Table of Contents

About this Guide ................................................................. 9
  Document Conventions .................................................. 9
  Documentation Installation ............................................. 9
  Online Information ...................................................... 10

Part I.  Understanding Command Central .................................. 13

1. Command Central Overview ............................................. 15
  About Command Central ................................................ 16
  Command Central Features .............................................. 16
  Command Central Architecture ........................................ 17
    Command Central User Interfaces .................................. 17
    Command Central Server ............................................. 18
    Platform Manager ..................................................... 18
    Platform Manager Installation and Configuration ............... 19
  Command Central Terminology ....................................... 19
  Getting Started .......................................................... 20

2. Using the Command Central Web User Interface ...................... 21
  Accessing Command Central .......................................... 22
  Understanding the Web User Interface ............................... 22
    View Environments ................................................... 22
    View Instances ...................................................... 23
      Monitor Instances .................................................. 23
      View Dashboard Information .................................... 24
      View Details of Instances ....................................... 25
      View Configuration Parameters ................................. 25
    View Installations .................................................. 26
      View Details of an Installation ................................ 27
      View Products in an Installation ................................ 27
      View Fixes Applied to the Products In an Installation ..... 27
    Change Authentication Mode ....................................... 27
    Manage Lifecycle Actions ......................................... 28
  Using Icons ............................................................... 28
    Installation Status Icons ......................................... 28
    Instance Status Icons .............................................. 28
    Alerts Icons .......................................................... 29

3. Administering Environments ............................................ 31
  About Administering Environments .................................. 32
  Adding Environments .................................................. 32
Filtering Environments ....................................................... 33
Editing Environments ....................................................... 33
Deleting Environments ....................................................... 34
Hiding/Showing Environments Pane .................................. 34

4. Administering Installations ........................................... 35
   About Administering Installations .................................. 36
   Adding Installations .................................................... 36
   Viewing Installations ................................................... 37
   Searching for Installations .......................................... 37
   Removing Installations ............................................... 38
   Linking Installations to Multiple Environments .................. 38
   Monitoring Installations ............................................. 39

5. Securing the Command Central Landscape ....................... 41
   About Securing the Command Central Landscape ............... 42
   Changing the Internal User Administrator Password .......... 42
   Setting Up Security ................................................... 42
   Setting Outbound Authentication ................................... 43
   Accessing Command Central through My webMethods .......... 44
   Accessing Administrative Interfaces through Command Central 44
   Configuring Ports ..................................................... 44
      Default Ports ....................................................... 45
   Configuring Port Connection Settings ............................. 45

6. Configuring Products .................................................. 47
   Product-Specific Configuration .................................... 48
   Configuring Instances ............................................... 48
   Testing a Configuration .............................................. 48
   References to File Locations in Product Configuration Files . 49
   Configuring OSGi Profiles ............................................ 50
      Protocols that Command Central Supports in OSGi Profiles 50
      Products that Support Port Configuration in OSGi Profiles 51
      JMX Port Authentication ......................................... 51
      Configuring Ports in OSGi Profiles .............................. 52
         Adding Ports .................................................. 52
         Viewing the Port Settings ................................... 56
         Editing and Testing OSGi Port Information .................. 56
         Deleting a Port ............................................... 57

7. Managing Command Central Licenses ............................... 59
   Command Central License Overview ................................. 60
   Viewing the Command Central License Information ............. 60
   Changing a Command Central License Key ........................ 60
   Renewing a Command Central License Key ........................ 61
8. Managing Users, Groups, and Roles ........................................ 63
   Managing Command Central Users, Groups, and Roles ............... 64
   Using Internally Defined User and Group Information ............... 64
      internaluserrepo Script ........................................... 65
      internaluserrepo Exit Codes ..................................... 66
   Adding Users to the Internal User Repository .......................... 67
   Deleting Users from the Internal User Repository ..................... 67
   Using Externally Defined User and Group Information ............... 67
      How Command Central Authenticates Externally Defined Clients .... 68
      Overview of Using LDAP ........................................... 68
      LDAP Profile Properties ......................................... 69
      Configuring LDAP Profile Properties ............................ 71
   Using JAAS with Command Central ...................................... 72
      JAAS Configuration File .......................................... 72
      Configuring the jaas.config File to Use LDAP/AD .................. 73
   Groups .................................................................. 74
      Default Group ....................................................... 75
      Managing Groups .................................................... 75
   Roles .................................................................. 75
      Default Roles ......................................................... 76
      Managing Roles ....................................................... 76

9. Viewing Product Inventory .................................................. 79
   About Inventory Management ............................................... 80
   Viewing Products in an Installation ...................................... 80
   Viewing Fixes Applied to Products in an Installation .................. 80

10. Administering Product Lifecycle ......................................... 81
    About Administering Product Lifecycle .................................. 82
    Lifecycle Actions ................................................................ 82
    Starting, Stopping, Pausing, Resuming, and Debugging Instances .. 82

11. Monitoring Instances ....................................................... 83
    About Monitoring Instances ............................................ 84
    Viewing the Status of an Instance or Its Components .............. 84
    Modifying the Status of an Instance or Its Components ............ 84
    About Monitoring KPIs .................................................. 84
    Viewing Alerts for an Instance or Its Components .................. 85
    Clearing Alerts for an Instance or Its Components ................. 86
    About Monitoring-Related Events ...................................... 87

12. Comparing Product Versions, Fixes, and Configurations ........... 89
    About Comparing Products ............................................ 90
    Comparing Product Versions ......................................... 90
    Comparing Fix Levels .................................................. 90
    Comparing Configuration Settings .................................... 91
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universal Messaging License Configuration</td>
<td>127</td>
</tr>
<tr>
<td>Changing Universal Messaging License</td>
<td>127</td>
</tr>
<tr>
<td>Universal Messaging Lifecycle Actions</td>
<td>127</td>
</tr>
<tr>
<td>Universal Messaging Ports Configuration</td>
<td>128</td>
</tr>
<tr>
<td>Port Configuration Attributes</td>
<td>128</td>
</tr>
<tr>
<td>Basic Port Connection Attributes</td>
<td>128</td>
</tr>
<tr>
<td>Port Security Attributes</td>
<td>129</td>
</tr>
<tr>
<td>Adding a Port</td>
<td>130</td>
</tr>
<tr>
<td>Editing a Port</td>
<td>130</td>
</tr>
<tr>
<td>Enabling or Disabling a Port</td>
<td>131</td>
</tr>
<tr>
<td>Universal Messaging KPIs</td>
<td>131</td>
</tr>
<tr>
<td>Viewing the KPIs of a Universal Messaging Instance</td>
<td>132</td>
</tr>
</tbody>
</table>

22. Administering CentraSite                                           | 133  |
| About Administering CentraSite                                     | 134  |
| Viewing CentraSite Components                                      | 134  |
| Viewing CentraSite Registry Repository (CRR) and CentraSite Application Server Tier (CAST) | 134  |

A. Command Central Task Quick Reference                               | 137  |
| Working with Authentication between Command Central and Managed Products | 137  |
| Working with Environments                                           | 137  |
| Working with Installations                                          | 139  |
| Working with Instances                                              | 141  |
| Working with Product Comparisons                                   | 143  |
| Working with Product Inventory                                     | 144  |
| Working with SMTP Configuration                                     | 145  |
| Working with Ports                                                 | 145  |
| Working with KPIs                                                  | 147  |
| Working with Security Credentials                                  | 148  |
| Working with Licenses                                               | 148  |
About this Guide

This guide provides information about working with Command Central, the browser-based Software AG application that enables you to configure, manage, and administer one or more installations of the webMethods product suite in your enterprise.

Document Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Identifies elements on a screen.</td>
</tr>
<tr>
<td><strong>Narrowfont</strong></td>
<td>Identifies storage locations for services on webMethods Integration Server, using the convention <em>folder.subfolder:service</em>.</td>
</tr>
<tr>
<td><strong>UPPERCASE</strong></td>
<td>Identifies keyboard keys. Keys you must press simultaneously are joined with a plus sign (+).</td>
</tr>
<tr>
<td><strong>Italic</strong></td>
<td>Identifies variables for which you must supply values specific to your own situation or environment. Identifies new terms the first time they occur in the text.</td>
</tr>
<tr>
<td><strong>Monospace font</strong></td>
<td>Identifies text you must type or messages displayed by the system.</td>
</tr>
<tr>
<td>{ }</td>
<td>Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.</td>
</tr>
<tr>
<td></td>
<td>Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the</td>
</tr>
<tr>
<td>[ ]</td>
<td>Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.</td>
</tr>
<tr>
<td>...</td>
<td>Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).</td>
</tr>
</tbody>
</table>

Documentation Installation

You can download the product documentation using the Software AG Installer. The documentation is downloaded to a central directory named _documentation in the main installation directory (SoftwareAG by default).
Online Information

You can find additional information about Software AG products at the locations listed below.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Go to...</th>
</tr>
</thead>
</table>
| Access the latest version of product documentation. | **Software AG Documentation website**  
  http://documentation.softwareag.com |
| Find information about product releases and tools that you can use to resolve problems. | **Empower Product Support website**  
  https://empower.softwareag.com |

See the [Knowledge Center](#) to:

- Read technical articles and papers.
- Download fixes and service packs (9.0 SP1 and earlier).
- Learn about critical alerts.

See the [Products area](#) to:

- Download products.
- Download certified samples.
- Get information about product availability.
- Access older versions of product documentation.
- Submit feature/enhancement requests.
<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Go to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access additional articles, demos, and tutorials.</td>
<td>Software AG Developer Community for</td>
</tr>
<tr>
<td></td>
<td>webMethods</td>
</tr>
<tr>
<td>Obtain technical information, useful resources, and</td>
<td><a href="http://communities.softwareag.com/">http://communities.softwareag.com/</a></td>
</tr>
<tr>
<td>online discussion forums, moderated by Software AG</td>
<td></td>
</tr>
<tr>
<td>professionals, to help you do more with Software AG</td>
<td></td>
</tr>
<tr>
<td>technology.</td>
<td></td>
</tr>
<tr>
<td>Use the online discussion forums to exchange best</td>
<td></td>
</tr>
<tr>
<td>practices and chat with other experts.</td>
<td></td>
</tr>
<tr>
<td>Expand your knowledge about product documentation,</td>
<td></td>
</tr>
<tr>
<td>code samples, articles, online seminars, and tutorials.</td>
<td></td>
</tr>
<tr>
<td>Link to external websites that discuss open standards</td>
<td></td>
</tr>
<tr>
<td>and many web technology topics.</td>
<td></td>
</tr>
<tr>
<td>See how other customers are streamlining their</td>
<td></td>
</tr>
<tr>
<td>operations with technology from Software AG.</td>
<td></td>
</tr>
</tbody>
</table>
Understanding Command Central
1 Command Central Overview

- About Command Central ......................................................... 16
- Command Central Features .................................................... 16
- Command Central Architecture .............................................. 17
- Command Central Terminology .............................................. 19
- Getting Started ................................................................. 20
About Command Central

webMethods Command Central is a tool that release managers, infrastructure engineers, system administrators, and operators can use to perform administrative tasks from a single location. Command Central can assist with the following configuration, management, and monitoring tasks:

- Infrastructure engineers can see at a glance which products and fixes are installed, where they are installed, and compare installations to find discrepancies.
- System administrators can configure environments by using a single web user interface or command-line tool. Maintenance involves minimum effort and risk.
- Release managers can prepare and deploy changes to multiple servers using command-line scripting for simpler, safer lifecycle management.
- Operators can monitor server status and health, as well as start and stop servers from a single location. They can also configure alerts to be sent to them in case of unplanned outages.

Command Central Features

Using Command Central, you can administer hundreds of managed product installations in your IT landscape from a central location. Command Central supports the following operations:

- View inventory of webMethods product installations, versions, and fixes.
- Compare the versions of the products installed in different installations.
- Compare the fixes applied to products in different installations.
- Configure ports, licenses, alerts, and email settings of product instances.
- Compare the configuration settings of product instances running on different installations.
- Perform lifecycle operations such as start, stop, restart, pause, resume, and debug on runtime processes.
- Monitor the health of product installations.
- Monitor run-time status, KPIs, and alerts of product instances.
- Create a template from an existing managed installation and apply the template to another managed installation to reproduce the same set of products, fixes and configuration parameters.
Command Central Architecture

Command Central is built on top of OSGi platform, which uses the OSGi (Open Services Gateway Initiative) framework. Product-specific features are in the form of plug-ins.

Command Central User Interfaces

Command Central users can communicate with Command Central Server using one of the following interfaces:

- Graphical web user interface, for administering products using the web
- Command line interface, for automating administrative operations

For information about how to use the command line interface, see *webMethods Command Central* and *webMethods Platform Manager Command Reference*. 
Command Central Server

Command Central Server accepts administrative commands that users submit through one of the three user interfaces and then directs the commands to the respective Platform Manager for execution.

An installation in Command Central means one or more instances of the products that Command Central can manage. Products that Command Central manages are referred to as managed products throughout this help.

Command Central can manage one or more installations of the following products:

- Platform Manager
- Command Central
- webMethods Broker
- webMethods Integration Server
- My webMethods Server
- CentraSite
- Universal Messaging

Command Central provides a common location for configuring managed products installed in different environments.

Platform Manager

Software AG Platform Manager manages Software AG products. Platform Manager enables Command Central to centrally administer the lifecycle of managed products. In a host machine, you might have multiple Software AG product installations. For each Software AG product installation, you need a separate Platform Manager to manage the installed products. For example, if you have these installation directories in a host machine:

- C:\SoftwareAG_production\n- C:\SoftwareAG_test\n
The Platform Manager that belongs to the C:\SoftwareAG_production installation manages the products installed under the C:\SoftwareAG_production installation, and the Platform Manager that belongs to the C:\SoftwareAG_test installation manages the products installed under the C:\SoftwareAG_test.

Important! To manage Software AG products using Platform Manager, you must install Platform Manager and the Platform Manager plug-in for the product you want to manage in the same installation directory.
Platform Manager Installation and Configuration

Platform Manager is installed using Software AG Installer. When you install Command Central or any of the Command Central managed products, Platform Manager is installed by default. Platform Manager service starts automatically after installation.

You can use one Command Central installation to centrally manage multiple Platform Managers, product installations, and other Command Central instances. You need not install Command Central in every environment.

For information about installation and configuration, see Installing webMethods Products.

Command Central Terminology

The following table defines common Command Central terms.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>An independent module that runs within a process but has its own configurable elements. A component can be started and stopped, administered, and monitored separately. The lifecycle of a component is dependent on the parent component. That is, a component stops if its parent component stops. For example, Platform Manager Core Services is a component of Platform Manager.</td>
</tr>
<tr>
<td>Environment</td>
<td>A collection of installations that you logically group together for easier management. For example, you can group the installations used for testing under an environment called Testing.</td>
</tr>
<tr>
<td>Installation</td>
<td>A set of Software AG products and fixes installed in the same installation directory.</td>
</tr>
<tr>
<td>Instance</td>
<td>A single copy of a running product. An instance of a product is defined by its configuration settings. Some products might have multiple instances in one installation. For example, Broker Server and My webMethods Server are instances.</td>
</tr>
<tr>
<td>Landscape</td>
<td>A collection of all environments that are managed under a single Command Central instance. Often the landscape design decisions are based on security requirements and physical network topology.</td>
</tr>
</tbody>
</table>
Getting Started

Perform these initial tasks to setup and start using Command Central:

1. Access the Command Central web user interface.
2. Understand the Command Central web user interface.
3. Create the Command Central landscape by adding the environments and installations.
4. Secure the landscape by performing the security tasks.
5. Configure ports in the OSGi profiles.

After you set up Command Central, you can centrally monitor and manage the products in the Command Central landscape, as follows:

- Configure the product instances
- View the inventory of products and fixes
- Perform lifecycle operations such as start, stop, restart, pause, resume, and debug on run-time processes
- Monitor the product instances
- Compare configuration settings of the products installed
- Compare the versions of the products installed
- Compare the fixes applied to the products
Using the Command Central Web User Interface

- Accessing Command Central .................................................. 22
- Understanding the Web User Interface ................................... 22
- View Environments ............................................................... 22
- View Installations ................................................................. 26
- View Products in an Installation ............................................. 27
- View Fixes Applied to the Products In an Installation ............. 27
- Manage Lifecycle Actions ....................................................... 28
- Using Icons ........................................................................... 28
Accessing Command Central

After you install webMethods Command Central using Software AG Installer, Command Central starts automatically as a service in the port you configured during installation. You can access the Command Central web user interface either from within or outside of My webMethods.

For information about how to install and configure Command Central, see Installing webMethods Products.

To access the Command Central web user interface, specify the following URL in your browser:

http://hostname:port/cce/web

For the hostname, specify localhost or the name of the host machine where you have installed the Platform Manager.

For the port, specify the port number where the Command Central instance is running.

To access Command Central from My webMethods, navigate to Application > Command Central. Make sure you have the administrative privileges to Command Central. For more information, see “Managing Command Central Users, Groups, and Roles”.

Understanding the Web User Interface

This section describes the Command Central web user interface. Software AG recommends you use either Chrome or Firefox browser.

When you use Internet Explorer 9, in the General tab of Internet Options, select the Every time I visit the webpage option under Check for newer versions of stored pages in the Browsing history settings. Otherwise, Internet Explorer 9 browser might not display the newly added environment or installation when you refresh the browser after you add an environment or installation.

Note: To terminate the session, close your web browser completely. Closing only the browser tab will not end the session.

View Environments

Use the Environments pane in the Command Central home page to view the environments that you have defined for administration through Command Central.

In the Environments pane, you can view, add, delete, modify, and search for environments.

The following table describes the fields and icons displayed in the Environments pane.
### View Instances

Use the Instances tab to view the details of the instances in the selected environment.

In the Instances tab, you can view instances and components, configure instances, view and change the status of instances, view alerts, and search for instances.

The following table describes the fields and icons displayed in the Instances tab.

