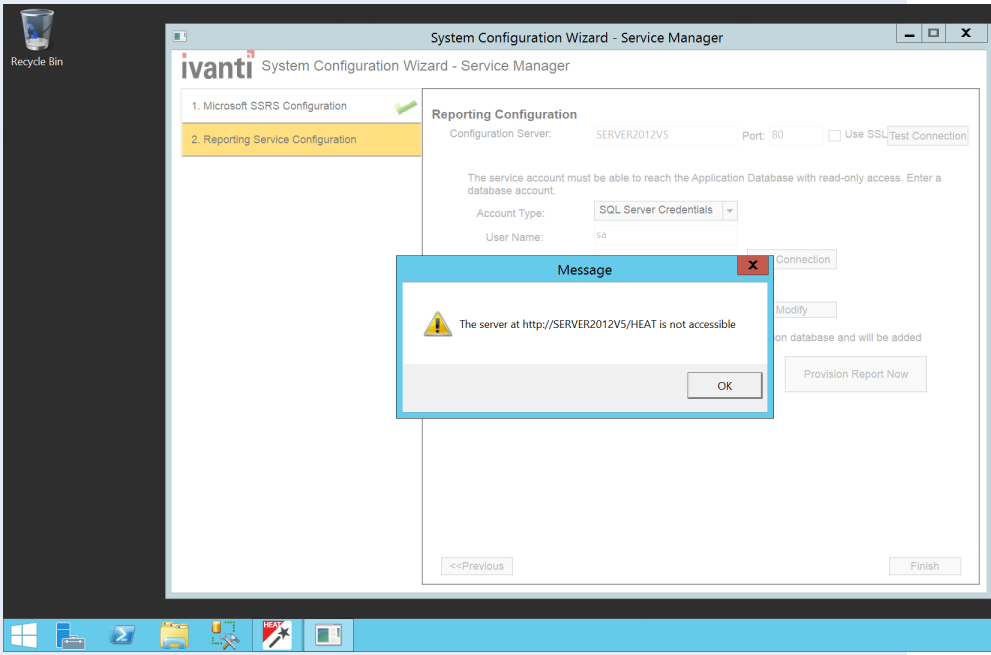
7. Bug 505677

Issue	<p>In self-service mobile, when searching with the string "optional software" in the home page search box, multiple records that are displayed for a single record and the request offerings are in the "Design" state.</p> <p>Steps to reproduce</p> <ol style="list-style-type: none"> 1. Log in to ISM in the "Self Service Mobile" role. 2. On the home page, search for "optional software". 																		
	<table> <thead> <tr> <th>Name</th><th>Summary</th><th>Status</th><th>Owner</th></tr> </thead> <tbody> <tr> <td> Optional Software Installation Request</td><td>Request software installation on-demand</td><td>Design</td><td>jb.ko</td></tr> <tr> <td> Optional Software Multiple Installation Request</td><td>Request multiple software installation on-demand</td><td>Design</td><td>jb.ko</td></tr> <tr> <td> Optional Software Uninstallation Request</td><td>Request Optional Software Uninstallation to DSM Server on-demand</td><td>Design</td><td>jb.ko</td></tr> </tbody> </table>			Name	Summary	Status	Owner	 Optional Software Installation Request	Request software installation on-demand	Design	jb.ko	 Optional Software Multiple Installation Request	Request multiple software installation on-demand	Design	jb.ko	 Optional Software Uninstallation Request	Request Optional Software Uninstallation to DSM Server on-demand	Design	jb.ko
Name	Summary	Status	Owner																
 Optional Software Installation Request	Request software installation on-demand	Design	jb.ko																
 Optional Software Multiple Installation Request	Request multiple software installation on-demand	Design	jb.ko																
 Optional Software Uninstallation Request	Request Optional Software Uninstallation to DSM Server on-demand	Design	jb.ko																

	
Actual Results	The system displays multiple records for a single request that is in design state.
Expected Results	A single record should get displayed for a single request that are in the "Published" state.

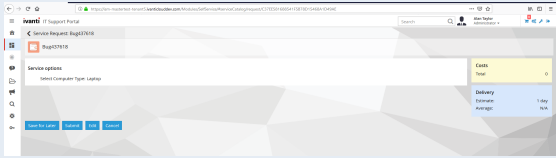
8. Bug 502699

Issue	SSRS configuration fails while trying to add the Provision report in SCW. Steps to reproduce 1. Configure the Reporting service configuration. 2. Click on "Provision report now".
--------------	--

	
Actual Results	Error message appears as shown above.
Expected Results	There should be no error and the URL should be accessible.

