webMethods Command Central Help

Version 9.6

April 2014

This document applies to webMethods Command Central Version 9.6 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Document ID: CC-OH-96-20140609

Table of Contents

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

Convention	Description
Bold	Identifies elements on a screen.
Narrowfont	Identifies storage locations for services on webMethods Integration Server, using the convention *folder.subfolder:service* .
UPPERCASE	Identifies keyboard keys. Keys you must press simultaneously are joined with a plus sign (+).
Italic	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.
`Monospace font`	Identifies text you must type or messages displayed by the system.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
|	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the | symbol.
[ ]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

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.

If you want to...	Go to...
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. 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.	**Empower Product Support website** https://empower.softwareag.com
■ Access additional articles, demos, and tutorials.	**Software AG Developer Community for webMethods**

If you want to...	Go to...
■ Obtain technical information, useful resources, and online discussion forums, moderated by Software AG professionals, to help you do more with Software AG technology. ■ Use the online discussion forums to exchange best practices and chat with other experts. ■ Expand your knowledge about product documentation, code samples, articles, online seminars, and tutorials. ■ Link to external websites that discuss open standards and many web technology topics. ■ See how other customers are streamlining their operations with technology from Software AG.	http://communities.softwareag.com/

I Understanding Command Central

1 Command Central Overview

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

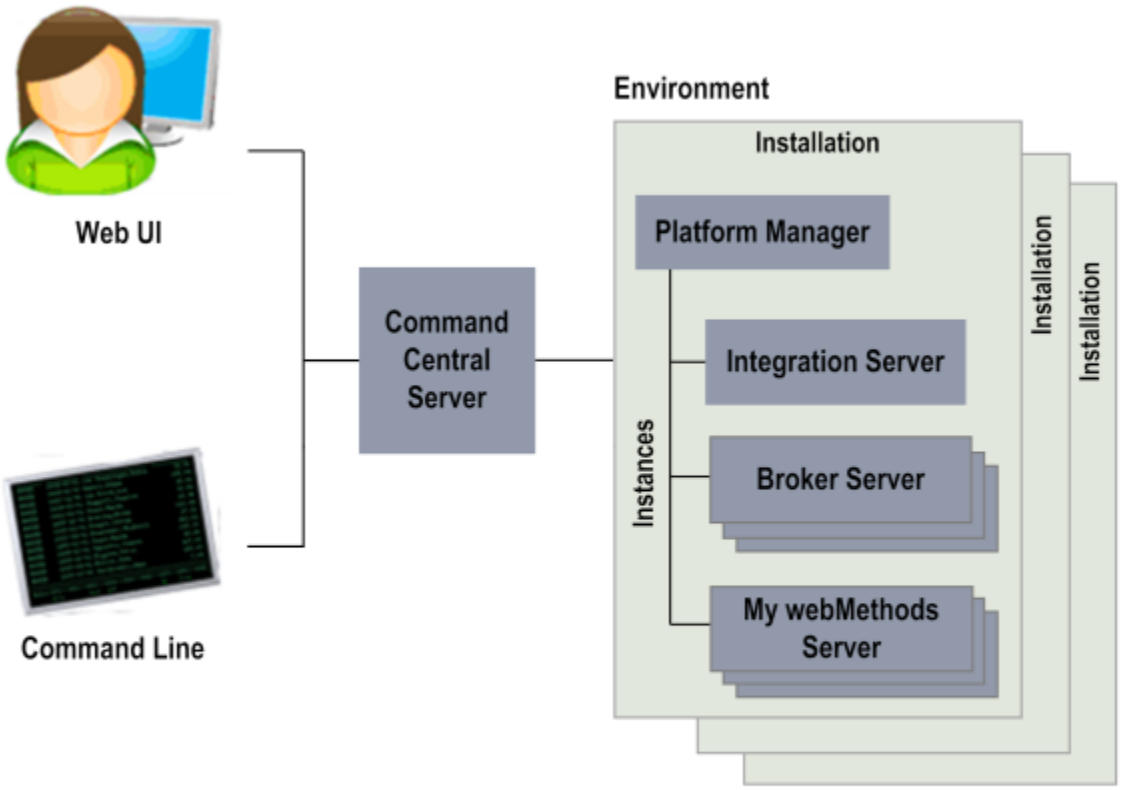
Using Command Central, you can administer hundreds of managed product installations in your IT landscape from a central location. Command Central supports the following operations:

- 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 configuration settings of product instances, such as ports, licenses, and alerts.
- 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 repeat the same set of products, fixes and configuration parameters.
- Create and manage multiple instances of a product in the same installation.

- Secure communication to the Command Central server.

Command Central Architecture

Command Central is built on top of Software AG Common 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

webMethods 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\
- C:\SoftwareAG_test\

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 and Intelligent Business Operations Products*.

Command Central Command Line Tool Upgrade

In all existing Command Central automation scripts and queries that use the Command Central REST API or command line tool commands, change the Integration Server instance ID for all Integration Server instances from:

`runtimeComponent=integrationServer-ENGINE`

to

`runtimeComponent=integrationServer-`*`instanceName`*

where *`instanceName`* is the name of the Integration Server instance, for example `integrationServer-default`.

Template-based Provisioning

With Command Central, you can use templates to install, patch, and configure the webMethods landscape.

You define a template by pointing to an existing managed installation and selecting the products, fixes, and configuration that you want to include in the template. Based on the intended use for the template you define, a template may contain any combination of products, fixes, and configuration available on the source installation. Command Central creates and stores the new template in the Command Central file system. The template contains all the required information about the installed products, the applied fixes, and the available configuration on the source installation. However, a template can contain only fixes or only configuration. For example, when you want to patch a number of existing installations, you can define a template that contains only the fixes you want to apply to each installation. If required, you can use a text editor to modify the template files.

After you create a template from a source instance, you can either apply the template immediately to clone the source installation, or store the template to create one or more instances at a later time. You can apply the template on a target machine that hosts only Platform Manager. When applying the template, Command Central installs the products and applies the fixes and configuration included in the template on the target machine.

When applying a stored template, you select which parts of the template you want to apply. As a result, the set of products, fixes and configuration on the target machine may be different from the set on the source installation. The following table lists some examples of situations when applying only one of the elements available in a template is required:

Apply only...	When...
Products	A different template is used to apply fixes or configuration.
Fixes	The products are already installed on the target machine and you need to apply fixes. In this scenario, you can test the fixes you want to apply in a test environment, create a fix-only template, apply the template to the staging environment where you test the fixes thoroughly, and finally apply the template to the production environment.
Configuration	Templates capture different product instances. For example, use one configuration template for a Platform Manager configuration, a second template for an Integration Server configuration (default instance), and a third template to configure Universal Messaging (default instance). When a template configuration is applied in replace mode, any local configuration changes on the target machine get rolled back to ensures compliance between the configuration on the source and target instances. To preserve the local configuration settings on the target machine, you must apply a template configuration in merge mode. **Important:** The configuration included in a template is limited to the configuration supported by the Command Central product plug-in.

To install the products and apply the fixes from the template, Command Central accesses a public product or fix repository that is registered with Command Central. For example, to install products from the Empower website, you must register the Empower website as a product repository with Command Central. When applying a template that contains products, Command Central will access the Empower website to install the relevant products. You can register two types of repositories with Command Central:

- **Master repository:** a remote product repository, for example the Empower website
- **Image repository:** an image file that contains products or fixes

To manage templates and repositories, you can use either the Command Central web user interface or the command line interface. For more information, see "Provisioning Using Templates" on page 123 and *webMethods Command Central and webMethods Platform Manager Command Reference*

Instance Management of Installed Products

Command Central allows you to create, update, and delete an instance of an installed product that supports multiple instances under the same installation directory. For example, you can create an instance of Integration Server with a different configuration or a different set of packages from an existing Integration Server installed in the same directory. You cannot change the name of an existing product instance, but you can update other configuration parameters provided when creating the instance. For example, you can update the list of recently installed packages for an Integration Server instance. You can also delete an installed product instance.

To manage instances of installed products, use the Command Central command line interface. For more information about how to use commands to manage product instances, see *webMethods Command Central and webMethods Platform Manager Command Reference*.

Command Central Terminology

The following table defines common Command Central terms.

Term	Description
Component	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.
Environment	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.
Installation	A set of Software AG products and fixes installed in the same installation directory.
Instance	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.

