Information Builders

iWay

iWay Sentinel User's Guide

Version 1.2

June 21, 2019

Contents

Preface

This documentation describes how to install, configure, and use iWay Sentinel. Sentinel provides a centralized solution to monitor and manage the health of your enterprise assets. It is intended for administrators and developers who deploy iWay Integration Applications (iIAs) in a distributed environment.

How This Manual Is Organized

This manual includes the following chapters:

	Chapter/Appendix	Contents
1	Introducing iWay Sentinel	Provides an introduction to iWay Sentinel.
2	Installing iWay Sentinel Components	Provides prerequisites and describes how to install iWay Sentinel components.
3	Managing and Monitoring Servers	Describes how to manage and monitor servers using the Single Pane of Glass interface for iWay Sentinel.
4	Managing and Monitoring Applications	Describes how to manage and monitor applications using iWay Sentinel.
5	Managing and Monitoring Channels	Describes how to manage and monitor channels using iWay Sentinel.
6	Administration	Describes how to enable the administration of iWay Sentinel, and the remote servers and applications that are being managed through an array of scriptable and scheduled tasks.
7	SSL Configuration	Describes how to configure Sentinel and Envoy security for SSL.
A	Sentinel Configuration Properties	Describes Sentinel configuration properties.
B	General Notes Related to the User Interface	Provides general notes related to the Single Pane of Glass (SPOG) Sentinel user interface.
C	iWay Sentinel Scripting	Describes how to develop scripts for use with iWay Sentinel.

Documentation Conventions

The following table describes the documentation conventions that are used in this manual.

Convention	Description
THIS TYPEFACE or this typeface	Denotes syntax that you must enter exactly as shown.
this typeface	Represents a placeholder (or variable), a cross-reference, or an important term. It may also indicate a button, menu item, or dialog box option that you can click or select.
underscore	Indicates a default setting.
Key + Key	Indicates keys that you must press simultaneously.
{ }	Indicates two or three choices. Type one of them, not the braces.
|	Separates mutually exclusive choices in syntax. Type one of them, not the symbol.
...	Indicates that you can enter a parameter multiple times. Type only the parameter, not the ellipsis (...).
. . .	Indicates that there are (or could be) intervening or additional commands.

Related Publications

Visit our Technical Documentation Library at *http://documentation.informationbuilders.com*. You can also contact the Publications Order Department at (800) 969-4636.

Customer Support

Do you have any questions about this product?

Join the Focal Point community. Focal Point is our online developer center and more than a message board. It is an interactive network of more than 3,000 developers from almost every profession and industry, collaborating on solutions and sharing tips and techniques. Access Focal Point at *http://forums.informationbuilders.com/eve/forums*.

You can also access support services electronically, 24 hours a day, with InfoResponse Online. InfoResponse Online is accessible through our website, *http://www.informationbuilders.com*. It connects you to the tracking system and known-problem database at the Information Builders support center. Registered users can open, update, and view the status of cases in the tracking system and read descriptions of reported software issues. New users can register immediately for this service. The technical support section of *http://www.informationbuilders.com* also provides usage techniques, diagnostic tips, and answers to frequently asked questions.

Call Information Builders Customer Support Services (CSS) at (800) 736-6130 or (212) 736-6130. Customer Support Consultants are available Monday through Friday between 8:00 a.m. and 8:00 p.m. EST to address all your questions. Information Builders consultants can also give you general guidance regarding product capabilities and documentation. Please be ready to provide your six-digit site code number (*xxxx.xx*) when you call.

To learn about the full range of available support services, ask your Information Builders representative about InfoResponse Online, or call (800) 969-INFO.

Help Us to Serve You Better

To help our consultants answer your questions effectively, be prepared to provide specifications and sample files and to answer questions about errors and problems.

The following tables list the environment information our consultants require.

Platform	
Operating System	
OS Version	
JVM Vendor	
JVM Version	

The following table lists the deployment information our consultants require.

Adapter Deployment	For example, JCA, Business Services Provider, iWay Service Manager
Container	For example, WebSphere

Version	
Enterprise Information System (EIS) - if any	
EIS Release Level	
EIS Service Pack	
EIS Platform	

The following table lists iWay-related information needed by our consultants.

iWay Adapter	
iWay Release Level	
iWay Patch	

The following table lists additional questions to help us serve you better.

Request/Question	Error/Problem Details or Information
Did the problem arise through a service or event?	
Provide usage scenarios or summarize the application that produces the problem.	
When did the problem start?	
Can you reproduce this problem consistently?	
Describe the problem.	
Describe the steps to reproduce the problem.	
Specify the error message(s).	

Request/Question	Error/Problem Details or Information
Any change in the application environment: software configuration, EIS/database configuration, application, and so forth?	
Under what circumstance does the problem *not* occur?	

The following is a list of error/problem files that might be applicable.

- ❑ Input documents (XML instance, XML schema, non-XML documents)
- ❑ Transformation files
- ❑ Error screen shots
- ❑ Error output files
- ❑ Trace files
- ❑ Service Manager package to reproduce problem
- ❑ Custom functions and agents in use
- ❑ Diagnostic Zip
- ❑ Transaction log

For information on tracing, see the *iWay Service Manager User's Guide*.

User Feedback

In an effort to produce effective documentation, the Technical Content Management staff welcomes your opinions regarding this document. Please use the Reader Comments form at the end of this document to communicate your feedback to us or to suggest changes that will support improvements to our documentation. You can also contact us through our website, *http://documentation.informationbuilders.com/connections.asp*.

Thank you, in advance, for your comments.

Information Builders Consulting and Training

Interested in training? Information Builders Education Department offers a wide variety of training courses for this and other Information Builders products.

For information on course descriptions, locations, and dates, or to register for classes, visit our website (*http://education.informationbuilders.com*) or call (800) 969-INFO to speak to an Education Representative.

Chapter 1

Introducing iWay Sentinel

This section provides an introduction to iWay Sentinel.

In this chapter:

iWay Sentinel Overview

iWay Sentinel uses Single Pane of Glass (SPOG) as a web-based interface to manage and monitor iWay Service Manager (iSM) instances, which are installed across an enterprise. Sentinel provides capabilities to detect failures in server status, message transmission, and performance issues across one or more instances of iSM. iWay Sentinel consists of two major components:

- Sentinel
- Envoy

Sentinel is the core component of the application, which can be accessed from the browser. Envoy is the component that runs on top of iSM and provides the connectivity between Sentinel and iSM.

Sentinel provides monitoring functions, such as server connectivity status, health status for servers, applications, and channels based their success, failures, and performance. Sentinel also assigns the health status to servers, applications, and channels by comparing the health statistics among them based on a customizable algorithm. Through Sentinel, users can start and stop the servers, applications, channels, and change properties. In addition, Sentinel enables users to monitor the performance of JVM at the memory and thread level for the server and component functions.

Sentinel simplifies management functionality, such as deploying applications, installing patches, and modifying the packages and components of iWay applications across multiple iWay servers. Servers and applications can be categorized in different groups, and management functions can be executed on top of them. You can also schedule specific tasks to execute at different days and times of the week as required. Sentinel allows users to view the status and queues related to the completed, ongoing, and pending status for the tasks.

Sentinel includes a repository to store iWay artifacts, such as applications, packages, and other deployable components. A key feature of SPOG is the ability to manage functions, which can be executed using Java scripts. Automated scripts combined with scheduling functionality allows enterprises to carry out their deployment functionality in the background, without human intervention.

Key Terms

This section lists and describes key terms that you should be familiar with when using the Single Pane of Glass (SPOG) and Sentinel.

- **Sentinel.** A standalone server that provides management and monitoring services across multiple iSM instances throughout the enterprise.
- **Single Pane of Glass (SPOG).** A web application interface to Sentinel that provides users with the ability to manage and monitor iWay Service Manager (iSM) in an enterprise environment.
- **Configuration.** An arrangement of descriptive ISM metadata is used to instantiate iSM. In Sentinel, configurations are packaged as .ita files, which are also known as templates.
- **Server.** A single instance of iSM running the master configuration (for example, base).
- **Application.** A deployed iSM runtime configuration, also known as an iWay Integration Application (iIA).
- **Envoy.** An iSM extension running on a Server, which provides monitoring and management services to Sentinel.
- **Package.** A .zip file containing a set of resources including iSM descriptive metadata and/or file artifacts.
- **User.** A person who interacts with SPOG.
- **Server Task.** A Sentinel task that offers services (subprograms). This is typically a batch task or asynchronous task.
- **Health Model.** An algorithm designed to detect server issues that could eventually result in service disruptions.
- **Ghosts.** Objects that once existed, have disappeared, but still exist in the Sentinel graph.
- **Zombies.** An iSM server or application that cannot respond to requests for status and for which Sentinel does not have a corresponding history to classify as severe health.

Quick Start Guide

This section provides a quick start guide that you can use to implement iWay Sentinel in your enterprise.

1. Install Sentinel. For more information, see *Installing Sentinel* on page 27.
2. Install iWay 8 and Envoy. For more information, see *Installing Envoy* on page 17.
3. Login to Sentinel
   a. Create users and assign passwords as required. For more information, see *Administration* on page 67.
   b. Register servers. For more information, see *Registering a Server* on page 35.
4. Import applications, packages, and other files into the Sentinel repository. For more information, see *Managing and Monitoring Applications* on page 53.
5. Create groups with servers, and applications as required for your enterprise. For more information, see *Configuring Groups* on page 67.
6. Deploy applications and packages. For more information, see *Managing and Monitoring Applications* on page 53.
   a. If required, schedule the management activities accordingly. For more information, see *Configuring Tasks* on page 70.
7. Start monitoring your servers, applications, and channels.
8. On a daily basis:
   a. Monitor the health status for servers, applications, and channels as required.
   b. Check whether the scheduled tasks are in progress or not. If tasks are not going to be completed, then cancel or reschedule the tasks.
   c. Check worker threads, JVM, server performance, and so on.
9. On a weekly basis:
   a. Check whether the health calculations are meaningful for the enterprise.
   b. Fine tune the weights being used for the health formula as required.
   c. Check whether the schedule for weekly tasks should be adjusted.
10. On a monthly basis:
    a. Check the artifacts in the repository to determine whether they should be stored or removed.
11. Ad-hoc schedule:
    a. If a server is not required to be monitored (for example, it is shut down or in another state that cannot be monitored), then remove this server from Sentinel monitoring.

Chapter 2

Installing iWay Sentinel Components

This section provides prerequisites and describes how to install iWay Sentinel components.

In this chapter:

iWay Sentinel Prerequisites

This section lists prerequisites for iWay Sentinel.

- The Single Pane of Glass (SPOG) web-based interface currently supports the Google Chrome web browser. No other web browsers are supported at this time.
- It is recommended for iWay Sentinel to be installed on a system with 16GB of RAM to ensure smooth performance when monitoring a large number of remote servers.
- iSM requires Java Version 1.7.0_55 or higher. If the machine is running Java JRE and not JDK, then it is required for the tools.jar file to be added to the /lib directory where JRE is installed.
- The remote start, stop, and restart operations on a server require an installation of PsService, which can be downloaded from the following website:

  http://technet.microsoft.com/en-us/sysinternals/bb897542.aspx

  The .zip file that is downloaded must be unzipped into the execution path directory (for example, \Windows\system32).

Installing Envoy

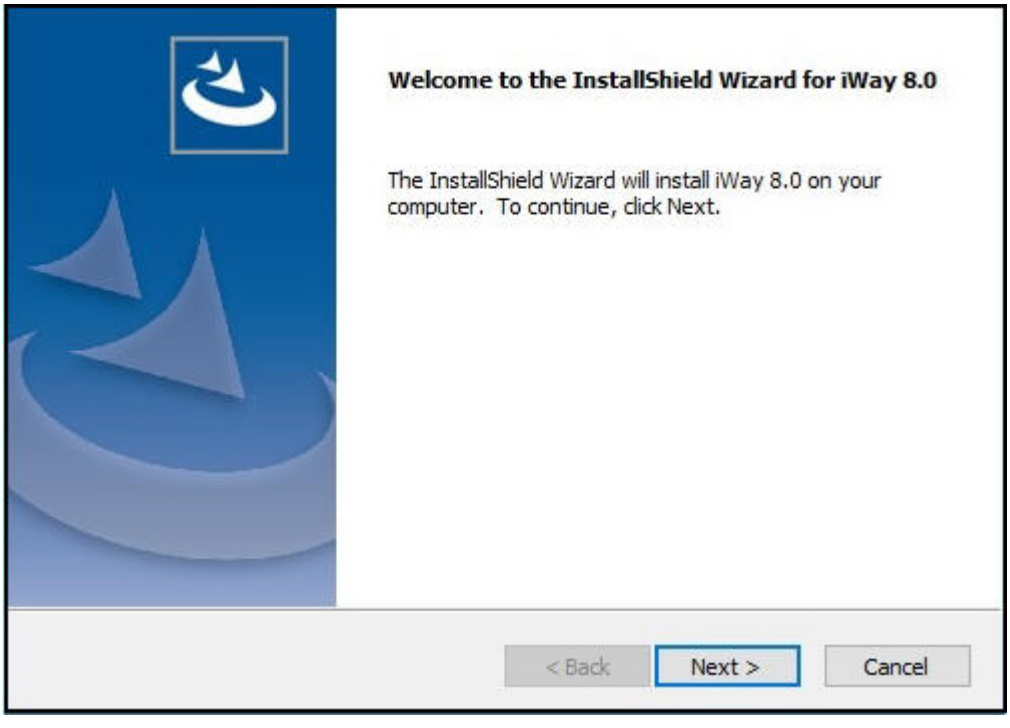
The iWay installation provides an additional option to install Envoy and register the iSM instance being installed for iWay Sentinel monitoring (remote management). Envoy is required for communication with iWay Sentinel.

Procedure: How to Install iWay Service Manager With Envoy for iWay Sentinel Monitoring

You must be an administrator for the local machine to run the installation.

1. Start the installation by executing the iway80.exe installation program.

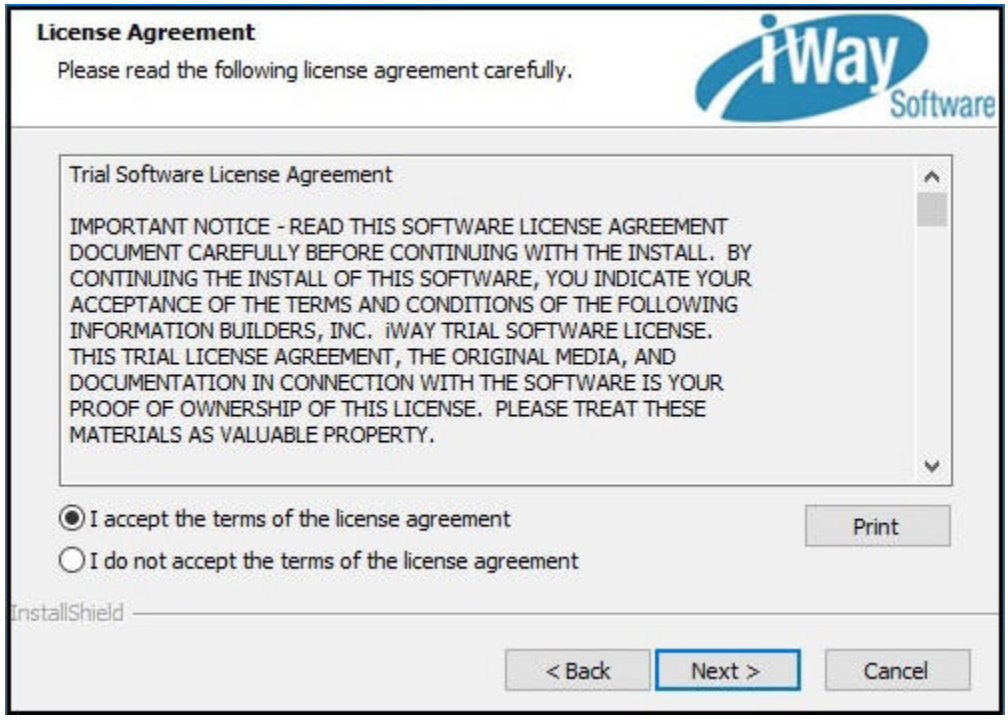
   The installation begins by temporarily copying files and analyzing your environment. This may take some time. When this process completes, the Welcome window opens, as shown in the following image.



Note: If you receive an error, ensure you are installing as an administrator and there is at least 2 GB of free space on your operating system drive.

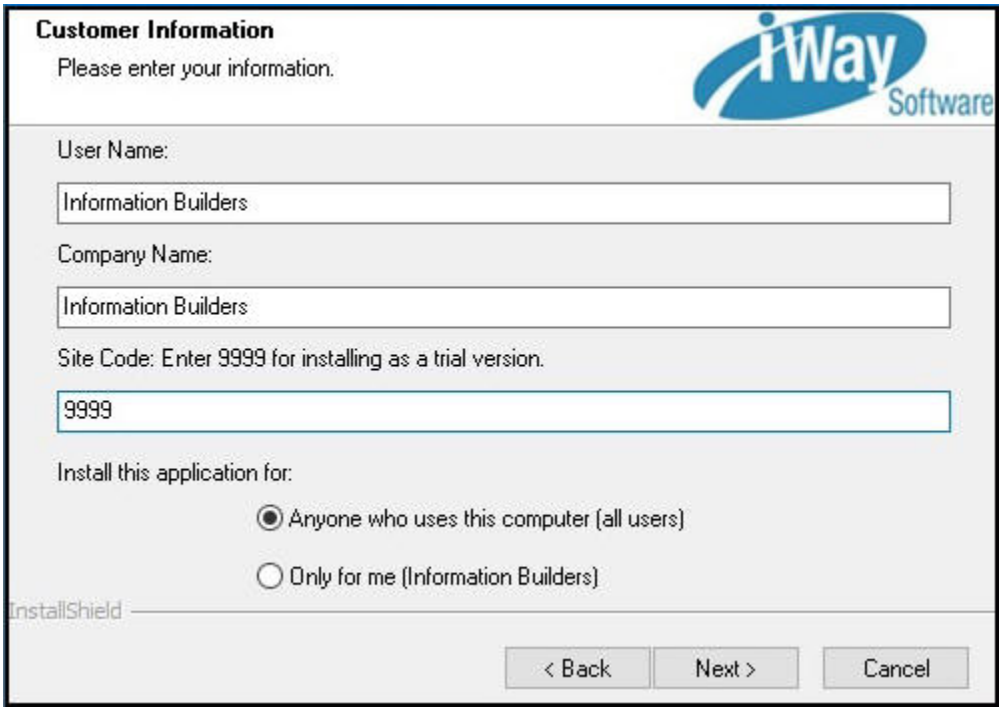
2. Click *Next*.

   The License Agreement window opens, as shown in the following image.



3. Review the information, and select the appropriate option. Click *Next* if you agree to the terms.

The Customer Information window opens, as shown in the following image.

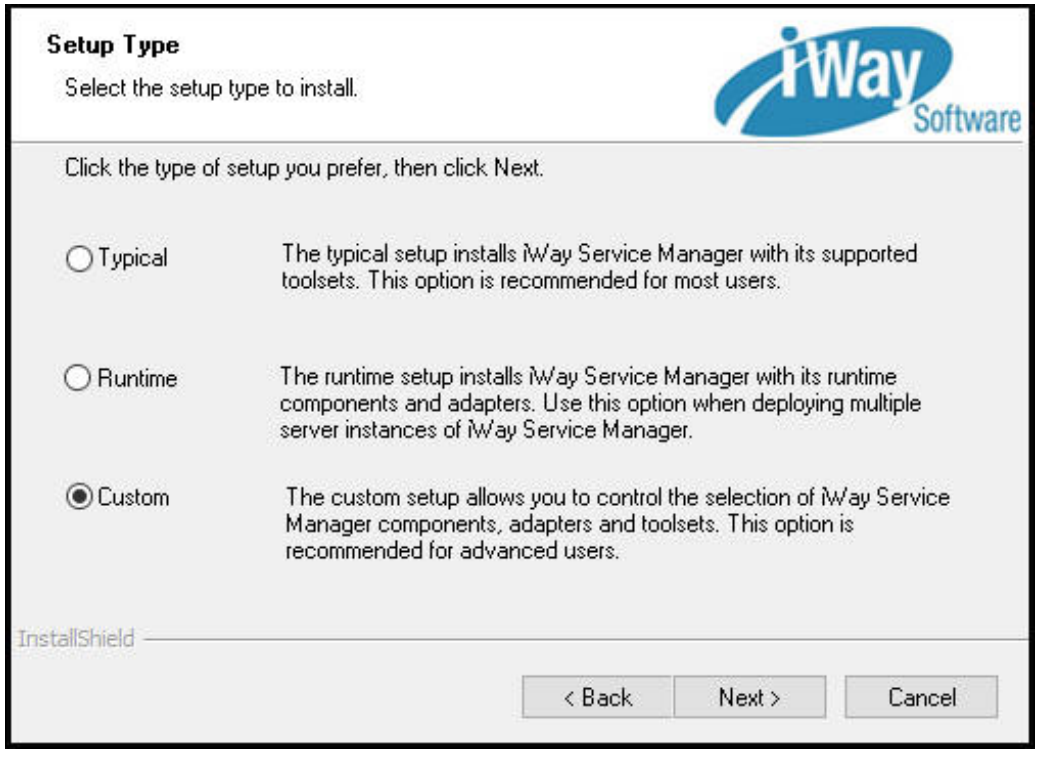


4. Provide your *User Name*, *Company Name*, and *Site Code*.

   Important: The site code is a unique company identifier associated with a specific machine. Be sure to enter a valid and accurate site code in this step because this entry is used when generating your permanent license during the registration process. If you need assistance with the site code, contact your iWay Software sales representative.

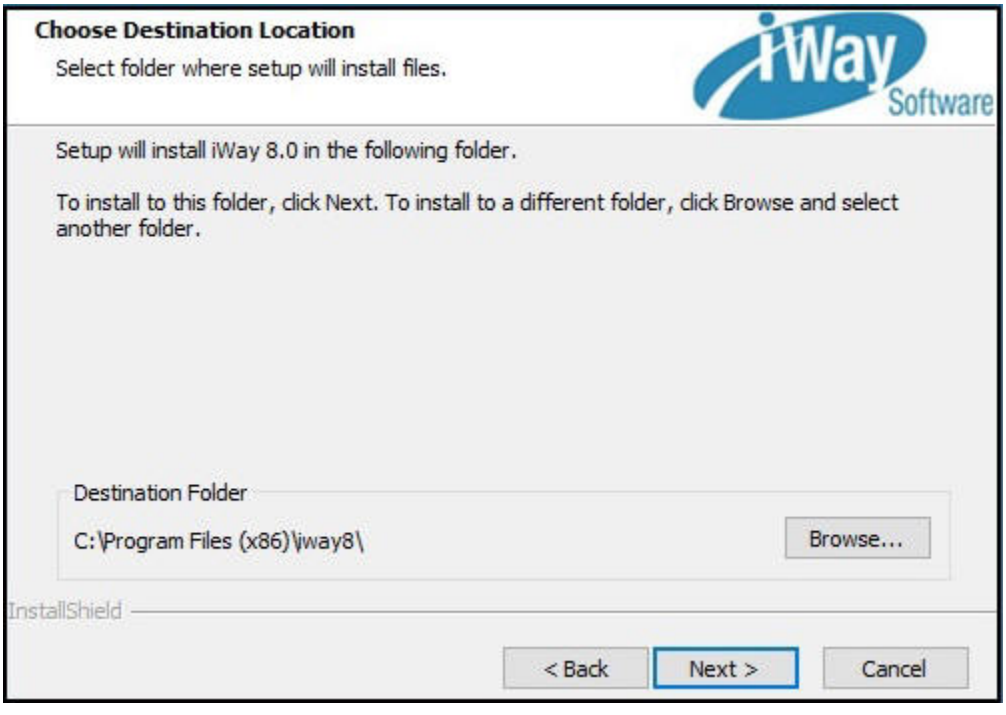
5. Click *Next*.