9. Bug 504840

Issue	<p>There is a browser compatibility issue (in Firefox and Microsoft Edge) for Self Service Mobile, in the UI price list/ Cost panel showing Zero(0).</p> <p>If a user selects an item, for example, Desktop, which is \$595 when he submits the request, the cost panel shows \$0. Hence, the severity must be kept to 2. In addition, customer bugs (which are linked) are getting blocked and hence, the priority should be set to 2.</p> <p>Steps to reproduce</p> <ol style="list-style-type: none"> 1. Login as an Admin. 2. Go to the Request Offerings workspace and import a .ROF file, publish, and save. 3. Switch to the Self Service (old UI) role. 4. Go to Service Catalog and open this offering. 5. Select Desktop type, then a Desktop and a Quantity. Notice that the price list looks correct for the selection.
--------------	--

	<ol style="list-style-type: none"> Without submitting or saving, go back and select Laptop type, a Laptop and a Quantity. Observe that the Costs panel is still correct and the originally selected Desktop item is removed. Switch to the Self Service Mobile UI. Go to Service Catalog and open this offering. Select Desktop type, then a Desktop and a Quantity. Observe that the price list looks correct for the selection. Without submitting or saving, go back and select Laptop type, a Laptop and a Quantity. Notice that the Costs panel retains the previously selected Desktop even though it should not.
Actual Results	<p>The Cost panel shows zero even if the product is selected.</p>  <p>This is working fine in Chrome, but not working in Firefox and Microsoft Edge.</p>
Expected Results	The Cost panel should display the correct value for the selected type.

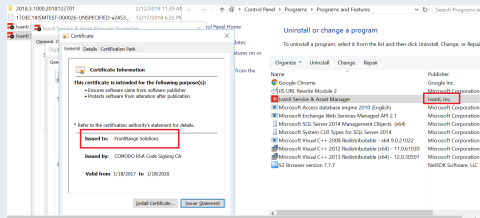
10. Bug 383101

Issue	<p>Japanese characters are shown as ? in the FRS_SurveyAnswer</p> <p>Steps to reproduce</p> <p>This error can be replicated in Demo 2017.3.1 and 2018.1 tenant: https://tenant-dev2.saasitpilot.com/.</p> <ol style="list-style-type: none"> Open FRS_SurveyAnswer# Go to field QuestionText or AnswerText Change type to unicode, Save.
Actual Results	Error: Unhandled system exception: The given key was not present in the dictionary.
Expected Results	Possibility to set this field to be unicode text.

11. Bug 359153

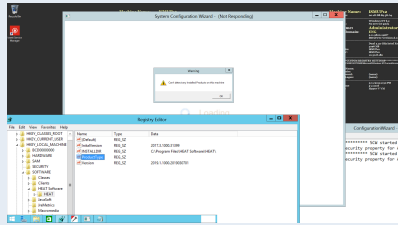
Issue	<p>Logout from the Self Service Mobile UI takes users to the ISM login instead of the Auth provider login.</p> <p>Steps to reproduce</p> <ol style="list-style-type: none"> 1. Set up the environment with SAML authentication. 2. Set up a logout URL as seen in the screenshot. 3. Log in as admin with the role of Self Service Mobile. 4. Log out later using the logout button.
Actual Results	Users are taken back to the ISM login page for only Self Service Mobile role.
Expected Results	Users should be taken back to the SAML login page.

12. Bug 508376

Issue	<p>The certificate issued for installer is "FrontRange Solution" and Publisher name is "Ivanti Inc." since the last couple of releases. The Windows certificate trust store never questioned the authenticity of the certificate earlier. However, somehow it is prompting the certificate trust question now on Windows OS like 2016, 2012 etc.</p> <p>Steps to reproduce</p> <ol style="list-style-type: none"> 1. Take the latest installer and install on vanilla OS (Win2016, 2012)
Actual Results	
Expected Results	Issue a new certificate to installer with "Ivanti Inc."
Workaround	Accept the certificate to add to MS trust store.

13. Bug 519086

Issue	If a user tries to directly upgrade from 2018.1.1 to 2019.1.0 or the latest version, the upgrade will fail.
--------------	---

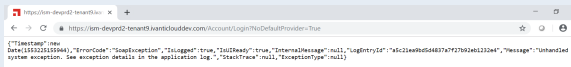
	<p>This is because SCW fails to launch the post installer update due to the missing registry key for ProductType. This entry should be retained during the upgrade, which is currently not working. 2018.1.1 build: 2018.1.1000.2018103001 @ 10/29/2018 2019.1.1 build: 2019.1.1000.2019030701</p> <p>The supported upgrade paths for 2018.1.1 to 2019.1.0 application version must be 2018.1.1 > 2018.3.1 > 2019.1.0.</p> <p>Steps to reproduce</p> <ol style="list-style-type: none"> 1. Upgrade the existing 2018.1.1 on-premise version to the 2019.1.0 on-premise version by skipping the 2018.3.1 upgrade path.
Actual Results	
Expected Results	<p>The product reg key must be created during an upgrade and SCW should launch without any error.</p>