Term	Description
	For example, Broker Server and My webMethods Server are instances.
Landscape	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.
Platform Manager	An architectural component of Command Central that provides a common remote management interface to a Software AG product installation.
Software AG Common Platform	A Java run-time environment based on the OSGi framework. It provides a standard platform on which to run Software AG products and the enterprise applications that you develop around those products. Software AG Common Platform hosts Software AG products such as Integration Server, My webMethods Server, and Command Central. Common Platform does not host native applications such as Broker Server and Universal Messaging.

Getting Started

Perform these initial tasks to set up 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.

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

- Configure ports in the OSGi profiles
- 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

2 Using the Command Central Web User Interface

Accessing Command Central

After you install webMethods Command Central using Software AG Installer, Platform Manager starts automatically as a service in the port you configured during installation. You start Command Central by starting the Windows service for Command Central. You can access the Command Central web user interface from all supported web browsers.

For information about how to install and configure Command Central, see *Installing webMethods and Intelligent Business Operations 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 Command Central.

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

Manually Starting and Stopping Command Central and Platform Manager on Windows

You can start Command Central or Platform Manager by starting the Windows service for Command Central or Platform Manager.

To shut down the Command Central or Platform Manager servers, stop the Windows service for Command Central or Platform Manager.

Manually Starting and Stopping Command Central and Platform Manager on Unix

To start Command Central or Platform Manager, execute the startup .sh script located in the following directories:

- For Command Central: *Software AG_directory*/profiles/CCE/bin
- For Platform Manager: *Software AG_directory*/profiles/SPM/bin

To shut down the Command Central or Platform Manager servers, execute the shutdown .sh script located in the following directories:

- For Command Central: *Software AG_directory*/profiles/CCE/bin
- For Platform Manager: *Software AG_directory*/profiles/SPM/bin

Troubleshooting Command Central and Platform Manager

Use the console.bat|sh script to troubleshoot Command Central or Platform Manager. The console.bat|sh script is located in the following directories:

- For Command Central: *Software AG_directory*\profiles\CCE\bin
- For Platform Manager: *Software AG_directory*\profiles\SPM\bin

The server logs are located in the following directories:

- For Command Central: *Software AG_directory*\profiles\CCE\logs
- For Platform Manager: *Software AG_directory*\profiles\SPM\logs

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.

Icon/Field	Description
	Type the filter criteria for searching the environments in the **Search Environments** field. The **Environments** pane lists only those environments with names that match the search criteria.

Icon/Field	Description
	Click  **Clear Filter** to clear the search filter and display all the environments.
All	Click **All** to view all the installations defined in Command Central. This is the default environment. This environment contains all the installations that can be administered by Command Central. The **All** environment includes all the installations grouped under other environments, as well as the installations that are not grouped under any environment.
	Click  **Add Environment** to add a new environment for administration through Command Central.
	Click  **Remove Environment** to remove the selected environment from Command Central administration.
	Click  **Edit Environment** to edit the details of the selected environment.

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.

Icon/Field	Description
	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.
	Click  **Clear Filter** to clear the search filter and list all the instances belonging to the selected installation.
	Click  **Compare Configuration** to select and compare the configurations of multiple instances.

Icon/Field	Description
	Click  to query the Platform Manager and refresh the changes made to the instances.
Name [Count]	Display name of the instance and the total number of child instances. Expand the instance node to view the list of child instances.
Component	Component name or the product code.
Status	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.
Alerts	Displays an alert flag if there is any alert for the component.
Installation	Name of the installation where the instance is installed.
Host	Name of the host used by the instance.

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.

Field	Description
Status	Current status of the instance or component. For more information, see Viewing the Status of an Instance or Its Components.
Alerts	Number of alerts. For more information, see Viewing Alerts for an Instance or Its Components.
Monitoring	Key performance indicators. For more information, see About Monitoring KPIs.

View Details of Instances

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

Field	Description
Display Name	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.
Component	Name of the component.
Host Name	Name of the host machine where the instance or component is installed.
Authentication	Authentication mode for administering the instance. The default is Fixed user. Click  to edit the user name and password for fixed user authentication.
Installation Name	Name of the installation where the instance or component is installed.

Field	Description
Installation Alias	Alias name of the installation where the instance or component is installed.

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.

Icon/Field	Description
	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.
	Click  **Clear Filter** to clear the search filter and list all the installations of the selected environment.
	Click  **Add Installation** 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 **All** environment.
	Click  **Remove Installation** to remove the selected installation from the specified environment. The removed installation will be listed under **All** environment. If you do not want an installation to be administered by Command Central, you must explicitly remove it from the **All** environment.

Icon/Field	Description
	Click  to select these options: ■ **Compare Products** ■ **Compare Fixes**
	Click  to query the Platform Manager and refresh the changes made to the installations.
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.
Host	Name of the host used by the installation node.
Port	Port number used by the installation node.
Code	Product code of the product in the installation node. Expand the installation node to view the list of products installed in the installation node.
Version	Version number of the Platform Manager or the product.

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.

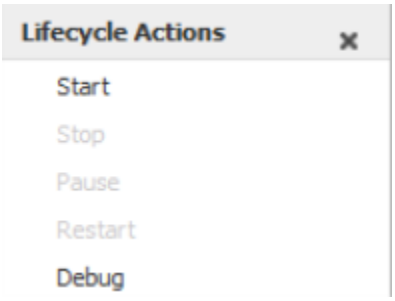
You can specify either **Delegated** authentication or **Fixed User** authentication for administering the products managed by a Platform Manager.

- 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.



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.

Icon	Status	Indicates
	Online	Command Central is able to connect to the installation host and port.
	Offline	Command Central cannot connect to the installation host and port.

Instance Status Icons

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

Icon	Status	Indicates...
	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.

Icon	Status	Indicates...
	Paused	The instance or instance component has paused.
	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.

Alerts Icons

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

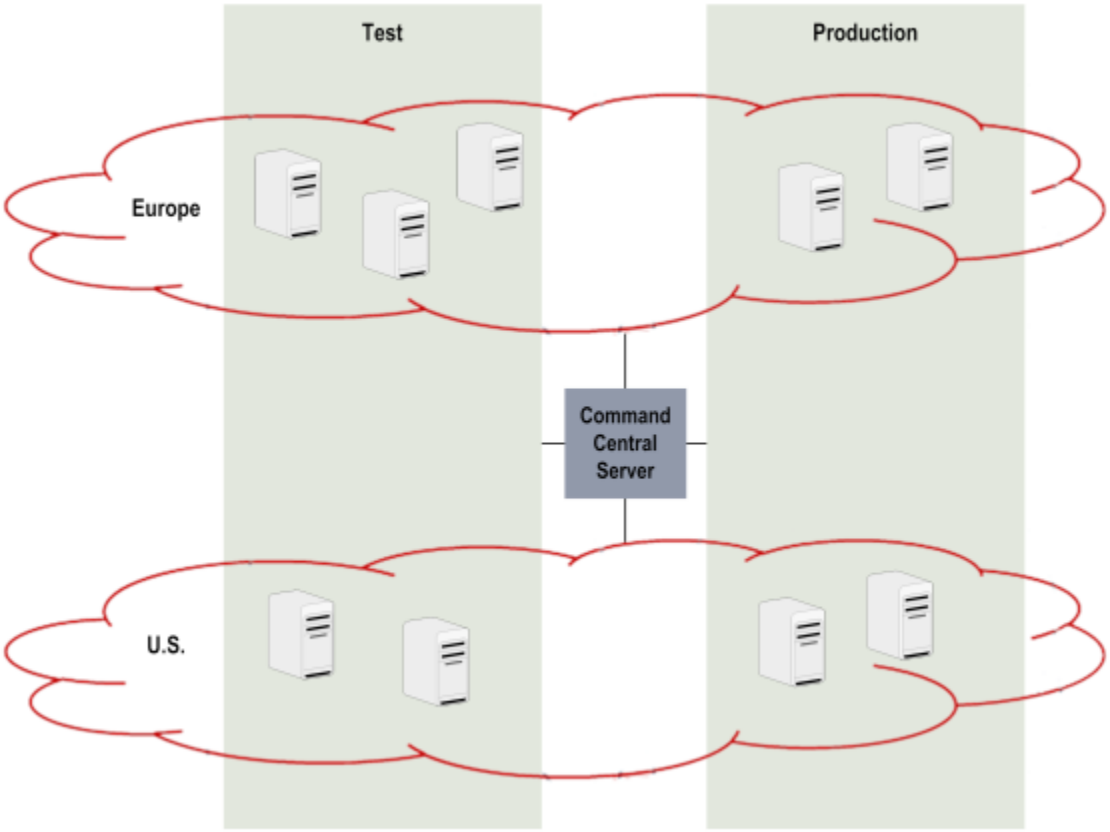
- The status of an instance or instance component changes.
- The value of a KPI (key performance indicator) changes.