The Setup Type window opens, as shown in the following image.



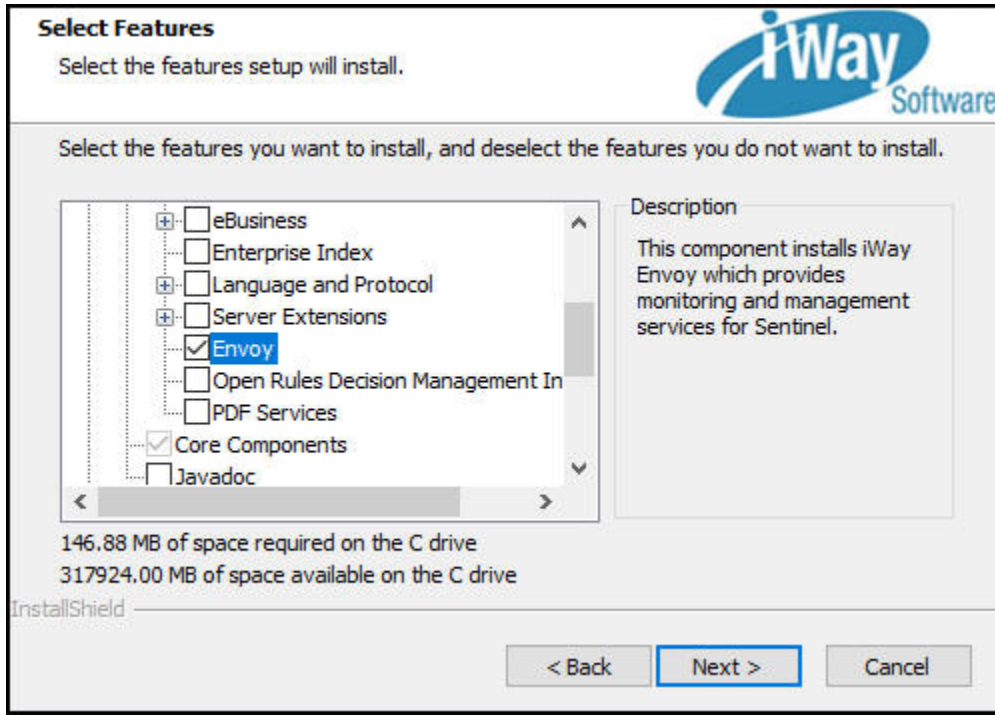
6. Select *Custom* for the setup type.
7. Click *Next*.

The Choose Destination Location window opens, as shown in the following image.



8. Accept the default location, which is C:\Program Files (x86)\iway8\, or click *Browse* to specify a new location. Then, click *Next*.

The Select Features window opens, as shown in the following image.

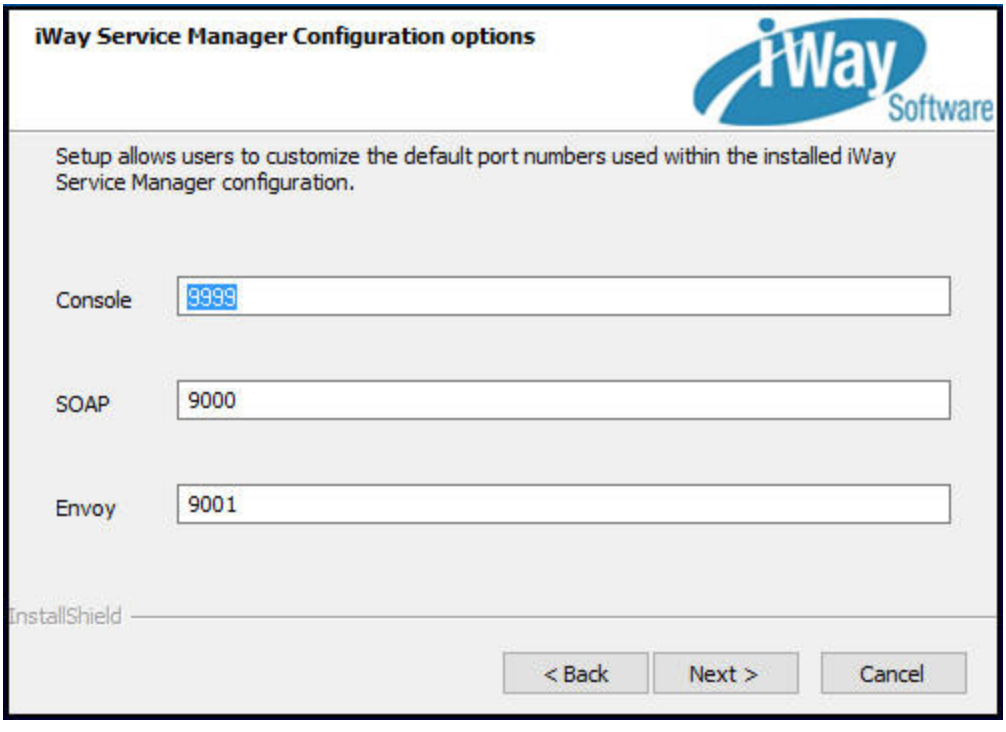


9. Ensure that the *Envoy* feature is selected.

   This feature should be selected only if iWay Sentinel has been licensed and installed. The selection of this feature will prompt you to provide additional configuration parameters to register the installed instance of iSM for remote monitoring and management through iWay Sentinel. If this feature is selected and iWay Sentinel is not available, your existing iSM instance or associated applications hosted by iSM are not affected. However, selecting this feature will pre-install Envoy components on the iSM instance that is being installed.

10. Click *Next*.

The iWay Service Manager Configuration options window opens, as shown in the following image.



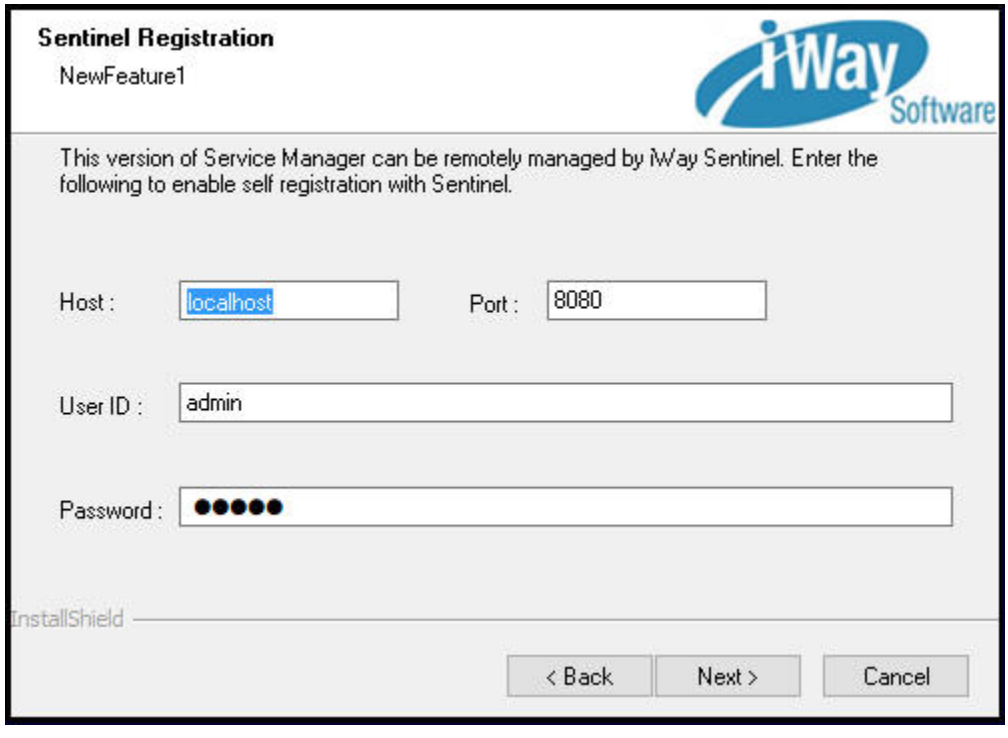
You are prompted to specify the ports that iWay Service Manager uses, as listed and described in the following table.

Name	Default Port	Purpose
Console Listener	9999	HTTP listener for the iWay Service Manager Administration Console.
SOAP Listener	9000	SOAP listener for iBSP and iWay Explorers.
Envoy	9001	Designated port for Envoy to allow Sentinel monitoring. **Note:** The default port for Envoy communication is configured to be 9001.

11. Accept the default values, or specify new values, and then click *Next*.

Note: Be sure to specify ports that are not being used by other programs or by another instance of iWay. If necessary, contact your system administrator for assistance in identifying available TCP ports.

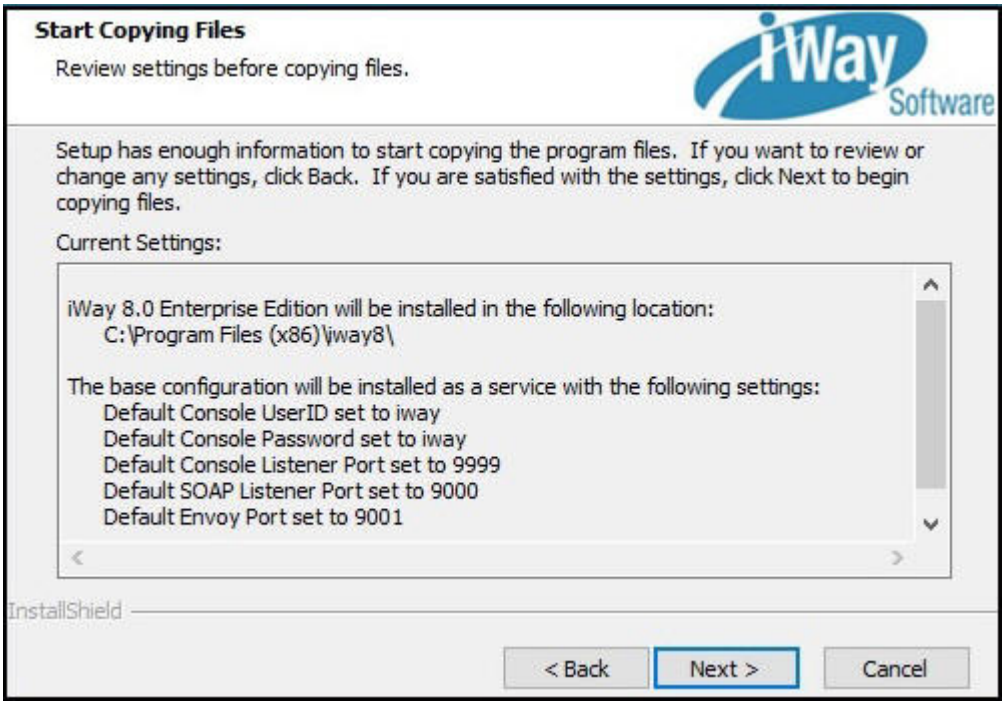
If you selected to install the Envoy feature, the Sentinel Registration window opens, as shown in the following image.



iWay Sentinel allows you to fully manage your current iSM instance remotely. By providing the requested information in this window, you will register the iSM instance that is being installed with iWay Sentinel

12. Enter the host, port, user ID, and password of your iSM instance that you want to register with iWay Sentinel.
13. Click *Next*.

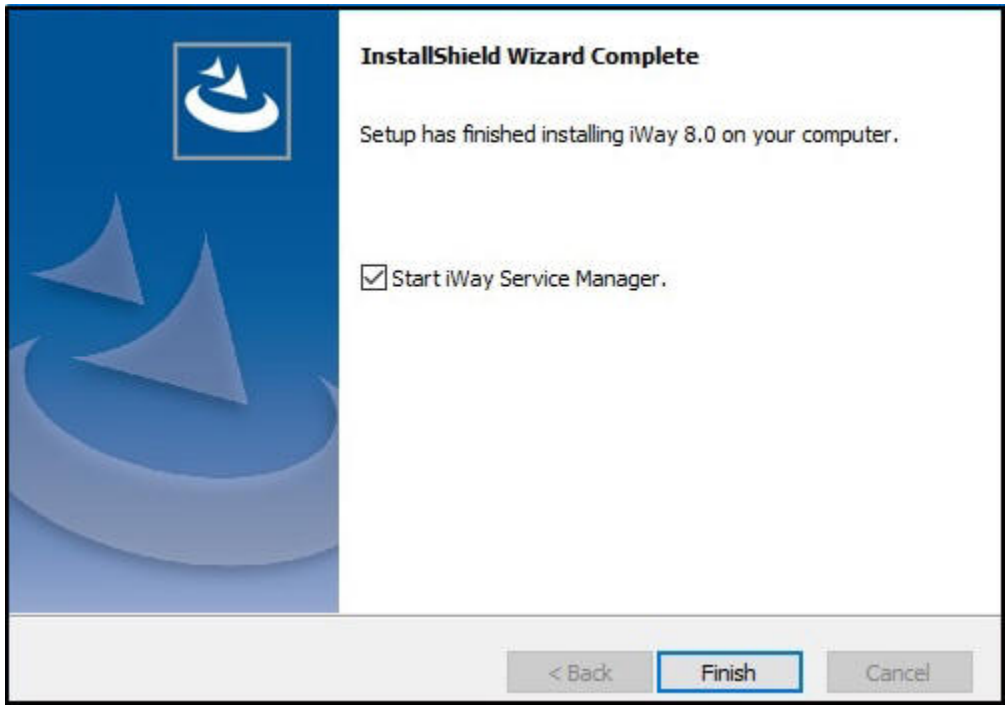
The Start Copying Files window opens, as shown in the following image.



14. Review the settings and then click *Next* to start the installation.

    Files are copied to your system in the directory you specified.

You have the option to start iSM when installation completes. If you choose this option, the iWay Service Manager Administration Console launches in your default web browser. You can log on to the iWay Service Manager Administration Console using the default user name, *admin*, and password, *admin*. You can also change the user name and password as required. For more information, see the *iWay Installation and Configuration Guide*.



15. Click *Finish* to complete the installation Wizard.

Installing Sentinel

Sentinel is delivered as a self-executable .jar file, which is executed and run directly from a command prompt. The components required for Sentinel to run will be installed in the location where the .jar file is running from during the initial execution.

Procedure: How to Install Sentinel

1. Download the sentinel-1.2.jar file and save it to an empty directory on your system.

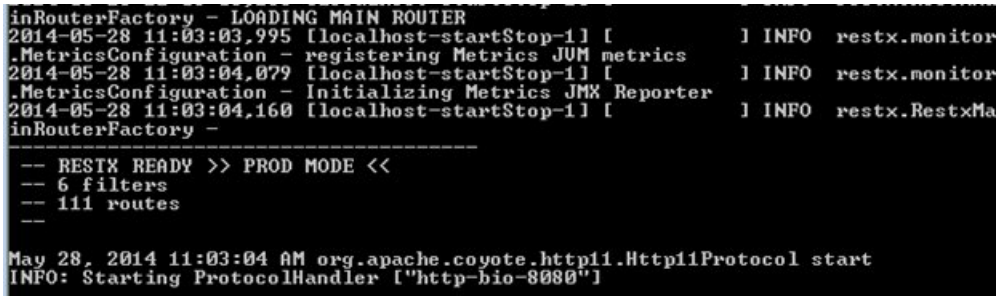
   This directory will become the Sentinel home directory.

2. Open a Command Prompt window and navigate to the Sentinel home directory where the .jar file has been saved.

3. Enter the following command:

```
java -jar sentinel-1.2.jar
```

When the start sequence has completed, the following message displays:



On the file system, the following directories have been created during the initial execution of the .jar file.

Directory	Description
<*Sentinel_Home*>\.extract	Runtime for Sentinel/SPOG.
<*Sentinel_Home*>\logs	Log files for Sentinel/SPOG.
\Users\<*user*>\spog	Generated when first accessing the SPOG user interface and contains SPOG graph, property files, and other runtime artifacts.

In this case, <*Sentinel_Home*> is the location from where the .jar file was executed and <*user*> is the system user who extracted the file.

4. Stop Sentinel by pressing Ctrl+C in the Command Prompt window and start it again, by re-executing the following command:

```
java -jar sentinel-1.2.jar
```

Sentinel and Single Pane of Glass (SPOG) are now ready to be used.

5. Access the Sentinel web user interface by opening a Google Chrome browser and entering the following URL:

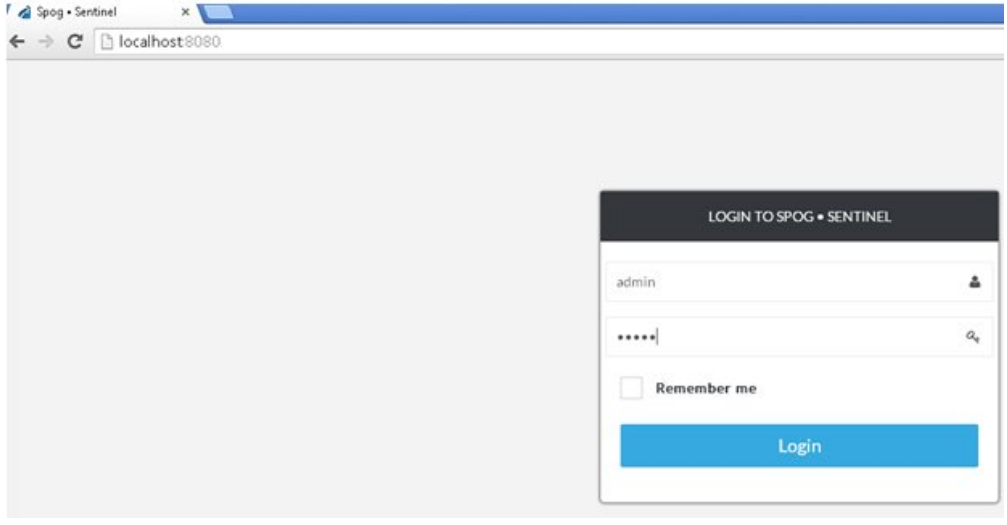
`http://host:8080`

where:

host

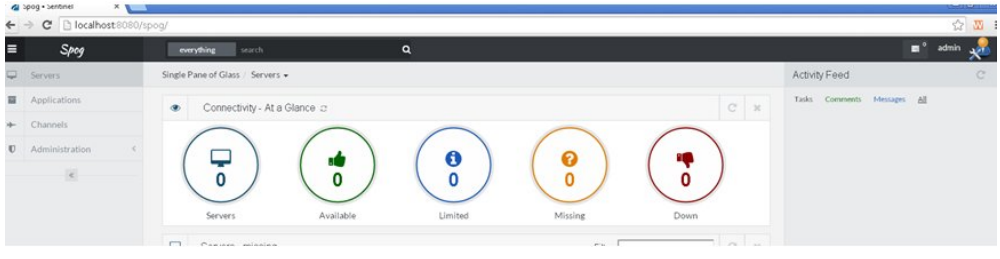
Is the machine/IP where Sentinel and SPOG have been installed.

A Login screen opens, as shown in the following image.



6. Log in using *admin* as the default user name and *admin* as the default password.

   The initial screen, Connectivity - At a Glance, is displayed indicating that SPOG is ready for use, as shown in the following image.



Chapter 3

Managing and Monitoring Servers

This section describes how to manage and monitor servers using Single Pane of Glass interface for iWay Sentinel.

In this chapter:

Server Communication to Sentinel

The term *server*, refers to a single instance of iWay Service Manager (iSM) running the master configuration, which is commonly known as the *base* configuration. The Envoy listener running on the server enables the REpresentational State Transfer (REST) style communication between the Sentinel and the iSM instance. The server has a communication link to its linked iWay Integration Applications (iIAs), which it can monitor and manage. It is important to understand that all communication from Sentinel to the server (and its linked applications) is handled through the Envoy listener that is deployed on the server.

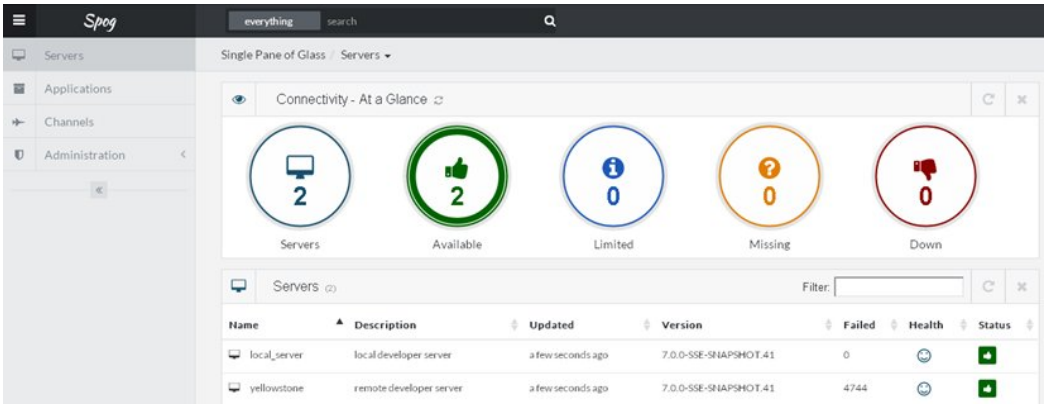
Server Connectivity

When iWay Sentinel is accessed through SPOG, the first screen that you are presented with is the Connectivity - At a Glance screen. This view provides an overall status of the connectivity to the registered servers. The connectivity status is presented, as listed and described in the following table.

Connectivity Status	Description
Down	Indicates that Sentinel believes the physical machine is not reachable. This is determined by trying to ping the machine on certain common port ranges to try and establish its connectivity on the network.

Connectivity Status	Description
Missing	Indicates that Sentinel was able to establish a connection to the machine by being able to ping it on one of the common ports. However, the configured iSM port is not reachable indicating that the iSM server is either not running or not installed on the machine.
Limited	Indicates that Sentinel was able to establish the connection to the iSM server running on the machine, but is not able to connect to the Envoy listener for further communication. This is usually indicative of Envoy not being installed, configured or running on the iSM server.
Available	iSM server is available for communication.
Servers	Total number of registered servers.

The following image shows the dashboard presented with the states of connectivity.



You can hover over each bubble to see the description of the connectivity status. The status of the connectivity is also shown under the Status column in the list of servers.

Clicking the status icon  for any given server, will take you directly into the iSM Administration Console for the specific server, using the credentials that were provided during server registration process.

Analyzing Server Health

When monitoring large number of servers with many applications, it is important to recognize an overall health of the enterprise being monitored. As health is a relative term and can have various meanings to different applications or users, a Health Model has been developed which can be manipulated to fit the monitoring needs.

The SPOG for Sentinel displays a health status for each Server based on various factors including service response times, message processing rate, error rates and others to calculate the health score based on a Health Model. Based on the calculated health score, the state of the health is assigned.