<table>
<thead>
<tr>
<th>Icon/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Search icon" /></td>
<td>Type the filter criteria for searching the instances in this field. The Instances tab lists only the instances with names that match the search criteria.</td>
</tr>
<tr>
<td><img src="image" alt="Clear Filter icon" /></td>
<td>Click <img src="image" alt="Clear Filter icon" /> to clear the search filter and list all the instances belonging to the selected installation.</td>
</tr>
<tr>
<td><img src="image" alt="Compare Configuration icon" /></td>
<td>Click <img src="image" alt="Compare Configuration icon" /> to select and compare the configurations of multiple instances.</td>
</tr>
</tbody>
</table>
Monitor Instances

Use the Overview tab of an instance to view the details about the instance such as the status, alerts, host name, and the installation alias. In addition, you can monitor the status and KPIs of the instance.

Click the name of an instance in the **Instances** tab, and then click the **Overview** tab to view the details about the instance and monitor the instance.

Click the administration link in the **Overview** tab and use the individual product interface to administer the following products.

- Broker Server
- Command Central
- Integration Server
- My webMethods Server

View Dashboard Information

Use the Dashboard panel in the Overview tab of an instance to view the following information.

<table>
<thead>
<tr>
<th>Icon/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Click ![icon] to query the Platform Manager and refresh the changes made to the instances.</td>
</tr>
<tr>
<td><strong>Name [Count]</strong></td>
<td>Display name of the instance and the total number of child instances.</td>
</tr>
<tr>
<td></td>
<td>Expand the instance node to view the list of child instances.</td>
</tr>
<tr>
<td><strong>Component</strong></td>
<td>Component name or the product code.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Indicates whether the installation is Online, Failed, Starting, Stopped, Stopping, Unknown, or Unresponsive. For more information about the instance status, see “Viewing the Status of an Instance or Its Components”. Click and select a lifecycle action to change the status.</td>
</tr>
<tr>
<td><strong>Alerts</strong></td>
<td>Displays an alert flag if there is any alert for the component.</td>
</tr>
<tr>
<td><strong>Installation</strong></td>
<td>Name of the installation where the instance is installed.</td>
</tr>
<tr>
<td><strong>Host</strong></td>
<td>Name of the host used by the instance.</td>
</tr>
</tbody>
</table>
View Details of Instances

Use the Details panel in the Overview tab of an instance to view the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Display name of the instance or component. You can edit the display name in line. Click ![ ] to modify the icon defined for the instance or component.</td>
</tr>
<tr>
<td>Component</td>
<td>Name of the component.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Name of the host machine where the instance or component is installed.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authentication mode for administering the instance. The default is Fixed user. Click ![ ] to edit the user name and password for fixed user authentication.</td>
</tr>
<tr>
<td>Installation Name</td>
<td>Name of the installation where the instance or component is installed.</td>
</tr>
<tr>
<td>Installation Alias</td>
<td>Alias name of the installation where the instance or component is installed.</td>
</tr>
</tbody>
</table>

View Configuration Parameters

Use the Configuration tab of an instance to configure its parameters such as ports, licenses, and emails. You can also configure the OSGi profiles of components.

Click the name of an instance in the Instances tab, and then click the Configuration tab, to configure the parameters of the instance.
View Installations

Use the Installations tab to view the details of all the installations that are part of the selected environment.

Command Central polls Platform Manager every 30 seconds to get the current status and alerts for the products in the installations when you view the Installations tab.

<table>
<thead>
<tr>
<th>Icon/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Filter Icon" /></td>
<td>Type the filter criteria for searching the installations in this field. The Installations tab lists only the installations with names that match the search criteria.</td>
</tr>
<tr>
<td><img src="image" alt="Clear Filter Icon" /></td>
<td>Click <strong>Clear Filter</strong> to clear the search filter and list all the installations of the selected environment.</td>
</tr>
<tr>
<td><img src="image" alt="Add Installation Icon" /></td>
<td>Click <strong>Add Installation</strong> to define an installation that you want to administer through Command Central. This installation will be grouped under the selected environment. If you have not specified any environment, the installation is added to the default <strong>All</strong> environment.</td>
</tr>
<tr>
<td><img src="image" alt="Remove Installation Icon" /></td>
<td>Click <strong>Remove Installation</strong> to remove the selected installation from the specified environment. The removed installation will be listed under <strong>All</strong> environment. If you do not want an installation to be administered by Command Central, you must explicitly remove it from the <strong>All</strong> environment.</td>
</tr>
<tr>
<td><img src="image" alt="Options Icon" /></td>
<td>Click <strong>Options</strong> to select these options:</td>
</tr>
<tr>
<td><img src="image" alt="Compare Products Icon" /></td>
<td><strong>Compare Products</strong></td>
</tr>
<tr>
<td><img src="image" alt="Compare Fixes Icon" /></td>
<td><strong>Compare Fixes</strong></td>
</tr>
<tr>
<td><img src="image" alt="Query Icon" /></td>
<td>Click <strong>Query</strong> to query the Platform Manager and refresh the changes made to the installations.</td>
</tr>
</tbody>
</table>

**Name [Count]**

Display name and the total number of products installed in the installation node.

Expand the installation node to view the list of products installed in the installation node.

Click an installation node to view the Overview, Products, and Fixes tabs.

**Status**

Indicates whether the installation is online or offline. Offline status indicates that the Platform Manager is not responding.
Using the Command Central Web User Interface

View Details of an Installation

Click the name of an installation in the Installations tab to view the Overview tab of the installation.

Use the Overview tab of an installation to view installation details, monitor the operating system KPIs such as utilization of the storage and memory, administer instances, and compare the configurations of instances belonging to that installation.

Command Central polls Platform Manager every 30 seconds to get the current status of the instances in the installation when you are viewing the Overview tab without navigating away from the tab.

View Products in an Installation

In the Installations tab, click the name of an installation and then click the Products tab, to view details about the products installed in the selected installation, including the product’s name, code, version, mechanism used to install the product, and date and time the product was installed.

View Fixes Applied to the Products In an Installation

In the Installations tab, click the name of an installation and then click the Fixes tab, to view the details of the fixes applied to the managed products in the selected installation.

Change Authentication Mode

In the instance Overview tab, click in the Authentication field to change the authentication mode using the Authentication Mode dialog box.

You can specify either Delegated authentication or Fixed User authentication for administering the products managed by a Platform Manager.

- If you specify Delegated authentication, Command Central authenticated users administer the products managed by that Platform Manager. This is the default.
If you specify **Fixed User** authentication, the authentication credentials for the Platform Manager will be fixed. Only the users authenticated using the credentials defined for that Platform Manager can administer the products.

When you specify the authentication mode for an instance, that authentication mode is also set for all the other instances belonging to the same installation.

**Manage Lifecycle Actions**

Use the Lifecycle Actions dialog to administer the managed products. To view the Lifecycle Actions dialog, click the status of an instance listed in the **Instances** tab or in the **Overview** tab of the instance. For information about the lifecycle actions, see “Administering Product Lifecycle”.

![Lifecycle Actions](image)

**Using Icons**

This section describes the icons used to identify the status of installations, instances, and alerts.

**Installation Status Icons**

The installation status indicates whether Command Central is able to connect to the installation using the Platform Manager of that installation.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅</td>
<td>Online</td>
<td>Command Central is able to connect to the installation host and port.</td>
</tr>
<tr>
<td>✖</td>
<td>Offline</td>
<td>Command Central cannot connect to the installation host and port.</td>
</tr>
</tbody>
</table>

**Instance Status Icons**

The instance status indicates whether the instance is currently running, started, stopped, or unresponsive.
### Alerts Icons

Alerts are raised or disabled when any of the following condition occurs.

- The status of an instance or instance component changes.
- The value of a KPI (key performance indicator) changes.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
<th>Indicates...</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>Online</td>
<td>The instance or instance component is currently running and the ping operation succeeds.</td>
</tr>
<tr>
<td>🔴</td>
<td>Failed</td>
<td>The instance or instance component is not running and the ping operation fails.</td>
</tr>
<tr>
<td>🔄</td>
<td>Starting</td>
<td>The instance or instance component is starting.</td>
</tr>
<tr>
<td>🔄</td>
<td>Stopped</td>
<td>The instance or instance component has stopped.</td>
</tr>
<tr>
<td>🔄</td>
<td>Stopping</td>
<td>The instance or instance component is stopping.</td>
</tr>
<tr>
<td>🔴?</td>
<td>Paused</td>
<td>The instance or instance component has paused.</td>
</tr>
<tr>
<td>🔴?</td>
<td>Unknown</td>
<td>The status of the instance or instance component cannot be determined.</td>
</tr>
<tr>
<td>🔴!</td>
<td>Unresponsive</td>
<td>The ping operation fails, but other indicators such as the process-id file indicate that the instance or instance component is running.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Icon</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔴</td>
<td>Instance warning or error.</td>
</tr>
<tr>
<td>🟢</td>
<td>Instance information.</td>
</tr>
</tbody>
</table>
3 Administering Environments

- About Administering Environments ................................................................. 32
- Adding Environments ....................................................................................... 32
- Filtering Environments .................................................................................... 33
- Editing Environments ....................................................................................... 33
- Deleting Environments ..................................................................................... 34
- Hiding/Showing Environments Pane ............................................................... 34
About Administering Environments

You manage installations by logically grouping installations under environments. This section describes how to add, view, and modify the environments in your landscape. For example, the image below shows Command Central administering the installations grouped under the Test, Production, Europe, and US environments.

Adding Environments

You add the environments that you want to centrally manage using Command Central. The default All environment contains the aggregate details of all the environments.
To add a new environment to your landscape

1. In the Environments pane, click `+`.
2. In the Add Environment dialog box, provide the following information.

<table>
<thead>
<tr>
<th>In this field...</th>
<th>Specify...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>A name for the new environment. The value of this field is automatically assigned to alias. More than one environment can have the same display name, but the alias must be unique.</td>
</tr>
<tr>
<td>Alias</td>
<td>A unique name for the environment. After you create an environment, you cannot edit the alias.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the environment.</td>
</tr>
</tbody>
</table>

3. Click `Add`. The Environments pane displays the newly added environment.

Filtering Environments

Use filters for your Command Central landscape environments when you want to work with specific environments.

To filter the list of environments displayed in the Environments pane

1. In the **Search Environments** field, type the filter criteria.

   The Environments pane displays only the environments with display names that contain the filter text.

2. Click `Clear Filter` to clear the filter condition and display all the environments.

Editing Environments

You can change the display name and the description of environments.

To edit the environment details

1. In the Environments pane, select the environment you want to edit and click **Edit Environment**.

2. In the Modify Environment dialog box, edit the values of the **Display Name** and **Description** fields as required.

3. Click **Ok**. The changes are saved and the Environments pane displays the changes.
Deleting Environments

You can remove an environment definition from your Command Central landscape. Be cautious while deleting environments because you cannot undo the environment deletion operation.

Note that when you remove an environment, the installations that were grouped under that environment are not removed from the server in which they are installed. The installations belonging to the removed environment will still be listed under the All environment.

To delete an environment from your Command Central landscape, in the Environments pane, select the environment you want to delete and click .

Hiding/Showing Environments Pane

You can manage the view by hiding or showing the Environments pane.

To hide or show the Environments pane, click or respectively.
Administering Installations

- About Administering Installations ................................................. 36
- Adding Installations ..................................................................... 36
- Viewing Installations .................................................................. 37
- Searching for Installations ........................................................... 37
- Removing Installations ................................................................. 38
- Linking Installations to Multiple Environments ........................... 38
- Monitoring Installations ............................................................... 39
About Administering Installations

You must specify the Software AG product installations you want to centrally manage through Command Central.

Adding Installations

When you add a Software AG product installation to an environment, Command Central can connect and manage the products in that installation.

To add installations to an environment

1. In the Environments pane, select the environment to which you want to add the installation.
2. Select the Installations tab.
3. On the Installations tab, click .
4. In the Add Installation dialog box, provide the following information:

<table>
<thead>
<tr>
<th>Field...</th>
<th>Specify...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>A name for the installation. The value of this field is automatically assigned to <strong>Alias</strong>. More than one installation can have the same <strong>Display Name</strong>.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The host machine on which the installation is running. Provide the fully qualified host name or IP address of the installation, so that the products under the installation can be administered remotely. For example, if you are adding an installation that exists in your local machine, instead of specifying <strong>localhost</strong> as the host name, specify <strong>mcdev001.us.ad.gov</strong> or <strong>12.23.0.1</strong>.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The port number used by Platform Manager of the installation.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Whether the installation requires HTTP or HTTPS authentication. Select <strong>Is Secure</strong> to specify HTTPS.</td>
</tr>
<tr>
<td>Alias</td>
<td>A unique name for the installation. No other installation in any of the environments can use this name.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the installation. This description is displayed in the Overview tab of the installation.</td>
</tr>
</tbody>
</table>
**Note:** When you provide `HostName:PortNumber` of an installation that is already grouped under another environment, that installation gets linked to the environment for which you are adding. An installation with the same or different display names can be linked to more than one environment.

5 Click **Add**. The Installations tab displays the newly added installation node.

### Viewing Installations

You can view the display name, host name, port, total number of products installed in an installation node, and whether the installation is online or offline. When you expand an installation node, you can view the list of products installed in that installation.

**To view the installations in an environment**

1 In the Environments pane, select the environment for which you want to view the installations.

   To view all the installations within all environments, select **All**.

2 Select the **Installations** tab.

   The Installations tab lists the installations in the selected environment. For information about the details displayed in the Installations tab, see “View Installations”.

### Searching for Installations

Use the search filters if you want to locate specific Software AG product installations.

**To filter the list of installations displayed in the Installations tab**

1 In the Environments pane, select the environment for which you want to filter the installations.

   To search for installations in all the environments, select **All**.

2 Select the **Installations** tab.

3 In the **Search Installations** field, type the filter text. The Installations tab displays only the installations that contain the filter text in any of its field values.
Removing Installations

Removing an installation from an environment means that you are un-grouping that installation from the environment. If you remove an installation from all the environments (including All), then you cannot administer that installation through Command Central.

When you remove an installation from the All environment, that installation is not removed from the server; rather, it is just disconnected from Command Central.

For example, suppose that Sales installation is grouped under two environments: Testing and Production. If you remove the Sales installation from the Testing environment, you can no longer manage it from the Production and All environments; however, you can manage the Sales installation grouped under Production environment and All environment in Command Central. If you then remove the Sales installation from the Production and All environments too, you will not be able to administer the installation from anywhere in Command Central.

To remove installations from an environment

1 In the Environments pane, select the environment from which you want to remove the installations.

   To view the installations of all environments, select All.

2 Select the Installations tab.

3 Select the installation you want to remove. To select multiple installations, hold down the Shift key or the Ctrl key.

4 Click \( \text{ } \) to remove the selected installations.

   Note: Even if you remove an installation from all the defined environments, that installation is still listed in the All environment until you explicitly remove it from the All environment.

Linking Installations to Multiple Environments

If you want an installation to be part of more than one environment, you can link that installation to multiple environments. For example, if an installation is used for both testing and development, you can link that installation to both testing and development environments.
To link installations to multiple environments

1. In the Environments pane, select the environment from which you want to link the installation(s) to an environment.

   To view the installations of all environments, select All.

2. Select the Installations tab.

3. Drag the installation(s) you want to link and drop it on the environment you want to link to. For selecting multiple installations, select the installations by holding down the Shift key or the Ctrl key.

   You can also link an installation to multiple environments by adding the installation (same HostName:PortNumber) grouped under one environment to another environment. For information about adding an installation to an environment, see “Adding Installations”.

4. Click the environment to view the installations linked to it.

Monitoring Installations

Command Central enables you to monitor the status of operating system Key Performance Indicators (KPIs) for the machine on which the installation is running.

To monitor an installation

1. In the Environments pane, select the environment for which you want to monitor the installation node.

2. Select the Installations tab.

3. Click the name of the installation you want to monitor.

4. Select the Overview tab, if it is not selected.

   The Overview tab displays the installation details, instances in the installation node, and the KPIs of the installation’s Platform Manager. For more information about KPIs, see “About Monitoring KPIs” on page 84.

   The Installation panel displays the display name, alias name, host name, port, alias, operating system, and the version of the operating system pertaining to the installation node.

   The Monitoring panel displays the KPIs of the installation’s Platform Manager.

   The Instances panel lists the instances of the components that are part of the installation. You can:

   - View the instances of the products installed in the installation node.
   - Search for instances.
   - Change the status of the instances.
- Compare configurations of the instances.
5 Securing the Command Central Landscape

- About Securing the Command Central Landscape ........................................... 42
- Setting Up Security ......................................................................................... 42
- Changing the Internal User Administrator Password ...................................... 42
- Setting Outbound Authentication .................................................................... 43
- Accessing Command Central through My webMethods ................................. 44
- Accessing Administrative Interfaces through Command Central ..................... 44
- Configuring Ports ............................................................................................. 44
About Securing the Command Central Landscape

When securing the Command Central landscape, you must consider user access to Command Central and Platform Manager, communication between Command Central and Platform Manager and the Software AG product installations, and external access to Command Central and Platform Manager. This chapter addresses the tasks that must be implemented to secure these interactions.

Changing the Internal User Administrator Password

You must change the default Command Central administrator password in the users.txt file. To do so, use the internaluserrepo script, as described in the following procedure.

To change the internal user repository’s default administrator password

1. From the command prompt, type the following command to change the directory:
   ```
   cd common\bin
   ```

2. Run the internaluserrepo script to change the Command Central administrator password. For example, to change the password for user Administrator to CC_Admin1 on a Windows system:
   ```
   internaluserrepo.bat -f ../conf/users.txt -p CC_Admin1 Administrator
   ```
   For more information about the script syntax, see “internaluserrepo Script” on page 65.

Setting Up Security

After installing Command Central, Software AG recommends you perform the following tasks to set up security:

1. Propagate the modified users.txt file to each of the nodes (installations) in the Command Central landscape using the `cc update configuration data` command. For syntax and usage, see *webMethods Command Central and webMethods Platform Manager Command Reference*.

2. Update the security credentials in the Command Central Server for communication between Command Central and Platform Manager using the `cc add security credentials` command. For syntax and usage, see *webMethods Command Central and webMethods Platform Manager Command Reference*.

3. Update the OSGi-* credentials, which are used for all internal calls, such as Platform Manager to Common Platform, using the `cc add security credentials` command. For syntax and usage, see *webMethods Command Central and webMethods Platform Manager Command Reference*.