Icon	Indicates
	Instance warning or error.
	Instance information.

3 Administering Environments

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.

In this field...	Specify...
Display Name	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.
Alias	A unique name for the environment. After you create an environment, you cannot edit the alias.
Description	A description for the environment.

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.

4 Administering Installations

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:

Field...	Specify...
Display Name	A name for the installation. The value of this field is automatically assigned to **Alias**. More than one installation can have the same **Display Name**.
Host Name	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 `localhost` as the host name, specify `mcdev001.us.ad.gov` or `12.23.0.1`.
Port Number	The port number used by Platform Manager of the installation.
Use SSL	Whether the installation requires HTTP or HTTPS authentication. Select **Is Secure** to specify HTTPS.
Alias	A unique name for the installation. No other installation in any of the environments can use this name.

Field...	Specify...
Description	A description of the installation. This description is displayed in the Overview tab of the installation.

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  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 109.

   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

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.

Setting Up the Administrator User Password for Command Central

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

To set up secure communication with Command Central

1. Change the default Command Central administrator password for the internal user repository in the users.txt file as follows:

   a. In the Command Central Command Line tool, run the internaluserrepo script using the following syntax: `*CommandCentral_directory*/common/bin/internaluserrepo[.bat|.sh] -f ../../profiles/CCE/configuration/security/ users.txt -p *newPassword* Administrator`

   b. To verify that the password change is successful, close all currently open browser windows, open the Command Central web user interface in a new browser window, and log on with the new password.

2. Update the cached security credentials for the Command Central profile:

   a. In the local installation in Command Central, go to **CCE > Overview > Details**.

   b. In the **Authentication** field, click  .

   c. Select **Fixed User** and enter `Administrator` as the user name and the new password.

   To verify the new credentials, click  and check the monitoring KPIs for the CCE component.

3. Update the Command Central Command Line tool configuration file:

   a. Execute a command, for example, `cc list landscape nodes`. The command returns ERROR 401.

   b. In a text editor, open the $HOME/.sag/cc.properties file and specify the new password in the `password` property.

   To verify the new credentials, execute the same command again, for example `cc list landscape nodes`. The command executes successfully.

4. Make sure that all nodes are online.

Using a Unix Shell Script to Change the Administrator Password for Command Central

You can use the following sample Unix shell script to change the Administrator user password for Command Central:

```
NODE_ALIAS=local   USERNAME=Administrator   PASSWORD=secret123
cc get configuration data $NODE_ALIAS OSGI-CCE-ENGINE SIN-INTERNAL-USERS
  -users.txt -o cce_users.txt   cc get security credentials nodeAlias=
$NODE_ALIAS runtimeComponentId  =OSGI-CCE -o cce_creds.xml
  $INSTALL_DIR/common/bin/internaluserrepo.sh -f cce_users.txt -
p $PASSWORD $USERNAME   sed "s,<password></password>,<password>
${PASSWORD}</password>,  g" cce_creds.xml > cce_creds_new.xml
cc update configuration data $NODE_ALIAS OSGI-CCE-ENGINE SIN-INTERNAL-USERS
  -users.txt -i cce_users.txt   cc add security credentials nodeAlias=
$NODE_ALIAS runtimeComponentId  =OSGI-CCE -i cce_creds_new.xml
  cc get landscape nodes -c 5 -w 30 -u $USERNAME -p $PASSWORD
sed "s,^password=.*$,password=${PASSWORD},g" $HOME/.sag/cc.properties >
  cc.properties   cp cc.properties $HOME/.sag/cc.properties
cc get landscape nodes
```

Setting Up the Administrator User Password for all Platform Managers

After installing Platform Manager, Software AG recommends you change the default Platform Manager administrator password for the internal user repository in the users.txt file.

You can specify a different password for each installed Platform Manager. The password you specify for Platform Manager can differ from the Command Central password.

To set up secure communication with Platform Manager

1. In the Command Central Command Line tool, run the internaluserrepo script using the following syntax:

   ```
   PlatformManager_directory /common/bin/internaluserrepo[.bat|.sh]
   -f ../../profiles/SPM/configuration/security/users.txt
   -p newPassword Administrator
   ```

2. Update connection security credentials for the Platform Manager node:

   a. In the local installation in Command Central, go to **SPM > Overview > Details**.

   Note: If Platform Manager is not successfully registered with Command Central or does not connect to Command Central because of wrong credentials, go to **Installations > Overview**.

b. Click  .

Platform Manager returns ERROR 401.

c. In the **Authentication** field, click  .

d. Select **Fixed User** and enter `Administrator` as the user name and the new password.

To verify the new credentials, click  and check the monitoring KPIs for the SPM component.

Using a Unix Shell Script to Change the Administrator Password for Platform Manager

You can use the following sample Unix shell script to change the Administrator user password for Platform Manager:

```
NODE_ALIAS=local
USERNAME=Administrator
PASSWORD=secret456

cc get configuration data $NODE_ALIAS OSGI-SPM-ENGINE SIN-INTERNAL-USERS
-users.txt -o spm_users.txt
cc get security credentials nodeAlias=$NODE_ALIAS runtimeComponentId=
OSGI-SPM -o spm_creds.xml

$INSTALL_DIR/common/bin/internaluserrepo.sh -f spm_users.txt
-p $PASSWORD $USERNAME
sed "s,<password></password>,<password>${PASSWORD}</password>,
g" spm_creds.xml > spm_creds_new.xml

cc update configuration data $NODE_ALIAS OSGI-SPM-ENGINE SIN-INTERNAL-USERS
-users.txt -i spm_users.txt
cc add security credentials nodeAlias=$NODE_ALIAS runtimeComponentId
=OSGI-SPM -i spm_creds_new.xml

cc get landscape nodes $NODE_ALIAS -e ONLINE -c 5 -w 60
cc list inventory components nodeAlias=$NODE_ALIAS refresh=true
```

Setting Outbound Authentication

As part of its normal operations, Command Central connects to applications and subsystems such as Integration Servers, Brokers, and My webMethods Server. Command Central, acting as a client, is required to supply basic authentication credentials, such as user name and password, to each of these systems before connecting to them. Command Central uses the basic credentials to identify itself or *authenticate to* the other systems.

When you configure Command Central to connect to a managed runtime, you specify the user name and password Command Central must send to the managed runtime to connect to it. Later, when a Command Central user makes a request that requires

the managed runtime, Command Central sends the configured basic authentication credentials to the managed runtime and connects to it.

Outbound authentication does not authorize access to resources.

To configure basic authentication for a product, managed by Command Central, you must use the product user interface to change the Administrator password for the product.

- For Integration Server, use the Integration Server Administrator user interface to change the Administrator password or create a new user who is a member of the Administrator group on the server instance. For more information, see *webMethods Integration Server Administrator's Guide*.
- For My webMethods Server, change the Administrator and sysadmin passwords using the My webMethods Server user interface. For more information, see *Administering My webMethods Server*.
- For CentraSite, Software AG Runtime, and the Infrastructure Data Collector, change the Administrator user password in the *Software AG_directory*/common/conf/users.txt file using the internaluserrepo script. For more information about how to use the internauserrepo script, see "internaluserrepo Script" on page 85.

In Command Central, use the following steps to update the Administrator user password for a product component with the new password:

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

To update the Administrator user password for managed products

1. In the Environments pane, select the environment that contains the product instance.
2. In the Instances table, select the instance of the product component for which you want to change the user credentials, as follows:
   - For Integration Server, select IS_*instancename* , for example IS_default, and its child Integration Server component.
   - For My webMethods Server, select MWS_*instancename* , for example MWS_default, and the My webMethods Server component.
   - For Software AG Runtime, select the CTP component.
   - For Infrastructure Data Collector, select the InfraDC component.
3. On the **Overview** tab, in the Details pane, click  in the **Authentication** field.
4. Enter the new **User Name** and **Password**.

Note: Command Central cannot manage a Broker Server or Universal Messaging Server that has authentication enabled. If you want to manage a Broker Server or Universal Messaging Server using Command Central, you must disable their authentication feature.