14. Bug 522220

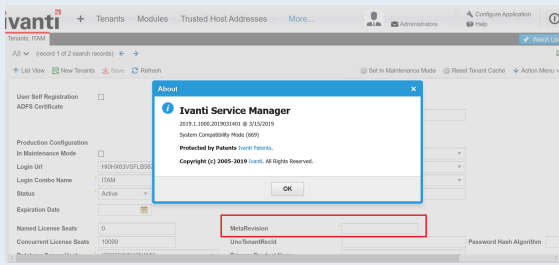
Issue	<p>Unable to create new CI due to the Asset Processor Configuration.</p> <p>After installing the GatewayDC(Discovery), Gateway CI is not getting generated and getting error message as "Unable to create new CI due to the Asset Processor configuration". This is can be found only on OOTB(IxM) on 2019.1 Builds Onwards.</p> <p>Steps to reproduce</p> <ol style="list-style-type: none"> 1. Pre-requisite: This issue can only be reproduced on OOTB(IxM). SO to reproduce OOTB(IxM) environment is required. 2. Login to the application. 3. Go to the Admin UI and download the GatewayDC/StandardGateway and install with proper credential on the above mentioned kind on tenants environment.
Actual Results	<p>Gateway is not getting created in under Gateway workSpace and Highlighted Error will comes in Message Queue Journal.</p>

Expected Results	-
------------------	---

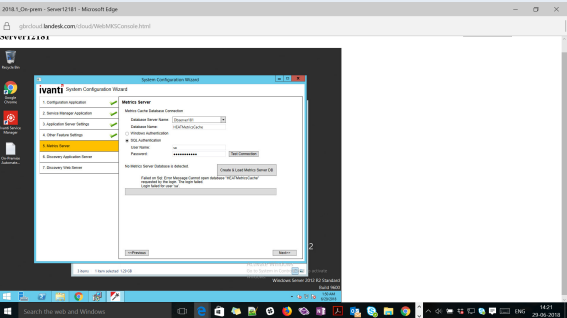
15. Bug 525479

Issue	<p>When Internal Services user is disabled in a tenant, then login page is not loading by throwing timestamp error.</p> <p>It is a regression issue as the 2018.3.1 environment login page is loading successfully if an Internal Services user is disabled. After 2019.1 deployment to FFT and NVD PLT landscapes where few customers login page is not loading by throwing the Timestamp Error. On Analyzing, ops team found Login "Internal Services" were disabled in those tenants. After enabling the login, they were able to login to the Tenant without any issues.</p> <p>Steps to reproduce</p> <ol style="list-style-type: none">1. Login to ISM as the Admin role.2. Open Employee workspace and search for "Internal Services" user.3. Disable "Internal Services" user and close the browser or try to logout.
Actual Results	<p>The system is throwing the Timestamp error while loading the login page.</p>  <p>A screenshot of a web browser window displaying a JSON error message. The URL bar shows 'https://sm-dept02-tenant@kamtcloud.com/account/Login?ICDefaultProvider=true'. The error message is: [{"timestamp": "Sun, 04/13/2020 15:04", "errorCode": "TimestampError", "isLogged": true, "isLoading": true, "internalMessage": null, "loginId": "xlc2awbds4867d7c70705d60220e4", "message": "Unhandled system exception. See exception details in the application log.", "status": "Fail", "exceptionType": null}].</p>
Expected Results	<p>After disabling "Internal Services" user, login page should be loaded properly without throwing any timestamp error.</p>
Workaround	<p>To work properly, we need to enable the "Internal Services" user.</p>