Health score is calculated based on the following formula:

```
score = -0.25 * rt + 1 * tp + 2 * mtp + -20 * ec + 0.5 * ac + 0.5 * cc +
-0.5 * qc
```

There are four available states which are then assigned as overall health of the server:

```
score > μ + o, then health is EXCELLENT
score < μ - o, then health is POOR
score < μ - o * 2, then health is SEVERE
else health is AVERAGE;
```

where:

`μ`

Is the statistical mean.

`o`

Is the standard deviation.

`rt`

Is the response time.

Note: rt only applies to server and does not factor in propagation delay.

`tp`

Is the throughput.

`mtp`

Is the maximum throughput.

`ec`

Is the error count.

ac

Is the active count.

cc

Is the completed count.

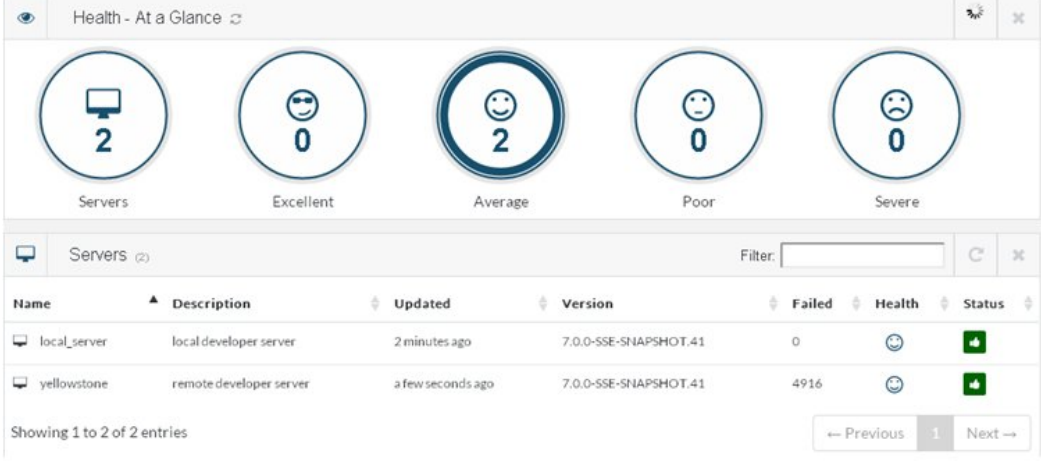
qc

Is the queued count.

The Health model is designed to be adjusted for the specific application monitoring needs and can be configured to change the weights. For more information, see *Sentinel Configuration Properties* on page 101.

To access the Health-At a Glance view, click on the icon next to Connectivity - At a Glance, as shown in the following image.

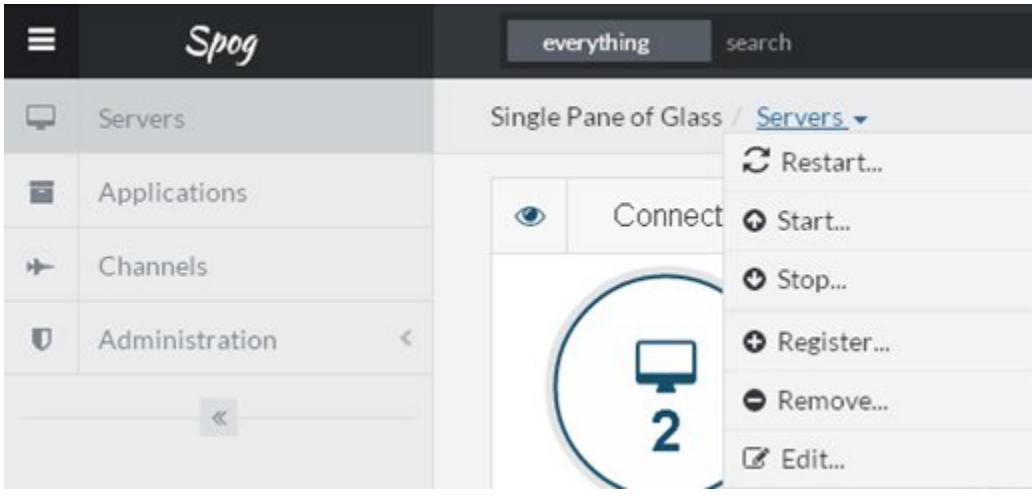
This Health - At a Glance view is displayed, as shown in the following image.



The health of the servers is shown in the bubble dashboard, as well as within the Health column for each server.

Managing Servers

Server management is performed through the available Servers link, as shown in the following image.



Click Servers to display the available list of actions, which include:

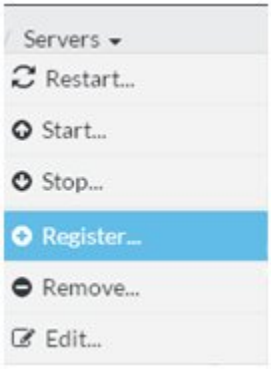
- Restarting the server. (Restart)
- Starting the server (Start).
- Stopping the server (Stop).
- Registering the server (Register).
- Removing the server (Remove).
- Editing the server (Edit).

Registering a Server

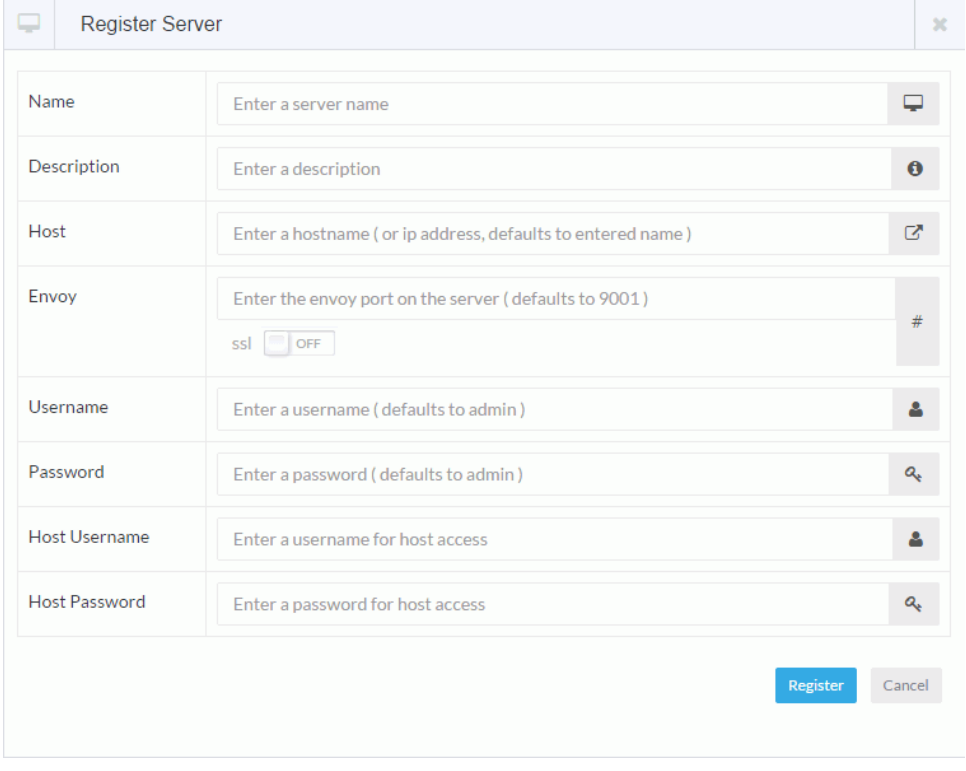
This section describes how to register a server using iWay Sentinel.

Procedure: How to Register a Server

1. To register a server for monitoring, click the *Servers* link and then select *Register...*, as shown in the following image.



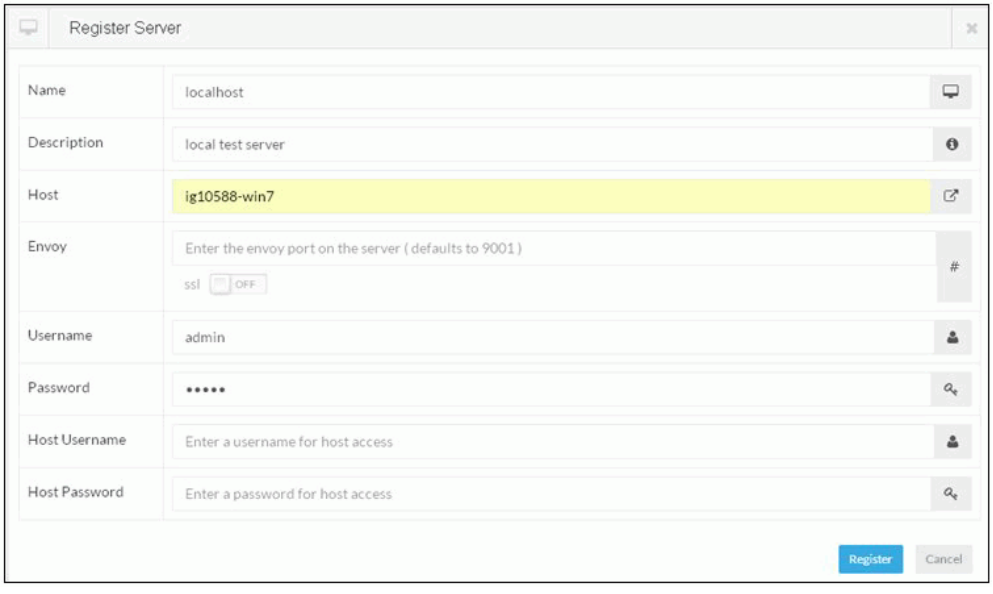
The Register Server screen opens, as shown in the following image.



2. Provide values for the parameters, as listed and described in the following table.

Parameter	Description
Name	Name of the server you want to register. This can be any name used to identify the server. If a value for the Host parameter is not provided, then this value will be attempted to be used as the host name.
Description	Description for the server being registered.
Host	IP address or host name of the physical server. If not provided, then the value specified for the Name parameter will be used as the default.
Envoy	Port number for the Envoy running on the server. If not provided, the default is 9001. An optional SSL setting is provided that can be enabled or disabled.
Username	A valid user name to connect to the iSM server. If not provided, the default value is *admin*.
Password	A valid password to connect to the iSM server. If not provided, the default value is *admin*.
Host Username	User name for the host machine where iSM is running. This is required only for OS level operating tasks, such as starting or stopping the iSM server, which requires proper access to the host machine.
Host Password	Password for the host machine.

The following image shows sample server registration in SPOG that has been completed.



3. Click *Register* to register the server.

   After the server has been registered it will first show up as Missing as Sentinel needs to get all information from the server.

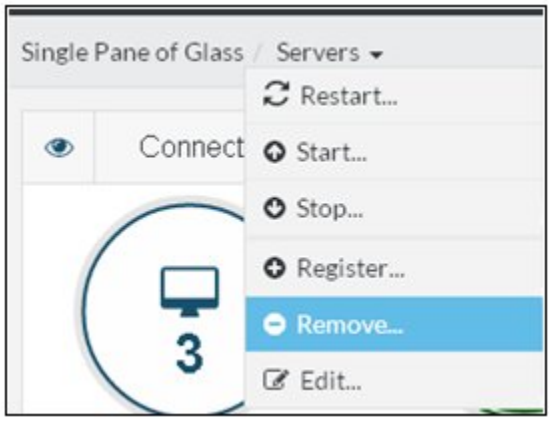
4. Click the refresh icon  to refresh the view and if available it will show up as *Available* under the Connectivity - At a Glance area.

Removing a Server

Removing a server from iWay Sentinel will not actually remove the physical server installation. Removing the server means that server will no longer be registered and monitored by Sentinel.

Procedure: How to Remove a Server

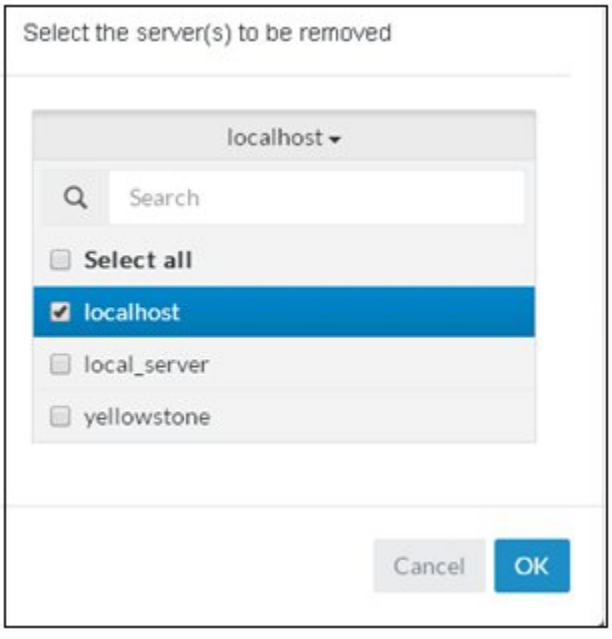
1. To remove a server from Sentinel monitoring, click the *Servers* link and then select *Remove...*, as shown in the following image.



The Select the server(s) to be removed prompt is displayed, as shown in the following image.

2. Click *None selected* to display a list of available servers.

3. Select the server(s) to be removed and then click *OK*, as shown in the following image.



A prompt to confirm the removal of the server from Sentinel is displayed, as shown in the following image.

4. Click *OK*.

Editing a Server

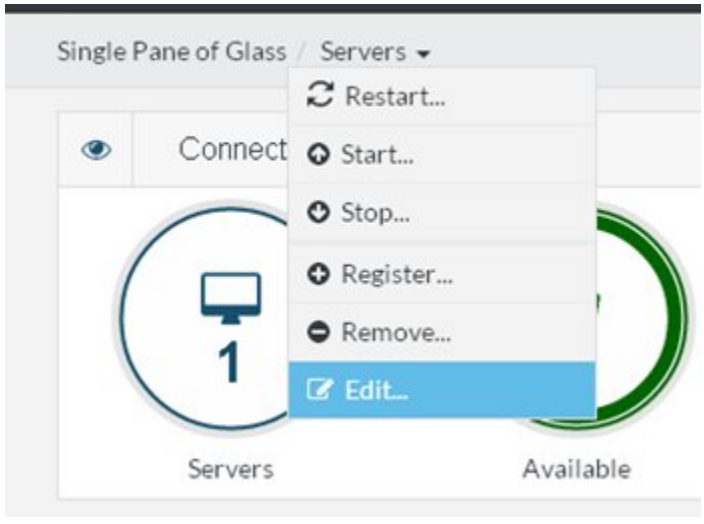
This section describes how to edit a registered server using Single Pane of Glass (SPOG) for iWay Sentinel.

Procedure: How to Edit a Server

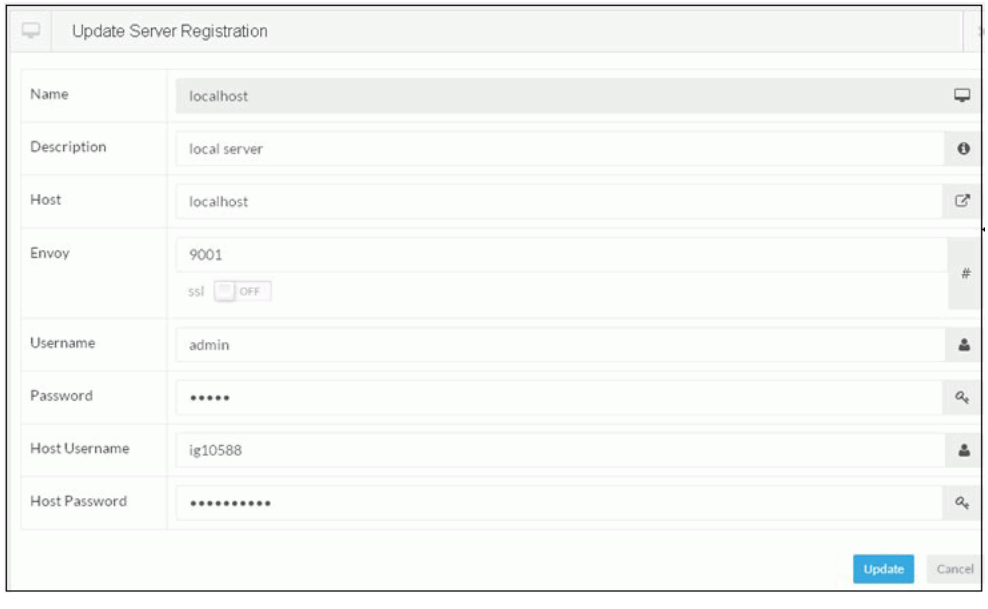
1. Select a server you want to edit by clicking on it from the list of available servers.

   The server will be highlighted and its details are displayed.

2. Click the *Servers* link and then select *Edit...*, as shown in the following image.



The Update Server Registration screen opens, as shown in the following image.



3. Provide updated information for the server as required and then click *Update*.

   The information for the registered server will be updated.

Starting a Server

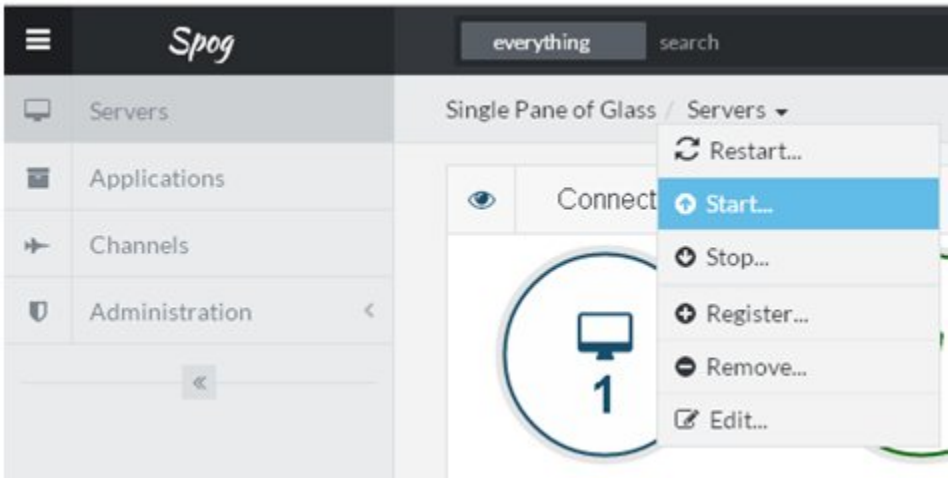
To start a remote server, the server must be installed as a Windows service and host credentials provided during the server registration process must enable the remote access.

Procedure: How to Start a Server

1. Select a server you want to start by clicking on it from the list of available servers.

   The server will be highlighted and its details are displayed.

2. Click the *Servers* link and then select *Start...*, as shown in the following image.



A prompt to confirm the start action for the server is displayed, as shown in the following image.

3. Click *OK*.

   The selected server will be started.

Stopping a Server

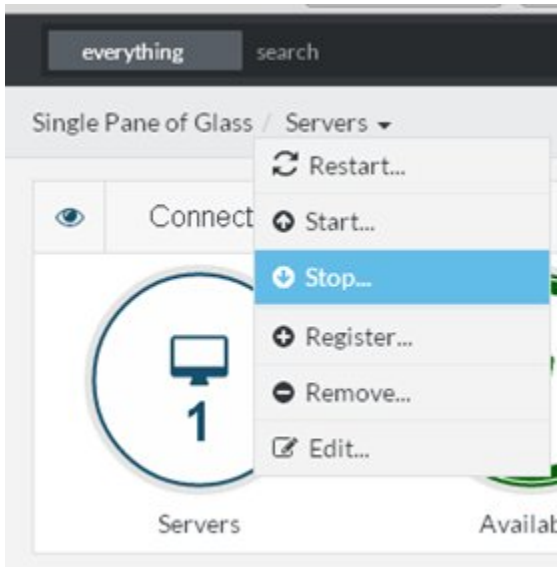
To stop a remote server, the server must be installed as a Windows service and host credentials provided during the server registration process must enable the remote access.

Procedure: How to Stop a Server

1. Select a server you want to stop by clicking on it from the list of available servers.

   The server will be highlighted and its details are displayed.

2. Click the *Servers* link and then select *Stop...*, as shown in the following image.



A prompt to confirm the stop action for the server is displayed, as shown in the following image.

3. Click *OK*.

   The selected server will be stopped.

Restarting a Server

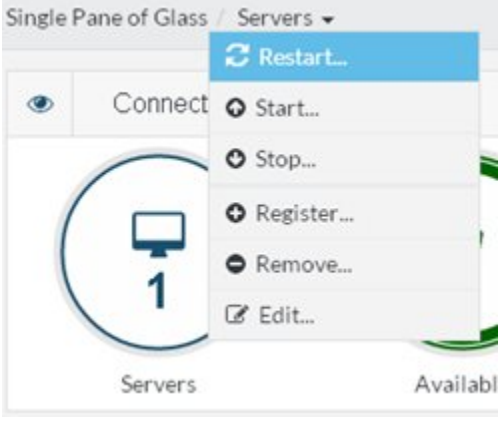
This section describes how to restart a server using iWay Sentinel.

Procedure: How to Restart a Server

1. Select a server you want to restart by clicking on it from the list of available servers.

   The server will be highlighted and its details are displayed.

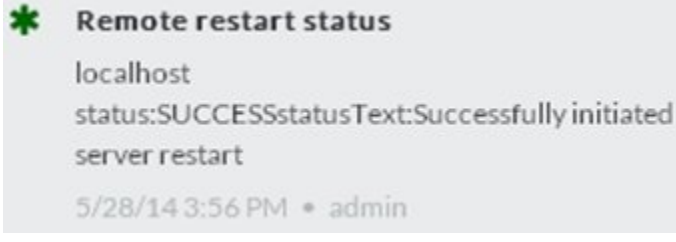
2. Click the *Servers* link and then select *Restart...*, as shown in the following image.



A prompt to confirm the restart action for the server is displayed, as shown in the following image.

3. Click *OK*.

Note: The process of restart a server can take a few minutes. If you monitor the Feeds section of Sentinel, you will see activity related to the restart process, as shown in the following image.



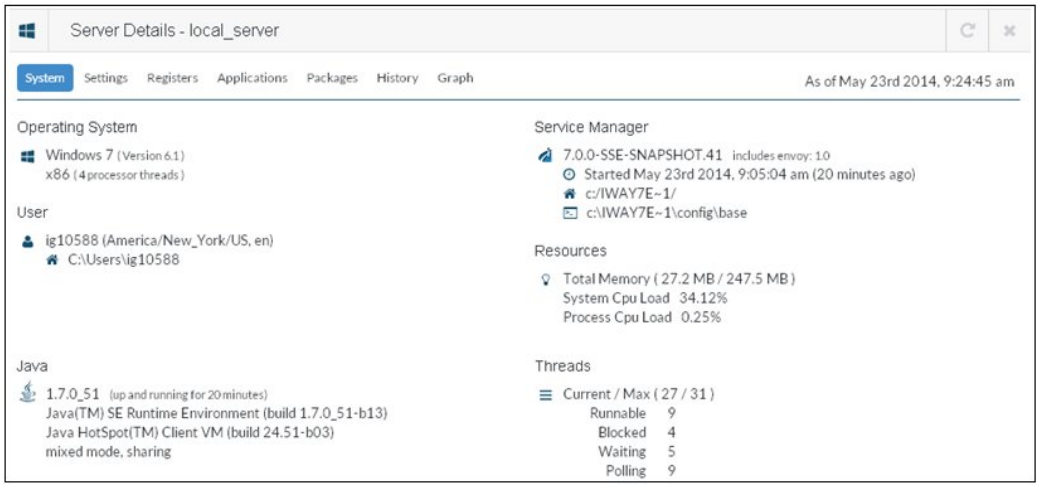
Viewing and Modifying Server Properties

As part of server monitoring, you have access to an array of statistics and information about overall server behavior, as well as ability to modify the runtime environment of the server directly.