Using Unix Shell Scripts to Change Connection Credentials for Managed Products

You can use the following sample Unix shell scripts to configure basic authentication credentials for product components managed by Command Central.

Integration Server

```
NODE_ALIAS=prodis*
USERNAME=Administrator
PASSWORD=secret890

cc get security credentials nodeAlias=$NODE_ALIAS runtimeComponentId
=OSGI-IS* -o prod_creds.xml
sed "s,<password></password>,<password>${PASSWORD}</password>,
g" prod_creds.xml > prod_creds_new.xml

cc add security credentials nodeAlias=$NODE_ALIAS runtimeComponentId
=OSGI-IS* -i prod_creds_new.xml
cc add security credentials nodeAlias=$NODE_ALIAS runtimeComponentId
=integrationServer* -i prod_creds_new.xml

# verification for 'default' instance
cc get monitoring runtimestatus $NODE_ALIAS OSGI-IS_default -e ONLINE
cc get monitoring runtimestatus $NODE_ALIAS integrationServer-default -e ONLINE
```

My webMethods Server

```
NODE_ALIAS=qa
USERNAME=Administrator
PASSWORD=secret890

cc get security credentials nodeAlias=$NODE_ALIAS runtimeComponentId
=OSGI-MWS* -o prod_creds.xml
sed "s,<password></password>,<password>${PASSWORD}</password>,
g" prod_creds.xml > prod_creds_new.xml

cc add security credentials nodeAlias=$NODE_ALIAS runtimeComponentId
=OSGI-MWS* -i prod_creds_new.xml
cc add security credentials nodeAlias=$NODE_ALIAS runtimeComponentId
=MwsProgramFiles* -i prod_creds_new.xml

# verification for 'default' instance
cc get monitoring runtimestatus $NODE_ALIAS OSGI-MWS_default -e ONLINE
cc get monitoring runtimestatus $NODE_ALIAS MwsProgramFiles-default -e ONLINE
```

CentraSite, Software AG Runtime, and Infrastructure Data Collector

```
NODE_ALIAS=qa
USERNAME=Administrator
PASSWORD=secret890

cc get configuration data $NODE_ALIAS OSGI-SPM-ENGINE SIN-INTERNAL-USERS
-common-users.txt -o common_users.txt
cc get security credentials nodeAlias=$NODE_ALIAS runtimeComponentId
=OSGI-* -o prod_creds.xml

$INSTALL_DIR/common/bin/internaluserrepo.sh -f common_users.txt
-p $PASSWORD $USERNAME
```

```
sed "s,<password></password>,<password>${PASSWORD}</password>,
g" prod_creds.xml > prod_creds_new.xml

cc update configuration data $NODE_ALIAS OSGI-SPM-ENGINE SIN-INTERNAL-USERS
-common-users.txt -i common_users.txt
cc add security credentials nodeAlias=$NODE_ALIAS runtimeComponentId
=OSGI-CTP -i prod_creds_new.xml
cc add security credentials nodeAlias=$NODE_ALIAS runtimeComponentId
=OSGI-InfraDC -i prod_creds_new.xml

# verification for CTP and InfraDC profiles
cc get monitoring runtimestatus $NODE_ALIAS OSGI-CTP -e ONLINE
cc get monitoring runtimestatus $NODE_ALIAS OSGI-InfraDC -e ONLINE
```

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.

Product	Alias	Port Type	Default Port Assignment
Command Central	defaultHttp	HTTP	8090

Product	Alias	Port Type	Default Port Assignment
	defaultHttps	HTTPS	8091
Platform Manager	defaultHttp	HTTP	8092
	defaultHttps	HTTPS	8093

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 187.

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

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:

To	Click
Add new data	
Edit data	
Test whether data is added or edited successfully. For example, you can test new configuration data to perform a field-level validation before you save the configuration data.	**Test**

7. Click **Save** to save the configuration data.

Testing a Configuration

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

When you test 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 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 typically 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.

Prerequisites to Configuring a Port for SSL

Command Central provides a default keystore and truststore that are available after installing Command Central. The keystore and truststore are files that function as repositories for storage of keys and certificates necessary for Secure Socket Layer (SSL) authentication, encryption/decryption, and digital signing/verification services. The default keystore and truststore contain signed certification authority (CA) certificates that the Command Central server uses to validate client certificates.

You can replace the Command Central default keystore and truststore files with custom files. For information about creating keystores and truststores, importing keys and certificates into keystores and truststores, and other operations with these files, refer to the documentation for your certificate management tool."

Before configuring an HTTPS port, you must configure the Command Central server to use SSL, using the Command Line tool. For more information about securing communication with the Command Central server, see *webMethods Command Central and webMethods Platform Manager Command Reference*.

7 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.

Use this port type...	To...
HTTP	Submit unsecured requests to the OSGi component.
HTTPS	Submit requests to the OSGi component using SSL encryption.

JMX	Allow administration and monitoring the JVM KPIs of the OSGi component.
	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.
	`<Values version="2.0">`
	`<value name="subsystem">true</value>`
	`</Values>`
	JMX port might be bound to a localhost.

SSH	Allow secure shell for the OSGi component.
JDWP	Allow OSGi component debugging by using the Java debug protocol over a TCP connection.

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.

Product	Product Code	Ports Enabled by Default
Command Central	CCE	JMX, HTTP, HTTPS
Integration Server	IS	JMX
My webMethods Server	MWS_*mwsinstancename* For example, MWS_default	JMX
Platform Manager	SPM	JMX, HTTP, HTTPS
Software AG Runtime	CTP	JMX, HTTP, HTTPS

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.

Note: 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 131. For more information about configuring a My webMethods Server instance, see "Configuring My webMethods Server Ports" on page 163 and "Configuring My webMethods Server Email" on page 165.

Port Authentication

The following table describes which user store products with OSGi profiles use to authenticate enabled ports.

Product	Product Code	Authenticates against user store in...	For...
Command Central	CCE	*Software AG_directory*\profiles\CCE\configuration\security\users.txt	All ports

Product	Product Code	Authenticates against user store in...	For...
Platform Manager	SPM	*Software AG_directory*\profiles\SPM\configuration\security\users.txt	All ports
Software AG Runtime	CTP	*Software AG_directory*\common\conf\users.txt	All ports
Infrastructure Data Collector	InfraDC	*Software AG_directory*\common\conf\users.txt	All ports
My webMethods Server	MWS_*instancename* For example, MWS_default	*Software AG_directory*\common\conf\users.txt	JMX and SSH
		user store managed by My webMethods Server	HTTP, HTTPS, AJP13
Integration Server	IS_*instancename* For example, IS_default	user store managed by Integration Server	All ports

Integration Server can open JMX port using a setting in the *Integration Server_directory*\instances*instance_name*\bin\setenv.bat file, where *instance_name* is the name of the Integration Server instance. 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:

Field	Description
Enabled	Whether the port is enabled.
Port Number	The number you want to use for the port. Select a number that is not already in use.
Alias	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 (-).
Keep Alive Timeout	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.
Spare Threads Min	The starting number of request processing spare threads.
Redirect Port	The port to use when redirecting a SSL connection requests.
Spare Threads Max	The maximum number of request processing spare threads.

Field	Description
Accept Count	The maximum number of simultaneous connection requests allowed in the connection queue.
Connection Timeout	The connection timeout in milliseconds. This attribute is not set by default on HTTPS ports.
HTTP Header Size Max	The maximum incoming URL length in characters.
Upload Timeout Disable	Indicates if using a longer connection timeout is allowed when waiting for the servlet container to update. ■ **Yes.** Allow longer connection time-outs while waiting for the servlet container. ■ **No.** Do not allow longer connection time-outs.
Lookups Enable	Indicates if DNS lookups are allowed to get the actual host name of a remote client. ■ **Yes.** DNS lookups allowed. ■ **No.** DNS lookups not allowed.
Key Manager Algorithm	For HTTPS port configurations. The certificate encoding algorithm.
SSL Protocol	For HTTPS port configurations. The version of the secure socket layer (SSL) protocol to use; when not specified Transport Layer Security ((TLS) is used.

- For JMX and SSH port configurations:

Field	Description
Enabled	Whether the port is enabled.
Port Number	The number you want to use for the port. Select a number that is not already in use. ■ For JMX, select the port for monitoring, managing, and implementing the Java process. ■ For SSH, select the port for remote shell services or execution processes.

Field	Description
Alias	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 (-).
JAAS Realm	For JMX and SSH port configurations. Specifies the realm name that authenticates the Java Authentication and Authorization (JAAS) service.