16. Bug 522214

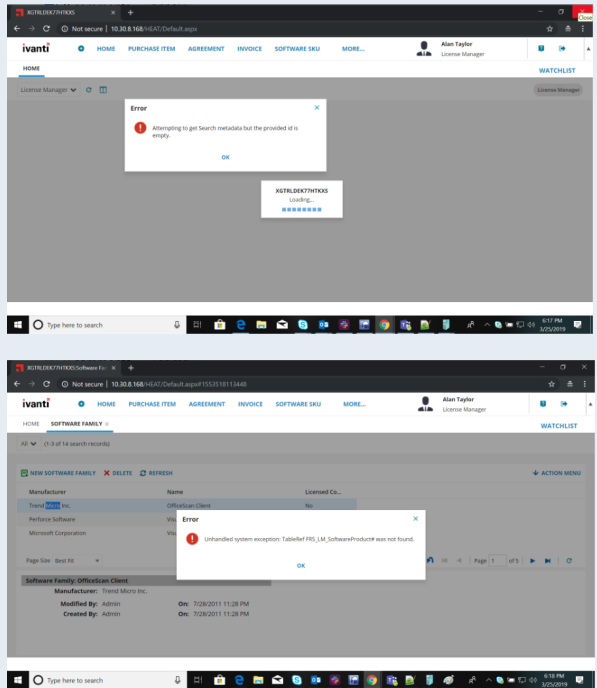
Issue	<p>After installation or upgrade of ISM/AM/IXM application, the metaRevision field is not updated. Regression: NO as it is observed in 2018.3.1 or an earlier version.</p> <p>Steps to reproduce</p> <ol style="list-style-type: none"> 1. Install & upgrade any of the above application 2. Check the MetaRevision version of the application tenant in configuration.
Actual Results	
Expected Results	<p>MetaRevision should be updated or should retain the old value (in case of no system table upgrade) as it is a mandatory field.</p>
Workaround	<p>User should manually enter "670" in this field and save it. This is a workaround only for 2019.1.</p>

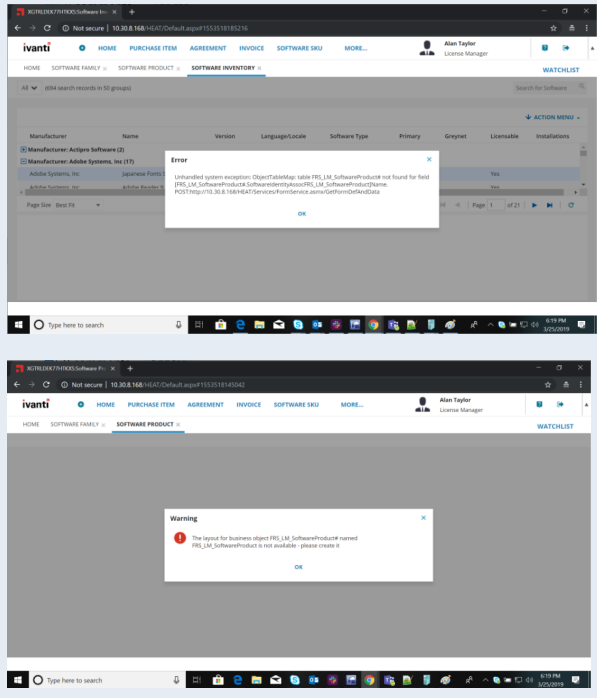
17. Bug 431449

Issue	<p>Version: 2018.1.1 On-premise</p> <p>OS: Windows 2016 SP1 & IIS version 10.0.14393.0</p> <p>Installation of Metric server for the first time fails with db connection error, however subsequent attempt of "recreate" works fine.</p>  <p>Steps to reproduce</p> <ol style="list-style-type: none"> 1. Install the latest 2018.1.1 build on Windows 2014 R2 or any OS. 2. Select the Metric Server configuration in SCW.
--------------	---

Actual Results	The application fails to create the Metric Server database after the "Create" action though the db test connection is successful. However, subsequent attempt on "recreate" works fine.
Expected Results	-

18. Bug 526262

Issue	<p>Upgraded ISM 2018.3.1 to 2019.1.0 and post upgrade accessing the below workspaces as LicenseManager role throws exception.</p> <p>Steps to reproduce</p> <p>Upgrade ISM 2018.3.1 to 2019.1.0.</p>
Actual Results	<p>LicenseManager home page fails to load.</p> <p>Accessing the Software Inventory, Software Product, Software Family and other workspaces as a LicenseManager throws error in UI.</p> 

<p>Expected Results</p>	 <p>The above mentioned modules should not be exposed to LicenseManager role.</p>
--------------------------------	---

19. Bug 485595

<p>Issue</p>	<p>The Sting "Self" is UNLOC shown under Self Service User - My Items > Benefits Package Claim.</p> <p>Steps to reproduce</p> <ol style="list-style-type: none"> 1. Log in to ISM and change the role to Self Service User. 2. Open the My Items workspace. 3. Select Benefits Package Claim. 4. Under Item Details, there is one unloc sting "Self" from "PATIENT INFORMATION".
<p>Actual Results</p>	<p>The Sting "Self" is UNLOC shown under Self Service User - My Items > Benefits Package Claim.</p>
<p>Expected Results</p>	<p>The UNLOC string should translated as "自我".</p>

20. Bug 235039

<p>Issue</p>	<p>Upgraded ISM 2018.3.1 to 2019.1.0 and post upgrade accessing the below workspaces as LicenseManager role throws exception.</p>
---------------------	---

	Steps to reproduce Upgrade ISM 2018.3.1 to 2019.1.0.
Actual Results	LicenseManager home page fails to load. Accessing the Software Inventory, Software Product, Software Family and other workspaces as a LicenseManager throws error in UI.
Expected Results	The above mentioned modules should not be exposed to LicenseManager role.