4. Make sure that all nodes are online.
Setting Outbound Authentication

As part of its normal operations, Command Central might connect to applications and subsystems such as Integration Servers, Brokers, and My webMethods Server. Command Central, acting as a client, is required to supply a password, referred to as an *outbound password*, to each of these systems before connecting to them. Command Central uses the outbound passwords to identify itself or authenticate to the other systems.

When you configure Command Central to connect to an application, you specify the password Command Central must send to the application to connect to it. Later, when a Command Central user makes a request that requires the application, Command Central sends the configured password to the application and connects to it.

Outbound authentication does not authorize access to resources.

**To set outbound authentication**

1. For Integration Server, use the Integration Server Administrator user interface to change the Administrator password or create a new ISAdmin user on the server instance. For more information, see *webMethods Integration Server Administrator’s Guide*.

2. In Command Central, configure credentials for the Integration Server instance to use the new user name and password.
   a. In the Environments pane, select the environment that contains the Integration Server instance.
   b. In the Instances table, select the instance of Integration Server for which you want to change the user credentials.
   c. On the **Overview** tab, in the Details pane, click **edit** in the **Authentication** field.
   d. Enter the new **User Name** and **Password**.

   **Note:** You can also configure credentials for the Integration Server instance using the `cc update configuration data` command. For syntax and usage, see *webMethods Command Central and webMethods Platform Manager Command Reference*.

3. For My webMethods Server, change the Administrator and sysadmin passwords using the My webMethods Server user interface. Because My webMethods Server uses trusted authentication, you do not have to configure connection credentials. For more information, see *Administering My webMethods Server*.

   **Note:** No authentication is required when managing webMethods Broker from Command Central and Platform Manager.
Accessing Command Central through My webMethods

You can access the Command Central user interface from My webMethods Server without logging on again by establishing a connection as follows:

1. A logon request is initiated from My webMethods Server to Command Central.
2. The My webMethods Server user is validated by Command Central.
3. A Command Central session is established.

The credentials stored in the My webMethods Server user database can be used to authenticate this request. This authentication mechanism is called Single Sign-On (SSO).

The underlying mechanism used for SSO is based on SAML 2.0 signed assertions. Information about the My webMethods Server user is placed in an assertion document, which is then signed and sent to Command Central. Command Central verifies the signature and expiration date, extracts the user ID from the assertion, and validates that the user ID corresponds to a valid Command Central user. Once validation is complete, the user session is established on Command Central.

The My webMethods Server user making the SSO request must be a valid Command Central user who has at least read-only access permission to Command Central. The default My webMethods Server Administrator is also a valid Command Central user. If My webMethods Server is configured to use LDAP/AD, the same LDAP/AD must be configured for Command Central authentication.

Accessing Administrative Interfaces through Command Central

In Command Central, single sign-on (SSO) is designed to manage webMethods products using an administrative link without any post-installation configuration. When performing advanced configuration tasks, you might need to access the product's primary administrative interface. Command Central provides a link to the administrative interface on the Instances Overview page for each managed product. For example, when you click the Integration Server link on the Overview page of an Integration Server instance, Command Central redirects the browser to the corresponding Integration Server Administrator URL.

Use Enterprise Manager to perform advanced configuration tasks of Universal Messaging. You cannot access Enterprise Manager through Command Central.

Configuring Ports

Command Central and Platform Manager listen for requests on ports that you specify. Each port is associated with a protocol, such as HTTP or HTTPS. In addition to these ports, Command Central uses JMX ports for alerts.
Default Ports

When you install Command Central and Platform Manager, Software AG Installer assigns the HTTP and HTTPS port numbers. If the default port numbers are used by other products, Installer displays available ports. You can select one of the available ports, or you can change the port manually.

The following table shows the default HTTP and HTTPS ports.

<table>
<thead>
<tr>
<th>Product</th>
<th>Alias</th>
<th>Port Type</th>
<th>Default Port Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Central</td>
<td>defaultHttp</td>
<td>HTTP</td>
<td>8090</td>
</tr>
<tr>
<td></td>
<td>defaultHttps</td>
<td>HTTPS</td>
<td>8091</td>
</tr>
<tr>
<td>Platform Manager</td>
<td>defaultHttp</td>
<td>HTTP</td>
<td>8092</td>
</tr>
<tr>
<td></td>
<td>defaultHttps</td>
<td>HTTPS</td>
<td>8093</td>
</tr>
</tbody>
</table>

As an administrator, you can change the default port assignments by modifying the configuration settings using the Command Central web user interface or the command line interface. For commands and options, see *webMethods Command Central and webMethods Platform Manager Command Reference.*

Configuring Port Connection Settings

Using the Command Central web user interface or the command line interface, you can change an instance’s port number and the connection settings related to the instance.

For more information about editing the configuration of an existing port using the command line interface, see “Command Central Task Quick Reference” on page 137.

To configure port connection settings for the web user interface

1. In the Environments pane, select the environment for which to configure the port settings.
2. In the **Instances** tab, select the name of the instance to configure.
3. Select the **Configuration** tab, and then select a port to edit.
4. In the *port_type* Port Configuration page, click **Edit**.
5. Select the connection attributes to change, and then click **Save**.
6. Restart the instance to implement the changes.
6 Configuring Products

- Product-Specific Configuration ......................................................... 48
- Configuring Instances ..................................................................... 48
- Testing a Configuration ................................................................... 48
- References to File Locations in Product Configuration Files .......... 49
Product-Specific Configuration

Using Platform Manager, you can configure settings that are common to all products, as well as settings that are specific to a given product. You can configure product ports, licenses, and emails.

Configuring Instances

This section describes how you can select and set the common and product-specific configuration data of a managed product.

To configure an instance

1. In the Environments pane, select the environment in which you want to configure a product instance.
2. Select the Instances tab.
3. Click the name of the instance you want to configure.
4. Select the Configuration tab.
5. From the list of available configuration types, select a configuration type.
   Command Central displays the configuration data already set for this instance.
6. Configure the selected instance as follows:

<table>
<thead>
<tr>
<th>To</th>
<th>Click</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add new data</td>
<td>+</td>
</tr>
<tr>
<td>Edit data</td>
<td>-</td>
</tr>
<tr>
<td>Test whether data is added or edited successfully.</td>
<td>Test</td>
</tr>
<tr>
<td>For example, you can test new configuration data to perform a field-level validation before you save the configuration data.</td>
<td></td>
</tr>
</tbody>
</table>

7. Click Save to save the configuration data.

Testing a Configuration

While configuring an instance, you can test a new configuration data before you save the configuration data for that instance.

When you test a configuration data, a field-level input validation is done. If you have entered a port setting, the availability of the port is also tested.
To test configuration data

1. Navigate to the Environment > Instances > Configuration tab of the product you want to configure.
2. Enter the configuration data.
3. Click Test.
4. Supply the appropriate data and click Save.

Note: If the test fails, Command Central displays a message that indicates the possible cause of the error. Resolve the error and try again until the test passes successfully.

References to File Locations in Product Configuration Files

Important! Software AG recommends that you place all local files on a managed product system that are referenced in the configuration file of the product managed by Command Central in the Software AG_directory.

When your product configuration refers to a local file on the managed product system, the type of path that you specify depends on the location of the referenced file.

- When the file is located in the Software AG_directory, use relative paths. The relative path depends on how the managed product resolves relative locations and is normally relative to one of the following:
  - The product home installation directory
  - The product bin folder
  - Software AG_directory
  - A supported location token

- When the file is not located in the Software AG_directory, use absolute paths.

Important! To minimize synchronization issues when using absolute paths, ensure that the absolute location is valid on all managed product systems. Note that when you manage products in both Windows and UNIX environments, the absolute paths are usually different.

Migrating Product-Specific Configurations

Product configurations that are migrated from the source managed product system to the target managed product system do not automatically migrate the files referenced in the product configuration. Ensure that the referenced files are available on the target system at the referenced location.
Configuring OSGi Profiles

Command Central uses the ports specified in the OSGi profiles of products for monitoring the managed products. You can add, modify, or delete the ports in the OSGi profiles.

Protocols that Command Central Supports in OSGi Profiles

Command Central supports HTTP, HTTPS, JMX, SSH, and JDWP. JMX, SSH, and JDWP protocols allow only one port each.

<table>
<thead>
<tr>
<th>Use this port type...</th>
<th>To...</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Submit unsecured requests to the OSGi component.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Submit requests to the OSGi component using SSL encryption.</td>
</tr>
<tr>
<td>JMX</td>
<td>Allow administration and monitoring the JVM KPIs of the OSGi component.</td>
</tr>
</tbody>
</table>

To monitor the product-specific KPI’s of the Integration Server, My webMethods Server, and Platform Manager instances, you need not enable the JMX port in the OSGi profile of the corresponding product.

To view the inventory, run-time status (enabled/disabled), and to start/stop (or enable/disable) the Integration Server packages, do the following:

- Enable the JMX port in the OSGi profile of Integration Server.
- Enable subsystem in the manifest file of the Integration Server package as shown below.

```xml
<Values version="2.0">
  <value name="subsystem">true</value>
</Values>
```

JMX port might be bound to a localhost.

<table>
<thead>
<tr>
<th>SSH</th>
<th>Allow secure shell for the OSGi component.</th>
</tr>
</thead>
<tbody>
<tr>
<td>JDWP</td>
<td>Allow OSGi component debugging by using the Java debug protocol over a TCP connection.</td>
</tr>
</tbody>
</table>

To enable the HTTP/HTTPS ports of Integration Server, configure the HTTP/HTTPS ports of the Integration Server instance, not the ports in the OSGi profile.

To enable the HTTP/HTTPS ports of My webMethods Server, configure the HTTP/HTTPS ports of the My webMethods Server instance, not the ports in the OSGi profile.
Products that Support Port Configuration in OSGi Profiles

The following table lists the products that have OSGi profiles that support port configuration.

<table>
<thead>
<tr>
<th>Product</th>
<th>Product Code</th>
<th>Ports Enabled by Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Central</td>
<td>CCE</td>
<td>JMX, HTTP, HTTPS</td>
</tr>
<tr>
<td>Integration Server</td>
<td>IS</td>
<td>JMX</td>
</tr>
<tr>
<td>My webMethods Server</td>
<td>MWS_mwsigninstanlename</td>
<td>JMX</td>
</tr>
<tr>
<td></td>
<td>For example, MWS_default</td>
<td></td>
</tr>
<tr>
<td>Platform Manager</td>
<td>SPM</td>
<td>JMX, HTTP, HTTPS</td>
</tr>
<tr>
<td>CentraSite</td>
<td>CTP</td>
<td>JMX, HTTP, HTTPS</td>
</tr>
<tr>
<td>(Common Tomcat Package</td>
<td></td>
<td></td>
</tr>
<tr>
<td>that hosts CentraSite)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All these products support SSH and JDWP port configuration. For information about configuring the ports in the OSGi profile of a product, see “Configuring Ports in OSGi Profiles”.

Integration Server and My webMethods Server have two profiles: OSGi profile and the instance profile. For more information about configuring an Integration Server instance, see “Configuring Integration Server Ports” on page 95. For more information about configuring a My webMethods Server instance, see “Configuring My webMethods Server Ports” on page 119 and “Configuring My webMethods Server Email” on page 121.

JMX Port Authentication

The JMX port authentication for the following OSGi profiles is done against the shared platform’s internal user repository (Software AG_directory\common\conf\users.txt file).

- Command Central
- Platform Manager
- My webMethods Server
- CentraSite Tomcat Server

If JMX port is enabled in the OSGi profile of Integration Server, then authentication is done against the Software AG_directory\common\conf\users.txt file.

Integration Server can open JMX port using a setting in the Integration Server_directory\bin\setenv.bat file. For more information about enabling JMX monitoring in Integration Server, see the webMethods Integration Server Administrator’s Guide.
Configuring Ports in OSGi Profiles

You configure ports in the Configuration tab of a product-specific OSGi instance.

Adding Ports

Perform the following procedure to configure new ports in the OSGi profiles.

To add a port

1. In the Environments pane, in the Instances tab, click the OSGi instance or component to which you want to add a port.
2. Click the Configuration tab.
3. Click the + to add a new port.
4. Select one of the following in Port Type and click OK:
   - HTTP
   - HTTPS
   - JMX
   - SSH
   - JDWP
5. In Connection Basics, configure the fields corresponding to the port type.
   - For HTTP and HTTPS port configurations:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Whether the port is enabled.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The number you want to use for the port. Select a number that is not already in use.</td>
</tr>
<tr>
<td>Alias</td>
<td>Name that you want to use for the port alias. Use an alias name that is unique for the instance or component and can be included in a user-friendly URL. The only valid characters in an alias name are ASCII characters, numbers, underscore (_), dot (.), and a hyphen (-).</td>
</tr>
<tr>
<td>Keep Alive Timeout</td>
<td>When to close the connection if the server has not received a request from the client within this timeout value (in milliseconds); or when to close the connection if the client has explicitly placed a close request with the server.</td>
</tr>
<tr>
<td>Spare Threads Min</td>
<td>The starting number of request processing spare threads.</td>
</tr>
<tr>
<td>Redirect Port</td>
<td>The port to use when redirecting a SSL connection requests.</td>
</tr>
<tr>
<td>Spare Threads Max</td>
<td>The maximum number of request processing spare threads.</td>
</tr>
<tr>
<td>Accept Count</td>
<td>The maximum number of simultaneous connection requests allowed in the connection queue.</td>
</tr>
<tr>
<td>Connection Timeout</td>
<td>The connection timeout in milliseconds. This attribute is not set by default on HTTPS ports.</td>
</tr>
<tr>
<td>HTTP Header Size Max</td>
<td>The maximum incoming URL length in characters.</td>
</tr>
<tr>
<td>Upload Timeout Disable</td>
<td>Indicates if using a longer connection timeout is allowed when waiting for the servlet container to update.</td>
</tr>
<tr>
<td></td>
<td>- Yes. Allow longer connection time-outs while waiting for the servlet container.</td>
</tr>
<tr>
<td></td>
<td>- No. Do not allow longer connection time-outs.</td>
</tr>
<tr>
<td>Lookups Enable</td>
<td>Indicates if DNS lookups are allowed to get the actual host name of a remote client.</td>
</tr>
<tr>
<td></td>
<td>- Yes. DNS lookups allowed.</td>
</tr>
<tr>
<td></td>
<td>- No. DNS lookups not allowed.</td>
</tr>
<tr>
<td>Key Manager Algorithm</td>
<td>For HTTPS port configurations. The certificate encoding algorithm.</td>
</tr>
</tbody>
</table>
For JMX and SSH port configurations:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Protocol</td>
<td>For HTTPS port configurations. The version of the secure socket layer (SSL) protocol to use; when not specified Transport Layer Security (TLS) is used.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether the port is enabled.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The number you want to use for the port. Select a number that is not already in use.</td>
</tr>
<tr>
<td>Alias</td>
<td>Name that you want to use for the port alias. Use an alias name that is unique for the instance or component and can be included in a user-friendly URL. The only valid characters in an alias name are ASCII characters, numbers, underscore (_), dot (.), and a hyphen (-).</td>
</tr>
<tr>
<td>JAAS Realm</td>
<td>For JMX and SSH port configurations. Specifies the realm name that authenticates the Java Authentication and Authorization (JAAS) service.</td>
</tr>
</tbody>
</table>

For JDWP port configurations:

Note: The JDWP port is only used when the profile is started in debug mode.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Number</td>
<td>The number you want to use for the port. Select a number that is not already in use.</td>
</tr>
<tr>
<td>Alias</td>
<td>Name that you want to use for the port alias. Use an alias name that is unique for the instance or component and can be included in a user-friendly URL. The only valid characters in an alias name are ASCII characters, numbers, underscore (_), dot (.), and a hyphen (-).</td>
</tr>
</tbody>
</table>
In Threadpool Configuration, for HTTP and HTTPS ports, complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspend</td>
<td>For JDWP port configurations. Select Yes if the runtime should be suspended until debugger connects.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether the listener uses this pool exclusively for dispatching requests. The existing thread pool is a global thread pool. If there is a very high load on this resource, there may be a delay until the global thread pool can process the request. However, with the private thread pool option enabled, requests coming into this port do not compete with other server functions for threads. When you view the port's details, the server reports the total number of private thread pool threads currently in use for the port. Click Yes to enable the private thread pool settings. If you do not need to use the thread pool feature, click No.</td>
</tr>
<tr>
<td>Threadpool Min</td>
<td>The minimum number of threads for this private thread pool. The default is 1.</td>
</tr>
<tr>
<td>Threadpool Max</td>
<td>The maximum number of threads for this private thread pool. The default is 5.</td>
</tr>
<tr>
<td>Threadpool priority</td>
<td>The Java thread priority. The default is 5.</td>
</tr>
</tbody>
</table>

Important! Use this setting with extreme care because it will affect server performance and throughput.

For secure connections, complete the security fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Enabled</td>
<td>Whether secure layering is enabled. Click Yes to enable the private thread pool settings. If you do not need to use the thread pool feature, click No.</td>
</tr>
<tr>
<td>Keystore Type</td>
<td>Select the keystore type. The keystore must contain the private key for secure communication.</td>
</tr>
</tbody>
</table>
Viewing the Port Settings

Use the following procedure to view the settings for an existing port.

**To view the platform manager ports**

1. In the Environments pane, click the environment in which you want to view the OSGi instance or component.
2. Click the **Instances** tab.
3. Click the name of the OSGi instance or component you want to view.
4. Click the **Configuration** tab.
5. In **Ports**, select the port. The field displays the parameters available for configuration.

**Editing and Testing OSGi Port Information**

Perform the following procedure to edit OSGi port information.

**Note:** You cannot change an existing port alias.

**To edit port information**

1. In the Environments pane, click the environment in which you want to edit the OSGi profile.instance from the **Instances** tab.
2. Click the **Instances** tab.
3. Click the name of the OSGi instance or component you want to view.
4. Click the **Configuration** tab.

### Field | Description
--- | ---
Server Location of Keystore | Specify the directory where the keystore file is located.
Password | Specify the password to open the keystore file.
Truststore Type | Select the truststore type. The truststore must contain the trusted root certificate for the CA that signed the OSGi component certificate associated with the key alias. The truststore also contains the list of CA certificates that OSGi component uses to validate the trust relationship.
Server Location of Truststore | Specify the directory where the truststore file is located.
Password | Specify the password to open the truststore file.
5 In **Ports**, select the port. The field displays the parameters available for configuration.