- For JDWP port configurations:

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

Field	Description
Port Number	The number you want to use for the port. Select a number that is not already in use.
Alias	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 (-).
Suspend	For JDWP port configurations. Select Yes if the runtime should be suspended until debugger connects.

6. In Threadpool Configuration, for HTTP and HTTPS ports, complete the following fields.

Field	Description
Enabled	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.

Field	Description
	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**.
Threadpool Min	The minimum number of threads for this private thread pool. The default is 1.
Threadpool Max	The maximum number of threads for this private thread pool. The default is 5.
Threadpool priority	The Java thread priority. The default is 5. **Important:** Use this setting with extreme care because it will affect server performance and throughput.

7. For secure connections, complete the security fields as follows:

Field	Description
SSL Enabled	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**.
Keystore Type	Select the keystore type.The keystore must contain the private key for secure communication.
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.

Field	Description
Server Location of Truststore	Specify the directory where the truststore file is located.
Password	Specify the password to open the truststore file.

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.
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.

8 The Java Service Wrapper

Command Central and Platform Manager run on the Software AG Common Platform, which in turn runs in a Java Virtual Machine (JVM). The Java Service Wrapper is an application developed by Tanuki Software, Ltd.. It is a utility program that launches the JVM in which Command Central and Platform Manager run.

In addition to launching the JVM, the Java Service Wrapper offers features for monitoring the JVM, logging console output, and generating thread dumps. The following sections describe how Command Central and Platform Manager use the features of the Java Service Wrapper. For an overview of the Java Service Wrapper, see the webMethods cross-product document, *Working with the webMethods Product Suite and the Java Service Wrapper*.

The Java Service Wrapper Configuration Files

For Command Central and Platform Manager, the configuration files for the Java Service Wrapper reside in the following directory:

- Command Central

  Software AG_directory/profiles/CCE/configuration

- Platform Manager

  Software AG_directory/profiles/SPM/configuration

When you start Command Central and Platform Manager, property settings in the following files determine the configuration of the JVM and the behavior of the logging and monitoring features of the Java Service Wrapper.

File name	Description
wrapper.conf	Contains property settings that are installed by Command Central and Platform Manager. *Do not modify the contents of this file unless asked to do so by Software AG.*
custom_wrapper.conf	Contains properties that modify the installed settings in wrapper.conf. If you need to modify the property settings for the Java Service Wrapper, you make your changes in this file.

The following sections describe configuration changes that Command Central and Platform Manager support for the Java Service Wrapper. Unless directed to do so by Software AG, do not make any configuration changes to the Java Service Wrapper other than the ones described here.

JVM Configuration

When the Java Service Wrapper launches the JVM, it provides configuration settings that, among other things, specify the size of the Java heap, the size of the PermGen area, and the directories in the classpath.

JVM Configuration Properties

The `wrapper.java` properties in the Java Service Wrapper configuration files determine the configuration of the JVM in which Command Central and Platform Manager run.

The JVM property settings that Command Central and Platform Manager install are suitable for most environments. For additional information about the JVM property settings, see the webMethods cross-product document, *Working with the webMethods Product Suite and the Java Service Wrapper*.

Property	Value
`wrapper.java.initmemory`	Initial size (in MB) of the Java heap. The default is `32`.
`wrapper.java.maxmemory`	Maximum size (in MB) to which the Java heap can grow. The default is `128`.
`wrapper.java.classpath.`*n*	Directory in the classpath.
`wrapper.java.additional.`*n*	Java option to be passed in on the command line.

The Wrapper Log File

The Java Service Wrapper records console output in a log file. The log contains the output sent to the console by the wrapper itself and by the JVM in which Command Central and Platform Manager are running. The wrapper log is especially useful when you run Command Central and Platform Manager as a Windows service, because console output is normally not available to you in this mode.

The Java Service Wrapper log is located in the following file:

- Command Central

  Software AG_directory\profiles\CCE\logs\wrapper.log

- Platform Manager

  Software AG_directory\profiles\SPM\logs\wrapper.log

To view the log, simply open the log file in a text editor.

Logging Properties

The `wrapper.console` and `wrapper.log` properties in the wrapper configuration files determine the content, format, and behavior of the wrapper log.

The logging settings that Command Central and Platform Manager install are suitable for most environments. However, you can modify the following properties if the installed settings do not suit your needs. For procedures and additional information, see the webMethods cross-product document, *Working with the webMethods Product Suite and the Java Service Wrapper*.

Property	Value
`wrapper.logfile.maxsize`	Maximum size to which the log can grow.
`wrapper.logfile.maxfiles`	Number of old logs to maintain.
`wrapper.syslog.loglevel`	Level of messages to write to the Event Log on Windows systems or the syslog on UNIX.

Fault Monitoring

The Java Service Wrapper can monitor the JVM for the certain conditions and then restart the JVM or perform other actions when it detects these conditions.

The following table describes the fault-monitoring features Command Central and Platform Manager use or allow you to configure. To learn more about these features, see the webMethods cross-product document, *Working with the webMethods Product Suite and the Java Service Wrapper*.

Feature	Enabled	User configurable
JVM timeout	Yes	No. Do not change the installed settings unless asked to do so by Software AG.
Deadlock detection	Yes	No. Do not change the installed settings unless asked to do so by Software AG.

Feature	Enabled	User configurable
Console filtering	No	No. Do not enable this feature.

Generating a Thread Dump

The Java Service Wrapper provides a utility for generating a thread dump of the JVM when Command Central and Platform Manager are running as Windows services. A thread dump can help you locate thread contention issues that can cause thread blocks or deadlocks.

For information about generating a thread dump using the Java Service Wrapper, see the webMethods cross-product document, *Working with the webMethods Product Suite and the Java Service Wrapper*.

9 Managing Command Central Licenses and Product License Reports

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**. Command Central displays the available licenses, their status, and expiration date.
6. In the License Type column, click **Command Central**. 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**. Command Central displays the available licenses, their status, and expiration date.
6. In the License Type column, click **Command Central**. The license key location and details appear.
7. In the **Command Central License** page, click **Edit**.
8. Click **Browse** in the **License Upload File** 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 Product License Reports

You can use Command Central to find out how many instances of webMethods products you have installed and monitor your license compliance. Command Central monitors a whole landscape and generates a license report snapshot of the current state of the landscape. The report contains information about all installed product instances and groups them based on license key. The report also counts the server cores and compares their total with the number of license keys. The summary section of the report shows whether the customer landscape is compliant with the available licenses. You can generate the report in XML, PDF, or JSON format, using either the Command Central web user interface or the command line tool.

Creating a License Report Snapshot

Use the following procedure to create a license report snapshot of a landscape.

To create a license report snapshot

1. In Command Central, go to **Views > Licenses**.
2. Click  .

Command Central creates the license report snapshot and lists the report in the License Reports table.

Viewing Details About License Reports

You view the details about a license report on the License Reports page in Command Central. Each license report is identified by a report ID that Command Central assigns automatically when creating the license report snapshot. You can use the report ID to search for a specific report. The License Keys and Server columns provide information about the number of licenses and server cores available in a landscape. The Status column presents the compliance status of a landscape. Valid values are:

- **OK** The landscape is complaint with the available licenses.
- **Capacity Exceeded** The number of server cores exceeds the available licenses.

You can also view information about when and who created the license report.

Sorting License Reports

You can sort the items in each column of the License Reports table by pointing your mouse to the column label and selecting the sorting option you require from the list.

Downloading License Reports

You must download a license report and save it on the file system to be able to view its detailed contents.

To download a license report

1. In Command Central, go to **Views > Licenses**.
2. From the License Reports table, select the license report you want to download.
3. In the Download column, click and select the format in which you want to download the report. Valid formats are: PDF, XML, and JSON.

Command Central downloads and saves the license report file to *Software AG_directory*\profiles\CCE\data\reports\license-tools or a location on the client file system that you specify.

Deleting License Reports

Use the following procedure to delete a license report snapshot of a landscape.

To delete a license report snapshot

1. In Command Central, go to **Views > Licenses**.
2. From the License Reports table, select the license report you want to delete.

3. Click  .

Command Central deletes the license report snapshot. The report is no longer available in the License Reports table.

10 Managing Users, Groups, and Roles

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 95.

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 96.

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 88.