21. Bug 533210

Issue	2019.1 premise installer seems to silently exit or crash after installing one of the pre-req modules. Steps to reproduce <ol style="list-style-type: none"> 1. Run installer exe as an admin. 2. Click Install to installer pre-reqs. A dialog box will appear, "Extracting Ivanti Service Asset Manager.msi." 3. Follow the wizard to where you select SM / AM / both. 4. Select any installation type, click next, then again next, select Complete, click next, and then click install. Just after the VC 2013 redistributable x64 finishes installing the installer exits silently.
Actual Results	Just after the VC 2013 redistributable x64 finishes the installing process, the installer exits silently.
Expected Results	Installer should progress normally.
Workaround	Re-run the installer EXE.

22. Bug 576301

Issue	During Update System on Update Application Database in SCW, the system receives a notification that it was updated with visible errors. Example: Patch 'AuthenticationPrincipal' has 5 error(s) Error during metadata commit operation for seq = 12482: System.Exception: Nom de colonne non valide : 'GlobalId'.
Workaround	If a customer receives the error for GlobalID and/or AuthenticationPrincipal, then: <ol style="list-style-type: none"> 1. Close SCW.

2. Restore the Application DB back to 2018.3.1.
3. Go to the AdminUI and import the "GlobalID_Contract_Identity.MetadataPatch" package.
4. Re-launch SCW.
5. Re-validate and re-select upgrade. The customer should be able to upgrade ISM DB with no errors.

Optimally, the customer should run through the following steps so they do not have to wade through a failing upgrade and then have to restore the 2018.3.1 Application DB, thus saving possibly hours of time.

1. After installing 2019.1.0 and before walking through the SCW, launch AdminUI.
2. Import the "GlobalID_Contract_Identity.MetadataPatch" package.
3. Walk through SCW and the customer should be able to upgrade DB.

Troubleshooting

If you have problems with your installation or deployment, check this section first.

- "Error Messages" below
- "Software Problems" on page 233

Error Messages

- "Login Errors" below
- "Upgrade Errors" on page 227
- "Backup Error" on page 228
- "Database Migration Errors" on page 228
- "Microsoft SQL Execution Errors" on page 230
- "Update Key Not Found Warnings" on page 230
- "Workflow Warnings" on page 233

Login Errors

Error Message

```
Error upon executing commands: The following error occurred when authenticating with the
tenant <tenantUrl>.
Status: TenantNotFound
```

Possible Cause

The tenant that you specified is invalid.

Solution

Ensure that the tenant URL and tenant ID are valid.

Error Message

```
Error upon executing commands: The following error occurred when authenticating with the
tenant <tenantUrl>.
Status: AccessDenied
```

Possible Cause

You entered an invalid user name or password.

Solution

Ensure that the user name and password are valid.

Error Message

```
Error upon executing commands: The following error occurred when authenticating with the
tenant APPSERVER.
Status: InvalidRole
```

Possible Cause

You do not have administrator rights.

Solution

Ensure that you have administrator rights. See "About Roles" on page 42.

Error Message

```
Error upon executing commands: Could not establish trust relationship for the SSL/TLS secure
channel with authority '<IP_address>'.
```

Possible Cause

You did not connect to the Service and Asset Manager application server using HTTPS.

Solution

Configure the Service and Asset Manager application server to use SSL. See "Optional SSL Configuration" on page 139. Enter the URL for the Service and Asset Manager application server that is configured to use SSL.

Error Message

```
Failed to execute applyPatch: The remote server returned an unexpected response: (400) Bad
Request.
```

Possible Cause

The database version is not up to date.

Solution

If the system table upgrade fails, review the log files and fix any metadata issues. Then upgrade the system table.

Problem

Cannot view the login dialog box. A message says:

Please use your subdomain when accessing the application, for example `https://yourname.saas.heatsoftware.com`

Possible Cause

The web.config file parameter "RequireTenantIdInURL" value is set to true.

Solution

1. Go to C:\Program Files\HEAT Software\HEAT\AppServer\ and open the web.config file.
2. Search for the parameter "RequireTenantIdInURL" and change its value to false.
3. Save and close the web.config file.

Upgrade Errors

Problem

After upgrading to the latest version of Service and Asset Manager, the list of tenants in the Operations Console is empty.

Possible Cause

During the upgrade, the system updated the connection strings for the landscape with the incorrect name for the data source.

Solution

In the Operations Console, edit each landscape to update the data source to the correct database server name. See "Upgrading Service and Asset Manager from an Earlier Release" on page 166 for more information on how to do this.