To access information about a server, select the specific server from the available list of servers. The information will be displayed on the bottom of the screen.

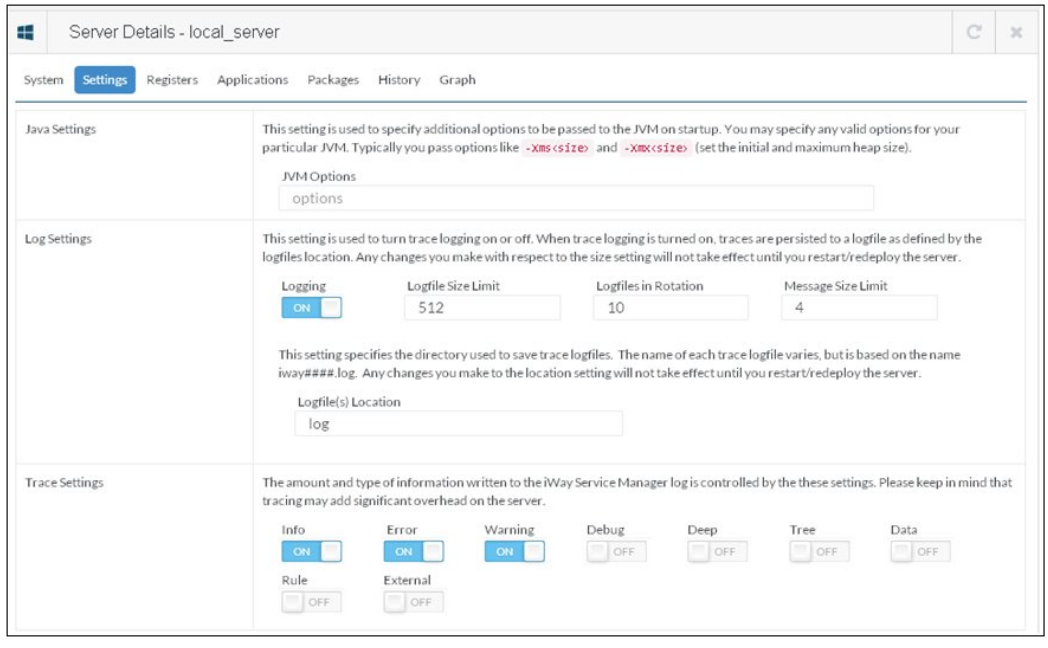
System Tab

The System tab provides overall information about the server, its location and resource utilization, as shown in the following image.



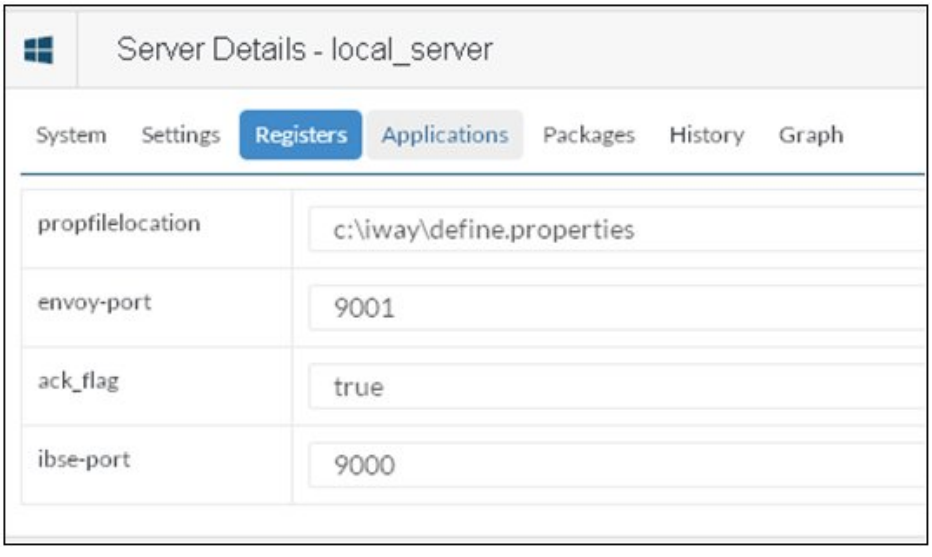
Settings Tab

The Settings tab enables the tuning of the server. This settings can be changed and will take affect directly on the server, as shown in the following image.



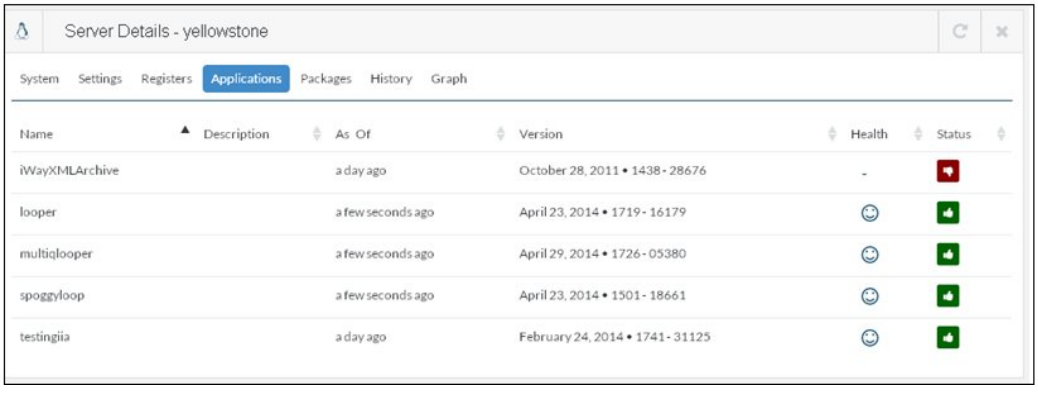
Registers Tab

The Registers tab enables the update of the server-level registers configured on the server, as shown in the following image.



Applications Tab

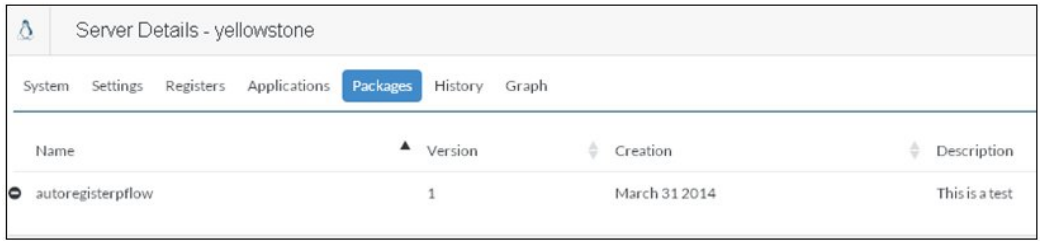
The Applications tab provides a summary view of the iWay Integration Applications running on the server, as shown in the following image.



For more information on managing and monitoring applications, see *Managing and Monitoring Applications* on page 53. Clicking on the application will take you to the detailed view of the application.

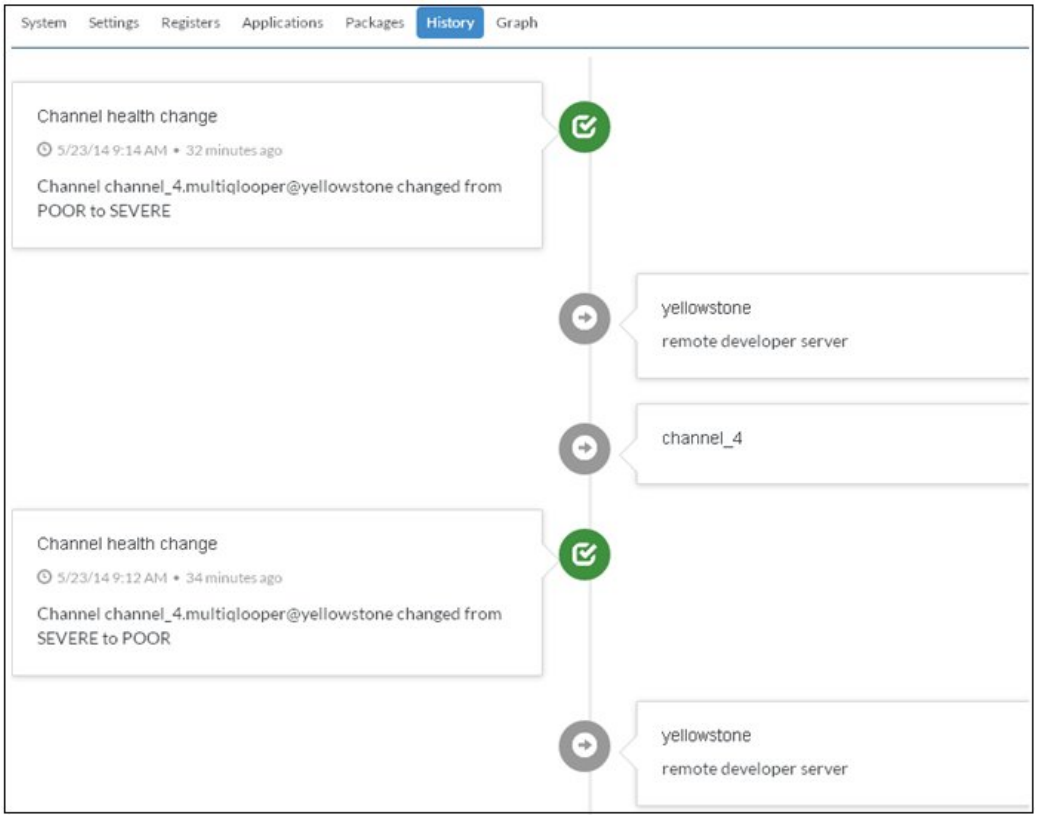
Packages Tab

The Packages tab provides information on the currently available packages on the server, as shown in the following image.



History Tab

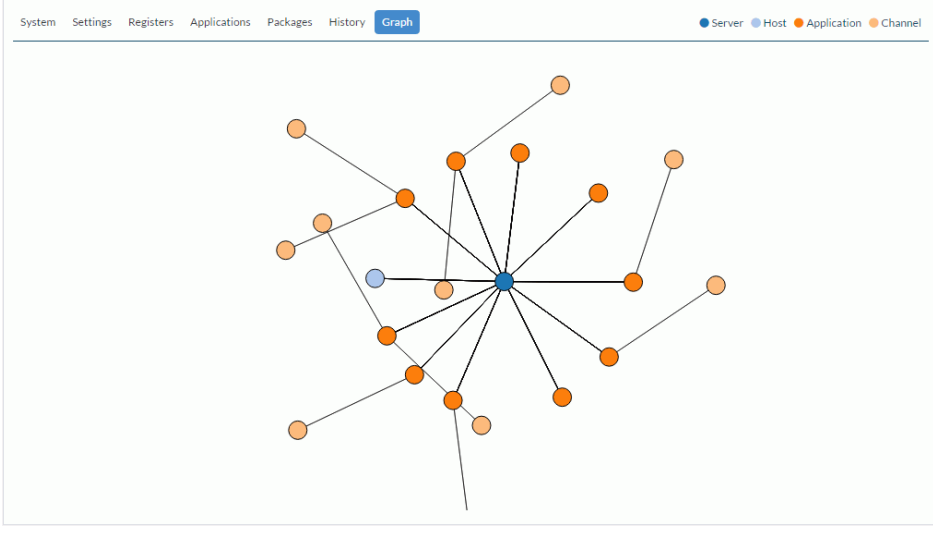
The History tab provides a historic view of the actions performed on the server and behavioral changes. These includes changes on the server itself, such as addition of a new application or a channel, as well as changes on the Sentinel side which would include things like change in the server health determination and overall status.



Graph Tab

The Graph tab provides a graphical representation of the components of a server as they relate to each other. You can hover over a specific node to see its information, as well as move the graph around to change its display.

The graph is centered around the orange node indicating a server which is being presented, with light-blue nodes representing the applications connected to this server, and then the blue nodes representing the channels associated with each application running on this server.



Chapter 4

Managing and Monitoring Applications

This section describes how to manage and monitor applications using iWay Sentinel.

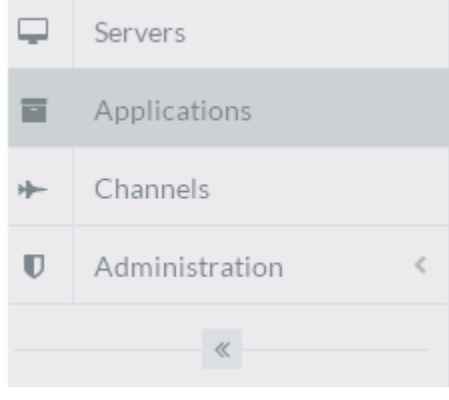
In this chapter:

Application Introduction

The term *application*, refers to a running instance of iSM that is deployed as an iWay Integrated Application (iIA). iIAs can be deployed across multiple servers, which enables distributed application deployment. However, each iIA runs on its own JVM and does not share its properties with other instances of the same iIA, deployed on a different server, or even on the same server with a different application name.

Monitoring Applications

To access the Application screen, click *Applications* in the left pane, as shown in the following image.



The Applications screen opens and lists all of the applications that are running across all monitored servers, as shown in the following image.

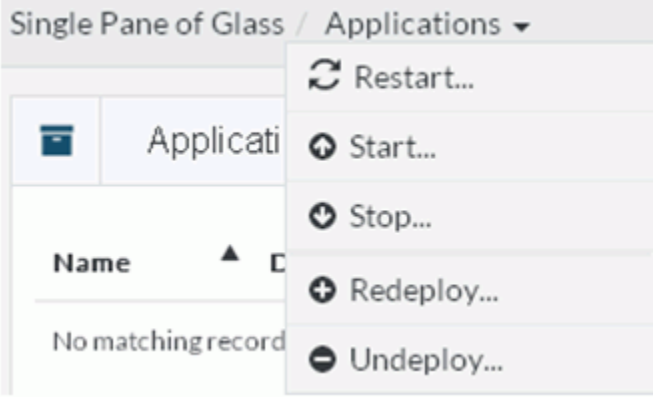
Applications (7) Filter:

Name	Description	Updated	Version	Server	Failed	Health	Status
iWayXMLArchive		a day ago	October 28, 2011 • 1438 - 28676	yellowstone	-	-	
looper		a few seconds ago	April 23, 2014 • 1719 - 16179	yellowstone	-		
multiqlooper		a few seconds ago	April 29, 2014 • 1726 - 05380	yellowstone	3602		
spoggyloop		a few seconds ago	April 23, 2014 • 1501 - 18661	yellowstone	-		
testingiia		a day ago	February 24, 2014 • 1741 - 31125	yellowstone	-		
testingiia	my application	a day ago	February 24, 2014 • 1741 - 31125	local_server	-	-	
testingiia_new	test	a day ago	February 24, 2014 • 1741 - 31125	local_server	-	-	

This view provides general information about the applications being monitored, such as overall health, status, and a cumulative count of failed transactions encountered by the application.

Managing Applications

Application management is performed through the available Applications link, as shown in the following image.



Click *Applications* to display the available list of actions, which include:

- Restart

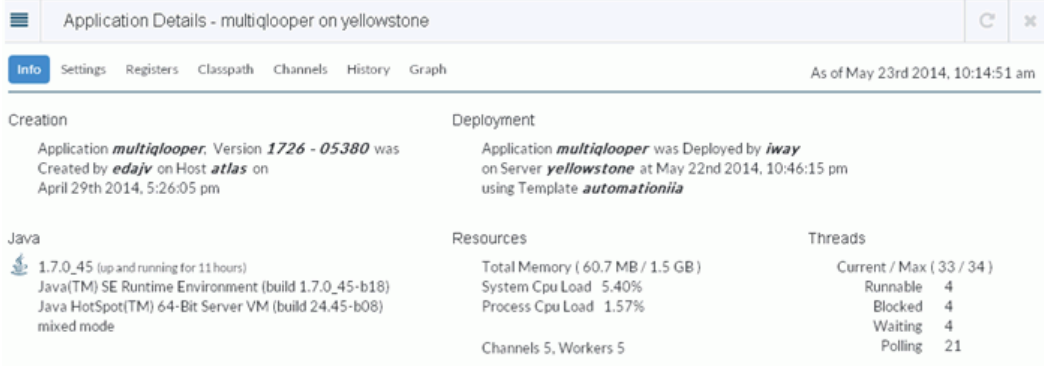
- Start
- Stop
- Redeploy
- Undeploy

Viewing and Modifying Application Properties

Selecting an application from the list of available applications displays properties related to the specific application. This section enables you to monitor and manage a selected application that is running on a specific server.

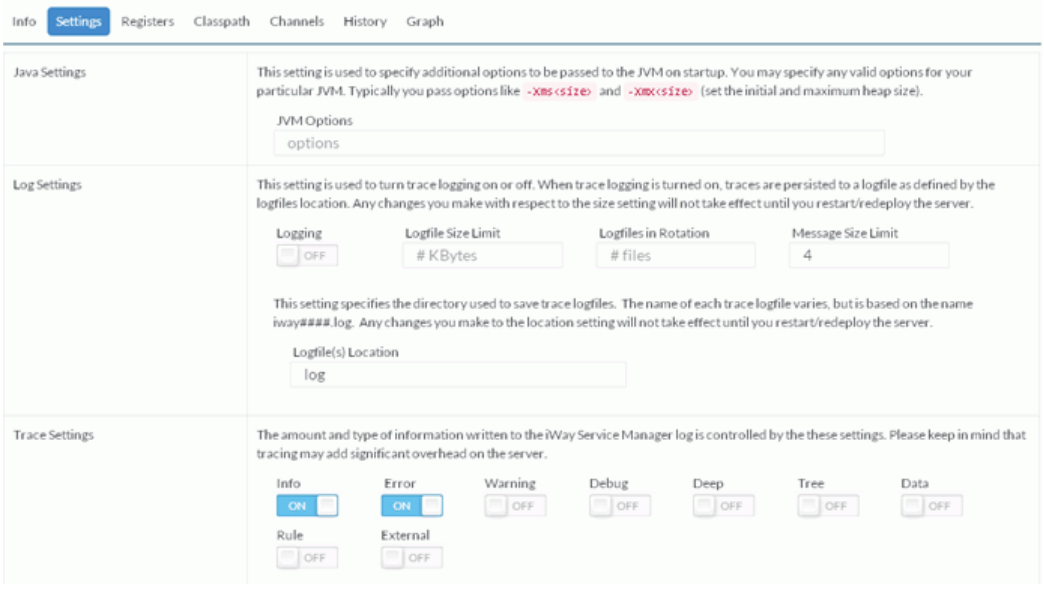
Info Tab

The Info tab, provides general information about a selected application and its environment (including resource utilization), as shown in the following image.



Settings Tab

The Settings tab exposes the general list of settings available for the selected application, as shown in the following image.



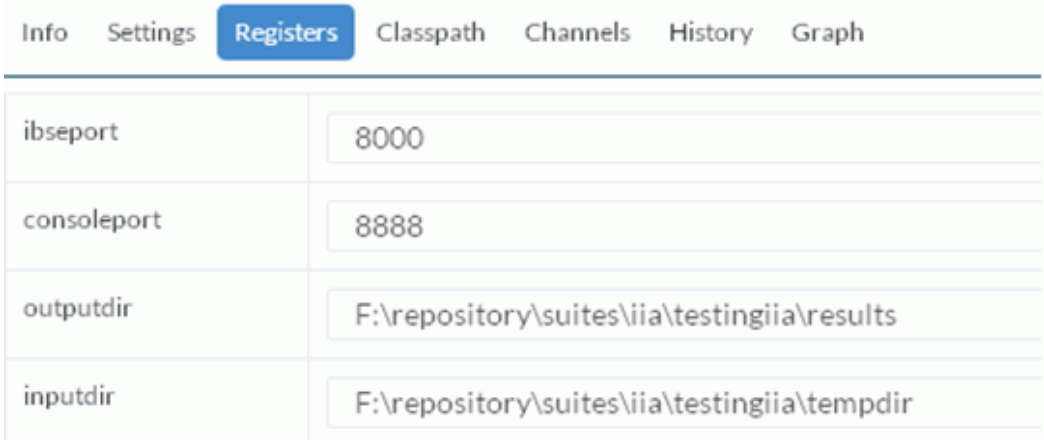
You can change and apply these settings directly within the runtime phase, without the need to rebuild or redeploy the application.

These settings are unique to a specific application that is running and are not shared across applications.

Note: Redeploying an application at any point will override the settings that are made directly from the deployed application.

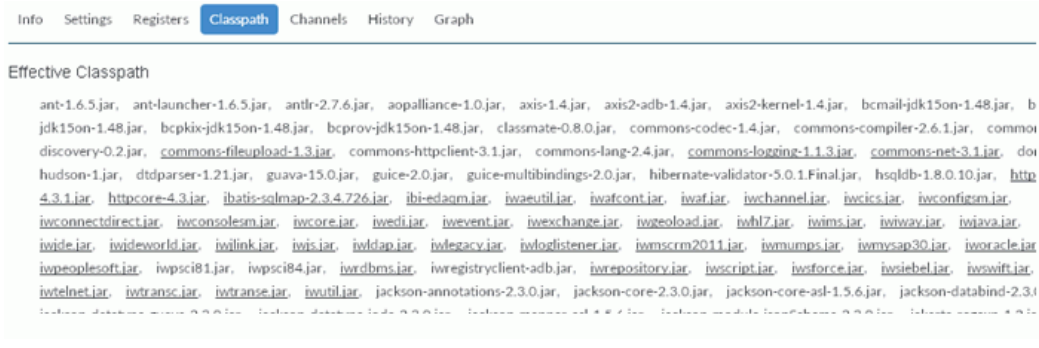
Registers Tab

The Registers tab enables you to update configured register settings at the server level for an application, as shown in the following image.



Classpath Tab

The Classpath tab, displays the current .jar files that are being loaded by the selected application, as shown in the following image.



Note: iWay-based .jar files are underlined. You can hover over these files to view build version information.

Channels Tab

The Channels tab provides monitoring capabilities for any channels that are running within the selected application, as shown in the following image.