Using Internally Defined User and Group Information

Command Central can authenticate users against information in the Command Central or Platform Manager internal user repositories, using the users.txt file located in the following directories:

- For Command Central: *Software AG_directory*\profiles\CCE\configuration\security
- For Platform Manager: *Software AG_directory*\profiles\SPM\configuration\security

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 following directories:

- For Command Central: *Software AG_directory*\profiles\CCE\configuration\security
- For Platform Manager: *Software AG_directory*\profiles\SPM\configuration\security

For more information, see "Groups" on page 95 and "Roles" on page 96.

Note: Immediately after logging on to Command Central for the first time, the administrator should change the default administrator password. For more information see "Setting Up the Administrator User Password for Command Central " on page 50.

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:

- "Setting Up the Administrator User Password for Command Central " on page 50
- "Adding Users to the Internal User Repository" on page 87
- "Deleting Users from the Internal User Repository" on page 88

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 86.

Arguments

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

Argument/Parameter	Description
userId	Required. Creates a new user when the users.txt file exists in the *Software AG_directory*\profiles\CCE |SPM \configuration\security directory. The specified user ID is added to the file and the `internaluserrepo` 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 *userID*.

Argument/Parameter	Description
	The following are valid characters for a user ID: `[a-z] [A-Z] [0-9] !()-.?[]@_~`
`[-f filename]`	Optional. Specifies the location and file name followed by the URL, or the path and name of the file to create.
`[-c]`	Optional. Creates a users.txt file in the directory where the command is executed when no other options are used.
`[-p password]`	Optional. Specifies the password. You can use up to 128 characters for the password. The following are valid characters for a password: `[a-z] [A-Z] [0-9] !()-.?[]@_~`
`[-d]`	Optional. Specifies the user to delete from the users.txt file.
`[-e]`	Optional. Checks whether a specified user exists in the users.txt file. When using option -e, you must also specify the file name and the file's URL using option -f.

internaluserrepo Exit Codes

The following table describes the exit codes you might encounter when using the `internaluserrepo.bat/sh` script.

Exit Code	Description
`-1`	The user ID specified with the -e option does not exist in the users.txt file.
`1`	The password is not set.
`2`	The user ID is too long.
`3`	The user ID contains invalid characters.
`4`	The password contains invalid characters.

Exit Code	Description
5	The password is too long.
6	The internal user repository contains multiple versions of the users.txt file.
7	An invalid version of the configuration file exists in the repository. Supported versions are 2.0 and above.
8	One of the following has occurred: ■ The file name is not specified in the command and the default file cannot be located. ■ The file specified cannot be located. Make sure you have entered the correct path and file name.
9	The `internaluserrepo` script cannot open or create the users.txt file.
10	The user ID is missing.
11	The command includes conflicting arguments or invalid parameters.

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 ../security/users.txt -c -p password userId
   ```

   For example, to add user Administrator1 with a password of manage1, enter:

   ```
   internaluserrepo.bat -f ../security/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 ../security/users.txt -d userId
   ```

   For example, to delete Administrator1, enter the following command:

   ```
   internaluserrepo.bat -f ../security/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 92.

Property Name	Default Value	Description
`alias`	None	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.
`url`	None	Optional. Specifies the URL for the LDAP server. If you want to use an SSL connection

Property Name	Default Value	Description
		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`
`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.
`dnprefix`	None	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.
`dnsuffix`	None	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.
`usecaching`	None	Optional. Indicates if the LDAP framework caches users or groups, or both.

Property Name	Default Value	Description
		Set to true to enable caching all users and groups. Set to false to disable caching LDAP users and groups.
`mattr`	None	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`.
`memberinfoingroups`	False	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.
`creategroups`	True	Optional. Indicates if the login module extracts groups of the logged-on user from the LDAP server. When `creategroups` is set to true, the login module extracts the groups of the logged-on user from the LDAP server. When `creategroups` is set to false, the login module does not extract the groups of the logged-on user from the LDAP server.
`gidprop`	None	Optional. Specifies the LDAP group attribute.

Property Name	Default Value	Description
		Use any string of characters as the valid value for `gidprop`.
`grouprootdn`	None	Optional. Specifies the location from which to start searches for groups. Use any string of characters as the valid value for `grouprootdn`.
`groupobjclass`	group	Optional. Indicates that the found object is a group. The login module uses the `groupobjclass` when searching for groups.
`personobjclass`	person	Optional. Indicates that the found object is a person. The login module uses the `personobjclass` when searching for users.

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:*Software AG_directory*\profiles\SPM\configuration \com.softwareag.platform.config.propsloader
   - For Command Central:*Software AG_directory*\profiles\CCE\configuration \com.softwareag.platform.config.propsloader
2. Update the LDAP properties based on your needs.
3. 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:

- For Command Central: *Software AG_directory*\profiles\CCE\configuration\security\jaas.config
- For Platform Manager: *Software AG_directory*\profiles\SPM\configuration\security\jaas.config

Note: Command Central does not use the JAAS configuration file located in the *Software AG_directory*\profiles\CCE|SPM\configuration directory.

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;
}
```

You can modify the JAAS configuration file to allow authentication against user stores other than the Command Central and Platform Manager internal user stores, for example LDAP or the Software AG Common Platform user store in the *Software AG_directory*\common\conf\users.txt file.

Configuring the jaas.config File to Use LDAP/AD

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

For more information about the LDAPLoginModule, see the Predefined Login Modules section in the *Software AG Security Infrastructure Documentation*

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:
   - For Command Central: *Software AG_directory*\profiles\CCE\configuration\security
   - For Platform Manager: *Software AG_directory*\profiles\SPM\configuration\security
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.
   ```

```
  SAMLAssertValidatorLoginModule sufficient;
//Internal repository login module (java based)
  com.softwareag.security.jaas.login.internal.InternalLoginModule optional
        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.sin.is.ldap.lm.LDAPLoginModule optional
        url="ldap://myldapserver:389"
        prin="CN=user,OU=myuser,DC=ldap,DC=server"
        cred="****"
        gidprop="CN"
        uidprop="CN"
        usecaching="false"
        userrootdn="DC=my,DC=ldap,DC=server"
        mattr="memberOf"
        memberinfoingroups=false
        grouprootdn="DC=my,DC=ldap,DC=server"
        groupobjclass="group"
        personobjclass="person"
        creategroups=true;
//Role repository login module
  com.softwareag.security.authz.store.jaas.login.RoleLoginModule requisite
        storage_location="/opt/softwareag/common/conf/roles.txt";
//SSOS login module for SAML sign assertion generation
//com.softwareag.security.idp.saml.lm.SAMLAssertIssuerLoginModule optional;
};
/*
 * Login context, used in common Platform for management channel .
 */
PlatformManagement {
  //SSOS login module for SAML signed assertion validation
  //used for delegated out only for JMX
    com.softwareag.security.idp.saml.lm.
    JMXDelegatedAuthLoginModule 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";
  //Role repository login module
    com.softwareag.security.authz.store.jaas.login.RoleLoginModule   optional
              storage_location="/opt/softwareag/common/conf/roles.txt";
}
```

4. 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:
   - For Command Central: *Software AG_directory*\profiles\CCE\configuration\security
   - For Platform Manager:*Software AG_directory*\profiles\SPM\configuration\security
2. To add a new group, create a new line and use the following format:

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

   where *unique ID* is a unique identifier for the group. For example:
   `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:

   ```
   *\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.

Permission	Description
`canread`	Provides read-only access to all information, including lists of products, components, configuration, and monitoring data.
`canwrite`	Provides the ability to create, update, delete all information managed by Command Central and Platform Manager, including nodes, environments, and product configuration.
`canexecute`	Provides the ability to execute lifecycle operations: start, stop, debug, and restart.

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 98 and "Groups" on page 95.

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 98.

Role	Permissions
readonlyadmin	`canread`, `canexecute`
superadmin	`canread`, `canwrite`, `canexecute`
viewer	`canread`

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 95 and "Managing Groups" on page 96.

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.