Error Message

Failed to execute applyPatch: The request channel timed out while waiting for a reply after 00:59:59.7741622. Increase the timeout value passed to the call to request or increase the SendTimeout value on the binding. The time allotted to this operation may have been a portion of a longer timeout.

Possible Cause

By default, the upgrade tool is set to wait for one hour for a response from the Service and Asset Manager application server. This message indicates that the Service and Asset Manager application server is still applying the patch or package. The patch can be completed at any time.

Solution

Check the status of the upgrade tool later by looking at the patch log in the Configuration Database.

Backup Error

Error Message

No database backup location specified in configuration database. Please contact support.
Backup failed for Server 'db_server'.

Possible Cause

- The backup location is not set in the configuration database.
- The backup failed to execute because of permissions issues.

Solution

Ensure that you have set the backup location and ensure that you have the correct permissions.

Database Migration Errors

Error Message

Error during metadata commit operation: System.Exception: The following errors were encountered when synchronizing the schema....:

Possible Cause

This indicates a serious problem in business object metadata and is a synchronization schema error. The system cannot synchronize the database schema change with the business object definition. If you get this error, the system usually stops upgrading the metadata.

Solution

If this happens in your production environment, restore the database from a backup that was made before the upgrade. Then contact Ivanti support so that they can look into the error. See "How to Contact Us" on page 7.

Error Message

```
Error during metadata commit operation: DataLayer.SaaSdbException:  
Invalid object name 'Frs_ITFM_Account_Status'. --->  
System.Data.SqlClient.SqlException: Invalid object name 'Frs_ITFM_  
Account_Status'.
```

Possible Cause

Part of the database is corrupt.

Solution

Contact Ivanti Software support. See "How to Contact Us" on page 7. They may suggest that you restore the database from a backup that was made before the upgrade.

Error Message

```
Error during metadata commit operation:  
System.Reflection.TargetInvocationException: Exception has been  
thrown by the target of an invocation. --->  
System.NullReferenceException: Object reference not set to an  
instance of an object.
```

Possible Cause

Part of the database is corrupt.

Solution

Contact Ivanti Software support. See "How to Contact Us" on page 7. They may suggest that you restore the database from a backup that was made before the upgrade.

Microsoft SQL Execution Errors

Error Message

```
An error occurred when applying patch named <some_filename>.sql in
package <some_package>.MetadataPackage to tenant <tenantUrl>.
Unable to execute SQL due to Invalid column name 'IPCMUrlPort'.
update FRS_IPCM_Integration set IPCMUrlPort = 2323 where IPCMUrlPort
is null
Unable to execute SQL due to Invalid column name 'IPCMUrl'.
update FRS_IPCM_Integration set IPCMUrl = 'http://' + IPCMServerHost
+ ':' + convert(varchar(6), IPCMUrlPort) where IPCMUrl is null and
IPCMServerHost is not null
```

Possible Cause

An embedded Microsoft SQL statement is corrupt.

Solution

Review the Microsoft SQL statements.

Update Key Not Found Warnings

Error Message – Business Object

```
Error during metadata update operation. MetadataType: BusinessObject,
ID: Frs_AuthenticationProvider#
SaaS.StandardizedMetadata.UpdateKeyNotFoundException: Update key not
found: key = Rel2s
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement
element, XElement differences)
at DataLayer.MetadataPatch.ApplyGroupedActions(IMetadataProvider
provider, ISessionContext sessionContext, IEnumerable`1
definitionGroup) in
c:\depot\Eng\SaaS\main\Platform\AppServer\MetadataServices\MetadataPa
tch.cs:line 1034
```

Possible Cause

There is a problem updating the metadata and the system did not update the business object.

Solution

Review the business object to make sure it was updated.

Error Message – Form

```
Error during metadata update operation. MetadataType: Form, ID:
Task.WorkOrder System.Exception: Update key not found: key = Details
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement
element, XElement differences) in
c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensio
ns.cs:line 1377
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement
element, XElement differences) in
c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensio
ns.cs:line 1359
at DataLayer.MetadataPatch.ApplyGroupedActions(IMetadataProvider
provider, ISessionContext sessionContext, IEnumerable`1
definitionGroup) in
c:\depot\Eng\SaaS\main\Platform\AppServer\MetadataServices\MetadataPa
tch.cs:line 1016
```