Info Settings Registers Classpath Channels History Graph

			Messages				Throughput			
Name	As Of	Uptime	Active	Completed	Successful	Failed	Current	Max	Health	Status
channel	a few seconds ago	12 hours ago	1	3734	3734	0	0.10019	0.13946		
channel_4	a few seconds ago	12 hours ago	1	3720	0	3720	0	0		
channel_2	a few seconds ago	12 hours ago	1	3732	3732	0	0.10019	0.127099		
channel_3	a few seconds ago	12 hours ago	1	3730	3730	0	0.08349	0.13946		
channel_1	a few seconds ago	12 hours ago	1	3733	3733	0	0.10019	0.127099		

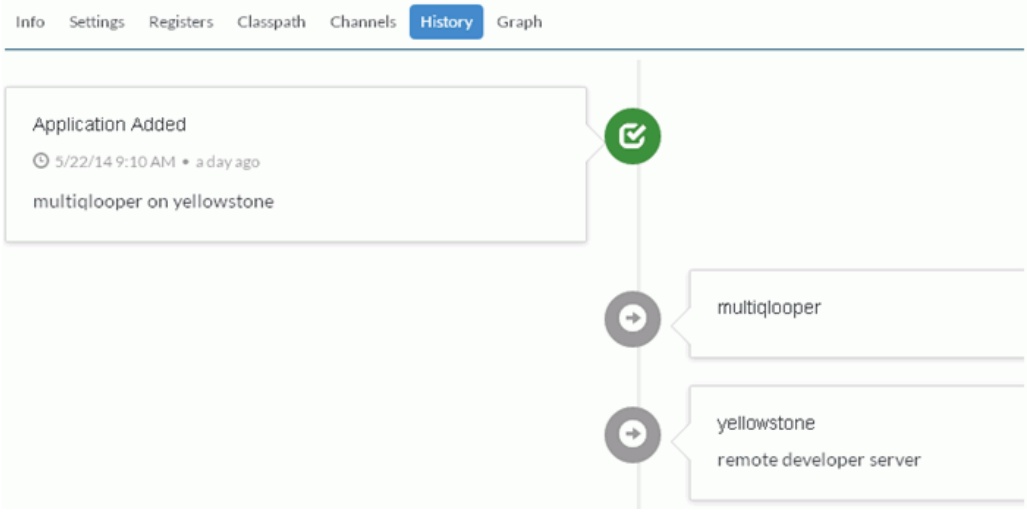
The Channels tab also provides general statistics for transactions that are being processed.

To start or stop a specific channel, click the corresponding icon in the Status column.

To view detailed information about a specific channel, click the name of the channel. For more information on managing and monitoring channels using Sentinel, see *Managing and Monitoring Channels* on page 61.

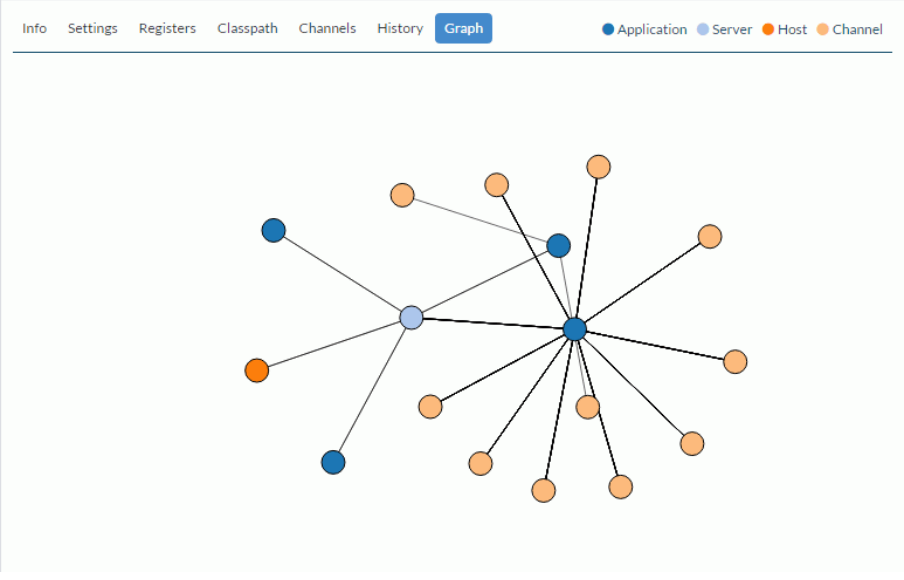
History Tab

The History tab provides a historic view of actions performed on the selected application and also any behavioral changes, as shown in the following image.



Graph Tab

The Graph tab provides a graphical representation of the components as they relate to each other, as shown in the following image.



You can hover over a specific node for more information and move the graph around to change its display.

Chapter 5

Managing and Monitoring Channels

This section describes how to manage and monitor channels using iWay Sentinel.

In this chapter:

Channel Introduction

The term *channel*, refers to a a component running within an application or a server, which is performing the actual message processing. Channels can be monitored across all applications and servers.

The Channels monitoring screen provides the standard information for transactional processing and overall channel status, as shown in the following image.

Channels (17) Filter:

Name	Type	Updated	Messages				Application	Server	Health	Status
			Active	Completed	Successful	Failed				
iWay_Archive_Loader_Channel		a day ago	0	0	0	0	iWayXMLArchive	yellowstone	-	
iWay_Archive_Query_Handler		a day ago	0	0	0	0	iWayXMLArchive	yellowstone	-	
testingiia.channel	FILE	2 minutes ago	0	0	0	0	testingiia	yellowstone	-	
testingiia.channel		a day ago	0	0	0	0	testingiia	local_server	-	
testingiia.channel		a day ago	0	0	0	0	testingiia_new	local_server	-	
channel	FILE	2 minutes ago	1	3874	3874	0	multiqlooper	yellowstone		
channel_1	Internal	2 minutes ago	1	3872	3872	0	multiqlooper	yellowstone		
channel_1	FILE	2 minutes ago	1	710	710	0	looper	yellowstone		

By default, the Channels monitoring screen can display a large number of channels that are available. As a result, you can filter the list of channels to find a specific channel within an application of interest. For more information on filtering, see *Filtering and Searching* on page 103.

Viewing and Modifying Channel Properties

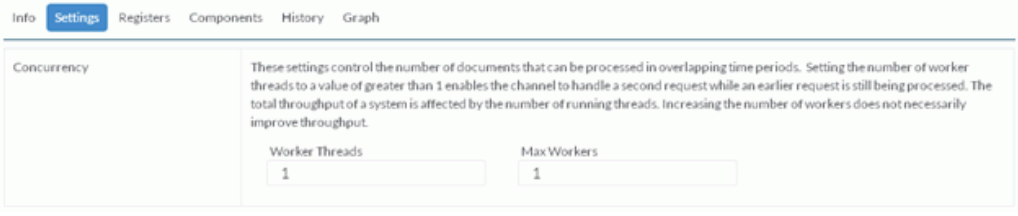
Selecting a channel from the list of available channels displays properties related to the specific channel. This section enables you to monitor and manage a selected channel that is associated and running on a specific application.

Info Tab

The Info tab provides general information about the channel and its message statistics, as shown in the following image.

Settings Tab

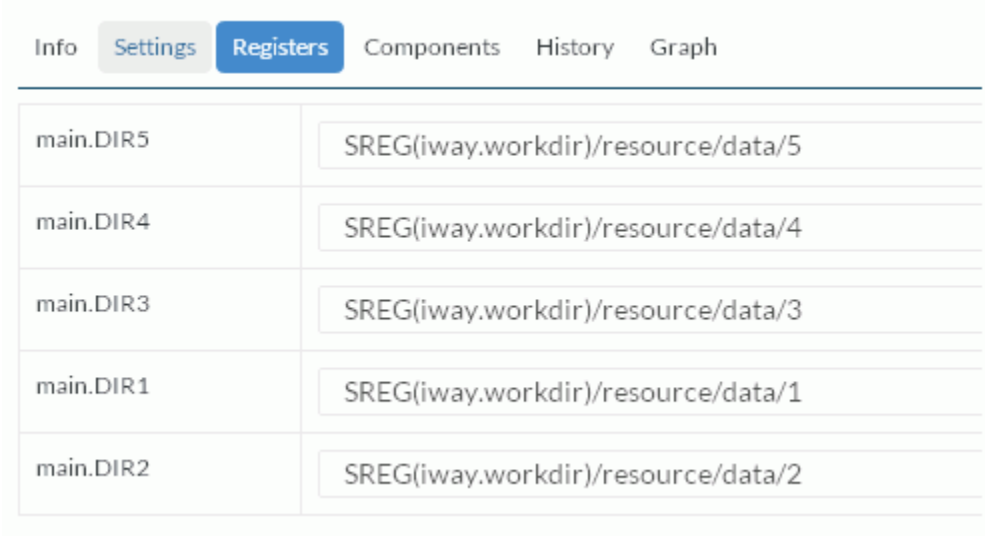
The Settings tab provides the ability to control the multithreading attributes of a channel, as shown in the following image.



Note: This is not a complete channel configuration, but exposes threading configuration, which enables you to tune a channel remotely.

Registers Tab

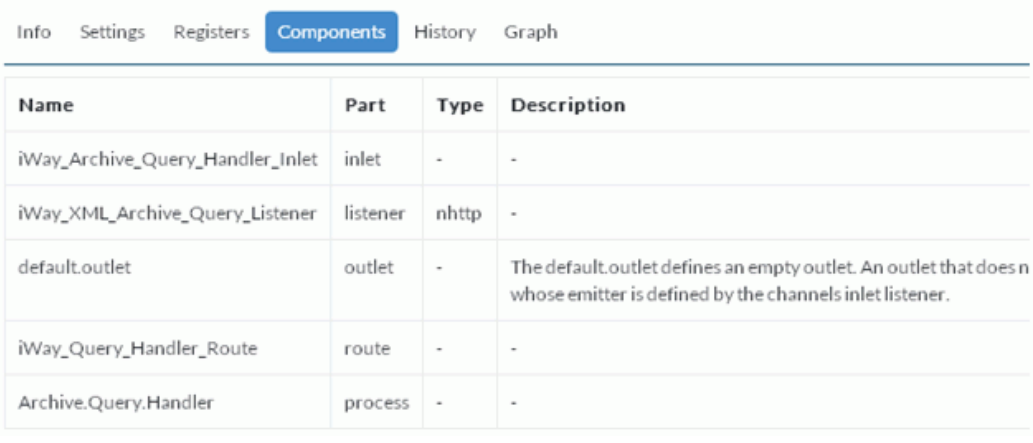
The Registers tab allows you to modify the register settings used by a selected channel, as shown in the following image.



The registers listed in this screen are associated with a channel register set.

Components Tab

The Components tab, provides a general overview of the components (inlets, routes, outlets) that comprise the channel, as shown in the following image.

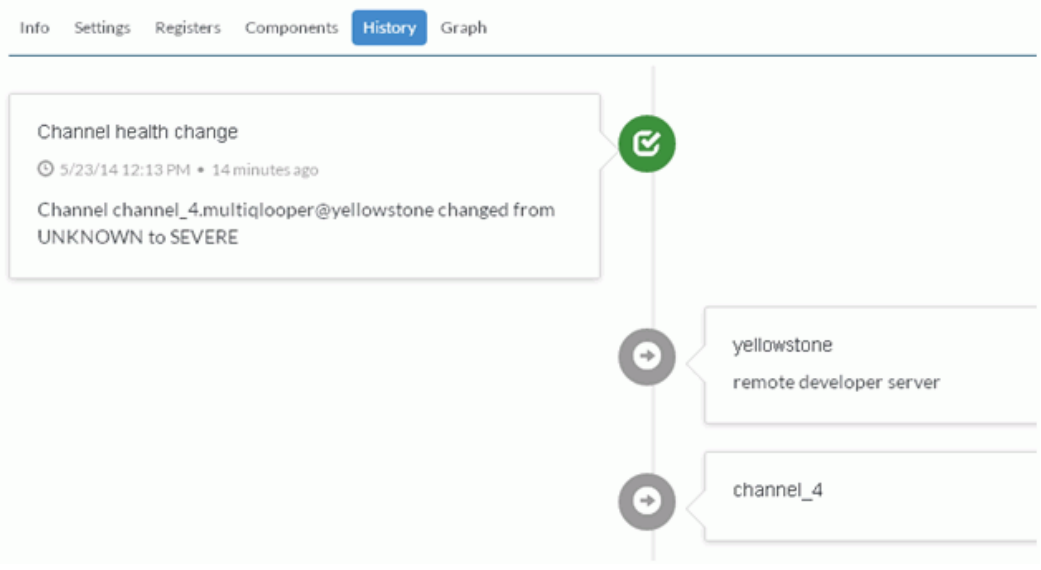


Name	Part	Type	Description
iWay_Archive_Query_Handler_Inlet	inlet	-	-
iWay_XML_Archive_Query_Listener	listener	nhttp	-
default.outlet	outlet	-	The default.outlet defines an empty outlet. An outlet that does n whose emitter is defined by the channels inlet listener.
iWay_Query_Handler_Route	route	-	-
Archive.Query.Handler	process	-	-

This allows you to easily identify the components being used and referenced by the selected channel.

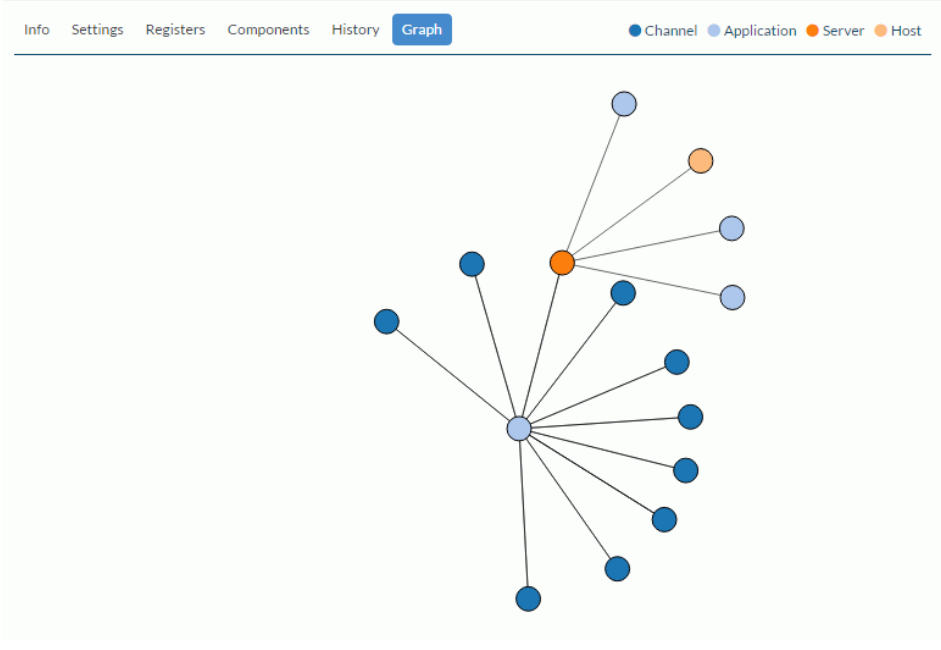
History Tab

The History tab provides a historic information view on channel communication and status updates as recognized by Sentinel, as shown in the following image.



Graph Tab

The Graph tab provides a graphical representation of the components as they relate to each other, as shown in the following image.



You can hover over a specific node for more information and move the graph around to change its display.

Chapter 6

Administration

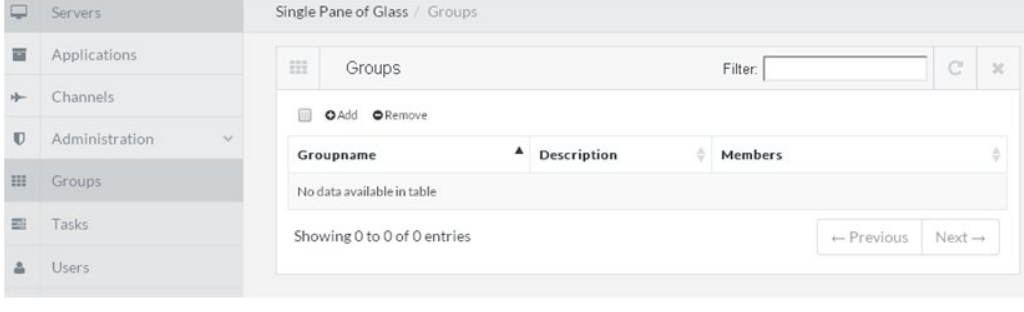
The administration section enables the administration of iWay Sentinel, and the remote servers and applications that are being managed through an array of scriptable and scheduled tasks.

In this chapter:

Configuring Groups

In an extensible multi-server/multi-application environment, it becomes imperative that there is a need to group entities together and perform certain actions on the entire group, rather than on a single entity. The iWay Sentinel grouping capability enables the creation and management of groups of servers and/or applications. These groups can then be used throughout Sentinel actions and have multiple tasks performed on them as a group, rather than performing actions on an individual level.

To access the Groups section, select *Groups* under the Administration section in the left pane. The Groups screen opens, as shown in the following image.

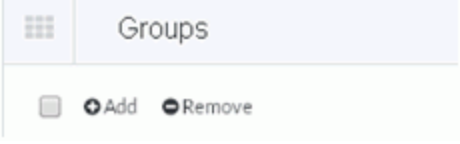


Adding a Group

This section describes how to add a group using iWay Sentinel.

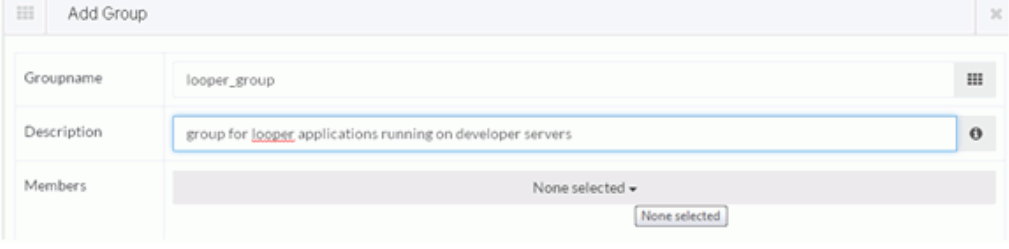
Procedure: How to Add a Group

1. To add a group, click *Add* in the Groups screen, as shown in the following image.

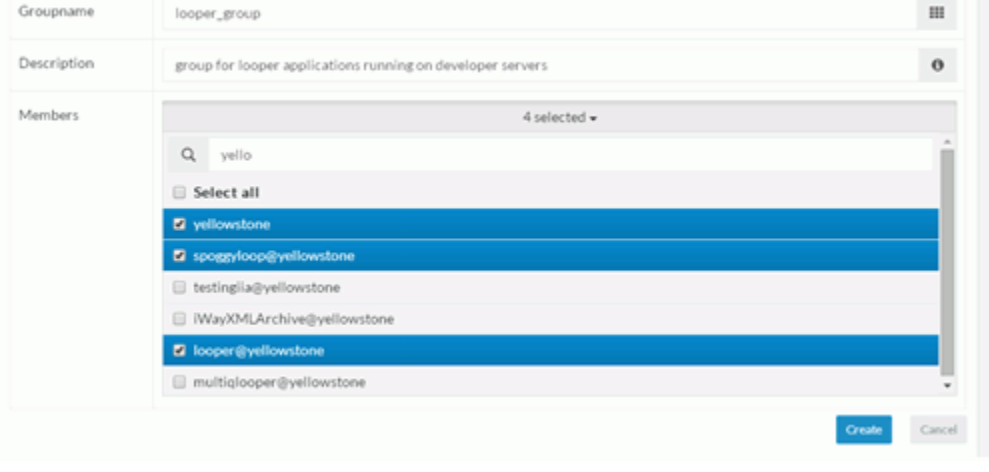


An Add Group screen is displayed.

2. Provide the group name, description, and select members into the group by clicking the Members drop-down list, as shown in the following image.



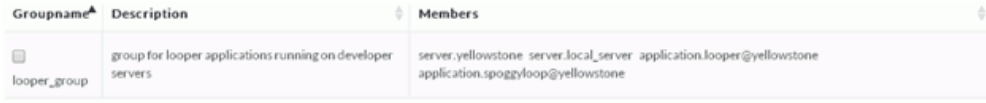
3. Select applications and/or servers to be added into the group. The search filter assists in finding all members that you wish to add.



Note: If the group contains both servers and applications, and is used for any action within Sentinel, only applicable members will be displayed from the group. As an example, if server-actions are performed on the group, only servers within the group will be visible and will have this action performed.

4. After members of the group have been selected, click *Create*.

   The group displays in the list of available groups with its members listed.



Groupname	Description	Members
looper_group	group for looper applications running on developer servers	server.yellowstone server.local_server application.looper@yellowstone application.spoggyloop@yellowstone

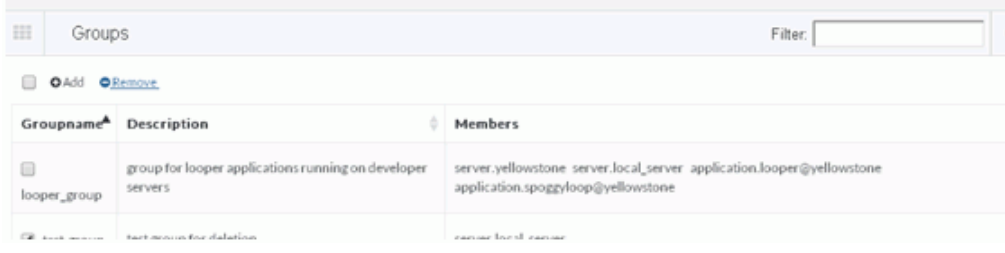
Note: The @ character in the member name represents a specific application deployed on a given server, for example *application@server*.

Removing a Group

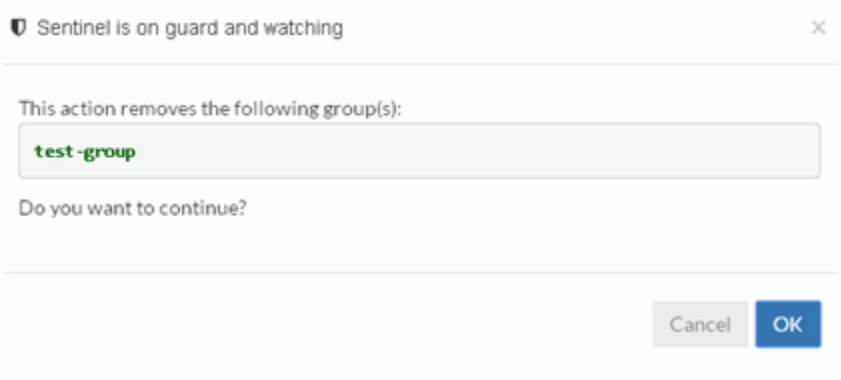
This section describes how to remove a group. Removing a group removes only the relationship between its members and the group itself, it does not remove, or unregister, the actual members of the group.

Procedure: How to Remove a Group

1. To remove a group, select the group and click *Remove*, as shown in the following image.



2. A confirmation prompt is displayed. Click *OK* to remove the group, as shown in the following image.

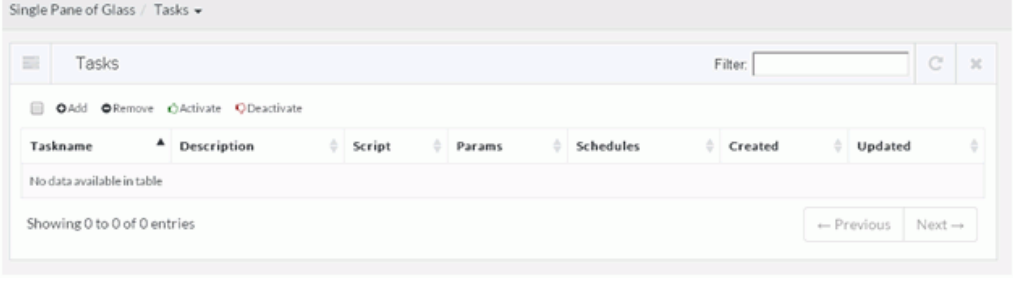


The group is deleted from the list.

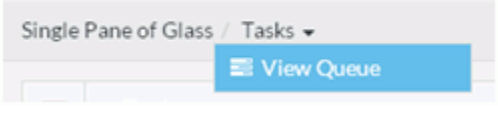
Configuring Tasks

Tasks enable you to create asynchronous action items that must take place in a scripted and manner that can be scheduled. Tasks are designed to run scripts, which can perform multiple actions in an automated fashion without direct user interaction.