```
[permissions]
permissions:allow=canwrite,canexecute,canread
[roles]role:superadmin=*
role:readonlyadmin=canread,canexecute
role:viewer=canread
[users]
user:"Administrator"=superadmin
[groups]
groups:"Administrators"=superadmin
```

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:
   - For Command Central: *Software AG_directory*\profiles\CCE\configuration\security
   - For Platform Manager:*Software AG_directory*\profiles\SPM\configuration\security
2. To add a new role, create a new line in the `roles` section using the following format:

   `role:`*`rolename`*`=`*`permissions`*

   For example, to add a new role, superadmin, that has permission to do everything, enter:

   ```
   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:

   ```
   *\Group1:25:Operator
   ```

5. In the `users` section, map the user from the users.txt file to the new role using the following format:

   ```
   user:"user_name"=role
   ```

   For example, to map the user, Administrator, to the superadmin role, specify the following:

   ```
   user:"Administrator"=superadmin
   ```

6. In the `groups` section, map the role to a group defined in the groups.txt file, using the following format:

   ```
   group:"group_name"=role name
   ```

7. Save and close the file.

11 Viewing Product Inventory

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.

12 Administering Product Lifecycle

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.

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

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.

Viewing Product Logs

You view run-time component or product logs with information about operations and errors that occur on the product using the Command Central web user interface or the Command Line tool. For information about using diagnostic logs commands, see *webMethods Command Central and webMethods Platform Manager Command Reference*.

To view the available logs for a product

1. In the Environments pane, select the environment for the product your require.
2. On the **Instances** tab, click the name of the product instance.
3. On the product instance page, select the **Logs** tab.

Command Central lists the available product logs on the Log Sources page.

Viewing the Contents of a Log

On the Log Sources page, you can view the contents of a log by clicking on the log alias in the Alias column.

In the search field, you can search for log entries by supplying either a regular expression or search text.

Note: When **Highlight** is selected, you cannot use regular expressions in searches.

By default, Command Central shows the last 100 log entries. Use the filtering options on the Logs page to view specific lines in the log as follows:

- When you select **Filter** and specify a regular expression or search text, Command Central shows the specified number of entries in the log that contain the search text. For example, if you type "JMX" in the search field and specify 20 lines, Command Central shows up to 20 log entries that contain the word "JMX".
- When you select **Filter**, but do not specify a regular expression or search text, Command Central shows the specified number of entries from the top or bottom of the log. For example, if the search field is empty and you select **First** and **20** lines, Command Central shows the first 20 entries in the log.
- When you select **Highlight** and specify a regular expression or search text, Command Central highlights the search text matches in the specified number of entries in the log that contain the search text.

Note: Switching from **Highlight** to **Filter** removes all highlighting from the text.

- When you select **Highlight**, but do not specify a regular expression or search text, Command Central shows the specified number of entries from the top or bottom of the log.

Downloading a Log

You can download one or more logs at a time.

To download a log

1. In the Download column on the Log Sources page, click  for the log that you want to download.
2. Select the format in which you want to download the log.

Downloading Multiple Logs

To download multiple logs

1. On the Log Sources page, select the logs you want to download.

   Note: If no logs are selected, Command Central downloads all available logs.

2. Click  .
3. Click **Download selected logs**.

13 Monitoring Instances

About Monitoring Instances

Command Centralallows 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 Centralalso 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 104.

About Monitoring KPIs

Command Centralallows 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:

- Name
- Current value
- Marginal threshold
- Critical threshold
- Maximum value

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 161.
- **Broker Server** For more information, see "Monitoring webMethods Broker KPIs" on page 155.
- **Integration Server** For more information, see "Monitoring KPIs of Integration Server Instances" on page 141.
- **My webMethods Server** For more information, see "Monitoring KPIs of My webMethods Server Instances" on page 167.

Viewing Alerts for an Instance or Its Components

Command Centralindicates 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:

oldStatus	newStatus	Alert	Severity
online	stopped	on	warning
online	unresponsive	on	error
online	failed	on	error
online	unknown	on	warning
not online	online	off	info

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:

oldZone	newZone	Alert	Severity
normal	marginal	on	warning
marginal	critical	on	error
normal	critical	on	error
critical	marginal	off	warning
marginal	normal	off	info
critical	normal	off	info

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 Centralallows 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 Centralalso 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 Centraland 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 109.

For more information about the detailed structure of monitoring-related events, go to *Software AG_directory*\common\EventTypeStore\WebM\PlatformManagement.

14 Comparing Product Versions, Fixes, and Configurations

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.

15 Repository Management

Creating an Image Repository

Use the following procedure to create an image repository on Command Central. You can point to an image repository created on the Command Central server when applying a template.

To create an image repository

1. In Command Central, go to **Views > Repositories**.
2. Click  and select **Image**.
3. In the Create image repository dialog box, specify:

Field	Description
Repository name	Required. A unique name for the repository. The only valid characters in a repository name are ASCII characters, numbers, underscore (_), dot (.), and a hyphen (-).
Repository description	Optional. A description of the repository. This description is displayed in the repositories list on the Repositories page.
Repository contents	Select whether the repository contains products or fixes.
Image file on server	Required. The fully qualified path to an existing image file on the Command Central server to which the repository refers. If you do not specify a path, you must upload an image file using the **Upload image file** field. Command Central populates the **Image file on server** field with the path to the uploaded image file.
Upload image file	Select and upload an existing image file (created with Installer for products or with the Update Manager for fixes) from the file system to the Command Central server.

4. Click **OK**.

Command Central adds the new image repository in the repositories list.

In the repositories list, you can view repository details, such as name, description, contents, and type.

Registering a Master Repository

Use the following procedure to register a master repository on Command Central. You can point to a master repository registered with Command Central when applying a template.

To register a master repository

1. In Command Central, go to **Views > Repositories**.
2. Click  and select **Master**.
3. In the Register master repository dialog box, specify values for the following fields:

Field	Description
Repository name	Required. A unique name for the repository. The only valid characters in a repository name are ASCII characters, numbers, underscore (_), dot (.), and a hyphen (-).
Repository description	Optional. A description of the repository. This description is displayed in the repositories list on the Repositories page.
Repository contents	Select whether the repository contains products or fixes.
Credentials	Required. Enter valid user name and password for the Empower website.
Version	Required. Select a product repository version. The version for a fix repository is populated automatically.
Advanced	Optional. The URL of the server from which to install products. **Important:** Use this field only if directed by Software AG Global Support.

4. Click **OK**.

Command Central adds the new master repository in the repositories list.

In the repositories list, you can view repository details, such as name, description, contents, and type.

Deleting a Repository

Use the following procedure to delete a repository registered with Command Central.

To delete a repository

1. In Command Central, go to **Views > Repositories**.
2. From the repositories list, select the repository to delete.
3. Click  .
4. Click **OK**.

When deleting an image repository, Command Central deletes both the repository and the image file that the repository refers to.

Editing Image Repository Details

You can edit the description for an image repository and update the image file to which the repository refers.

To edit a registered image repository

1. In Command Central, go to **Views > Repositories**.
2. Click the name of the repository that you want to edit.
3. In the Edit image repository dialog box, you can edit *only* the values in the following fields:

Use this field...	To...
Repository description	Replace the repository description.
Image file on server	Change the fully qualified path to an existing image file on the Command Central server which the repository uses by reference. If you do not specify a path, you must upload an image file using the **Upload image file** field. Command Central populates the **Image file on server** field with the path to the uploaded image file.
Upload image file	Select and upload a new image file that replaces the image file you uploaded when adding the repository.

4. Click **OK**.

Editing Master Repository Details

You can edit the description for a master repository and change your repository credentials.

To edit a registered master image repository

1. In Command Central, go to **Views > Repositories**.
2. Click the name of the repository that you want to edit.
3. In the Edit master repository dialog box, you can edit *only* the values in the following fields:

Use this field...	To...
Repository description	Replace the repository description.
Credentials	Change the user name and password for the registered master repository.
Version	Change the product or fix version.
Advanced	Specify a different server URL from which to download products or fixes.

4. Click **OK**.

16 Provisioning Using Templates

Creating a Template

With Command Central you create a new template by pointing to an existing managed installation from which you include the products, fixes, and configuration you want to provision.

To create a template from a managed installation

1. In the Environments pane, select the environment that contains the installation you want.
2. Select the **Installations** tab.
3. On the **Installations** tab, click the installation from which you want to create a template.
4. Click  and select **Save as template**.
5. In the Save Template dialog box, provide the following information:

Field...	Specify...
Alias	A unique name for the template. The only valid characters in a template name are ASCII characters, numbers, underscore (_), dot (.), and a hyphen (-).
Description	Optional. A description of the template. This description is displayed in the template list on the Template page of the Apply Template wizard.
Include Products	Whether to include products in the template. Select the check box to include products (default).
Include Fixes	Whether to include fixes in the template. Select the check box to include fixes (default).
Include Configuration	Whether to include configuration in the template. Select the check box to include product configuration (default).
Include Files	Whether to include files in the template. Select the check box to include files (default).