6 Locate the port whose details you want to edit, and click on the port number.

7 Click **Edit**.

8 Make changes to the port and click **Test** or **Save**.

**Deleting a Port**

Use the following procedure to delete a port configuration from an OSGi profile.

---

**To delete a port**

1 In the Environments pane, click the environment in which you want to view the OSGi instance.

2 Click the **Instances** tab.

3 Click the name of the OSGi instance or component.

4 Click the **Configuration** tab.

5 Select the port that you want to delete and click **』**.

**Note:** You can only delete ports that are disabled.
Managing Command Central Licenses

- Command Central License Overview ................................................................. 60
- Viewing the Command Central License Information ......................................... 60
- Changing a Command Central License Key ..................................................... 60
- Renewing a Command Central License Key ..................................................... 61
Command Central License Overview

When you purchase Command Central, your organization is granted a license to use it with certain features and functionality, and with a specified number of nodes to be added for administration and configuration. The license expires after a time period specified by your particular purchase agreement.

When you install Command Central, the setup program copies the license file to the Software AG_directory\profiles\CCE\configuration directory with the name cce-license.xml.

Viewing the Command Central License Information

Use the following procedure to view the license details for Command Central.

To view licensing information

1. In Command Central, click the Instances tab.
2. Click CCE.
3. In the left pane, click Command Central Server.
4. Click the Configuration tab.
5. From the drop-down list, select Licenses. The license type, status, and expiration date for the Command Central license appear below the drop-down list.
6. Click the Command Central license type. The license location and details appear. The PriceQuantity field displays the number of CCE nodes allowed.
   - If the number of nodes connected is more than that specified, Command Central will shut down in 30 minutes.
   - If the number of nodes connected is equal to the one that is specified, Command Central will not allow you to add another node.
   - If the license has expired, Command Central will shut down in 30 minutes.

Changing a Command Central License Key

Use the following procedure to change your license key when your license expires or if you change your license to include different features.

To change the license key

1. In Command Central, click the Instances tab.
2. Click CCE.
3 In the left pane, click Command Central Server.

4 Click the Configuration tab.

5 In the Configuration drop-down list, select Licenses. The license type, status, and expiration date for the Command Central license appear below the drop-down list.

6 In the License Type column, click the Command Central link. The license key location and details appear.

7 In the Licenses Configuration page, click Edit.

8 Click Browse in the License Upload Location section, and then navigate to the new license file.

   **Note:** You will not be able to change the server license location. The new license file that you select is uploaded to the license location as shown in the Server License Location section.

9 Click Save.

### Renewing a Command Central License Key

If you need to obtain a new Command Central license key or renew your Command Central license, contact your Software AG sales representative.
Managing Users, Groups, and Roles

- Managing Command Central Users, Groups, and Roles ......................... 64
- Using Internally Defined User and Group Information .......................... 64
- Using Externally Defined User and Group Information .......................... 67
- Using JAAS with Command Central ..................................................... 72
- Groups ......................................................................................... 74
- Roles ......................................................................................... 75
Managing Command Central Users, Groups, and Roles

Command Central uses user, role, and group information to authenticate users and determine the resources a user is allowed to access. This information is stored in the internal user repository.

A user is defined by a user name or user ID. Users can be members of groups. They can also be assigned roles within the repository.

A group is a defined collection of users. Command Central and Platform Manager support groups as a way to manage users. A user does not have to be a member of any group, but a user can be a member of more than one group. For more information about groups, see “Groups” on page 74.

A role is a defined collection of privileges within Command Central. A role consists of specific access control rights or permissions. For more information about roles, see “Roles” on page 75.

Roles are assigned to individual users and to groups. When a role is assigned to a group, all members of the group inherit that role. The roles assigned to a user control what permissions the user has when using Command Central and Platform Manager.

You must have administrative credentials to access the Command Central web user interface’s administration links to Integration Server, Broker Server, and My webMethods Server.

After installing Command Central, configure the internal user repository with new users, roles, and groups by adding users, adding groups and assigning users to them, and mapping users to roles and roles to groups.

For information about using LDAP and external repositories, see “Using Externally Defined User and Group Information” on page 67.

Using Internally Defined User and Group Information

Command Central can authenticate users against information in the shared platform’s internal user repository, which is located in the Software AG_directory\common\conf\users.txt file.

When managing users within the internal user repository, you should assign users and groups to roles in the roles.txt file, and assign users to groups in the groups.txt files. You can find the roles.txt and the groups.txt files in the Software AG_directory\common\conf directory. For more information, see “Groups” on page 74 and “Roles” on page 75.

Note: Immediately after logging on to Command Central for the first time, the administrator should change the default administrator password. For more information see “Changing the Internal User Administrator Password” on page 42.
**internaluserrepo Script**

The `internaluserrepo.bat/sh` script creates or modifies the users.txt file, adds and deletes users in the file, and changes specified internal user passwords.

The `internaluserrepo.bat/sh` script is located in the following directory:

`Software AG_directory/common/bin`

To use `internaluserrepo.bat/sh`, open a command prompt or console and change the directory to the `internaluserrepo.bat/sh` script's location. For more information, see:

- “Changing the Internal User Administrator Password” on page 42
- “Adding Users to the Internal User Repository” on page 67
- “Deleting Users from the Internal User Repository” on page 67

**Syntax**

At the command prompt, use the following syntax:

```
internaluserrepo.bat/sh [-f filename] [-c] [-p password] [-d | -e] userId
```

When the command syntax is not correct, `internaluserrepo.bat/sh` reports an exit status code. When the command syntax is correct, the command prompt returns without any additional information. For more information about exit codes, see “`internaluserrepo Exit Codes`” on page 66.

**Arguments**

The following table provides descriptions for the arguments that can be made to the `internaluserrepo.bat/sh` script.

<table>
<thead>
<tr>
<th>Argument/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>userId</code></td>
<td>Required. Creates a new user when the users.txt file exists in the <code>Software AG_directory/common/bin</code> directory. The specified user ID is added to the file and the <code>internaluserrepo</code> script prompts you for the new user's password. When the specified user ID exists in the users.txt file, the password is changed for that user ID. You can use up to 128 characters for <code>userId</code>. The following are valid characters for a user ID: <code>[a-z] [A-Z] [0-9] ()-.?[]@_~</code></td>
</tr>
<tr>
<td><code>[-f filename]</code></td>
<td>Optional. Specifies the location and file name followed by the URL, or the path and name of the file to create.</td>
</tr>
<tr>
<td><code>[-c]</code></td>
<td>Optional. Creates a users.txt file in the directory where the command is executed when no other options are used.</td>
</tr>
</tbody>
</table>
The following table describes the exit codes you might encounter when using the internaluserrepo.bat/sh script.

<table>
<thead>
<tr>
<th>Exit Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>The user ID specified with the -e option does not exist in the users.txt file.</td>
</tr>
<tr>
<td>1</td>
<td>The password is not set.</td>
</tr>
<tr>
<td>2</td>
<td>The user ID is too long.</td>
</tr>
<tr>
<td>3</td>
<td>The user ID contains invalid characters.</td>
</tr>
<tr>
<td>4</td>
<td>The password contains invalid characters.</td>
</tr>
<tr>
<td>5</td>
<td>The password is too long.</td>
</tr>
<tr>
<td>6</td>
<td>The internal user repository contains multiple versions of the users.txt file.</td>
</tr>
<tr>
<td>7</td>
<td>An invalid version of the configuration file exists in the repository. Supported versions are 2.0 and above.</td>
</tr>
<tr>
<td>8</td>
<td>One of the following has occurred:</td>
</tr>
<tr>
<td></td>
<td>■ The file name is not specified in the command and the default file cannot be located.</td>
</tr>
<tr>
<td></td>
<td>■ The file specified cannot be located. Make sure you have entered the correct path and file name.</td>
</tr>
<tr>
<td>9</td>
<td>The internaluserrepo script cannot open or create the users.txt file.</td>
</tr>
<tr>
<td>10</td>
<td>The user ID is missing.</td>
</tr>
</tbody>
</table>
Adding Users to the Internal User Repository

In addition to the default user (Administrator) in the users.txt file, you can add users, such as Guest, Viewer, and Operator, to the internal user repository by running the internaluserrepo script. You must have administrator credentials to add users to the internal user repository.

To add a user to the internal user repository

1. At the command prompt, type the following command to change the directory:
   ```
   cd common\bin
   ```
2. Type the following command:
   ```
   internaluserrepo.bat -f ../conf/users.txt -c -p password userId
   ```
   For example, to add user Administrator1 with a password of manage1, enter:
   ```
   internaluserrepo.bat -f ../conf/users.txt -c -p manage1 Administrator1
   ```
   **Note:** A user name can be fully qualified, such as, LDAP Distinguished Name.

Deleting Users from the Internal User Repository

You can delete users from the internal user repository (users.txt file).

To delete a user from the internal user repository

1. At the command prompt, type the following command to change the directory:
   ```
   cd common\bin
   ```
2. Enter the following command:
   ```
   internaluserrepo.bat -f ../conf/users.txt -d userId
   ```
   For example, to delete Administrator1, enter the following command:
   ```
   internaluserrepo.bat -f ../conf/users.txt -d Administrator1
   ```

Using Externally Defined User and Group Information

Command Central can use externally defined information for the same purposes it uses internally-defined user and group information:

- To authenticate clients using user names and passwords
To control who can configure and manage Command Central

You can set up Command Central to access information from an external directory if your site uses one of the following external directories for user and group information:

- Lightweight Directory Access Protocol (LDAP)
- Microsoft Active Directory (AD) acting as an LDAP server

**Note:** Externally defined user and group information does not replace roles and permissions. To control actions within Command Central, as well as access to data, you still need to set up roles and associate users and groups with those roles to allow or deny access to specific actions.

### How Command Central Authenticates Externally Defined Clients

When Command Central is authenticating a client using user names and passwords, it first attempts to find the user name and password in its internal user repository. If it finds an internally-defined user account for the supplied user name, the server authenticates the client using the internally-defined information. If the supplied password is correct, the server proceeds with the request. If the supplied password is not correct, the server rejects the request.

If the server cannot find an internally-defined user account for the supplied user name, the server accesses the external directory (LDAP) to obtain user name and password information for the client. If it finds an externally defined user account, the server authenticates the client using the externally defined information.

If the server cannot find either an internally or externally defined user account for the user, the server rejects the request.

### Overview of Using LDAP

If your site uses Lightweight Directory Access Protocol (LDAP) for user and group information, you can configure Command Central to obtain user and group information from the external directory. You can configure Command Central to use more than one LDAP directory at a time, allowing Command Central to work with different LDAP directories for users in different locations or different organizations. In addition, you can maintain multiple LDAP directories so that one directory serves as a backup for another.

LDAP protocols are designed to facilitate sharing information about resources on a network. Typically, they are used to store profile information, such as user name and password. You can also use them to store additional information. Command Central uses LDAP for performing external authentication.

Using your existing LDAP information allows you to take advantage of a central repository of user and group information. System administrators can add and remove users from the central location. Users do not need to remember a separate password for
webMethods applications; they can use the same user names and passwords that they
use for other applications. Remember to use your LDAP tools to administer users or
groups stored in an external directory.

**LDAP Profile Properties**

When you want to use LDAP or Active Directory as an LDAP server for authentication
purposes instead of using the internal user repository, you must update the LDAP profile
properties.

The following table describes the profile properties for all LDAP connections. Use this
information to help you update the LDAP profile. For information about how to
configure LDAP profile properties, see “Configuring LDAP Profile Properties” on
page 71.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias</td>
<td>None</td>
<td>Optional. Specifies the alias for the LDAP configuration entry. When alias is not specified, its value is set to match the url property. Use any string of characters as the valid value.</td>
</tr>
</tbody>
</table>
| url           | None          | Optional. Specifies the URL for the LDAP server. If you want to use an SSL connection to the LDAP server, ensure the URL starts with ldaps, and provide the truststore or keystore parameters. Use one of the following formats:  
  - ldap://host:port  
  - ldaps://host:port |
<p>| prin          | None          | Optional. Specifies the distinguished name (DN) of the technical user who connects to the LDAP server if anonymous access to the LDAP server is not allowed. |
| cred          | None          | Optional. Specifies the password of the technical user who connects to the LDAP server. Use cred with the prin property. Use any string of characters as the valid value. |
| useaf         | false         | Indicates if an affix (dnprefix or dnsuffix) is used with the LDAP directory entry’s distinguished name (dn). When useaf is set to true, the distinguished name uses affixes. When useaf is set to false, the distinguished name does not use affixes. |</p>
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dnprefix</td>
<td>None</td>
<td>Optional. Specifies the string prefix to add to the DN user name when performing operations on the LDAP server. To use dnprefix, you must set useaf to true. Use any string of characters as the valid value.</td>
</tr>
<tr>
<td>dnsuffix</td>
<td>None</td>
<td>Optional. Specifies the suffix to append to the DN user name when performing operations on the LDAP server. To use dnsuffix, you must set useaf to true. Use any string of characters as the valid value.</td>
</tr>
<tr>
<td>usecaching</td>
<td>None</td>
<td>Optional. Indicates if the LDAP framework caches users or groups, or both. Set to true to enable caching all users and groups. Set to false to disable caching LDAP users and groups.</td>
</tr>
<tr>
<td>mattr</td>
<td>None</td>
<td>Optional. Indicates the type of member search operation that is performed using the value in memberinfoingroups. When memberinfoingroups is set to true, mattr points from the group to the users that are members of the group. When memberinfoingroups is set to false, mattr points from a user entry to the groups for which the user is a member. Use any string of characters as the valid value for mattr.</td>
</tr>
<tr>
<td>memberinfoingroups</td>
<td>False</td>
<td>Optional. Indicates if the login module searches for users that are members of a group or searches for the groups for which a user is a member. You can only use memberinfoingroups when the value that is provided in mattr is applied to users or groups. When memberinfoingroups is set to true, the login module searches users in a group. When memberinfoingroups is set to false, the login module searches groups for a user.</td>
</tr>
</tbody>
</table>
Configuring LDAP Profile Properties

When you want to use LDAP or Active Directory as an LDAP server for authentication purposes instead of using the internal user repository, you must update the LDAP profile properties using one of two methods:

- Update the JAAS configuration file directly using the command line interface. This method allows you to configure only one LDAP connection. For more information, see webMethods Command Central and webMethods Platform Manager Command Reference.

- Update the com.softwareag.security.ldap.pid.properties file, as described in the following procedure. This method allows you to configure connections to multiple LDAPs.

To configure LDAP properties using the ldap properties file

1. In a text editor, open the com.softwareag.security.ldap.pid.properties file located in the following directories:

   - For Platform Manager:
8 Managing Users, Groups, and Roles

Update the LDAP properties based on your needs.
2 Save and close the file.

Using JAAS with Command Central

Java Authorization and Authentication Service (JAAS) provides a standards-based mechanism for deploying custom login modules. Using JAAS, you can write your own custom login module to take over the Command Central authentication process. For more information, see the Developing Login Modules section in the webMethods Suite Security Infrastructure documentation.

By making use of the JAAS framework for extending Java code-based security, you can customize Command Central authentication so that multiple login modules can be called during the authentication process. JAAS allows you to specify:

- The order in which custom login modules are called.
- Whether a login module is required or optional.
- The points at which control can pass from a login module back to the controlling application.

When implementing custom login modules using JAAS, you must:

- Write the login module.
- Configure your login module within the appropriate login context in the JAAS configuration file.

**Note:** A JAAS custom login module deals only with authentication of Command Central users. You cannot use JAAS for Command Central authorization.

JAAS Configuration File

The JAAS configuration file controls which login modules to use within a JVM. Command Central configures the JVM to use

Software AG_directory\profiles\SPM\configuration\com.softwareag.platform.config.propsloade

For Command Central:

Software AG_directory\profiles\CCE\configuration\com.softwareag.platform.config.propsloade

A set of JAAS login modules are grouped into what is termed a login context. Within each login context, the login modules are specified with their full name, optional parameters, and a designation of the actions to take based on their success or failure. These designations are classified as REQUIRED, REQUISITE, SUFFICIENT, and OPTIONAL. For the login to succeed, the complete login context must succeed.
The JAAS configuration file lists the:

- Available login contexts
- Login modules that will execute
- Order in which the modules will execute
- Settings that determine which actions to take if a module fails

Following is a portion of the default JAAS configuration file for Command Central.

```
Default {
    //SSOS login module for SAML signed assertion validation
    //com.softwareag.security.idp.saml.lm.
    //SAML1AssertValidatorLoginModule sufficient;
    //Internal repository login module (java based)
    com.softwareag.security.jaas.login.internal.InternalLoginModule required
    template_section=INTERNAL
    logCallback=true
    internalRepository="C:/wm/kga/common/conf/users.txt"
    create_group_principal=true
    groupRepositoryPath="C:/opt/common/conf/groups.txt";
    //Role repository login module
    com.softwareag.security.authz.store.jaas.login.RoleLoginModule optional
    storage_location="C:/SoftwareAG/common/conf/roles.txt";
    //SSOS login module for SAML sign assertion generation
    //com.softwareag.security.idp.saml.lm.SAML1AssertIssuerLoginModule optional;
}
```

**Configuring the jaas.config File to Use LDAP/AD**

The following procedure describes how to configure the jaas.config file to use LDAP/AD.

1. Use a text editor to open the jaas.config file located in the following directory:
   
   ```
   Software AG_directory\profiles\CCE\configuration
   ```

2. Ensure the InternalLoginModule’s resolution is set to optional as follows:
   ```
   com.softwareag.security.jaas.login.internal.InternalLoginModule optional
   ```

3. Replace with the following:
   ```
   Default {
    //SSOS login module for SAML signed assertion validation
    //com.softwareag.security.idp.saml.lm.
    //SAML1AssertValidatorLoginModule sufficient;
    //Internal repository login module (java based)
    com.softwareag.security.jaas.login.internal.InternalLoginModule required
    template_section=INTERNAL
    logCallback=true
    internalRepository="/opt/softwareag/common/conf/users.txt"
    create_group_principal=true
    groupRepositoryPath="/opt/softwareag/common/conf/groups.txt";
    com.softwareag.security.authz.store.jaas.login.RoleLoginModule optional
    storage_location="/opt/softwareag/common/conf/roles.txt";
    com.softwareag.security.idp.saml.lm.SAML1AssertIssuerLoginModule optional;
    com.softwareag.security.sin.is.ldap.lm.LDAPLoginModule optional
    url="ldap://myldapserv:389"
   }
   ```
Managing Users, Groups, and Roles

Save and close the file.