To access Tasks screen, on the left hand side under the Administration, select *Tasks*. The screen will display a list currently defined tasks.



Click the down-arrow on the Single Pane of Glass / Tasks menu, to bring up a list of queued tasks for execution.



The list of queued tasks represents not only user-defined tasks, but also system level tasks being performed.

Queue (18) all • running • completed • failed • pending • canceled Filter:

Name	Status	Mode	Next Run	Last Run	Last Success
Connectivity	completed		in a few seconds	a few seconds ago	a few seconds ago
Graph export	completed		-	5 minutes ago	5 minutes ago
Health	completed		in a few seconds	38 minutes ago	39 minutes ago
MetaData	completed		in a minute	a few seconds ago	a few seconds ago
Updating 100 channel	completed		-	2 hours ago	2 hours ago
Updating 108 channel_4	completed		-	35 minutes ago	35 minutes ago
Updating 124 channel_3	completed		-	35 minutes ago	35 minutes ago
Updating 132 channel_1	completed		-	2 hours ago	2 hours ago
Updating 180 testingiia.channel	completed		-	37 minutes ago	37 minutes ago

The general status of the task and its execution is displayed. The Mode is indicated as either a recurring task which is denoted by a round arrow, or as a onetime task which is denoted as a small clock.

To filter by task status, you may click on the filters shown on the top of the Queue menu to see tasks of specific status, such as failed or pending.

Queue (18) all • running • completed • failed • pending • canceled

To switch back to the Task Management view, click on the Single Pane of Glass /Queue drop-down and select Manage Tasks.

Adding Tasks

This section describes how to add a task.

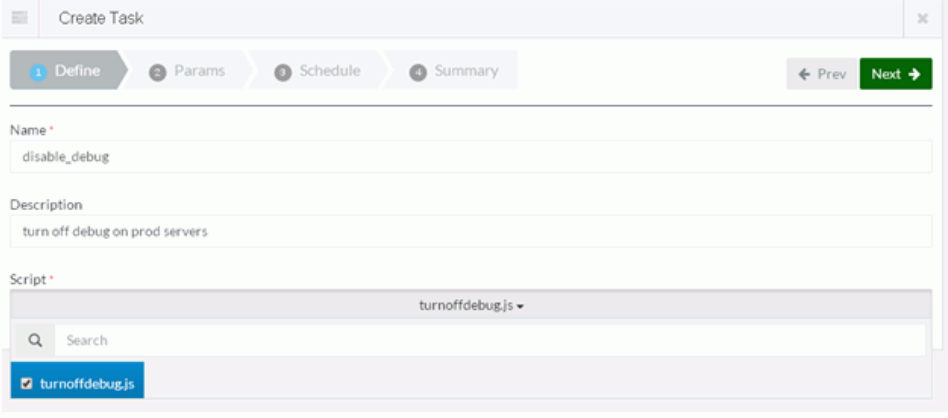
Procedure: How to Add a Task

1. Under the Managed Tasks view, click *Add* to add a new task.

   A Create Task screen is displayed.

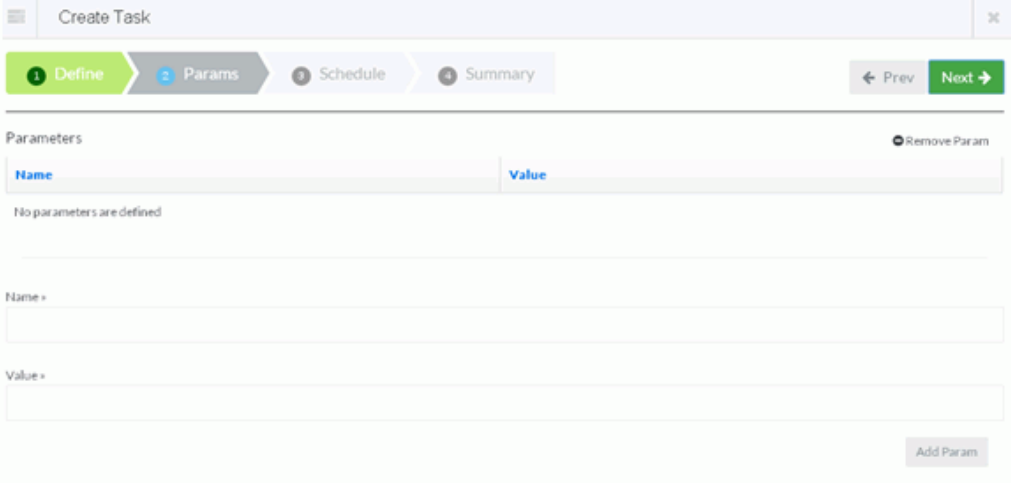
Note: Before a task can be added, a task execution script must exist on the system. For more information on script management, see *Managing Files and Artifacts* on page 79.

2. Provide the name and description for the task being created.



3. From the drop-down, select the script(s) being associated with the task for execution. Click *Next*.

4. If the script expects parameters for execution, they can be provided on the next screen. Fill in the Name/Value for the parameter and click *Add Param*. Repeat this step to add multiple parameters, as shown in the following image.

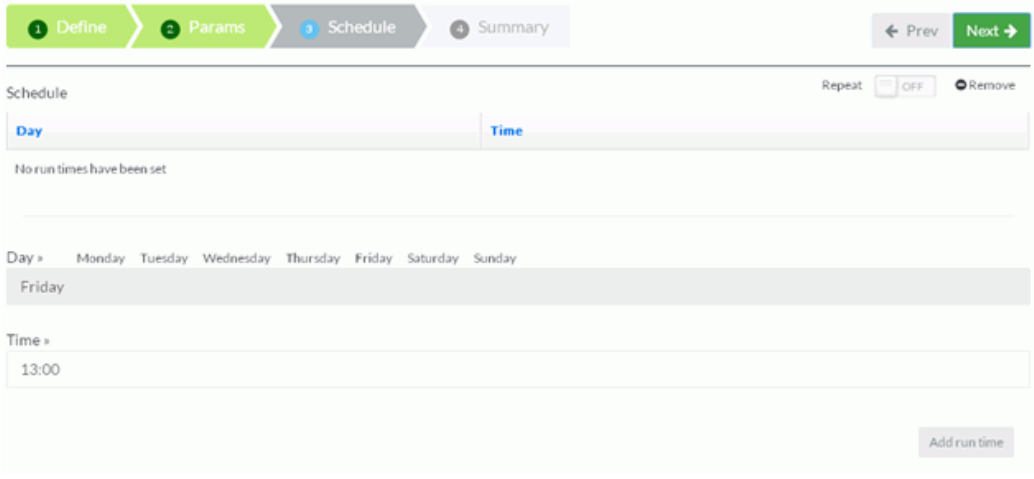


5. Click *Next*.

   The scheduling screen is displayed.

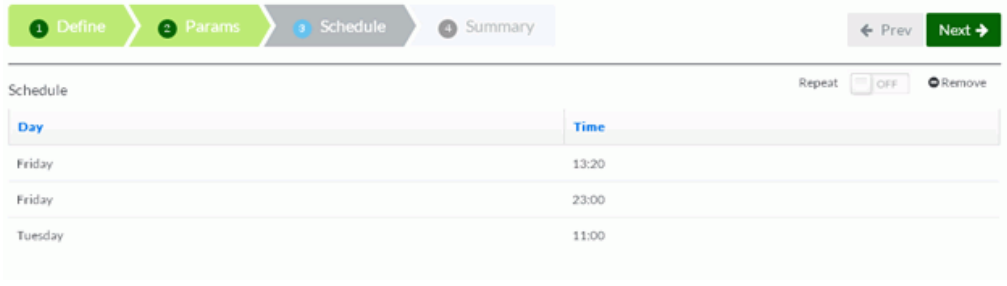
If no scheduled date is defined, the script will be executed right away upon creation and run only once.

6. To add specific execution date/time, click on the day of the week and provide a time (using *hh:mm* format) based on a 24-hour system. Click *Add run time*, as shown in the image below. Repeat the steps to add multiple times for execution.



The configured execution times are displayed for review.

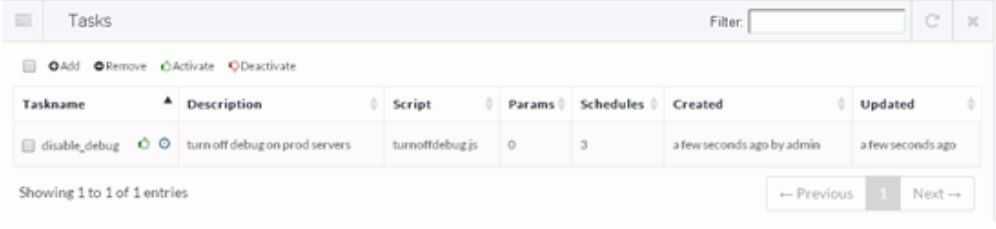
The Repeat switch can be turned on/off by sliding the bar. If task is repeating, then it will execute on a given day/time every week. If the task is non-repeating, it will execute only once on a given schedule.



7. Click *Next* to review the summary of the task, as shown in the following image.

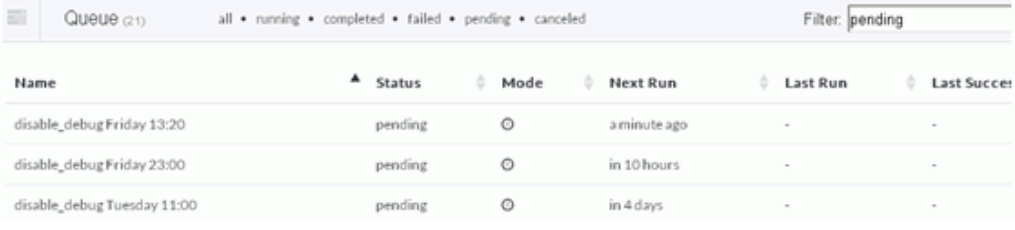
8. Click *Finish* to complete the process.

When the screen is updated, the task is can be viewed in a list of available tasks.



Going into the Queue view of the tasks will show all scheduled executions for the task and their status.

Note: The scheduling is approximate within minute and long running tasks will be displayed in pending status during execution.

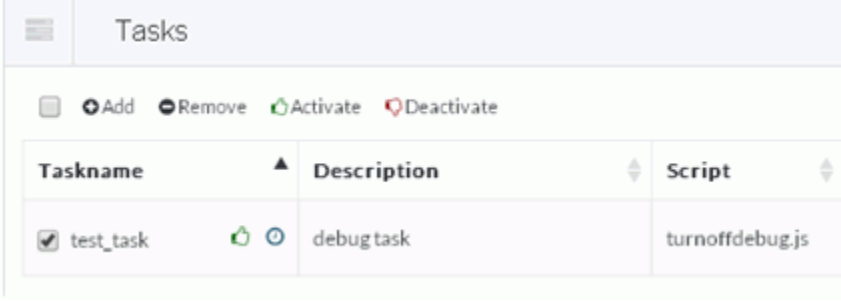


Removing a Task

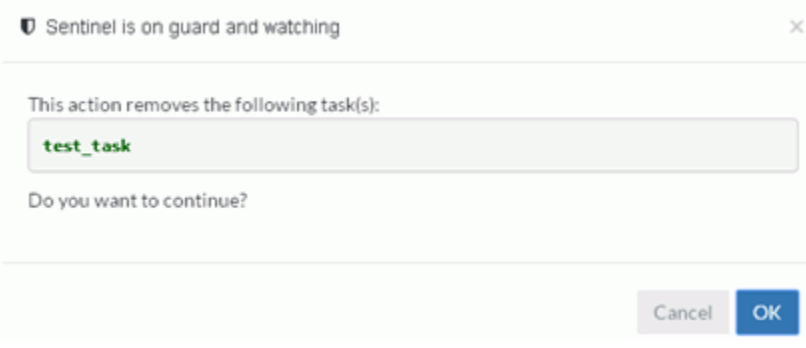
This section describes how to remove a task.

Procedure: How to Remove a Task

1. Under the Managed Tasks view, click the *Remove* link to remove a task.

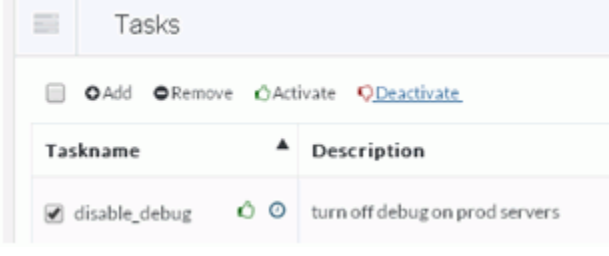


2. A confirmation message is displayed. Click *OK* to remove the task.



The task will be removed from the system.

The task can also be Deactivated from execution rather then removed by selecting a task and clicking on the Deactivate link. This will retain the task, but not execute it.

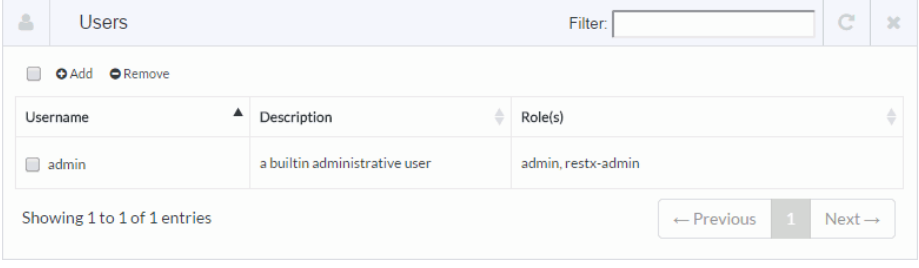


The task will be flagged as deactivated which is denoted by the down-hand.

Configuring Users

A user is identified by a unique name and may have additional propoerties such as description, password, role and group memberships. Groups are formed of users who require similar capabilities, or access to the same resources,

To access Users screen, on the left hand side under the Administration, select Users. The screen will display a list currently users.



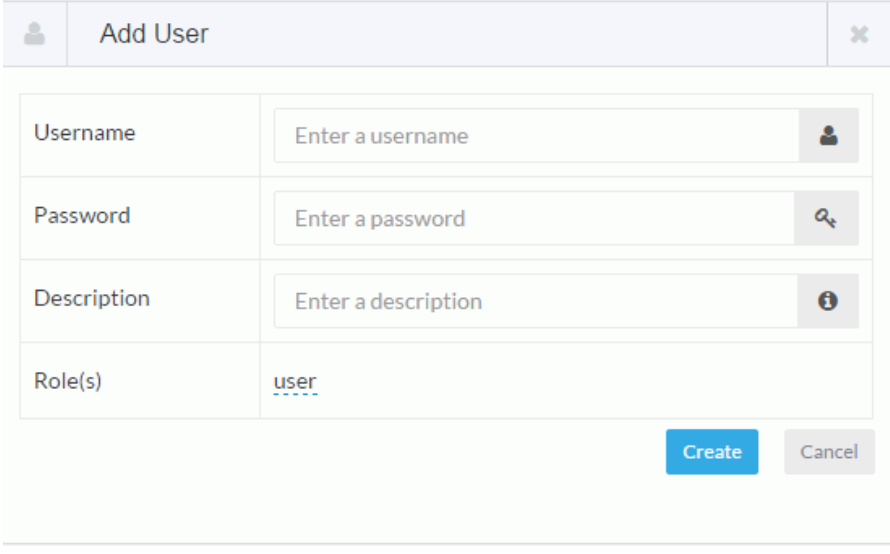
Adding Users

This section describes how to add a user.

Procedure: How to Add a User

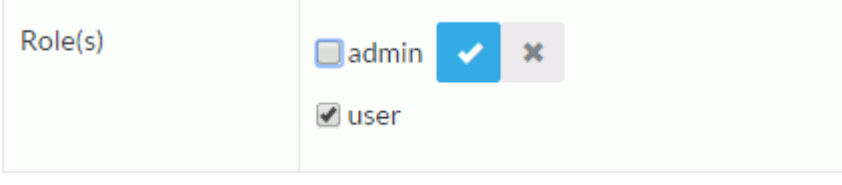
1. Under the Managed Users view, click *Add* to add a new user.

An Add User screen opens, as shown in the following image.



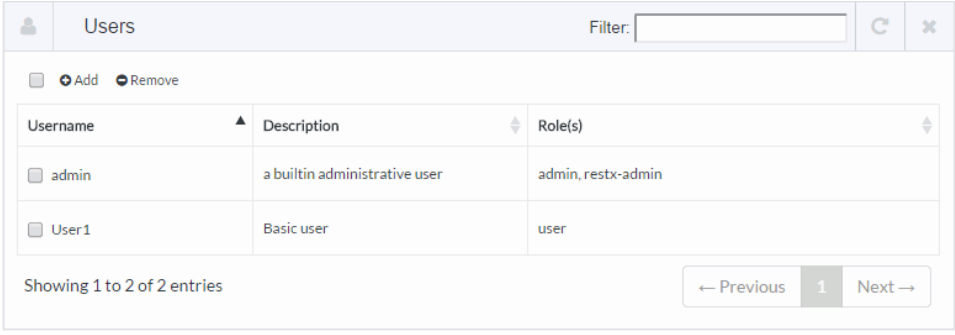
2. Provide the following information:

   - **Username.** Enter an appropriate user name for the new user.
   - **Password.** Enter the password for the new user.
   - **Description.** Enter a description for the new user.
   - **Role(s).** Select either *User* or *Admin*, as shown in the following image.



3. Click *Create*.

When the screen is updated, the new user can be viewed in the list of users, as shown in the example below.

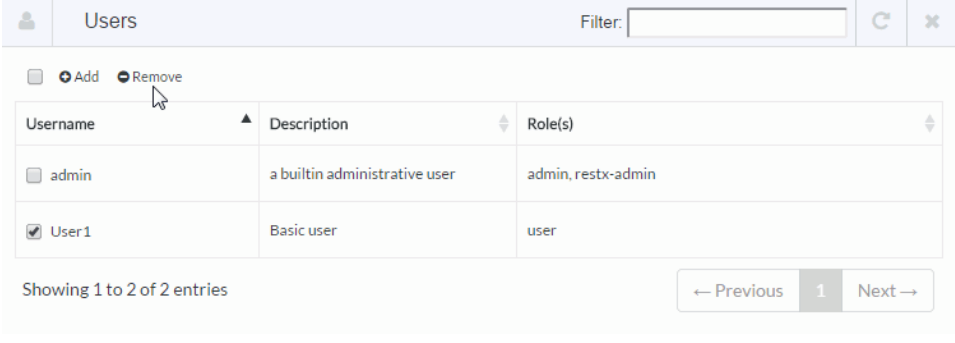


Removing Users

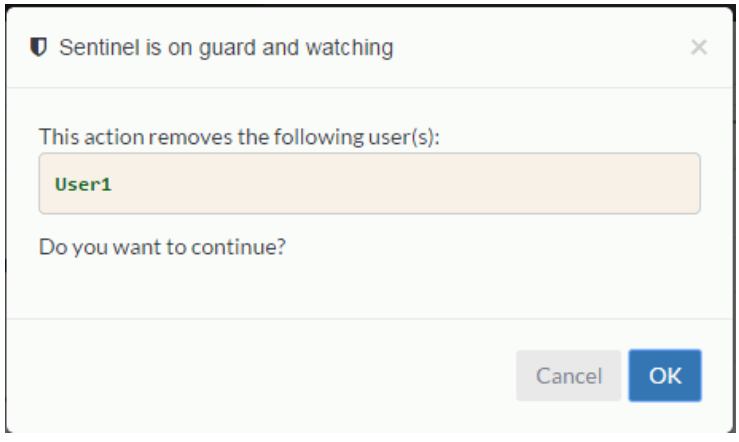
This section describes how to remove a User.

Procedure: How to Remove a User

1. Under the Managed Users view, select the user you would like to remove.
2. Click the *Remove* link to remove a User.



3. A confirmation message is displayed. Click *OK* to remove the user, as shown in the following image.

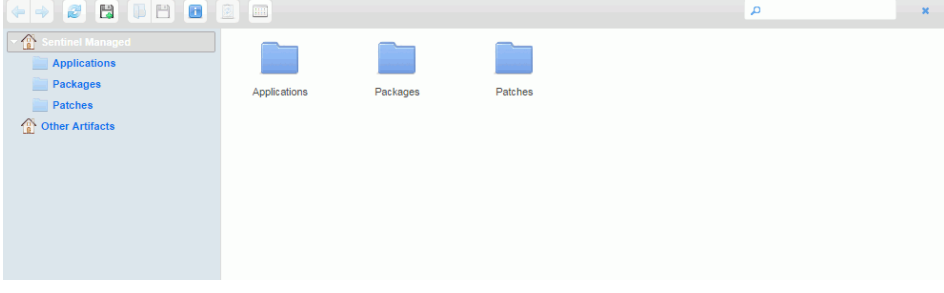


The user is removed from the system.

Managing Files and Artifacts

The Files section of iWay Sentinel administration enables the management of various artifacts within the Sentinel environment. Artifacts can represent anything, from actual iWay Integration Applications (iIAs) and Templates to third-party libraries and plain files. The artifacts maintained in Sentinel repository via SPOG can then be used to be distributed to remote servers for various uses such as installation, deployment, updates. This enables centralized distribution of environment updates to multiple end points from a single environment.

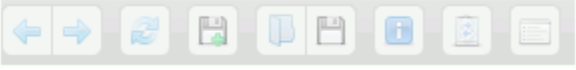
When Files view opens, it presents the following layout.



The two sections presented are *Sentinel Managed* and *Other Artifacts*.

Sentinel Managed include specific artifacts, such as iWay Integration Applications (iIAs), Templates (iIA templates), Packages (iSM packages) and Patches. Other Artifacts include property files, libraries, and so on, which might need to be stored and distributed through Sentinel.

A standard toolbar is available for file interaction:



- Navigate back and forward
- Refresh
- Upload/Add artifact
- Open
- Download
- Information
- Delete
- Icon/List view

Managing Applications

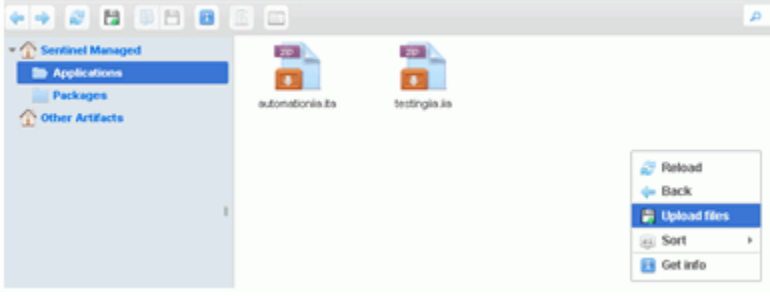
Sentinel Managed components include Applications and Packages. Application is what we know as the iWay Integrated Application (iIA) and its associated Templates, which define the runtime environment. Packages, are the iSM packages which can be published and deployed onto the iSM server to update the server environment.

Adding an Application Component

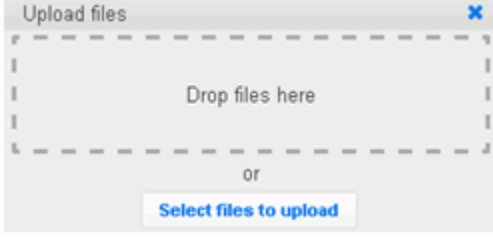
This section describes how to add an Application Component.