Error Message – Dashboard

```
Error during metadata update operation. MetadataType: Dashboard, ID:
8e2cce05-c593-4545-bf4d-5f719a9bd5a5 System.Exception: Update key not
found: key = OLA Target Compliance ( e94a602f-959e-4cf1-9c07-
be4d5eb0da68 )
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement
element, XElement differences) in
c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensio
ns.cs:line 1377
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement
element, XElement differences) in
c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensio
ns.cs:line 1359
at DataLayer.MetadataPatch.ApplyGroupedActions(IMetadataProvider
provider, ISessionContext sessionContext, IEnumerable`1
definitionGroup) in
c:\depot\Eng\SaaS\main\Platform\AppServer\MetadataServices\MetadataPa
tch.cs:line 1016
```

Error Message – Validation Data

```
Error during metadata update operation. MetadataType: ValidationData,
ID: Justification# System.Exception: Update key not found: key =
Justification#_culture#pt-BR
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement
element, XElement differences) in
c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensio
ns.cs:line 1377
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement
element, XElement differences) in
c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensio
ns.cs:line 1359
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement
element, XElement differences) in
c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensio
ns.cs:line 1359
at DataLayer.MetadataPatch.ApplyGroupedActions(IMetadataProvider
provider, ISessionContext sessionContext, IEnumerable`1
definitionGroup) in
c:\depot\Eng\SaaS\main\Platform\AppServer\MetadataServices\MetadataPa
tch.cs:line 1016
```

Error Message – Rule

```
Error during metadata update operation. MetadataType: Rule, ID:
Incident# System.Collections.Generic.KeyNotFoundException: The given
key was not present in the dictionary.
at System.Collections.Generic.Dictionary`2.get_Item(TKey key)
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement
element, XElement differences) in
c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensio
ns.cs:line 1386
at SaaS.StandardizedMetadata.MetadataExtensions.Patch(XElement
element, XElement differences) in
c:\depot\Eng\SaaS\main\Platform\StandardizedMetadata\MetadataExtensio
ns.cs:line 1359
at DataLayer.MetadataPatch.ApplyGroupedActions(IMetadataProvider
provider, ISessionContext sessionContext, IEnumerable`1
definitionGroup) in
c:\depot\Eng\SaaS\main\Platform\AppServer\MetadataServices\MetadataPa
tch.cs:line 1016
```

Possible Cause

There is a problem updating the metadata.

Solution

You do not need to do anything.

Workflow Warnings

Error Messages

```
Error during metadata delete operation. MetadataType: workflow, ID:
69d31c7248b54f92bc1bffa415cd29e0f System.Exception: Could not
deactivate workflow definition RecId:
69d31c7248b54f92bc1bffa415cd29e0f ---> System.Exception: Error
updating existing active workflow definition to inactive, RecId
69d31c7248b54f92bc1bffa415cd29e0f
at SaaS.WebUI.WorkflowMetadataServices.WorkflowMetadataUpdate.Delete
(MetadataType metadataType, String id) in
c:\depot\Eng\SaaS\main\Platform\AppServer\BPE\src\workflowMetadataSer
vices.cs:line 409
Error during metadata insert operation. MetadataType: workflow, ID:
871d9466c4754fa19ffb03de179cd057 System.Exception: Inactive
definition exists with the same RecId: Name:LDAP Sync_LC_
133k134k135k13k14k15k16k17k18k19k, ObjectType:ScheduleEntry,
Definition RecId 871d9466c4754fa19ffb03de179cd057 at
SaaS.WebUI.WorkflowMetadataServices.WorkflowMetadataUpdate.CreateWork
flowDefinition(String name, String objectType, String defRecId,
String typeRecId, XElement workflow) at
SaaS.WebUI.WorkflowMetadataServices.WorkflowMetadataUpdate.Insert
(MetadataType metadataType, XElement workflow) at
SaaS.StandardizedMetadata.MetadataProvidersContainer.Insert
(MetadataType metadataType, XElement definition) at
DataLayer.MetadataPatch.ApplyGroupedActions(IMetadataProvider
provider, ISessionContext sessionContext, IEnumerable`1
definitionGroup)
```

Possible Cause

There is a problem updating the workflows.

Solution

You do not need to do anything.

Software Problems

- "Discovery cannot detect assets on the network." on the next page
- "System cannot search." on the next page
- "The Service and Asset Manager demo database does not load properly." on page 235
- "Web servers do not work correctly." on page 235
- "Provision report now returns an exception: Cannot Decrypt the Symmetric Key." on page 235

- "Dashboard and report controls (such as charting, pivoting, and copy/paste) and the Service Catalog attachment control do not work." on page 236
- "Cannot download or edit reports in Chrome." on page 236
- "Cannot download or edit reports in Firefox." on page 236
- "Cannot download files or run controls in Internet Explorer." on page 237
- "Cannot open websites in Internet Explorer." on page 237
- "Logging into a tenant using Internet Explorer fails. " on page 237
- "Unable to use integrated components, such as Voice." on page 238
- Application redirects the user from <http://localhost/HEAT> to <https://localhost> on the machine where SSL is not setup.