Groups

A group is a defined collection of users. Groups reflect organizational structure, for example, departments within the organization. When a group is assigned a particular role, all members of the group inherit the permissions granted by this role.

Using groups is optional. Use the internal repository groups and users only when LDAP/AD is not used or is unavailable.

When using LDAP/AD, groups can be nested within other groups. However, members of nested groups do not inherit the parent group's roles and their assigned permissions. You must be a direct member of a group to inherit a role and its permissions.
**Default Group**

Command Central comes with the default group, Administrators, which contains the default user, Administrator.

**Managing Groups**

Groups are managed in the groups.txt file. Using a text editor, you can add, modify, or delete groups.

### To add, modify, or delete groups in the groups.txt file

1. Use a text editor to open the groups.txt file located in the following directory:
   
   ```markdown
   Software AG_directory\common\conf\groups.txt
   ```

2. To add a new group, create a new line and use the following format:

   ```markdown
   group_name:unique_ID:user_name1,user_name2,...user_NameN
   ```

   where `unique ID` is a unique identifier for the group. For example:
   
   ```markdown
   Administrators:1:Administrator
   ```

   **Note:** A group name can be fully qualified, such as, LDAP Distinguished Name.

3. To modify an existing group, edit the group’s information, as needed.

4. To delete a group, delete the group’s line in the file.

   **Note:** You can also comment out a group’s information by including an asterisk (*) as the first character. For example:
   
   ```markdown
   *\Group1:25:Operator
   ```

5. Save and close the file.

**Roles**

A **role** is a collection of access control rights or permissions within Command Central. Roles are assigned to individual users and to groups. When a role is assigned to a group, all members of the group inherit that role. The roles assigned to a user control what permissions the user has when using Command Central and Platform Manager.

Permissions are managed in the roles.txt file. They are assigned to users at run time. Permissions can manage multiple levels of access (for example, installation node, service, resource type, instance) and different actions (for example, create, read, update, delete).

The following table describes the permissions that can be assigned to roles.
In the roles.txt file, you assign permissions to the roles, and map the roles to users or groups. Users are granted permissions based on the group to which they are a member. For more information, see “Managing Roles” on page 76 and “Groups” on page 74.

**Note:** While it is possible to map users to roles, Software AG recommends mapping groups to roles instead. Mapping groups to roles simplifies the authorization model maintenance. Define your authorization model once, and do not implement changes. The only change that should occur in production is mapping users to groups, which is normally done when LDAP/AD is implemented.

### Default Roles

By default, Command Central supports the following roles and their corresponding permissions. For information about adding roles of your own, see “Managing Roles” on page 76.

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>readonlyadmin</td>
<td>canread, canexecute</td>
</tr>
<tr>
<td>superadmin</td>
<td>canread, canwrite, canexecute</td>
</tr>
<tr>
<td>viewer</td>
<td>canread</td>
</tr>
</tbody>
</table>

### Managing Roles

Roles are managed in the roles.txt file. Using a text editor, you can add roles, set permissions for each role, and map roles to groups. Also, you can modify or delete roles.

**Note:** The users and groups in the roles.txt file must match the users and groups in the user repository. For more information, see “Groups” on page 74 and “Managing Groups” on page 75.

The following sample illustrates a roles.txt file. The table following the sample describes each section of the file. The examples used in the procedure correspond to the sample.
Section | Description
--- | ---
permissions | Lists the permissions that are allowed, such as `canread`.
roles | Defines roles and the permissions assigned to them. An asterisk (*) denotes all permissions are assigned to the role.
users | Maps users from the `users.txt` file to roles.
groups | Maps roles to groups defined in the `groups.txt` file.

To add, modify, and delete roles and permissions to the `roles.txt` file

1. Use a text editor to open the `roles.txt` file located in the following directory:
   ```plaintext
   Software AG_directory\common\conf\roles.txt
   ```
2. To add a new role, create a new line in the `roles` section using the following format:
   ```plaintext
   role:rolename=permissions
   ```
   For example, to add a new role, `superadmin`, that has permission to do everything, enter:
   ```plaintext
   role:superadmin=* 
   ```
3. To modify an existing role, edit the role's information, as needed.
4. To delete a role, delete the role's line in the file.

   **Note:** You can also comment out a role's information by including an asterisk (*) as the first character. For example:
   ```plaintext
   *\Group1:25:Operator
   ```
5. In the `users` section, map the user from the `users.txt` file to the new role using the following format:
   ```plaintext
   user: "user_name"=role
   ```
   For example, to map the user, `Administrator`, to the `superadmin` role, specify the following:
   ```plaintext
   user: "Administrator"=superadmin
   ```
6. In the `groups` section, map the role to a group defined in the `groups.txt` file, using the following format:
   ```plaintext
   group: "group_name"=role name
   ```
7. Save and close the file.
9 Viewing Product Inventory

- About Inventory Management ................................................................. 80
- Viewing Products in an Installation ......................................................... 80
- Viewing Fixes Applied to Products in an Installation ............................. 80
About Inventory Management

Command Central queries the Platform Manager for information about the installed products, versions, and fixes of all the managed products that are part of the installation where the Platform Manager is installed.

Viewing Products in an Installation

You can view information about the products, versions, and the components of the products installed in different installations. Use the following procedure to view the details of the products installed in an installation.

To view the products in an installation
1. In the Environments pane, select the environment from which you want to view the products details.
2. Select the Installations tab.
3. Click the name of the installation you want to inspect.
4. Select the Products tab.

Viewing Fixes Applied to Products in an Installation

Use the following procedure to view the details of fixes applied to products in an installation.

To view the fixes applied to the products in an installation
1. In the Environments pane, select the environment in which you want to view the fix details.
2. Select the Installations tab.
3. Click the name of the installation you want to inspect.
4. Select the Fixes tab.
10 Administering Product Lifecycle

- About Administering Product Lifecycle .............................................................. 82
- Starting, Stopping, Pausing, Resuming, and Debugging Instances ....................... 82
About Administering Product Lifecycle

The following sections show how to centrally administer the lifecycle of managed products.

Lifecycle Actions

The lifecycle actions are specific to a product instance. A lifecycle action is disabled if it is not applicable for a product instance. See the product-specific description for each of these actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Starts an instance that was stopped or not started.</td>
</tr>
<tr>
<td>Stop</td>
<td>Stops an instance that was started earlier.</td>
</tr>
<tr>
<td>Pause</td>
<td>Pauses an instance that was started earlier.</td>
</tr>
<tr>
<td>Restart</td>
<td>Restarts an instance that was running or stopped earlier.</td>
</tr>
<tr>
<td>Debug</td>
<td>Starts stopped instance in debug mode.</td>
</tr>
<tr>
<td>Resume</td>
<td>Resumes an instance that was paused earlier. Resume works differently for different product instances. See the product-specific description for this action.</td>
</tr>
<tr>
<td>Safe mode</td>
<td>Runs an instance in safe mode for diagnostic purpose.</td>
</tr>
</tbody>
</table>

Starting, Stopping, Pausing, Resuming, and Debugging Instances

Use the following procedure to change the status of an instance.

To change the status of an instance

1. In the Environments pane, select the environment in which you want to change the status of an instance.
2. Select the Instances tab.
3. Expand the instance node and click the corresponding status icon.
4. Select the required action from the Lifecycle Actions dialog.

Command Central performs the selected action on the instance through Platform Manager and lists the updated instance status on the Instances tab.

You can also change the status of an instance in the Overview tab of the instance.
11 Monitoring Instances

- About Monitoring Instances ................................................................. 84
- Viewing the Status of an Instance or Its Components .............................. 84
- Modifying the Status of an Instance or Its Components ............................ 84
- About Monitoring KPIs ........................................................................... 84
- Viewing Alerts for an Instance or Its Components ..................................... 85
- Clearing Alerts for an Instance or Its Components .................................... 86
- About Monitoring-Related Events ............................................................ 87
About Monitoring Instances

Command Central allows you to monitor the overall health of an instance or its components. You can view and modify the statuses and alerts, and you can view the KPIs (key performance indicators) of an instance or its components. The status, alert, and KPI information is normally retrieved regularly by a polling mechanism from the instance or its component, but Command Central also reacts to monitoring-related events.

Viewing the Status of an Instance or Its Components

An instance or instance component can have one of the following statuses:

- **Online**: The instance or instance component is currently running and the ping operation succeeds.
- **Failed**: The instance or instance component is not running and the ping operation fails.
- **Starting**: The instance or instance component is starting.
- **Stopped**: The instance or instance component has stopped.
- **Stopping**: The instance or instance component is stopping.
- **Unknown**: The status of the instance or instance component cannot be determined.
- **Unresponsive**: The ping operation fails, but other indicators such as the process-id file indicate that the instance or instance component is running.

To view the status of an instance or its components

1. In the **Environments** pane, select the environment that contains the instance or instance component that you want to monitor.
2. Click the **Instances** tab.

The **Status** field in the table shows the status of the instance. To see the status of its components, expand the instance node.

Modifying the Status of an Instance or Its Components

You can modify the status of an instance or its component. For more information, see “Starting, Stopping, Pausing, Resuming, and Debugging Instances” on page 82.

About Monitoring KPIs

Command Central allows you to view up to three basic KPIs (key performance indicators) for each instance or instance component that is in online status.

Each KPI consists of the following information:
KPIs are displayed as bar charts. A bar can have one of the following colors:

- **Green**: The current value is below the marginal threshold, indicating normal operation.
- **Yellow**: The current value is above the marginal threshold, indicating that performance or stability may be affected if it rises further.
- **Red**: The current value is above the critical threshold, indicating that performance or stability are probably impacted as a result.

KPIs are provided for the following products:

- **Software AG Platform Manager** For more information, see “Monitoring KPIs of Software AG Platform Manager Instances” on page 117.
- **Broker Server** For more information, see “Monitoring webMethods Broker KPIs” on page 111.
- **Integration Server** For more information, see “Monitoring KPIs of Integration Server Instances” on page 103.
- **My webMethods Server** For more information, see “Monitoring KPIs of My webMethods Server Instances” on page 123.

### Viewing Alerts for an Instance or Its Components

Command Central indicates whether there is an alert for an instance or for one of its components.

Alerts are raised or disabled when the status of an instance or instance component changes. In this case, the alert behavior is as follows:

<table>
<thead>
<tr>
<th>oldStatus</th>
<th>newStatus</th>
<th>Alert</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>online</td>
<td>stopped</td>
<td>on</td>
<td>warning</td>
</tr>
<tr>
<td>online</td>
<td>unresponsive</td>
<td>on</td>
<td>error</td>
</tr>
<tr>
<td>online</td>
<td>failed</td>
<td>on</td>
<td>error</td>
</tr>
<tr>
<td>online</td>
<td>unknown</td>
<td>on</td>
<td>warning</td>
</tr>
<tr>
<td>not online</td>
<td>online</td>
<td>off</td>
<td>info</td>
</tr>
</tbody>
</table>
Alerts are also raised or disabled when the value of a KPI (key performance indicator) changes. In this case, the alert behavior is as follows:

<table>
<thead>
<tr>
<th>oldZone</th>
<th>newZone</th>
<th>Alert</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>marginal</td>
<td>on</td>
<td>warning</td>
</tr>
<tr>
<td>marginal</td>
<td>critical</td>
<td>on</td>
<td>error</td>
</tr>
<tr>
<td>normal</td>
<td>critical</td>
<td>on</td>
<td>error</td>
</tr>
<tr>
<td>critical</td>
<td>marginal</td>
<td>off</td>
<td>warning</td>
</tr>
<tr>
<td>marginal</td>
<td>normal</td>
<td>off</td>
<td>info</td>
</tr>
<tr>
<td>critical</td>
<td>normal</td>
<td>off</td>
<td>info</td>
</tr>
</tbody>
</table>

**To view the alerts for an instance or its components**

1. In the **Environments** pane, select the environment that contains the instance or instance component that you want to monitor.

2. Click the **Instances** tab.

   **Note:** If there is an alert for an instance or instance component, the respective **Alert** field shows a flag.

3. To see more information about the alert, select an instance or an instance component from the table.

4. Click the **Overview** tab.

5. The **Alerts** field in the **Dashboard** shows the number of alerts. Point to the number to see the message texts and dates.

**Clearing Alerts for an Instance or Its Components**

Command Central allows you to clear the alerts for an instance or for one of its components.

**To clear the alerts for an instance or its components**

1. In the **Environments** pane, select the environment that contains the instance or instance component that you want to monitor.

2. Click the **Instances** tab.

   **Note:** If there is an alert for an instance or instance component, the respective **Alert** field shows a flag.

3. Select an instance or an instance component from the table.
4 Click the **Overview** tab.

5 The **Alerts** field in the **Dashboard** shows the number of alerts. Click the number.

6 In the resulting pop-up window, click **Clear**.

---

**About Monitoring-Related Events**

The monitoring information is normally retrieved by a polling mechanism, but Command Central also reacts to monitoring-related events. To use monitoring-related events, you must configure NERV (Network for Event Routing and Variation) for each instance of Command Central and of Software AG Platform Manager as described in Implementing Event-Driven Architecture with webMethods Products, Configuring NERV.

Using monitoring-related events enables integrated solutions with other Software AG products or third party products.

The following event types exist for integrated solutions:

- **RuntimeStatusChange** This event type is emitted when the status of an instance or instance component changes.

- **RuntimeStateChange** This event type is emitted when the value of a KPI (key performance indicator) changes.

- **Alert** This event type is emitted when changes occur in the instance’s or instance component’s status or state. For detailed information, see “Viewing Alerts for an Instance or Its Components” on page 85.

For more information about the detailed structure of monitoring-related events, go to *Software AG_directory\common\EventTypeStore\WebM\PlatformManagement*. 
12 Comparing Product Versions, Fixes, and Configurations

- About Comparing Products .......................................................... 90
- Comparing Product Versions ...................................................... 90
- Comparing Fix Levels ............................................................... 90
- Comparing Configuration Settings ............................................. 91
About Comparing Products

You can compare installed products for a quick view of their versions, fixes, and configuration settings. Specifically, you can compare:

- Versions of products existing in the same installation or in different installations.
- Fixes applied to the products existing in the same installation or in different installations.
- Configuration settings of instances of an installation.

Comparing Product Versions

When you compare product versions, you can see the version numbers of the products in the selected installations as well as the servers on which the products are installed.

To compare the versions of the products installed
1. In the Environments pane, select the environment for which to compare the version numbers of the products.
   - To view the installations of all environments, select All.
2. Select the Installations tab.
3. In the Installations tab, select two or up to a maximum of five installations for which you want to compare the product versions.
4. Click and select Compare Products.

Comparing Fix Levels

When you compare fix levels, you can see the fixes that are applied to the products in the selected installations.

You can also select an installation and click the Fixes tab to see the fix names, who installed the fix, whether the fix was installed using Software AG Update Manager, and the date and time when the fix was installed.

To compare the fixes applied to the installed products
1. In the Environments pane, select the environment for which you want to compare the fix levels.
   - To view the installations of all environments, select All.
2. Select the Installations tab.
3 In the **Installations** tab, select two or up to a maximum of five installations for which you want to compare the details of the fixes applied to the products.

4 Click ⚙️ and select **Compare Fixes**.

**Comparing Configuration Settings**

When you can compare the configuration settings of instances, you can quickly identify if there are any differences in the settings.

**To compare the configuration settings of instances**

1 In the Environments pane, select the environment for which you want to compare the product configuration settings.

   To view the instances of all environments, select **All**.

2 Select the **Instances** tab.

3 In the **Instances** tab, select two, or up to a maximum of five, instances for comparison.

4 Click ⚙️ and select **Compare Configuration**.

5 In the drop-down list, select the configuration type (port or license) that you want to compare.

6 Click ⬅️ to return to the **Instances** view.
Understanding Product-Specific Administration
### Configuring Integration Server Ports

- **About Ports** ................................................................. 96
- **Configuring Ports** ...................................................... 96
- **Testing Ports** ............................................................... 101
- **Setting the Primary Port** ........................................... 101
- **Editing Port Information** .............................................. 101
- **Enabling and Disabling Ports** ..................................... 102
About Ports

You can use Command Central to configure the ports for multiple Integration Servers managed by Software AG Platform Manager. Each port is configured to work with a specific protocol. You can associate an HTTP, HTTPS, FTP, or FTPS with one or more additional ports as needed. By default, Integration Server is pre-configured with HTTP and diagnostic ports at 5555 and 9999, respectively.

Note: This section assumes that you are familiar with adding ports in the Integration Server Administrator. For more information about the Integration Server Administrator or Integration Server ports, see *webMethods Integration Server Administrator’s Guide*.

You can configure Integration Server ports for HTTP, HTTPS, FTP, and FTPS protocols. In addition, Integration Server supports HTTP and HTTPS diagnostic ports. Diagnostic ports are ports that use threads from a dedicated thread pool to accept requests via HTTP or HTTPS. Diagnostic ports use a dedicated thread pool so that you can access Integration Server when it becomes unresponsive.

Note: You can configure only one diagnostic port per Integration Server.

<table>
<thead>
<tr>
<th>Use this port type...</th>
<th>To...</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Submit unsecured requests to the server.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Submit requests to the server using SSL encryption.</td>
</tr>
<tr>
<td>FTP</td>
<td>Move files to and from the server.</td>
</tr>
<tr>
<td>FTPS</td>
<td>Move files to and from the server using SSL encryption.</td>
</tr>
<tr>
<td>HTTP Diagnostic</td>
<td>Access Integration Server Administrator when the server becomes unresponsive.</td>
</tr>
<tr>
<td>HTTPS Diagnostic</td>
<td>Access Integration Server Administrator using SSL encryption when the server becomes unresponsive.</td>
</tr>
</tbody>
</table>

Before configuring an HTTPS or FTPS port, you must configure Integration Server to use SSL. Use the Integration Server Administrator to create keystore and truststore aliases and certificate mappings. For more information about configuring a port for SSL, see *webMethods Integration Server Administrator’s Guide*.