Procedure: How to Add an Application Component

1. Click the disk icon with the green +. This will open up a file browser window and enable you to browse to the application to be added to the Sentinel's repository. You may also right-click in the space and select *Upload Files* as shown in the image below.



2. Drag in the files you wish to add to the repository, as shown in the image below. Make sure to upload the *.ita* and *.iia* files for application management. They are necessary for deployment of iWay Integration Application.

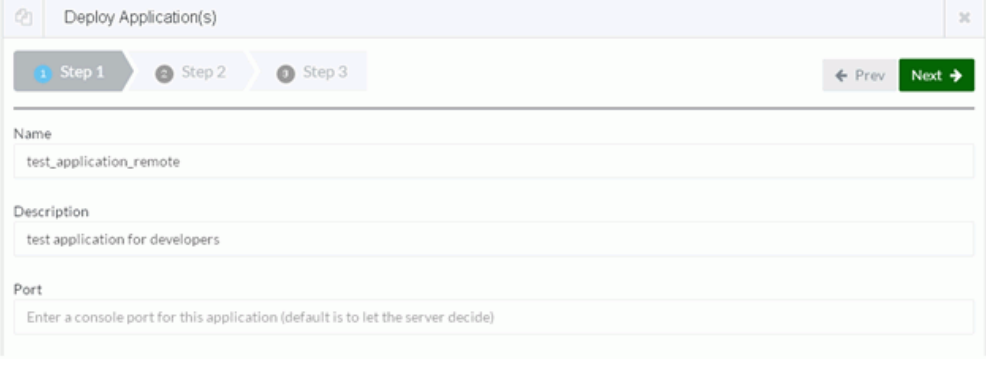


The uploaded files are displayed in the list of available files, as shown in the following example.

3. To deploy an application from repository to remote servers, right-click the *.iia* file and select *Deploy*, as shown in the following image.

A Deploy Application(s) screen opens.

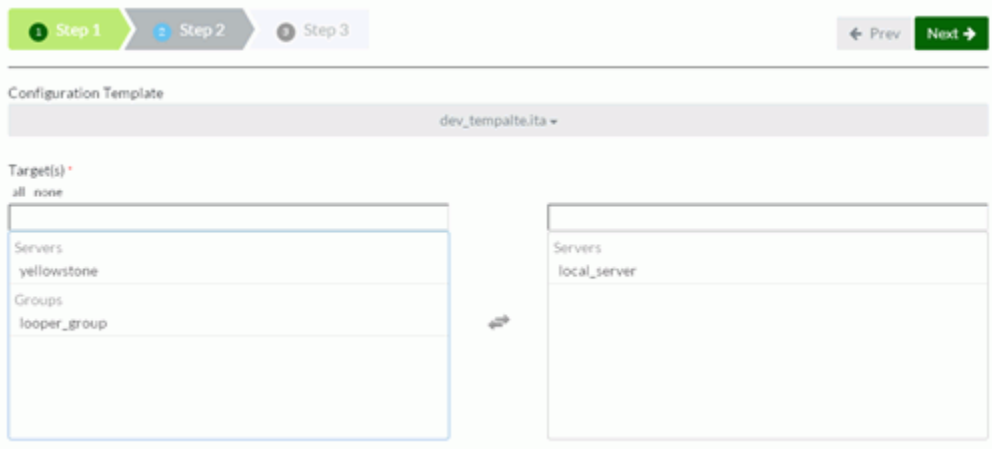
4. Provide a name and optional description for the application to be deployed.



5. Click *Next*.

The Step 2 tab is displayed.

6. Select the template to be used for deployment and the list of possible target servers, or group of servers, as shown in the image below.



7. Click *Next*.

   A confirmation summary message is displayed for the review.

8. Click *Finish*.

The application is deployed in the stopped mode to the specified server.

Managing Artifacts

Other Artifacts folder is designed to store non-application specific components. This is also where you would store the JS script files which can be used to schedule Sentinel tasks for execution.

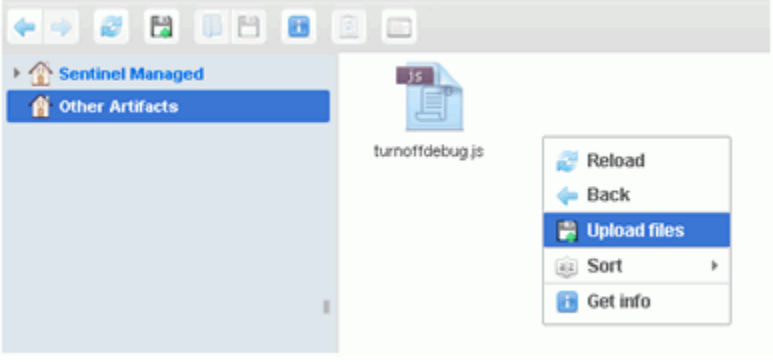
To distribute non-application specific components such as properties files, jar files or any other artifact not managed by application, the artifact needs to be uploaded to the Sentinel's repository and then package needs to be created.

Uploading Artifacts

This section describes how to upload an artifact.

Procedure: How to Upload an Artifact

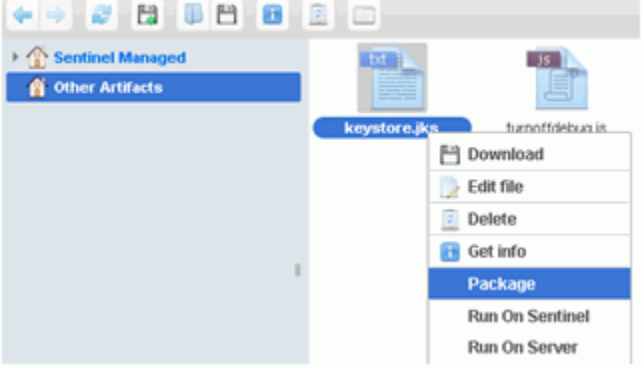
1. To upload an artifact into Sentinel's repository, click the disk icon with green + sign, or right-click and select *Upload Files*.



2. Drag and drop, or browse to the artifact you wish to import into the repository.

   Once imported the artifact is available for use.

3. Right-click the file (or files by highlighting multiples). An options menu is displayed with standard file operations options and Sentinel specific options, as showin in the image below.



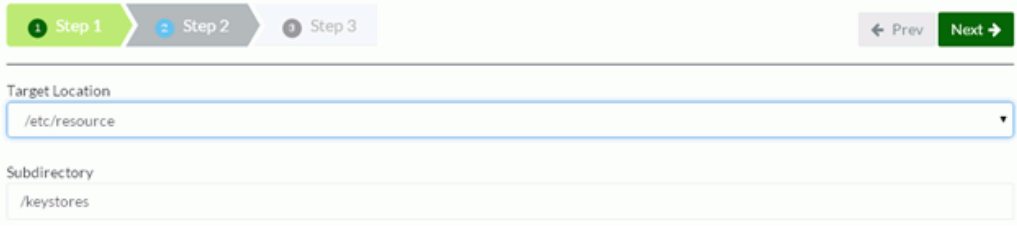
The following options are available:

- **Download.** Download the file locally.
- **Edit file.** Open the file for editing.

- **Delete.** Delete the file from the repository.
- **Get info.** Display information for the selected file.
- **Package.** Create an iSM package for deployment.
- **Run on Sentinel.** Only applicable to scripts, executes the script on the Sentinel server.
- **Run on Server.** Only applicable to scripts, executes the script on an iSM server, which distributes the work.

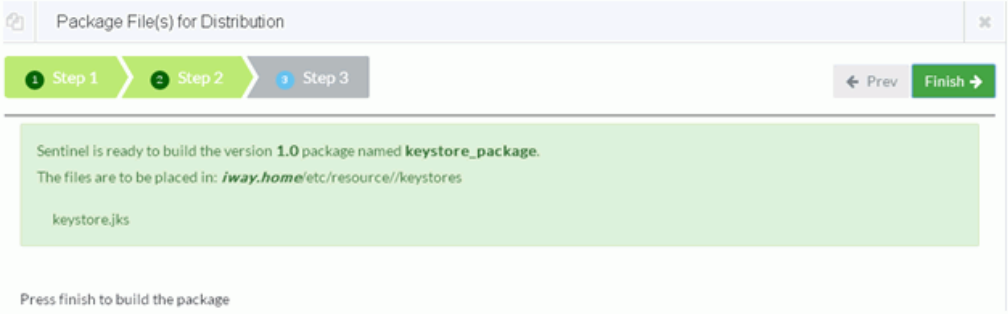
4. To package a component for distribution, select *Package*.
5. Provide the name for the package with optional description and version, as shown in the following image.

6. Click *Next*. Step 2 opens, as shown in the following image.



7. Provide the location hierarchy for how the files should be packaged, as follows:
   - **Target Location.** Location as it relates to the iWay Home directory. Drop down is predefined with common locations.
   - **Subdirectory.** Subdirectory to be created under the Target Location.

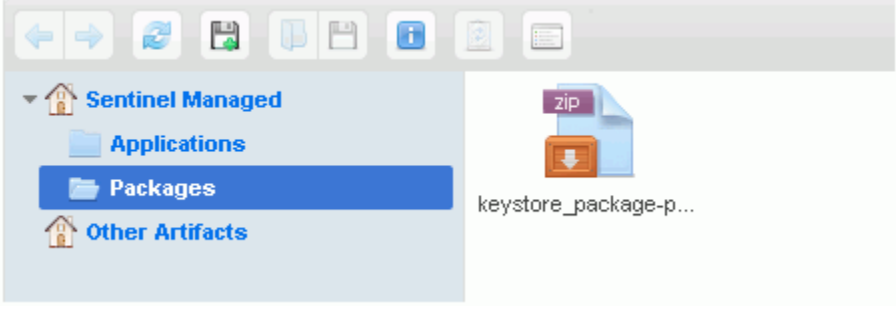
8. Click *Next*. Step 3 opens, as shown in the following image.



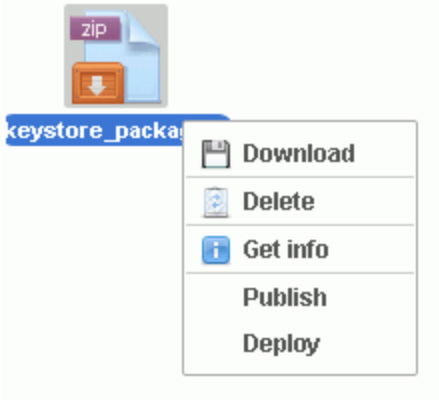
Step 3 provides the confirmation and summary of the package.

9. Review and click *Finish*.

The created package is available under the Packages folder of the Sentinel repository, as shown in the example below.



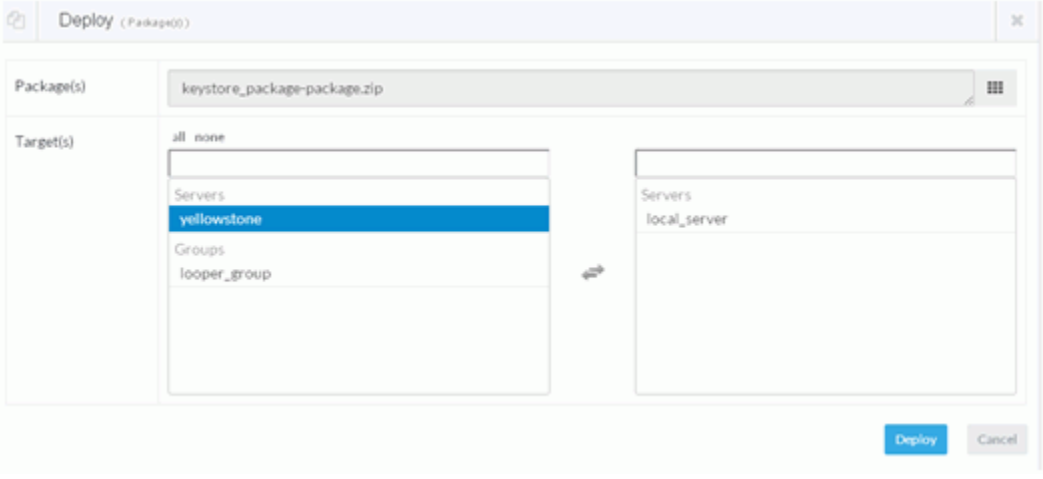
Right-clicking the package presents a menu of available options, as shown in the following image.



The options include:

- **Download.** Download the package to local directory.
- **Delete.** Delete a package.
- **Get info.** Get information for the package.
- **Publish.** Upload the package to the remote server(s). This will only upload but not install the package.
- **Deploy.** Install the package into the remote server(s).

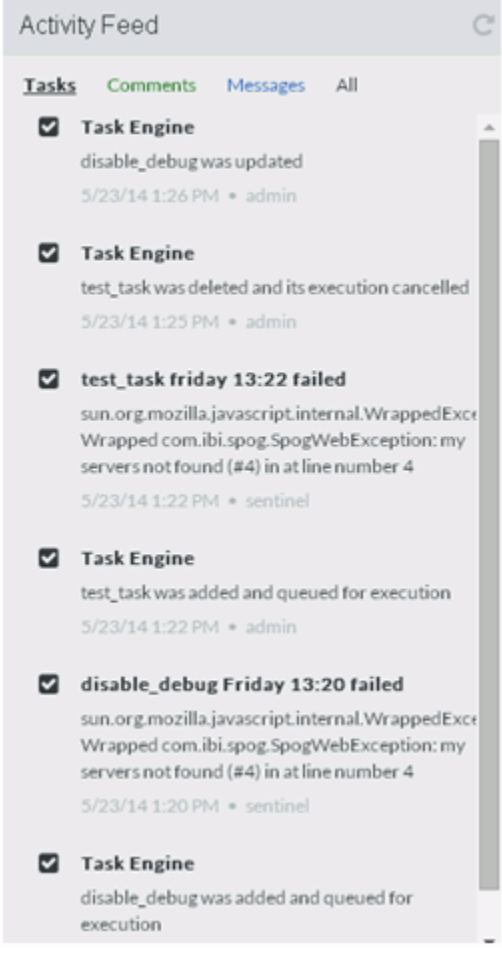
To distribute the package to multiple servers and install it, select *Deploy*. A screen with a selection of servers where it should be deployed is displayed. Select server(s), or a group where the package should be deployed and click *Deploy*.



A confirmation message of successful deployment will be displayed. The package has been installed at the remote server at this point.

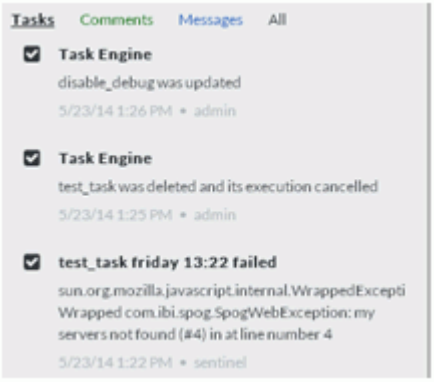
Viewing Activity Feeds

An Activity Feed provides visibility into reflective activity that is recorded by Sentinel. It provides a log of interactions between users and Sentinel, as well as Sentinel and the end server.

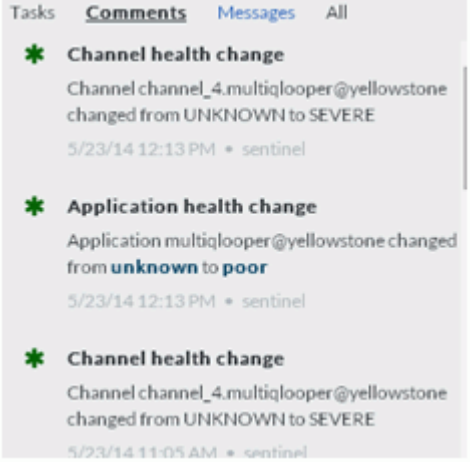


The feeds are separated into the following areas based on their origin:

- **Tasks.** Provide feeds based on the task activity, such as the task being added, scheduled, executed, and its status.



- **Comments.** Provide feeds based on Sentinel activity, such as changes in application health, status, or any other recorded activity being captured and tracked by Sentinel automatically. This activity can also be reflective from actions done through tasks, such as updating servers, starting/stopping applications, and so on.



- **Messages.** Provide feeds based on user interactions with SPOG.

Chapter 7

SSL Configuration

Note: This functionality is applicable only to monitoring iWay Release 8.0.3 or higher servers.

When first installed, Sentinel and Envoy communicate over HTTP. To secure the communication with SSL, see *How to Configure Sentinel for SSL* on page 93 and *How to Configure Envoy for SSL* on page 94.

Sentinel and Envoy can automatically detect when the iWay Service Manager console is secured with SSL. This does not require any special configuration in Sentinel and Envoy.

In this chapter:

Configuring Sentinel and Envoy Security for SSL

The following procedures describe the steps for configuring Sentinel and Envoy security for SSL.

Procedure: How to Configure Sentinel for SSL

1. Create a keystore file that contains the Sentinel private key.
2. Create a keystore file that will be used as a truststore. This file must contain the certificate of the Certificate Authority that signed the Envoy server certificate.
3. Start Sentinel by typing the following syntax on one line:

```
java -Dcom.ibi.spog.ssl.ignoreHostnameVerify
  -Djavax.net.ssl.trustStore=tsPath
  -Djavax.net.ssl.trustStorePassword=tsPassword
  -Djavax.net.ssl.trustStoreType=tsType
  -Djavax.net.ssl.keyStore=ksPath
  -Djavax.net.ssl.keyStorePassword=ksPassword
  -Djavax.net.ssl.keyStoreType=ksType
  -jar sentinel.jar -httpsPort=port -keyAlias=alias
```

where:

tsPath

Is the absolute path to the truststore file.

tsPassword

Is the password of the truststore file.

tsType

Is the truststore file type, for example, JKS.

ksPath

Is the absolute path to the keystore file.

ksPassword

Is the password of the keystore file.

ksType

Is the keystore file type, for example, PKCS12.

port

Is the HTTPS port, for example 8443.

alias

Is the alias for the Sentinel private key entry in the keystore file.

If the Common Name (CN) of the Envoy certificate reflects the correct host name, you can enable host name verification by omitting the following option:

```
-Dcom.ibi.spog.ssl.ignoreHostnameVerify
```

4. Open the Sentinel console with an HTTPS URL at the chosen port, for example:

   ```
   https://localhost:8443
   ```

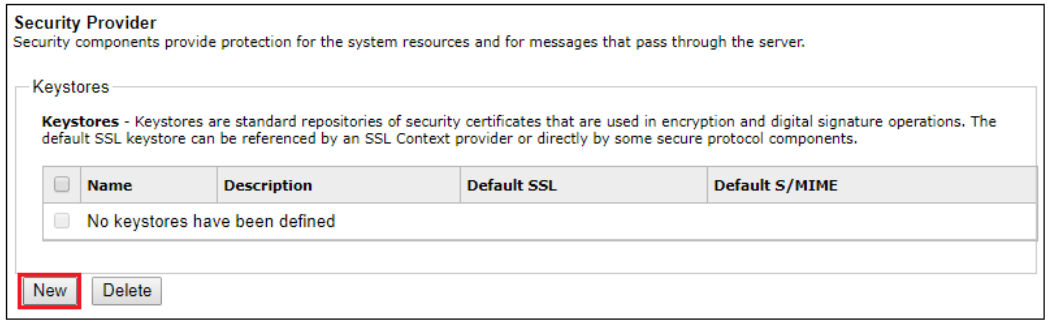
5. Optionally, create a shell script or batch file with this command to make it easier to start Sentinel the next time.

Procedure: How to Configure Envoy for SSL

1. Create a keystore file that contains the Envoy server private key.
2. Create a keystore file that will be used as a truststore. This file must contain the certificate of the Certificate Authority that signed the Sentinel server certificate.
3. Start iWay Service Manager (iSM) and open the iSM Administration Console.

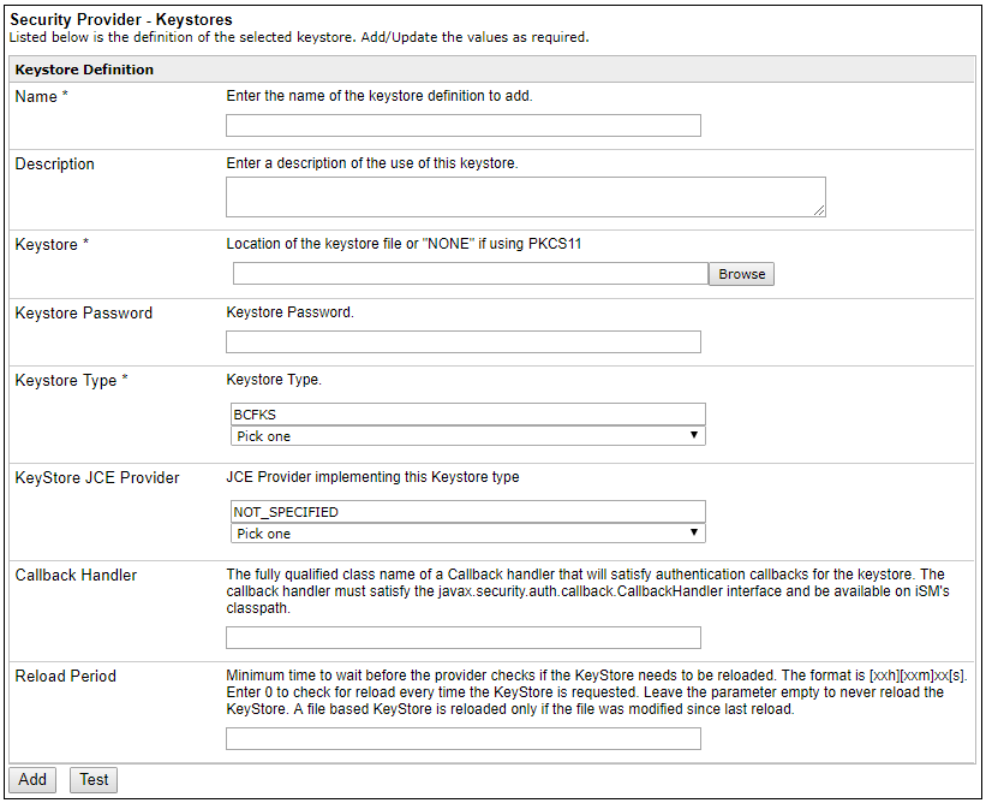
4. In the left pane, select *Security Provider*, as shown in the following image.

The Security Provider page opens, as shown in the following image.



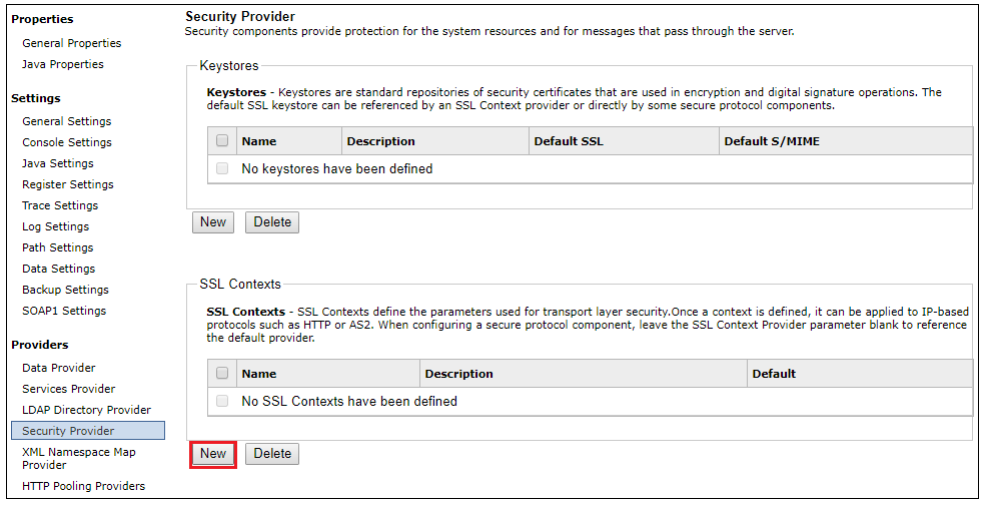
5. Click *New* to create a Keystore provider for the keystore in step 1.