Problem

Discovery cannot detect assets on the network.

Possible Causes

- Service Center Configuration Manager (SCCM) service is stuck in starting mode.
- You are using a domain account for running all Service and Asset Manager services but the domain account has insufficient rights.

Solution

Use your local system account and restart Service and Asset Manager.

Problem

System cannot search.

Possible Cause

Full-text search is disabled.

Solution

Enable full-text search. See "Enabling Full-Text Search" on page 52.

Problem

The Service and Asset Manager demo database does not load properly.

Possible Cause

Full-text search is disabled.

Solution

Enable full-text search. See "Enabling Full-Text Search" on page 52.

Problem

Web servers do not work correctly.

Possible Cause

In multi-server environments, each Service and Asset Manager web server must meet the system requirements.

Solution

Refer to the *System Requirements and Compatibility Matrix for Service and Asset Manager* for more information.

Problem

Provision report now returns an exception: **Cannot Decrypt the Symmetric Key**.

Possible Cause

The Service and Asset Manager reporting server cannot use the symmetric key to access the data from the report server database.

Solution

1. Click **OK**, but do not close the System Configuration Wizard.
2. Start the Reporting Services Configuration Manager and connect to your Microsoft SRSS instance.
3. Select **Encryption Keys** from the list in the left panel.
4. Click **Delete** and then click **Yes** at the confirmation message.
5. Return to the wizard and click **Provision Report Now**.

Problem

Dashboard and report controls (such as charting, pivoting, and copy/paste) and the Service Catalog attachment control do not work.

Possible Cause

Browser does not have, or does not support, Adobe Flash.

Solution

- Install Adobe Flash. Go to <https://get.adobe.com/flashplayer/>.
- If your current browser does not support Adobe Flash, upgrade the browser.

Problem

Cannot download or edit reports in Chrome.

Possible Cause

The Chrome ClickOnce extension is not installed.

Solution

Install the ClickOnce extension for Chrome. Navigate to <https://chrome.google.com/webstore/detail/eeifaoomkminpbbeebjdmdojbhmagncnl#> and download the extension.

Problem

Cannot download or edit reports in Firefox.

Possible Cause

The Firefox Microsoft .NET framework assistant extension is not installed.

Solution

Install the Microsoft .NET framework assistant extension. Navigate to <https://addons.mozilla.org/en-US/firefox/addon/9449> to download the extension.

Problem

Cannot download files or run controls in Internet Explorer.

Possible Cause

Scripting is disabled.

Solution

Set properties in Internet Explorer as follows:

1. Go to the **Tools > Internet Options > Security > Custom level** page.
2. Set the following options to **enable**:
 - Run ActiveX controls and plug-ins
 - File download
 - Scripting > Active scripting

Problem

Cannot open websites in Internet Explorer.

Possible Cause

You have not set Service and Asset Manager to be a trusted site.

Solution

Set properties in Internet Explorer as follows:

1. Go to the **Tools > Internet Options > Security** page.
2. Highlight **Trusted sites** and click **Sites**.
3. Click **Add**.

Problem

Logging into a tenant using Internet Explorer fails.

Internet Explorer displays this message: **You cannot login to the system now. Please contact your administrator. Additional information is available in the logs.**

Possible Cause

Internet Explorer does not accept cookies if the host name of the DNS server or the server NetBIOS names contain an underscore '_'.

Solution

- Change the host name of your DNS server or its NetBIOS names so they no longer contain an underscore '_'.
- Use a Chrome or Firefox browser.

Problem

Unable to use integrated components, such as Voice.

Possible Cause

You must use the Microsoft Windows operating system when you use integrated components.

Solution

Change to the Microsoft Windows operating system. Refer to the *System Requirements and Compatibility Matrix for Service and Asset Manager* for more information.

Problem

When trying to access the Configuration Database, the application redirects the user from `http://localhost/HEAT` to `https://localhost` on the machine where SSL is not setup.

Possible Cause

There is a known limitation in the 2018.3.1 release with respect to FedRamp requirements related to the URL redirect configuration.

Solution

To resolve this, there is a need to update an entry in the `web.config` file. Set the parameter highlighted below to 'false' and restart IIS. Once the process is completed, try to access **Configuration Database**.

```
</rule>
<rule name="HTTP to HTTPS redirect" stopProcessing="true">
  <match url="(.*)">
  </match>
```

```
<conditions>
<add input="{SERVER_NAME}" pattern="^localhost$" negate="true">
</add>
<add input="{HTTPS}" pattern="off" ignoreCase="true">
</add>
</conditions>
<action type="Redirect" url="https://{HTTP_HOST}/{R:1}" redirectType="Permanent">
</action>
</rule>
```