Configuring Ports

Perform the following procedure to configure Integration Server ports over Command Central.
To configure ports

1. Select the Integration Server environment from the Environment pane, then click the instance from the Instances tab.
2. Click the Configuration tab.
4. Click Add Port. Command Central displays the Select Port Type dialog box.
5. Select one of the following from the Port Type drop-down list and click OK:
   - HTTP
   - HTTPS
   - FTP
   - FTPS
   - HTTP Diagnostic
   - HTTP Diagnostic
6. Expand Connection Basics and complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Specify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Whether the port is enabled.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The number you want to use for the port. Select a number that is not already in use.</td>
</tr>
<tr>
<td>Alias</td>
<td>Name that you want to use for the port alias. Use an alias name that is unique for the instance or component and can be included in a user-friendly URL. The only valid characters in an alias name are ASCII characters, numbers, underscore (_), dot (.), and a hyphen (-).</td>
</tr>
<tr>
<td>Bind Address</td>
<td>IP address to which to bind this port. Specify a bind address if your machine has multiple IP addresses and you want the port to use this specific address. If you do not specify a bind address, the server picks one for you.</td>
</tr>
<tr>
<td>Backlog</td>
<td>How long a connection request should stay in the queue for a suspended port, before the request is rejected. The default is set to 200 milliseconds (ms), with a maximum permissible value of 65535 ms.</td>
</tr>
</tbody>
</table>
13 Configuring Integration Server Ports

<table>
<thead>
<tr>
<th>Field</th>
<th>Specify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep Alive</td>
<td>When to close the connection if the server has not received a request from the client within this timeout value (in milliseconds); or when to close the connection if the client has explicitly placed a close request with the server.</td>
</tr>
<tr>
<td>Keep Alive</td>
<td>When to close the connection if the server has not received a request from the client within this timeout value (in milliseconds); or when to close the connection if the client has explicitly placed a close request with the server.</td>
</tr>
<tr>
<td>Package Name</td>
<td>The package associated with this port. When you enable the package, the server enables the port. When you disable the package, the server disables the port. If you replicate this package, Integration Server creates a port with this number and the same settings on the target server. If a port with this number already exists on the target server, its settings remain intact. This feature is useful if you create an application that expects input on a specific port. The application will continue to work after it is replicated to another server.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether the listener will use this pool exclusively for dispatching requests. The existing thread pool is a global thread pool. If there is a very high load on this resource, the user may have to wait for the global thread pool to process his request. However, with the private thread pool option enabled, requests coming into this port will not have to compete with other server functions for threads. When you view the port’s details, the server reports the total number of private thread pool threads currently in use for the port. Click Yes to enable the private thread pool settings. If you do not need to use the thread pool feature, click No.</td>
</tr>
<tr>
<td>Threadpool Min</td>
<td>The minimum number of threads for this private thread pool. The default is 1.</td>
</tr>
<tr>
<td>Threadpool Max</td>
<td>The maximum number of threads for this private thread pool. The default is 5.</td>
</tr>
<tr>
<td>Threadpool Priority</td>
<td>The Java thread priority. The default is 5.</td>
</tr>
</tbody>
</table>

**Important!** Use this setting with extreme care because it will affect server performance and throughput.
If you are creating an HTTPS, HTTPS diagnostic, or FTPS port, expand Security Configuration and complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Specify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Authentication</td>
<td>The type of client authentication you want Integration Server to perform for requests that arrive on the port. Select:</td>
</tr>
<tr>
<td></td>
<td>- Username/Password if you want to use basic authentication.</td>
</tr>
<tr>
<td></td>
<td>- REQUEST_CERTIFICATE if you want Integration Server to request client certificates for all requests. If the client does not provide a certificate, the server prompts the client for a userid and password. If the client provides a certificate:</td>
</tr>
<tr>
<td></td>
<td>- The server checks whether the certificate exactly matches a client certificate on file and is signed by a trusted authority. If so, the client is logged in as the user to which the certificate is mapped in Integration Server. If not, the client request fails, unless central user management is configured.</td>
</tr>
<tr>
<td></td>
<td>- If central user management is configured, the server checks whether the certificate is mapped to a user in the central user database. If so, the server logs the client on as that user. If not, the client request fails.</td>
</tr>
<tr>
<td></td>
<td>- REQUIRE_CERTIFICATE if you want Integration Server to require client certificates for all requests. The server behaves as described for REQUEST_CERTIFICATE, except that the client must always provide a certificate.</td>
</tr>
<tr>
<td>Keystore Alias</td>
<td>Optional. A user-specified, text identifier for an Integration Server keystore.</td>
</tr>
<tr>
<td></td>
<td>The alias points to a repository of private keys and their associated certificates. Although each listener points to one keystore, there can be multiple keys and their certificates in the same keystore, and more than one listener can use the same keystore alias.</td>
</tr>
<tr>
<td>Key Alias</td>
<td>Optional. The alias for the private key, which must be stored in the keystore specified by the above keystore alias.</td>
</tr>
<tr>
<td>Truststore Alias</td>
<td>Optional. The alias for the truststore. The truststore must contain the trusted root certificate for the CA that signed the Integration Server certificate associated with the key alias. The truststore also contains the list of CA certificates that Integration Server uses to validate the trust relationship.</td>
</tr>
</tbody>
</table>
9 Expand **IP Access Restrictions** and specify the following to allow or deny access from specified ports:

<table>
<thead>
<tr>
<th>Field</th>
<th>Specifies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Global Default</td>
<td>That the port should use the global IP access settings set in Integration Server. This is the default.</td>
</tr>
<tr>
<td>Allow by Default</td>
<td>That the port should allow requests from all hosts except for ones you explicitly deny. This setting overrides Integration Server's global IP access setting for this port. Use this approach if you want to allow most hosts and deny a few.</td>
</tr>
<tr>
<td>Deny by Default</td>
<td>That the port should deny requests from all hosts except for ones you explicitly allow. This setting overrides Integration Server's global IP access setting for this port. Use this approach if you want to deny most hosts and allow a few.</td>
</tr>
<tr>
<td>Hosts to allow</td>
<td>The host names (example, workstation5.webmethods.com) or IP addresses (example, 132.906.19.22 or 2001:db8:85a3:8d3:1319:8a2e:370:7348) of hosts from which the server is to accept inbound requests. Enter each host name on a separate line. The host names or IP addresses can include upper and lower case alphabetic characters, digits (0-9), hyphens (-), and periods (.) but cannot include spaces. For IPv6, IP addresses can also include colons (:) and brackets ([]).</td>
</tr>
</tbody>
</table>

10 Expand **URL Access Restrictions** and specify the following to allow or deny access to specified service URLs:

<table>
<thead>
<tr>
<th>Field</th>
<th>Specifies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Global Default</td>
<td>That the port should use the default mode access settings set in Integration Server. This is the default.</td>
</tr>
<tr>
<td>Deny by Default</td>
<td>That the port should deny requests from all service URLs except for ones you explicitly allow. Use this approach if you want to deny most URLs and allow a few.</td>
</tr>
<tr>
<td>Allow by Default</td>
<td>That the port should allow requests from all service URLs except for ones you explicitly allow. Use this approach if you want to deny most hosts and allow a few.</td>
</tr>
<tr>
<td>URLs to deny</td>
<td>The service URLs from which Integration Server is to accept inbound requests. Enter each service URL on a separate line.</td>
</tr>
</tbody>
</table>

11 Click **Test** to test the port.

12 Click **Save**.
Testing Ports

To test ports

1. Select the Integration Server environment from the Environment pane, then click the instance from the Instances tab.
2. Click the Configuration tab.
3. Select Ports in the drop-down list.
4. From the Port column, locate the port you want to test, and click on the port number.
5. Click Test.

Setting the Primary Port

To set the primary port

1. Select the Integration Server environment from the Environment pane, then click the instance from the Instances tab.
2. Click the Configuration tab.
3. Select Ports in the drop-down list.
4. Locate the port you want to designate as the primary port and click on the port number.
5. Click ⚙️ and then Set as Primary.
6. Click Ok on the confirmation prompt.

Editing Port Information

Perform the following procedure to edit port information.

Note: You cannot change an existing port alias.

To edit port information

1. Select the Integration Server environment from the Environment pane, then click the instance from the Instances tab.
2. Click the Configuration tab.
3. Select Ports in the drop-down list.
From the Port column, locate the port whose details you want to edit, and click on the port number.

Click Edit.

Make changes to the port and click one of the following:

- Test to test the port.
- Save to change your edits to the port.
- Cancel to cancel the edits to the port.

**Enabling and Disabling Ports**

Perform the following procedure to enable or disable a port.

**To enable or disable a port**

1. Select the Integration Server environment from the Environment pane, then click the instance from the Instances tab.
2. Click the Configuration tab.
3. Select Ports in the drop-down list.
4. From the Port column, locate the port you want to enable or disable, and click on the port number.
   - The ✓ icon indicates that the port is enabled.
   - The ❌ icon indicates that the port is disabled.
5. Expand Threadpool Configuration and enable or disable the port.
To view the KPIs of Integration Server instances

1. On the **Environments** pane, select the environment you want to monitor.
2. Click the **Instances** tab.
3. In the table, select the Integration Server you want to monitor.
4. Click the **Overview** tab.

The **Monitoring** section in the **Dashboard** shows the KPIs of the Integration Server instance. Integration Server returns the following three KPIs:

<table>
<thead>
<tr>
<th>Name</th>
<th>Marginal Value</th>
<th>Critical Value</th>
<th>Maximum Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average response time (in ms)</td>
<td>80% of maximum</td>
<td>95% of maximum</td>
<td>5000</td>
</tr>
<tr>
<td>Service errors</td>
<td>70% of maximum</td>
<td>90% of maximum</td>
<td>5</td>
</tr>
<tr>
<td>Running services</td>
<td>80% of maximum</td>
<td>95% of maximum</td>
<td>10</td>
</tr>
</tbody>
</table>
Administering webMethods Broker

- About webMethods Broker Administration ................................................. 106
- Configuring Broker Server License ......................................................... 106
- Configuring SSL in Broker Server .......................................................... 107
- Retrieving Configuration Details of Broker Server Base Port ..................... 108
- Pausing and Resuming Message Publishing in Broker Servers .................... 109
- Using the Administration Link of Broker Server ......................................... 109
About webMethods Broker Administration

You can administer Broker Servers through Command Central. Note that because Platform Manager uses Broker Monitor to obtain information about Broker Servers, Broker Monitor must be running if you want to administer Broker Servers through Command Central.

You can use Command Central to perform the following operations on webMethods Broker.

- View the number of Broker Servers running in each environment of your IT landscape
- View the versions of Broker Servers
- View the fixes applied to Broker Servers
- Configure Broker Server license
- Configure SSL in a Broker Server
- Retrieve Broker Server base port and SSL configuration details
- Start, stop, and restart Broker Server
- Pause and resume message publishing in Broker Server
- Monitor Broker Server installations
- Monitor run-time status, KPIs, and alerts of Broker Server instances
- Use the administration link of Broker Server

Note: webMethods Broker does not support Debug and Safe mode lifecycle operations.

Configuring Broker Server License

To change Broker Server license

1. In the Environments pane, select the environment in which Broker Server is installed.
2. Click the Instances tab.
3. Click the Broker Server instance for which you want to change the license.
4. Click the Configuration tab.
5. Select Licenses from the drop-down

   The license type, status, and expiration date for the Broker Server license appear below the drop-down
6 In the **License Type** column, click the Broker Server link.

Command Central displays the license key location. You can view the license file details when you expand **License Key Details**.

7 Click **Edit**.

8 Click **Browse** in the **License Upload Location** field, and then navigate to the new license file.

The new license file that you select is uploaded to the license location as shown in the **Server License Location** field.

9 If you want to change the licence file location, edit the new path in the **Server License Location** field. The new location of the server license file is updated in the awbroker.cfg configuration file that resides in Broker Server’s data directory.

10 Click **Save** to save the new license.

### Configuring SSL in Broker Server

**To enable or disable SSL in Broker Server**

1 In the Environments pane, select the environment in which you want to configure the Broker Server.

2 Click the **Instances** tab.

3 Click the name of the Broker Server instance for which you want to configure SSL.

4 Click the **Configuration** tab.

5 Select **Ports** in the drop-down list to view the port settings configured.

Command Central displays the Broker Server port.

6 Click the name of the port and click **Edit**.

**Connection Basics** displays the following non-editable fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabled</strong></td>
<td>Whether the Broker Server base port is enabled.</td>
</tr>
<tr>
<td><strong>Port Number</strong></td>
<td>The Broker Server base port number.</td>
</tr>
</tbody>
</table>

To change the base port, stop the Broker Server and change the port setting using the `server_config` command line utility in webMethods Broker. For information about the `server_config` command line utility in webMethods Broker, see *Administering webMethods Broker*. 
Expand **Security Configuration** and specify the following SSL settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Specify</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Enabled</td>
<td>Whether SSL port is enabled. Click <strong>Yes</strong> to enable the SSL port settings. If you do not want to use SSL, click <strong>No</strong>.</td>
</tr>
<tr>
<td>Keystore Type</td>
<td>The keystore type. Select the keystore type.</td>
</tr>
<tr>
<td></td>
<td>■ PEM</td>
</tr>
<tr>
<td></td>
<td>■ PKCS12</td>
</tr>
<tr>
<td>Server Location of Keystore</td>
<td>The directory where the keystore file is located.</td>
</tr>
<tr>
<td>Password</td>
<td>The password to open the keystore file.</td>
</tr>
<tr>
<td>Truststore Type</td>
<td>The truststore file format. Select the truststore type.</td>
</tr>
<tr>
<td></td>
<td>■ PEM</td>
</tr>
<tr>
<td></td>
<td>■ DIR</td>
</tr>
<tr>
<td>Server Location of Truststore</td>
<td>The directory where the truststore file is located.</td>
</tr>
</tbody>
</table>

8 Click **Test** to verify the port settings.

9 Click **Save** to save the port changes.

**Retrieving Configuration Details of Broker Server Base Port**

Using Command Central, you can retrieve the configuration details of Broker Server's base port.

**Note:** You cannot use Command Central to configure the Broker Server base port. If you want to configure the base port assigned to a Broker Server, stop the Broker Server and change the port setting using the `server_config` command line utility. For information about the `server_config` command line utility, see *Administering webMethods Broker*.

**Retrieving a Broker Server's base port configuration details**

1 In the Environments pane, select the environment in which Broker Server is installed.

2 Click the **Instances** tab.
3 Click the Broker Server instance for which you want to view the port settings.
4 Click the Configuration tab.
5 Select Ports from the drop-down list to view the following read-only Broker Server port details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Indicates whether the Broker Server port is enabled or disabled.</td>
</tr>
<tr>
<td>Port</td>
<td>Indicates the base port of the Broker Server.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Indicates the protocol used by the Broker Server.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates the type of Broker Server port.</td>
</tr>
</tbody>
</table>

**Pausing and Resuming Message Publishing in Broker Servers**

When the publishing load increases in a Broker Server, you can pause publishing, clear queues, and later resume the publishing.

**To pause and resume message publishing in a Broker Server**

1 In the Environments pane, select the environment in which Broker Server is installed.
2 Select the Instances tab.
3 Click the status icon corresponding to the Broker Server and select the required lifecycle operation:
   - Click Pause to pause message publishing in all the Brokers belonging to the selected Broker Server. The status of the Broker Server changes toPaused. Use the icon to refresh the status immediately. You can continue to perform administrative tasks on paused Brokers. The clients of a paused Broker can access and retrieve the messages from the Broker queue.
   - Click Resume to resume message publishing in all the paused Brokers belonging to the Broker Server.

The status of the Broker Server changes to Online. Use the icon to refresh the status immediately.

**Using the Administration Link of Broker Server**

When you have the administrative credentials to access the administration link of Broker Server in Command Central, you can use the Broker Server Details page in My webMethods.
By default, My webMethods Server running on localhost:8585 is available for you when you click the Broker Server Details link. If you want to use My webMethods Server running on a different host machine, configure the host and port of the My webMethods Server you want to use.

Configuring the Host and Port of My webMethods Server

The default host and port of the My webMethods Server specified for Broker Server administration is localhost:8585.

Use Command Central command line interface to configure the host and port of My webMethods Server. For more information, see webMethods Command Central and webMethods Platform Manager Command Reference.

Pre-requisites for Viewing the Broker Server Details Page in My webMethods

You can access the Broker Server Details page in My webMethods only if the following conditions are true for the corresponding installation:

- My webMethods Server is installed.
- webMethods Broker user interface in My webMethods is installed.
- My webMethods Server is running.
- You have administrative credentials to access the Broker Server Details page in My webMethods.
- The Broker Server that you want to administer is added in My webMethods. For information about how to add a Broker Server in My webMethods, see Administering webMethods Broker.

Viewing the Broker Server Details Page in My webMethods

To view the Broker Server Details page in My webMethods

1. In the Environments pane, select the environment in which the Broker Server you want to administer is installed.
2. Select the Environments > Instances tab.
3. Click the name of the Broker Server you want to administer.
4. In the Overview tab, click Broker Server Details.
16 Monitoring webMethods Broker KPIs

- Overview ................................................................. 112
- Storage Utilization KPI .............................................. 112
- Memory Utilization KPI ............................................. 114
- Stalled Queues KPI .................................................. 114
Overview

The visual key performance indicators (KPIs) and alerts enable you to monitor webMethods Broker’s health.

The following KPIs help you administer, troubleshoot, and resolve performance issues in webMethods Broker:

<table>
<thead>
<tr>
<th>KPI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Storage or Configuration Storage</td>
<td>Indicates the utilization of either the run-time data storage or the configuration data storage of Broker Server.</td>
</tr>
<tr>
<td>Memory</td>
<td>Indicates the utilization of Broker Server memory.</td>
</tr>
<tr>
<td>Stalled queues</td>
<td>Indicates the performance of the message queues.</td>
</tr>
</tbody>
</table>

Storage Utilization KPI

Broker Server storage utilization indicator helps you to take corrective actions when either the run-time data storage or the configuration data storage of Broker Server reaches a critical value.