The Keystore Definition pane opens, as shown in the following image.

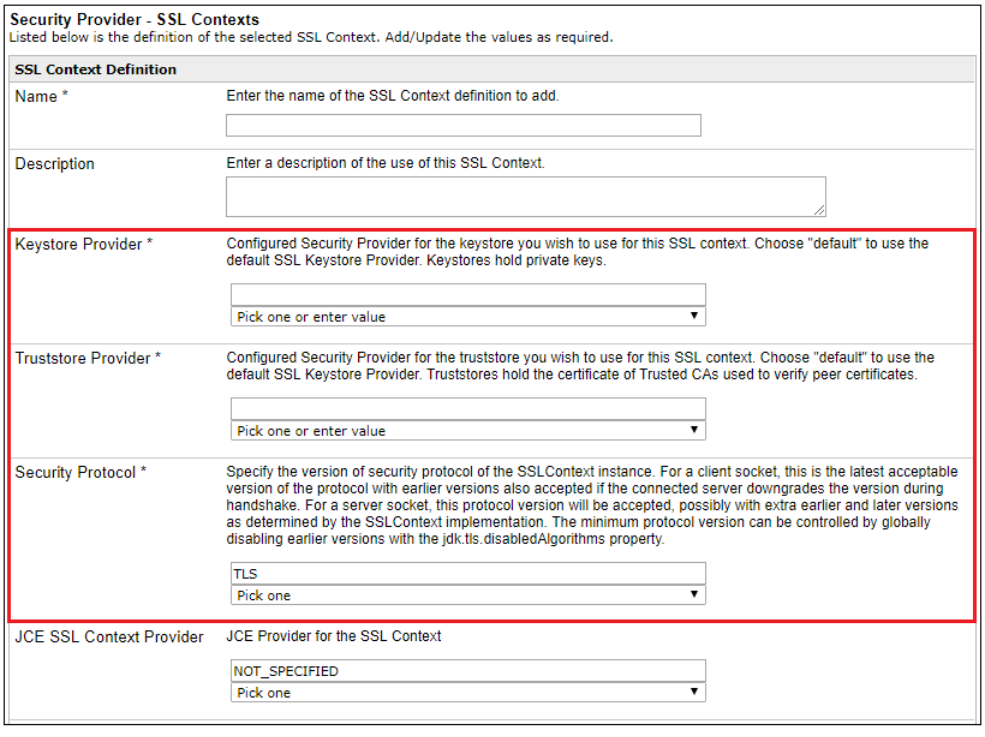


6. Specify values for the configuration parameters based on the keystore file you created in step 1.
7. Click *Test* to confirm your keystore settings, and then click *Add* to finish.
8. Repeat steps 5-7 to create a Keystore provider for the truststore in step 2.

9. Return to the Security Provider page and click *New* in the SSL Contexts section to create an SSL Context Provider for Envoy, as shown in the following image.



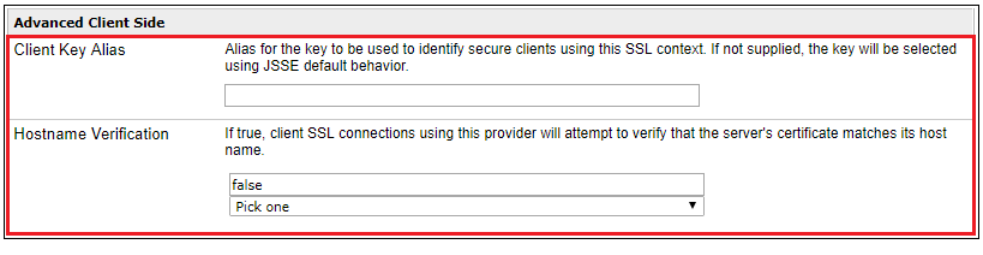
The SSL Context Definition pane opens, as shown in the following image.



a. Select the Keystore Provider and Truststore Provider from the corresponding drop-down lists.

b. Choose the Security Protocol for the version of TLS.

c. Scroll down the page to view additional configuration parameters, as shown in the following image.

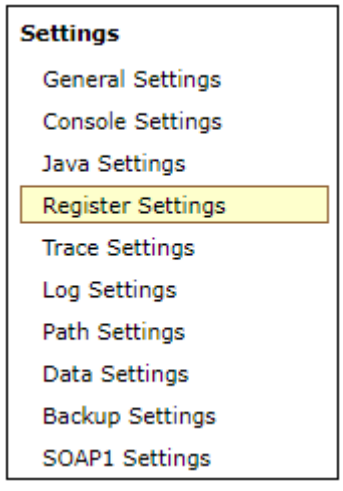


d. Specify a Client Key Alias if the Keystore in step 1 contains keys other than the Envoy private key.

e. Enable Hostname Verification if the Common Name (CN) in the Sentinel certificate reflects the correct host name, otherwise disable Hostname Verification.

f. When you are finished specifying values for the SSL Context Provider configuration parameters, scroll down the page and click *Add*.

10. In the left pane, select *Register Settings*, as shown in the following image.



The Register Settings page opens.

11. Click the special register named *envoy-secure* and change the value to *true*.
12. Click the special register named *envoy-sslcontextprov* and change the value to the name of the SSL Context Provider created in step 5.
13. To configure Envoy to register with Sentinel the next time it starts, perform the following steps, otherwise skip to step 14.

    a. Edit or add the special register *sentinel-url*. The value is the Sentinel URL. A typical value would be *http://host:8080* or *https://host:8443*.

    b. Edit or add the special register *sentinel-uid*. The value is the user name to log into Sentinel. A typical value would be *admin*.

    c. Edit or add the special register *sentinel-pwd*. The value is the password to log into Sentinel. A typical value would be *admin*.

14. Restart iSM.
15. If you have not configured Envoy to register with Sentinel again, you must go in the Sentinel console and edit the corresponding server registration to turn on the SSL toggle. You must do this only once per server.

Appendix A

Sentinel Configuration Properties

Sentinel creates a file called sentinel.properties, which is located in the following folder:

`C:\Users\userid\spog`

Before making any changes to this file, it is recommended to create a backup copy so you can revert to the default settings.

This section describes the available Sentinel configuration properties.

In this appendix:

Configuring the Health Model Properties

To modify the health calculations, the following properties can be changed:

```
sentinel.health.responsetime = -0.25
sentinel.health.throughput = 1
sentinel.health.maxthroughput = 2
sentinel.health.error = -20
sentinel.health.active = 0.5
sentinel.health.completed = 0.5
sentinel.health.queued = -0.5
```

Note that the absolute value of the number is the actual weight for the calculation, which means how important the value is. The minus (-) sign indicates if we want the value to be lower for the health to be better. For example, you would want the error count to be lower to indicate a healthy system, so you would indicate this by having a minus (-) sign in front of the value.

Preserved Properties

The following properties within the sentinel.properties file should not be changed, as it will cause an adverse effect and will destabilize the system. The values shown below are just default values, which vary based on your installation and should not be changed to match these sample values.

```
storage.directory = C:\\Users\\sk10803\/spog\/graph
storage.backend = persistit
storage.transactions = true
storage.buffercount = 10000
cache.db-cache = true
fast-property = true
storage.buffer-size = 0
```

Appendix B

General Notes Related to the User Interface

This section provides general notes related to the Single Pane of Glass (SPOG) Sentinel user interface.

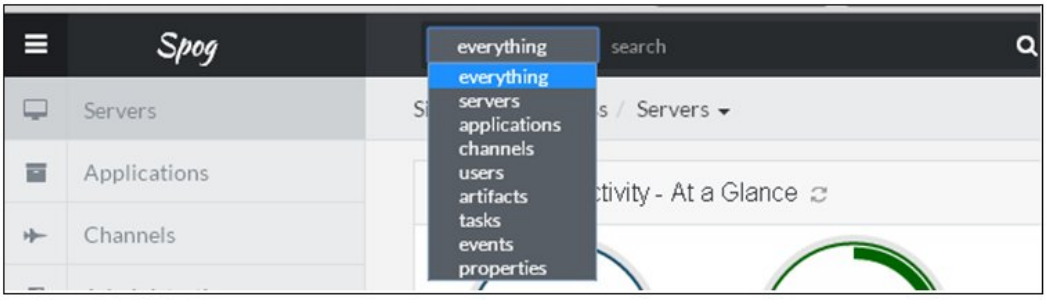
In this appendix:

Filtering and Searching

All the screens within the Sentinel interface have the ability to filter for specific components. The filter is available on most levels including servers, applications, channels, and others. The Filter field is located in the upper-right corner of each section, as shown in the following image.

The filtering action returns those components that contain the name of the specified filter string.

There is also a global search available on the top banner with a selection of components which you want to search for. You can also search across all components by selecting everything from the drop-down list, as shown in the following image.

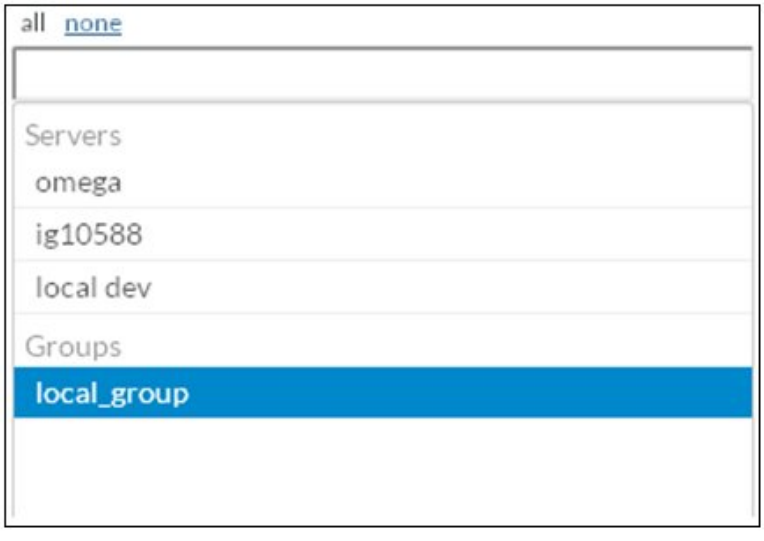


Sorting and Ordering Columns

Under each main section of component such as server, application and its details, the data is presented as a table with columns which can be sorted. Each column in the table contains arrows that enable you to switch the sorting within the column and identify which column should be used for sorting.

Groups

Management and monitoring actions throughout Sentinel can be performed on single instance of the component or on a group of components. Once group is defined as noted in the Groups section, it becomes available for selection throughout the monitoring and management actions. The groups will show up under the Groups section of the selection window if action supports such activity, as shown in the following image.



The selection screens also have an option to select *all* or *none*, which is represented by the two hyperlinks above the selection field.

Groups can also be used to filter information for monitoring. For example, click the *Servers* hyperlink while viewing a list of servers to display a selection of groups that can be filtered.

You can then select a desired group and the list displayed will be updated with components only within the selected group, as shown in the following image.

Appendix C

iWay Sentinel Scripting

This appendix describes the rules and methods that are required to develop scripts for use with iWay Sentinel. Examples are provided accordingly.

In this appendix:

Obtaining Sentinel Objects

iWay Sentinel provides a way to obtain handlers for Sentinel objects outlined in the next section. For example, the following code sample shows how to retrieve a list of servers in script:

```
var srvrs = $(".server").list();
for(index in srvrs)
{
    println(srvrs[index].name+","+srvrs[index].description);
}
```

This script will return a native array of Server objects that you can iterate in a for-loop, where `$(".server")` retrieves a handler for a Sentinel class.

iWay Sentinel Classes

There is a set of classes iWay Sentinel makes available in scripts. All classes passed into the $ method must be singular and lower-case, as shown in *Obtaining Sentinel Objects* on page 107. Below is a list of classes hat can be passed into $ and their methods.

Common Fields

All of these classes (except package) have this set of fields that can be consumed in a script.

The following table lists and describes these common fields.

Field Name	Description
name	The name of the object.
description	The object description.
created	Indicates when the object was created.
modified	Indicates when the object was modified.
id	The auto-assigned unique ID.
asof	Indicates the last time the object was checked or accessed.

Common Fields That Can be Monitored

Objects that can be monitored include server, application, and channel. All of these objects have a set of common fields.

The following table lists and describes these common fields that can be monitored.

Field Name	Description
responseTime	Applicable only for servers. Indicates the time it takes to ping a server. Does not account for propagation time.
queueSize	The number of messages in queues.
messagesInprocess	The number in messages active or in process.
messagesCompleted	The number of successful messages processed.
messagesFailed	The number of successful messages failed.
maxThroughput	The objects maximum message throughput in seconds.
throughput	The objects current message throughput since last query.
health	The health of the object.

Field Name	Description
status	The connectivity status for a server, which is represented by the UP/DOWN indicator for applications and channels.

server

An object that represents an instance of an iSM master, typically the *base* configuration. Servers must be registered in SPOG/Sentinel either manually or by an import script. A server requires an Envoy for it to communicate with iWay Sentinel. Servers are referenced by their name or alias you provide during registration, and not by their URLs. As a result, you can register the same server under different aliases and SPOG/Sentinel will treat them as separate servers.

Fields

Field Name	Description
url	The URL to a server Envoy.
username	The user name to the server.
password	The password to the server.
version	The server version.
host	The host name where the server resides.
envoyPort	The Envoy port on the server.
consolePort	The console port of the server.
hostUsername	The host user name.
hostPassword	The host password.

Methods

Method Name	Description
list()	Returns a list of all servers registered in iWay Sentinel.
property(serverName, key, value)	Sets a server property or Special Register (SREG). This does not set a value in any property file on the server.
remove(serverName)	Removes the server from iWay Sentinel.
get(serverName)	Gets a server.
start(serverName)	Starts a server (Windows only and requires PsService installed on the SPOG/Sentinel host). Also requires the server to be running as a service.
stop(serverName)	Stops a running server.
restart(serverName)	Restarts a running server (Windows only). Also requires the server to be running as a service.

application

An object that represents an application deployed in a Server. You can have an application with the same name deployed into different servers, so you typically must have the server of the application when referencing it.

Fields

Field Name	Description
server	The server name of the application.
version	The server version of the application.

Methods

Method Name	Description
list()	Gets all applications for all servers.
property(serverName, applicationName, key, value)	Sets an iSM property in the application.
start(serverName, applicationName)	Starts an application.
stop(serverName, applicationName)	Stops an application.
get(serverName, applicationName)	Gets an application.
channels(serverName, applicationName)	Gets the channels of an application.
deploy(serverName, applicationName, applicationArtifactIIA, port, template, description, overwrite)	Deploys an iWay Integration Application (iIA) to a server to become an application.
undeploy(serverName, applicationName)	Undeploys an application.
redeploy(serverName, applicationName)	Redeploys an application that has already been published into the server.

channel

An object that represents the channels in an application. You need the server and application name to reference it.

Fields

Field Name	Description
uptime	The length of time the channel has been up.
type	The type of listener the channel is configured to use.

Field Name	Description
workerCount	The number of workers the channel is configured to use.

Methods

Method Name	Description
list()	Returns all changes from all applications in all servers registered in SPOG/Sentinel.
start(id)	Starts a channel by its ID. You must know the application of the channel in order to get the ID of the channel.
stop(id)	Stops a channel by its ID.
property(serverName, applicationName, channelName, key, value)	Sets an iSM property on the channel.

group

An object that represents groups in SPOG/Sentinel. Groups can contain servers, applications, users and artifacts.

Fields

Field Name
servers
users
artifacts
applications

Methods

Method Name	Description
upsert(group)	Inserts or updates a group. Takes a group object.
get(groupName)	Returns a group.
list()	Returns an array of all groups.
delete(groupName)	Delete a group from SPOG/Sentinel.

user

An object that represents a user in SPOG/Sentinel.

Fields

Field Name	Description
roles	User roles in SPOG/Sentinel.
password	Password to SPOG/Sentinel.

Methods

Method Name	Description
upsert(user)	Inserts or updates a user in SPOG/Sentinel.
get(userName)	Returns a user.
list()	Returns all users.
delete(userName)	Delete a user from SPOG/Sentinel.

task

An object that represents the sentinel backend task processing.

Fields

Field Name	Description
active	If true, then the task is queued for execution.
continuous	If true, then the task is executed repeatedly.
script	The name of the JavaScript artifact that the task will execute.
schedules	A complex object that defines the delay and wait period for executions.
params	The parameters of the task it will set when executing a script.

Methods

Method Name	Description
list()	Returns all tasks.
upsert(task)	Takes a task object and inserts or updates it.
get(taskId)	Returns a task.
delete(taskId)	Returns a task.

artifact

An object that represents a file uploaded into the file browser in SPOG. Artifacts are referenced by file name only and not by its directory path. When requesting an artifact from a script, do not provide its directory path.

Fields

Field Name	Description
path	The directory path of the artifact.
mimeType	The mime type of the artifact.

Methods

Method Name	Description
get(artifactName)	Gets an artifact by name, not by path.

package

An object that represents a package that can be used to apply changes to an existing Server or Application.

Fields

This object does not exist.

Methods

Method Name	Description
publish(serverName, artifactName)	Publishes a package to a server.
deploy(serverName, artifactName)	Deploys a package to a server.

Script Host

The host can be referenced by the code listed and described in the following table.

Code	Description
`$("#")`	Returns the script host.
`$("#").progress`	A numeric value between 0 - 100 that sets the progress of a running script.
`$("#").stop`	A boolean value that can be set by SPOG requesting for your script to stop executing.
`$("#").log("hello!")`	A function that will enter a task message in the activity feed in SPOG.

Available variables include *logger*, which is an Apache commons logger.

Task Script Examples

This section provides examples that can only be executed as a Task because they require parameters to be set. Executing them in the file browser will result in an error appearing in the activity feed.

Note: All variables underlined must be defined when creating a Task.

Change Channel Worker Threads

The following example sets the number of worker threads for a channel to 2.

```
$(".channel").property(serverName, applicationName, channelName,
"config.count", "2");
```

Change Server JVM Options

The following example sets the JVM options for a server.

```
$(".server").property(serverName, "config.JVM_OPTION", "-Xmx=512");
```

Deploy a Package

The following example deploys a package to a server. You must create a package from SPOG prior to deploying in a script. You cannot create a package in a script.

```
$(".package").deploy(serverName, packageArtifactName);
```

Undeploy a Package

The following example undeploys a package.

```
$(".package").undeploy(serverName, packageArtifactName);
```

Deploy an Application

The following example deploys an application. An example of portNumber could be 10003.

```
$(".application").deploy(serverName,
                         applicationName,
                         iiaArtifactName,
                         portNumber,    // integer
                         templateArtifactName,
                         description,
                         overwrite     // boolean
                         );
```

Undeploy an Application

The following example undeploys an application.

```
$(".application").undeploy(serverName, applicationName)
```

Start an Application

The following example starts an application.

```
$(".application").start(serverName, applicationName);
```

Stop an Application

The following example stops an application.

```
$(".application").stop(serverName, applicationName);
```

Start a Channel

The following example retrieves all the channels from an application and starts the channel matching the channelName.

```
var channels = $(".application").channels(serverName, applicationName);
for(i in channels) {
        if(channels[i].name == channelName) {
              $(".channel").start(channels[i].id);
              break;
        }
}
```

Stop a Channel

The following example retrieves all the channels from an application and stops the channel matching the channelName.

```
var channels = $(".application").channels(serverName, applicationName);
for(i in channels) {
        if(channels[i].name == channelName) {
              $(".channel").stop(channels[i].id);
              break;
        }
}
```

Other Script Examples

The scripts described in this section can be executed as a task or from the file browser. They do not require a parameter to be set.

Server Import

The following example creates an array of servers and upserts them into iWay Sentinel. The script also checks to see if an admin requested to stop the script and sets the progress while it is running.

```
var servers = [
    {
name:"localhost",
description:"a default description for an installed server on your
localhost",
url:"http://localhost:9001",
username:"admin",
password:"admin",
hostUsername:"hostadmin",
hostPassword:"hostadmin"
     },
];
var step = 100 / servers.length;
for(index in servers)
{
if($("#").stop) break;
    $("#").progress += step;
    $(".server").upsert(servers[index]);
logger.info("upserted "+servers[index]);
}
```

Turn On Debug by Group

The following example creates a group called *my servers* containing all servers and upserts it into iWay Sentinel. Then the scripts gets the group, iterates through its servers and changes the debug configuration to *true* if the status of the server is UP and its Health is either POOR or SEVERE. Notice the Status.UP, Health.POOR and Health.SEVERE objects. The package is imported in which these objects reside and is used to check the status of the server.

```
importClass(com.ibi.spog.models.Status);
importClass(com.ibi.spog.models.Health);
var servers = $(".server").list();
var group =  { name:"my servers",  description:"All Servers", servers :
[ ] }
for(index in servers) group.servers.push(servers[index]);
$(".group").upsert(group);
var servers = $(".group").get("my servers").servers;
var step = 100 / servers.length;
for(index in servers)
{
    if($("#").stop)   break;
    $("#").progress += step;
    if(servers[index].status == Status.UP &&
    (servers[index].health == Health.POOR || servers[index].health ==
Health.SEVERE))
    {
        $(".server").property(servers[index].id, "config.debug", "true");
    }
}
```

Increase Throughput

The following example tries to increase throughput by increasing the number of worker threads for channels that have a max throughput below 0.5 messages per second.

```
$("#").log("Checking throughput");
var servers = $(".group").get("my servers").servers;
var step = 100 / servers.length;
for(i in servers)
{
    if($("#").stop) break;
    $("#").progress += step;
    var apps = $(".server").applications(servers[i].name);
    for(j in apps)
    {
        var channels = apps[j].channels(servers[i].name, apps[j].name);
        for(k in channels)
        {
            if(channels[k].maxThroughput < 0.5)
            {
                $(".channel").property(
                        servers[i].name,
                        apps[j].name,
                        channels[k].name,
                        "config.count",
                        "2");
            }
        }
    }
}
```

Feedback

Customer success is our top priority. Connect with us today!

Information Builders Technical Content Management team is comprised of many talented individuals who work together to design and deliver quality technical documentation products. Your feedback supports our ongoing efforts!

You can also preview new innovations to get an early look at new content products and services. Your participation helps us create great experiences for every customer.

To send us feedback or make a connection, contact Sarah Buccellato, Technical Editor, Technical Content Management at *Sarah_Buccellato@ibi.com.*

To request permission to repurpose copyrighted material, please contact Frances Gambino, Vice President, Technical Content Management at *Frances_Gambino@ibi.com.*

Information Builders

iWay

iWay Sentinel User's Guide

Version 1.2

DN3502152.0619

Information Builders, Inc.
Two Penn Plaza
New York, NY 10121-2898