Marginal, Critical, and Maximum Values for Broker Server's Storage Utilization

The marginal, critical, and maximum values of run-time data storage and configuration data storage of Broker Server depend on the maximum storage size that you have configured for the Broker Server by using the `server_config` command.

<table>
<thead>
<tr>
<th>Marginal Value</th>
<th>Critical Value</th>
<th>Maximum Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>60% of the Broker Server’s maximum storage size.</td>
<td>80% of the Broker Server’s maximum storage size.</td>
<td>Broker Server’s maximum storage size.</td>
</tr>
</tbody>
</table>
## Storage Utilization Display

The values of run-time data storage and configuration data storage define whether the storage indicator indicates the utilization of data storage or configuration data storage.

The storage indicator displays **Data Storage** if any of these conditions are true:

- The threshold category of both Broker Server data and configuration data storage are the same. That is, both the storage values are:
  - Less than marginal (green 🟢)
  - Greater than marginal but less than critical (yellow 🟡)
  - More than critical and less than maximum (red 🟥)

- Broker Server data storage has reached a higher threshold compared to configuration data storage. For example, when Broker Server data storage is at the critical threshold (yellow 🟡) and configuration data storage is less than marginal (green 🟢), then storage indicator displays the data storage value.

The storage indicator displays **Configuration Storage** if the configuration data storage has reached a higher threshold compared to the Broker Server data storage. For example, when configuration data storage is at the maximum threshold (red 🟥) and Broker Server data storage is more than the marginal but less than critical threshold (yellow 🟡), then storage indicator displays the configuration data storage value.

<table>
<thead>
<tr>
<th>Storage Utilization Broker Server Data</th>
<th>Storage Utilization Configuration Data</th>
<th>Storage Value Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than marginal value</td>
<td>Less than marginal value</td>
<td>Broker Server Data</td>
</tr>
<tr>
<td>Less than marginal value</td>
<td>More than marginal value,</td>
<td>Configuration Data</td>
</tr>
<tr>
<td></td>
<td>but less than critical value</td>
<td></td>
</tr>
<tr>
<td>Less than marginal value</td>
<td>More than critical value,</td>
<td>Configuration Data</td>
</tr>
<tr>
<td></td>
<td>but less than maximum value</td>
<td></td>
</tr>
<tr>
<td>More than marginal value,</td>
<td>Less than marginal value</td>
<td>Broker Server Data</td>
</tr>
<tr>
<td>but less than critical value</td>
<td>More than marginal value,</td>
<td>Broker Server Data</td>
</tr>
<tr>
<td></td>
<td>but less than critical value</td>
<td></td>
</tr>
<tr>
<td>More than marginal value,</td>
<td>More than critical value,</td>
<td>Configuration Data</td>
</tr>
<tr>
<td>but less than critical value</td>
<td>but less than maximum value</td>
<td></td>
</tr>
<tr>
<td>More than marginal value,</td>
<td>Less than marginal value</td>
<td>Broker Server Data</td>
</tr>
<tr>
<td>but less than maximum value</td>
<td>More than critical value,</td>
<td>Configuration Data</td>
</tr>
<tr>
<td></td>
<td>but less than maximum value</td>
<td></td>
</tr>
<tr>
<td>More than critical value,</td>
<td>Less than marginal value</td>
<td>Broker Server Data</td>
</tr>
<tr>
<td>but less than maximum value</td>
<td>More than critical value,</td>
<td>Configuration Data</td>
</tr>
</tbody>
</table>
Memory Utilization KPI

The memory utilization indicator helps you monitor Broker Server's memory.

Marginal, Critical, and Maximum Values for Memory Utilization

The marginal, critical, and maximum values of memory utilization depend on the Broker Server's memory defined by the `max-memory-size` parameter in the Broker Server configuration file (awbroker.cfg).

<table>
<thead>
<tr>
<th>Marginal Value</th>
<th>Critical Value</th>
<th>Maximum Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>80% of the <code>max-memory-size</code> parameter value.</td>
<td>95% of the <code>max-memory-size</code> parameter value.</td>
<td>Broker Server's memory limit defined in the <code>max-memory-size</code> parameter.</td>
</tr>
</tbody>
</table>

Stalled Queues KPI

The stalled queues indicator alerts you if messages are stuck for a long time or if messages are never retrieved from queues that are connected to clients.

A queue is considered to be stalled only if all these conditions are true:

- A client is connected to the queue
- The queue contains at least one message
- It has been more than five minutes since the client retrieved a message from the queue
<table>
<thead>
<tr>
<th>Marginal Value</th>
<th>Critical Value</th>
<th>Maximum Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 queue.</td>
<td>50% of the maximum value.</td>
<td>Defined by whichever of these values is greater:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 1 queue.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 5% of the total number of client queues or forward queues in Brokers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Current number of stalled queues.</td>
</tr>
</tbody>
</table>

For example, if the number of stalled queues is zero, and 5% of the sum of client queues and forward queues is less than 1, then the maximum value is 1 queue.
17  Monitoring KPIs of Software AG Platform Manager Instances

Software AG Platform Manager returns the following three KPIs:

<table>
<thead>
<tr>
<th>Name</th>
<th>Margin Value</th>
<th>Critical Value</th>
<th>Maximum Value</th>
<th>Limitation Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used machine physical memory (in MB)</td>
<td>80%</td>
<td>95%</td>
<td>Physical memory of machine.</td>
<td></td>
</tr>
<tr>
<td>Used machine disk space (in MB)</td>
<td>80%</td>
<td>95%</td>
<td>Physical disk space of machine.</td>
<td></td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>80%</td>
<td>90%</td>
<td>100%</td>
<td>- This KPI is only displayed, if you use Java 7.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- This KPI is not displayed when running on HP-UX.</td>
</tr>
</tbody>
</table>

To view the KPIs of Software AG Platform Manager instances

1  On the Environments pane, select the environment you want to monitor.
2  Click the Instances tab.
3  In the table, select the Platform Manager you want to monitor.
4  Click the Overview tab.

The Monitoring section in the Dashboard shows the KPIs of the Platform Manager instance.
18 Configuring My webMethods Server Ports

- Configuring My webMethods Server Ports .................................................. 120
- Editing Port Settings .................................................................................. 120
Configuring My webMethods Server Ports

My webMethods Server listens for client requests on one or more ports. When a port receives a message or request, My webMethods Server invokes the appropriate services. Each port is configured to work with a specific protocol. You can associate HTTP or HTTPS with one or more additional ports as needed. By default, My webMethods Server is pre-configured with HTTP at 8585.

The MWS_default component is the OSGi profile. The My webMethods Server component is the standard profile for the server instance. You can edit configuration settings for the My webMethods Server component, but you cannot add or delete them.

To configure My webMethods Server ports

1. In the Environments pane, select the environment in which you want to view the My webMethods Server instance.
2. Select the Instances tab.
3. Expand the MWS_mwsinstancename node containing the My webMethods Server instance you want to configure.
4. Click My webMethods Server in the name column.
5. Select the Configuration tab. Make sure My webMethods Server is selected in the left pane.
6. Select Ports from the drop-down list box. The AJP13 port is deprecated.
7. Test and Save the port.

Editing Port Settings

Perform the following procedure to change the port settings.

To enable or disable a port

1. Select the My webMethods Server environment from the Environments pane, then click the My webMethods Server instance you want to edit from the Instances tab.
2. Click the Configuration tab.
3. Select Ports in the drop-down list.
4. Click the number of the port you want to edit and click Edit. The port settings are now editable. Make the necessary changes to the port settings.
5. Test and Save the changes.
Perform the following procedure to configure My webMethods Server email.

To configure email

1. Select the My webMethods Server environment from the Environment pane, then click the instance from the **Instances** tab.

2. Click the **Configuration** tab.

3. Select **Email** in the drop-down list.

   Command Central displays the My webMethods Server SMTP Server Configuration.

4. Click **Edit**.

5. In **Connection Basics**, complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Specify</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Name</strong></td>
<td>The SMTP server's host name. For example: smtp.server.com.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>The SMTP server's port number.</td>
</tr>
<tr>
<td><strong>Sender Name</strong></td>
<td>The default name to use in the From field of the email messages sent by the server.</td>
</tr>
<tr>
<td><strong>Sender Email</strong></td>
<td>The default email address to use in the From field of the email messages sent by the server.</td>
</tr>
</tbody>
</table>

6. Expand **Advanced Settings** and complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SMTP Username</strong></td>
<td>Optional. The user name that My webMethods Server has to supply for authentication. If the SMTP server requires authentication, specify the user name.</td>
</tr>
<tr>
<td><strong>SMTP Password</strong></td>
<td>Optional. The password associated with the SMTP Username. If the SMTP server requires authentication, specify the appropriate password.</td>
</tr>
</tbody>
</table>

7. Click **Test** and **Save** the email settings.
Monitoring KPIs of My webMethods Server Instances

To view the KPIs of My webMethods Server instances

1. On the Environments pane, select the environment you want to monitor.
2. Click the Instances tab.
3. Select the My webMethods Server you want to monitor.
4. Click the Overview tab.

The Monitoring section in the Dashboard shows the KPIs of the My webMethods Server instance.

My webMethods Server returns the following three KPIs.

<table>
<thead>
<tr>
<th>Name</th>
<th>Marginal Value</th>
<th>Critical Value</th>
<th>Maximum Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of user sessions</td>
<td>80% of maximum</td>
<td>95% of maximum</td>
<td>At least 100, or high water mark.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(High water mark is the highest value ever reached.)</td>
</tr>
<tr>
<td>JDBC connection pool size (maximum</td>
<td>80% of maximum</td>
<td>95% of maximum</td>
<td>As configured.</td>
</tr>
<tr>
<td>number of connections to JDBC)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average response time (in milliseconds)</td>
<td>50% of maximum</td>
<td>90% of maximum</td>
<td>At least 10 seconds, or high water mark.</td>
</tr>
</tbody>
</table>
21 Administering Universal Messaging

- About Administering Universal Messaging ................................................................. 126
- How Does Command Central Communicate with a Universal Messaging Realm Server? .... 126
- Universal Messaging Inventory .................................................................................. 126
- Universal Messaging License Configuration ............................................................... 127
- Universal Messaging Lifecycle Actions ...................................................................... 127
- Universal Messaging Ports Configuration ................................................................. 128
- Universal Messaging KPIs .......................................................................................... 131
About Administering Universal Messaging

This section describes the details specific to Universal Messaging administration. You can discover the Universal Messaging realm servers installed in the Command Central landscape, configure the license and ports of the realm servers, and monitor the health of the realm servers.

Command Central administers a Universal Messaging realm server by using one of the ports (interfaces) of the realm server.

To perform advanced configuration tasks, use Universal Messaging Enterprise Manager. You cannot access Enterprise Manager through Command Central. For information about Enterprise Manager, see the Universal Messaging documentation.

How Does Command Central Communicate with a Universal Messaging Realm Server?

Command Central checks the ports (interfaces) of a Universal Messaging realm server in the following order and chooses the first port (interface) that connects with the realm server:

1. Interfaces that use HTTP protocol (nhp)
2. Interfaces that use socket protocol (nsp)
3. Interfaces that use HTTPS protocol (nhps)
4. Interfaces that use SSL protocol (nsps)

At any point, if there is a disconnection between Command Central and the realm server, Command Central will identify another port using the same order to check the next available port for communicating with the realm server.

**Note:** Command Central will use a secured port (nhps and nsps) to connect with a realm server only if the client-side certificates are not required for establishing the connection. Command Central does not use ports that use shared memory protocol (shm).

For information about configuring ports (interfaces), see “Universal Messaging Ports Configuration” on page 128.

Universal Messaging Inventory

When you view installations in an environment, Command Central displays the Universal Messaging realm servers listed in the UniversalMessaging_installationDirectory\nirvana\server directory of an installation. Command Central lists all the folders (except the templates) in the server directory.
Universal Messaging Run-time Statuses

The run-time status of a Universal Messaging realm server instance states if the realm server is online, failed, stopped, unresponsive (when none of the realm server interfaces are connected to the realm server), or unknown. Universal Messaging does not report the starting and stopping statuses.

Universal Messaging License Configuration

For a Universal Messaging realm server, you can configure the license, view the details of the license that is configured, and retrieve the location of the license file. You cannot change the location of a Universal Messaging license file.

Changing Universal Messaging License

Perform the following procedure to change the Universal Messaging license:

To configure the Universal Messaging license

1. Select the Universal Messaging environment from the Environment pane, then click the instance from the Instances tab.
2. Click the Configuration tab.
3. Select Licenses in the drop-down list.
4. In the License Type column, click Universal Messaging.
5. To change the license file:
   a. Click Edit.
   b. Click Browse to locate the new license file.
   c. Click Save.

Universal Messaging Lifecycle Actions

You can perform the following lifecycle actions on a Universal Messaging realm server.

- **Start.** Start a realm server that is stopped.
- **Stop.** Stop a running realm server.
- **Restart.** Restart a running realm server.
Universal Messaging Ports Configuration

This section describes how to configure the realm server interfaces by using the port settings. The port on which you install the Universal Messaging realm server is the primary port (interface) of the realm server.

You can view, create, enable, disable, edit the Universal Messaging realm server ports (interfaces). You can delete only the non-primary ports (interfaces).

**Note:** Command Central does not use or report the Universal Messaging realm server ports that use shared memory protocol (shm).

Port Configuration Attributes

When you add a new port (interface), configure the attributes of the port. Set the security attributes for the secured ports that use either the HTTPS protocol or the SSL protocol.

**Basic Port Connection Attributes**

The table describes the basic connection attributes of a port.

<table>
<thead>
<tr>
<th>Configure this...</th>
<th>To specify...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Type</td>
<td>Which protocol, the port (interface) must use:</td>
</tr>
<tr>
<td></td>
<td>- Socket protocol (nsp)</td>
</tr>
<tr>
<td></td>
<td>- HTTP protocol (nhp)</td>
</tr>
<tr>
<td></td>
<td>- HTTPS protocol (nhps)</td>
</tr>
<tr>
<td></td>
<td>- SSL protocol (nsps)</td>
</tr>
<tr>
<td></td>
<td>You cannot change this attribute after you create the port.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The number of the port.</td>
</tr>
<tr>
<td></td>
<td>You cannot change this attribute after you create the port.</td>
</tr>
<tr>
<td>Bind Address</td>
<td>The IP address to which to bind this port, if your machine has multiple IP addresses and you want the port to use this specific address.</td>
</tr>
<tr>
<td></td>
<td>You cannot change this attribute after you create the port.</td>
</tr>
<tr>
<td>Configure this...</td>
<td>To specify...</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Backlog</td>
<td>The maximum size of the IP socket queue. When the incoming socket request queue reaches this maximum value, the incoming connection requests are refused. The requests will be serviced only when the queue size is less than the maximum size.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether the port is enabled or disabled.</td>
</tr>
</tbody>
</table>

**Note:** If Command Central fails to enable a port, check the Universal Messaging logs to find out the reason for failure.

### Port Security Attributes

The table describes the security attributes you can configure for a secure SSL enabled port.

<table>
<thead>
<tr>
<th>Configure this...</th>
<th>To specify...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Authentication</td>
<td>Whether or not Universal Messaging requires client certificates for all requests. Select:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>None</strong> if Universal Messaging does not require client certificates for all requests.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>REQUIRE_CERTIFICATE</strong> if you want Universal Messaging to require client certificates for all requests.</td>
</tr>
<tr>
<td>SSL Enabled</td>
<td>Whether the port is SSL enabled or not. This attribute is always set to true for nhps and nsps port.</td>
</tr>
<tr>
<td>Keystore Type</td>
<td>File type of the keystore file. Universal Messaging supports only the JKS file type.</td>
</tr>
<tr>
<td>Server Location of Keystore</td>
<td>Location of the keystore file.</td>
</tr>
<tr>
<td>Keystore Password</td>
<td>Password required to access the SSL certificate in the keystore file.</td>
</tr>
<tr>
<td>Keystore Key Password</td>
<td>Password required to access a specific private key in the keystore file.</td>
</tr>
<tr>
<td>Truststore Type</td>
<td>File type of the truststore file. Universal Messaging supports only the JKS file type.</td>
</tr>
<tr>
<td>Server Location of Truststore</td>
<td>Location of the truststore file.</td>
</tr>
</tbody>
</table>
Adding a Port

Perform the following procedure to add a new port (interface) to a realm server. For information about the port attributes you can configure, see “Port Configuration Attributes” on page 128.

To add a new port (interface)

1. Select the Universal Messaging environment from the Environment pane, then click the instance from the Instances tab.
2. Click the Configuration tab.
3. Select Ports in the drop-down list.
4. Click 
5. Select the protocol for the port from the Port Type drop-down list and click OK.
6. Expand Connection Basics and provide the values for the fields.
7. If you are creating a secured SSL port, expand Security Configuration and provide the values for the fields.
8. Click Save.

Editing a Port

Perform the following procedure to edit the backlog and security attributes of a port. For information about the port attributes, see “Basic Port Connection Attributes” on page 128 and “Port Security Attributes” on page 129. If you change the SSL certificates of a secured interface, you must restart the interface.

To edit a port

1. Select the Universal Messaging environment from the Environment pane, then click the instance from the Instances tab.
2. Click the Configuration tab.
3. Select Ports in the drop-down list.
4. From the Port column, click the number of the port you want to edit.
5. Click Edit.
6. Make changes to the port and click Save.
**Enabling or Disabling a Port**

Perform the following procedure to enable or disable a port (interface).

**To enable or disable port (interface)**

1. Select the Universal Messaging environment from the Environment pane, then click the instance from the **Instances** tab.
2. Click the **Configuration** tab.
3. Select **Ports** in the drop-down list.
4. In the **Port** column, locate the port you want to enable or disable, and click on the port number.
5. Expand **Connection Basics** and enable or disable the port.

**Universal Messaging KPIs**

This section describes the key performance indicators (KPIs) of Universal Messaging. These KPIs enable you to monitor the health of the Universal Messaging realm servers:

<table>
<thead>
<tr>
<th>KPI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JVM Memory</td>
<td>Indicates the utilization of JVM memory. The marginal, critical, and maximum values for this KPI depend on the maximum memory size of the JVM.</td>
</tr>
<tr>
<td></td>
<td>- Marginal is 80% of the maximum JVM memory.</td>
</tr>
<tr>
<td></td>
<td>- Critical is 95% of the maximum JVM memory.</td>
</tr>
<tr>
<td></td>
<td>- Maximum is 100% of the maximum JVM memory.</td>
</tr>
<tr>
<td>Fanout Backlog</td>
<td>Indicates the total number of events currently waiting to be processed by the fanout engine. If the fanout backlog is more than the critical value, there is a possibility that the subscribers receive the published events after some delay.</td>
</tr>
<tr>
<td></td>
<td>The KPI uses the following marginal, critical, and maximum values:</td>
</tr>
<tr>
<td></td>
<td>- Marginal is 80% of the maximum value.</td>
</tr>
<tr>
<td></td>
<td>- Critical is 95% of the maximum value.</td>
</tr>
<tr>
<td></td>
<td>- Maximum is 100% of the peak value (high-water mark) of fanout backlog. Default is 100.</td>
</tr>
</tbody>
</table>
Perform the following procedure to view the KPIs of a Universal Messaging realm server instance.

### Queued Tasks

- **Indicates the total number of tasks in the read, write, and common read/write pools. If the number of read and write tasks queued is more than the critical value, it indicates that the Universal Messaging realm server is unable to match the speed of the publishers and subscribers.**

The KPI uses the following marginal, critical, and maximum values:

- **Marginal** is 80% of the maximum value.
- **Critical** is 95% of the maximum value.
- **Maximum** is 100% of the peak value (high-water mark) of read and write tasks queued. Default is 100.

### Viewing the KPIs of a Universal Messaging Instance

Perform the following procedure to view the KPIs of a Universal Messaging realm server instance.

**To view the KPIs of a realm server instance**

1. On the Environments pane, select the environment you want to monitor.
2. Click the **Instances** tab.
3. Select the Universal Messaging realm server instance you want to monitor.
4. Click the **Overview** tab.
22 Administering CentraSite

- About Administering CentraSite .................................................. 134
- Viewing CentraSite Components .................................................. 134
- Viewing CentraSite Registry Repository (CRR) and CentraSite Application Server Tier (CAST) 134
About Administering CentraSite

CentraSite installation contains two components:

- CentraSite Registry Repository (CRR)
- CentraSite Application Server Tier (CAST)

You can use Command Central to perform the following administration tasks on your CentraSite installation:

- View the CentraSite components. For more information, see “Viewing CentraSite Components”.
- Start, stop, restart, and debug the CentraSite Registry Repository. If you start or restart CentraSite Registry Repository when it is on debug mode, the debug mode turns off, and CentraSite Registry Repository works on normal mode.

CentraSite Application Server Tier, a component of CentraSite, runs in the Software AG Runtime. You cannot start, stop, or restart the CentraSite Application Server Tier independent of the Software AG Runtime (CTP).

- Create log files for debugging. When you perform the Debug action on the CentraSite Registry Repository, CentraSite writes status and other information to the following log files in the `CentraSite_directory\data` directory, where `CentraSite_directory` is the installation directory of CentraSite.

<table>
<thead>
<tr>
<th>Log File...</th>
<th>Stores...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry.log (CentraSite.AAB.log.1.xml CentraSite.AAB.log.0.xml)</td>
<td>The request logs (middle level information).</td>
</tr>
<tr>
<td>A file with type &quot;2X0&quot;</td>
<td>The data store request logs (low level information).</td>
</tr>
</tbody>
</table>

For more information about how to start, stop, restart, and debug a CentraSite Registry Repository, see “Starting, Stopping, Pausing, Resuming, and Debugging Instances”.

Viewing CentraSite Components

Viewing CentraSite Registry Repository (CRR) and CentraSite Application Server Tier (CAST)

CentraSite Registry Repository is a process.
CentraSite Application Server is an engine.
To view CRR and CAST

1. In the Environments pane, select the environment that contains the CentraSite installation you want to view.

2. Click the Instances tab.

3. To view CRR, click **CentraSite Registry Repository**. If there is more than one CRR instance, click the one that you want to work with.

4. To view CAST, expand the **CTP** node.

5. Click **CentraSite Application Server**.
Command Central Task Quick Reference

The following sections list common Command Central tasks and how to perform them using the Command Central web user interface and the Command Central command line interface.

For more information about the interface navigation and commands listed in this quick reference, including usage notes, arguments, and options, see the appropriate documentation for the interface you are using:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Where to Find More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>webMethods Command Central Help</td>
</tr>
<tr>
<td>Command line interface</td>
<td>webMethods Command Central and webMethods Platform Manager Command Reference</td>
</tr>
</tbody>
</table>

Working with Authentication between Command Central and Managed Products

This section provides a quick reference to the Command Central tasks that pertain to authentication between Command Central and the products it manages.

Changing the Fixed User Password

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Authentication Mode (select an Environment, click the Instances tab, select an Instance, click the Overview tab, click the ✏️ Authentication Edit button)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc add security credentials</td>
</tr>
</tbody>
</table>

Working with Environments

This section provides a quick reference to the Command Central tasks that pertain to managing environments.
A Command Central Task Quick Reference

**Searching for an Environment**

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Environments pane (type search criteria in the <strong>Search Environments</strong> box)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><code>cc list landscape environments</code></td>
</tr>
</tbody>
</table>

**Viewing Details about an Environment**

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Environments pane (select an environment)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><code>cc get landscape environments</code></td>
</tr>
<tr>
<td></td>
<td><code>cc list landscape environments</code></td>
</tr>
</tbody>
</table>

**Adding an Environment**

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Environments pane (click the <strong>Add Environment</strong> button)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><code>cc create landscape environments</code></td>
</tr>
</tbody>
</table>

**Editing Environment Details**

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Environments pane (select an environment, click the <strong>Options</strong> button in the Environments pane, select <strong>Edit Environment</strong> button)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><code>cc update landscape environments</code></td>
</tr>
</tbody>
</table>

**Deleting an Environment**

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Environments pane (select an environment, click the <strong>Delete Environment</strong> button)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><code>cc delete landscape environments</code></td>
</tr>
</tbody>
</table>
Working with Installations

This section provides a quick reference to the Command Central tasks that pertain to managing installations.

Searching for an Installation

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Installations tab (select an Environment, click the Installations tab, type search criteria in the Search Installations box)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc list landscape nodes</td>
</tr>
</tbody>
</table>

Viewing Details about an Installation

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Installations tab (select an Environment, click the Installations tab, select an Installation)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc get landscape nodes</td>
</tr>
<tr>
<td></td>
<td>cc list landscape nodes</td>
</tr>
</tbody>
</table>

Viewing Products Installed in an Installation

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Installation Products tab (select an Environment, click the Installations tab, select an Installation, click the Products tab)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc get inventory products</td>
</tr>
<tr>
<td></td>
<td>cc list inventory products</td>
</tr>
</tbody>
</table>

Viewing Fixes Installed in an Installation

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Installation Fixes tab (select an Environment, click the Installations tab, select an Installation, click the Fixes tab)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc list inventory fixes</td>
</tr>
</tbody>
</table>

Adding an Installation

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Installations tab (select an Environment, click the Installations tab, click the Add Installation button)</td>
</tr>
</tbody>
</table>
### Updating the Properties of an Installation

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line interface</td>
<td>cc create landscape nodes</td>
</tr>
</tbody>
</table>

### Monitoring the Status of Product Instances in an Installation

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Installation Overview tab (select an Environment, click the Installations tab, select an Installation, click the Overview tab)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc update landscape nodes</td>
</tr>
</tbody>
</table>

### Linking an Installation to Multiple Environments

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Installations tab (select an Environment, click the Installations tab, drag an installation to the desired environment)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc add landscape environments nodes</td>
</tr>
</tbody>
</table>

### Creating a Unique ID for an Existing Installation

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Not supported</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc exec landscape nodes generateNodeId</td>
</tr>
</tbody>
</table>

### Removing an Installation from an Environment

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Installations tab (select an Environment, click the Installations tab, select the installation to remove, click the Remove Installations button)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc remove landscape environments nodes</td>
</tr>
</tbody>
</table>
## Working with Instances

This section provides a quick reference to the Command Central tasks that pertain to managing instances.

### Viewing a List of Instances in an Environment

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instances tab (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><code>cc list inventory components</code></td>
</tr>
</tbody>
</table>

### Viewing Details about an Instance

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instances tab (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, select an <strong>Instance</strong>)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><code>cc get monitoring</code> &lt;br&gt;<code>cc get inventory components</code></td>
</tr>
</tbody>
</table>

### Changing the Display Name of an Instance

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instance Overview tab (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, select an <strong>Instance</strong>, click the <strong>Overview</strong> tab, update the <strong>Display Name</strong> field, press Enter)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><code>cc update inventory components</code></td>
</tr>
</tbody>
</table>

### Changing the Icon Representing an Instance

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instance Overview tab (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, select an <strong>Instance</strong>, click the <strong>Overview</strong> tab, click the arrow next to the display name icon in the Details section)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><code>cc list resources icons</code> &lt;br&gt;<code>cc update inventory components</code></td>
</tr>
</tbody>
</table>
### Viewing or Clearing Instance Alerts

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instance Overview tab (select an Environment, click the Instances tab, select an Instance, click the Overview tab, point to the flag in the Alerts area to view alert details, click the number in the Alerts area to clear the alerts)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc list monitoring alerts cc delete monitoring alerts</td>
</tr>
</tbody>
</table>

### Starting an Instance

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instances tab (select an Environment, click the Instances tab, click the Status button next to the instance, select Start)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc exec lifecycle</td>
</tr>
</tbody>
</table>

### Stopping an Instance

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instances tab (select an Environment, click the Instances tab, click the Status button next to the instance, select Stop)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc exec lifecycle</td>
</tr>
</tbody>
</table>

### Restarting an Instance

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instances tab (select an Environment, click the Instances tab, click the Status button next to the instance, select Restart)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc exec lifecycle</td>
</tr>
</tbody>
</table>

### Pausing an Instance

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instances tab (select an Environment, click the Instances tab, click the Status button next to the instance, select Pause)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc exec lifecycle</td>
</tr>
</tbody>
</table>
Resuming an Instance

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instances tab (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, click the <strong>Status</strong> button next to the instance, select <strong>Resume</strong>)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><strong>cc exec lifecycle</strong></td>
</tr>
</tbody>
</table>

Debugging an Instance

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instances tab (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, click the <strong>Status</strong> button next to the instance, select <strong>Debug</strong>)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><strong>cc exec lifecycle</strong></td>
</tr>
</tbody>
</table>

Working with Product Comparisons

This section provides a quick reference to the Command Central tasks that pertain to comparing products in an installation.

Comparing Product Versions

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Compare Products page (select an <strong>Environment</strong>, click the <strong>Installations</strong> tab, select two or more <strong>Installations</strong>, click the <strong>Options</strong> button, select <strong>Compare Products</strong>)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><strong>cc get inventory products compare</strong></td>
</tr>
</tbody>
</table>

Comparing Fix Levels

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Compare Fixes page (select an <strong>Environment</strong>, click the <strong>Installations</strong> tab, select two or more <strong>Installations</strong>, click the <strong>Options</strong> button, select <strong>Compare Fixes</strong>)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><strong>cc get inventory fixes compare</strong></td>
</tr>
</tbody>
</table>
### Comparing Configuration Settings

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Compare Configurations page (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, select two or more <strong>Instances</strong>, click the OPTIONS button, select <strong>Compare Configuration</strong>)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><strong>cc</strong> get configuration compare</td>
</tr>
</tbody>
</table>

### Working with Product Inventory

This section provides a quick reference to the Command Central tasks that pertain to maintaining product inventory.

#### Viewing Component Inventory

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td><strong>Instances</strong> tab (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, click the arrow to the left of an instance name)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><strong>cc</strong> get inventory components</td>
</tr>
<tr>
<td></td>
<td><strong>cc</strong> list inventory components</td>
</tr>
</tbody>
</table>

#### Viewing Product Inventory

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td><strong>Installations</strong> tab (select an <strong>Environment</strong>, click the <strong>Installations</strong> tab, click the arrow to the left of an installation name)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><strong>cc</strong> get inventory products</td>
</tr>
<tr>
<td></td>
<td><strong>cc</strong> list inventory products</td>
</tr>
</tbody>
</table>

#### Viewing Fix Inventory

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td><strong>Installation Fixes</strong> tab (select an <strong>Environment</strong>, click the <strong>Installations</strong> tab, select an <strong>Installation</strong>, click the <strong>Fixes</strong> tab)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><strong>cc</strong> list inventory fixes</td>
</tr>
</tbody>
</table>
Working with SMTP Configuration

This section provides a quick reference to the Command Central tasks that pertain to managing SMTP configuration.

Editing and Testing Common SMTP Settings

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instance Configuration tab (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, select an <strong>Instance</strong>, click the <strong>Configuration</strong> tab, select a component from the list/tabs on the left, select Email from the list at the top of the page, click the <strong>Edit</strong> button)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc get configuration common</td>
</tr>
<tr>
<td></td>
<td>cc list configuration types</td>
</tr>
<tr>
<td></td>
<td>cc get configuration types</td>
</tr>
<tr>
<td></td>
<td>cc list configuration instances</td>
</tr>
<tr>
<td></td>
<td>cc get configuration data</td>
</tr>
<tr>
<td></td>
<td>cc create configuration data</td>
</tr>
<tr>
<td></td>
<td>cc add configuration data</td>
</tr>
<tr>
<td></td>
<td>cc update configuration data</td>
</tr>
<tr>
<td></td>
<td>cc delete configuration instance</td>
</tr>
</tbody>
</table>

Working with Ports

This section provides a quick reference to the Command Central tasks that pertain to managing ports.

Adding a Port

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instance Configuration tab (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, select an <strong>Instance</strong>, click the <strong>Configuration</strong> tab, select a component from the list/tabs on the left, select <strong>Port</strong> from the list at the top of the page, click the <strong>Add Port</strong> button)</td>
</tr>
</tbody>
</table>
### If you are using this interface... | Use these navigation steps or commands...
---|---
Command line interface | cc get configuration types  
cc list configuration types  
cc list configuration instances  
cc get configuration data  
cc create configuration data  
cc add configuration data  
cc update configuration data  
cc delete configuration instance  
cc exec configuration validation

### Enabling or Disabling a Port

| If you are using this interface... | Use these navigation steps or commands... |
---|---|
Web user interface | Instance Configuration tab (select an Environment, click the Instances tab, select an Instance, click the Configuration tab, click the port number, click the Edit button) |
Command line interface | cc get configuration data and then  
cc update configuration data |

### Editing the Configuration of an Existing Port

| If you are using this interface... | Use these navigation steps or commands... |
---|---|
Web user interface | Instance Configuration tab (select an Environment, click the Instances tab, select an Instance, click the Configuration tab, click the port number, click the Edit button) |
Command line interface | cc get configuration data  
cc exec configuration validation update  
cc update configuration data |

### Configuring Ports or Licenses for an Instance

| If you are using this interface... | Use these navigation steps or commands... |
---|---|
Web user interface | Instance Configuration tab (select an Environment, click the Instances tab, select an Instance, click the Configuration tab, select a component from the list on the left, select Ports or Licenses from the list) |
### Viewing Configuration Details for a Port

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instance Configuration tab (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, select an <strong>Instance</strong>, click the <strong>Configuration</strong> tab)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><strong>cc</strong> get configuration common</td>
</tr>
<tr>
<td></td>
<td><strong>cc</strong> get configuration data</td>
</tr>
<tr>
<td></td>
<td><strong>cc</strong> get configuration types</td>
</tr>
<tr>
<td></td>
<td><strong>cc</strong> list configuration types</td>
</tr>
</tbody>
</table>

### Deleting a Port

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instance Configuration tab (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, select an <strong>Instance</strong>, click the <strong>Configuration</strong> tab, select the row of the port you want to delete, click the <strong>Delete Port</strong> button)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><strong>cc exec configuration validation delete and then</strong></td>
</tr>
<tr>
<td></td>
<td><strong>cc delete configuration data</strong></td>
</tr>
</tbody>
</table>

### Working with KPIs

This section provides a quick reference to the Command Central tasks that pertain to working with key performance indicators (KPIs).

#### Viewing KPIs

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Instance Overview tab, Monitoring section (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, select an <strong>Instance</strong>, click the <strong>Overview</strong> tab)</td>
</tr>
</tbody>
</table>
Working with Security Credentials

This section provides a quick reference to the Command Central tasks that pertain to managing security credentials.

Retrieving Security Credentials

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Authentication Mode (select an Environment, click the Instances tab, select an Instance, click the Overview tab, click the Authentication Edit button)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc get security credentials</td>
</tr>
</tbody>
</table>

Adding Security Credentials

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Authentication Mode (select an Environment, click the Instances tab, select an Instance, click the Overview tab, click the Authentication Edit button)</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc add security credentials</td>
</tr>
</tbody>
</table>

Deleting Security Credentials

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Not supported</td>
</tr>
<tr>
<td>Command line interface</td>
<td>cc delete security credentials</td>
</tr>
</tbody>
</table>

Working with Licenses

This section provides a quick reference to the Command Central tasks that pertain to managing product licenses.
### Viewing Details about a License

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Licenses (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, select an <strong>Instance</strong>, click the <strong>Configuration</strong> tab, select <strong>Licenses</strong> from the list at the top of the page, select a license type)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><code>cc get configuration common</code></td>
</tr>
<tr>
<td></td>
<td><code>cc get configuration types</code></td>
</tr>
<tr>
<td></td>
<td><code>cc list configuration types</code></td>
</tr>
<tr>
<td></td>
<td><code>cc get configuration data</code></td>
</tr>
</tbody>
</table>

### Selecting a New License or Changing the Server License Location

<table>
<thead>
<tr>
<th>If you are using this interface...</th>
<th>Use these navigation steps or commands...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Licenses (select an <strong>Environment</strong>, click the <strong>Instances</strong> tab, select an <strong>Instance</strong>, click the <strong>Configuration</strong> tab, select <strong>Licenses</strong> from the list at the top of the page, select a license type, click <strong>Edit</strong>)</td>
</tr>
<tr>
<td>Command line interface</td>
<td><code>cc get configuration data</code></td>
</tr>
<tr>
<td></td>
<td><code>cc exec configuration validation update</code></td>
</tr>
<tr>
<td></td>
<td><code>cc update configuration data</code></td>
</tr>
</tbody>
</table>