6. Click **Save**.

Platform Manager creates the new template and transfers the files to the Command Central file system.

Modifying a Template

You can modify a template created with Command Central before applying the template on a target machine. For example, you can delete products, fixes, or configuration that you do not want to apply from the template. You can make changes to the template directly by editing the template files on the file system. To edit the template files on the file system, go to *Software AG_directory*\profiles\CCE\data\templates*template_alias* and open the files in a text editor. You can also export the template to the client machine using the Command Central command line tool, edit the template files locally, and import the template back to the Command Central server using the Command Central command line tool.

Software AG does not recommend adding new products, fixes, files, and configurations to a created template.

Note: Before modifying configuration data property values, ensure that the values you specify are valid.

Applying a Template

You can select which elements from a template of a managed installation, available in the Command Central file system, to apply to a target machine.

To apply a template to a new node

1. In the Environments pane, select the environment that contains the installation to which you want to apply a template.
2. Select the **Installations** tab.
3. On the **Installations** tab, click the installation to which you want to apply a template.
4. Click  and select **Apply template**.
5. In the Apply Template wizard, from the **Alias** column on the Template page, select the name of the template you want to apply.

   You can also view the description, details, and contents of the selected template.
6. On the Products page, specify:

Field	Description
Install products from template	Whether to install the products included in the template. Select the check box to install products (default).

Field	Description
Product repository	The product repository from which to install the products. The list includes only product repositories configured in Command Central. For information about how to add a product repository in Command Central, see "Repository Management" on page 117.

7. On the Fixes page, specify:

Field	Description
Install products from template	Whether to install the fixes included in the template. Select the check box to install fixes (default).
Fix repository	The repository from which to install the fixes. The list includes only fix repositories configured in Command Central. For information about how to add a fix repository in Command Central, see "Repository Management" on page 117.

8. On the Configuration page, specify:

Note: When applying template configuration, Command Central does not automatically restart product components. You must restart product components that require restart to use configuration changes manually.

Field	Description
Include configuration from template	Whether to apply the product configuration included in the template. Select the check box to apply the configuration (default). When this check box is selected, you also specify whether Command Central will merge or replace the existing configuration on the target node with the configuration from the template.
Include files from template	Whether to apply the files included in the template. Select the check box to apply files (default).

9. On the Confirm page, verify the template details and the apply actions you selected.

10. Click **Finish**.

Command Central applies the template to the new node to create a copy of the source installation, following the actions you specified.

Known Limitations When Applying A Template

With some products, for example Integration Server, you need to apply a template in several consecutive steps. When you are applying an Integration Server template that contains products, fixes, and configuration, you must:

1. Apply the products.
2. Restart the IS_*instancename* component, where *instancename* is the name of the Integration Server instance, and verify that its status is **Online**.
3. Apply the fixes.
4. Repeat step 2.
5. Apply the configuration.

> **Note:** Software AG recommends restarting the IS_*instancename* component after applying a configuration.

Generally, the template configuration will be applied successfully on product components that are running. However, some products, for example OSGI-CTP, do not require that the product is running to apply fixes or configuration. With these products you can apply a template with products, fixes, and configuration in one step.

II Understanding Product-specific Administration

17 Configuring Integration Server Ports

About Ports

You can use Command Central to configure the ports for multiple Integration Servers managed by webMethods 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.

Use this port type...	To...
HTTP	Submit unsecured requests to the server.
HTTPS	Submit requests to the server using SSL encryption.
FTP	Move files to and from the server.
FTPS	Move files to and from the server using SSL encryption.
HTTP Diagnostic	Access Integration Server Administrator when the server becomes unresponsive.
HTTPS Diagnostic	Access Integration Server Administrator using SSL encryption when the server becomes unresponsive.

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

   Command Central displays the Integration Server ports.
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:

Field	Specify
Enabled	Whether the port is enabled.
Port Number	The number you want to use for the port. Select a number that is not already in use.
Alias	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 (-).
Bind Address	IP address to which to bind this port. Specify a bind address if your machine has multiple IP addresses and you want the

Field	Specify
	port to use this specific address. If you do not specify a bind address, the server picks one for you.
Backlog	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.
Keep Alive Timeout	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.
Package Name	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.

7. Expand **Threadpool Configuration** and complete the following fields:

Field	Specify
Enabled	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**.
Threadpool Min	The minimum number of threads for this private thread pool. The default is 1.

Field	Specify
Threadpool Max	The maximum number of threads for this private thread pool. The default is 5.
Threadpool Priority	The Java thread priority. The default is 5. **Important:** Use this setting with extreme care because it will affect server performance and throughput.

8. If you are creating an HTTPS, HTTPS diagnostic, or FTPS port, expand **Security Configuration** and complete the following fields:

Field	Specify
Client Authentication	The type of client authentication you want Integration Server to perform for requests that arrive on the port. Select: ■ **Username/Password** if you want to use basic authentication. ■ **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: ■ 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. ■ 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. ■ **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.
Keystore Alias	Optional. A user-specified, text identifier for an Integration Server keystore. 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

Field	Specify
	the same keystore, and more than one listener can use the same keystore alias.
Key Alias	Optional. The alias for the private key, which must be stored in the keystore specified by the above keystore alias.
Truststore Alias	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.

9. Expand **IP Access Restrictions** and specify the following to allow or deny access from specified ports:

Field	Specifies
Use Global Default	That the port should use the global IP access settings set in Integration Server. This is the default.
Allow by Default	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.
Deny by Default	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.
Hosts to allow	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 ([]).

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

Field	Specifies
Use Global Default	That the port should use the default mode access settings set in Integration Server. This is the default.
Deny by Default	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.
Allow by Default	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.
URLs to deny	The service URLs from which Integration Server is to accept inbound requests. Enter each service URL on a separate line.

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

Testing Ports

Perform the following procedure to test Integration Server 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

Perform the following procedure to set the Integration Server 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.
4. From the **Port** column, locate the port whose details you want to edit, and click on the port number.
5. Click **Edit**.
6. 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.

18 Monitoring KPIs of Integration Server Instances

Perform the following procedure to monitor KPIs of Integration Server instances.

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:

Name	Marginal Value	Critical Value	Maximum Value
Average response time (in ms)	80% of maximum	95% of maximum	5000
Service errors	70% of maximum	90% of maximum	5
Running services	80% of maximum	95% of maximum	10

19 Configuring Integration Server

About Integration Server Configuration Types

You can use the various configuration types that Command Central provides to configure the following settings on Integration Server:

- Keystore and truststore aliases
- Integration Server loggers and server log facilities
- Server configuration parameters
- Database functional aliases
- webMethods Messaging settings
- Integration Server Core and Terracotta license files
- Ports
- JDBC connection pools
- JMS settings
- JNDI settings
- Resource settings
- Global variables
- Email settings

Note: Integration Server must be running if you want to administer Integration Server through Command Central. This section assumes that you are familiar with Integration Server Administrator. For more information about the Integration Server Administrator, see *webMethods Integration Server Administrator's Guide*.

Working with Integration Server Configuration Types

Perform the following procedure to add, edit, or delete items for Integration Server configuration type items over Command Central.

Note: Ensure that Integration Server is running before performing the following procedure.

To add, edit, or delete an item for an Integration Server configuration type

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 the configuration type from the drop-down list.

   Command Central displays the available or default values, if any for the selected Integration Server configuration type.

4. To add an item for the Integration Server configuration type, click  . Enter the required values in the displayed fields and click **Save**.

   Note: For more information about the usage and field descriptions of the Integration Server configuration types, see *webMethods Integration Server Administrator's Guide* or *webMethods Integration Server Online Help*.

5. To edit an item for a configuration type, click on the item that you want to update and click **Edit**. Make the necessary changes and click one of the following:

   - **Test** to test the configuration type item.
   - **Save** to save your changes.
   - **Cancel** to cancel the edits to the configuration type item.

6. To delete an item for a configuration instance, click 

20 Administering webMethods Broker

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 Serverlicense 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 Centraldisplays theBroker Server port.
6. Click the name of the port and click **Edit.**

   Connection Basics displays the following non-editable fields.

Field	Description
Enabled	Whether theBroker Server base port is enabled.
Port Number	The Broker Server base port number. 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*.

7. Expand **Security Configuration** and specify the following SSL settings.

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

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 `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:

Field	Description
Enabled	Indicates whether the Broker Server port is enabled or disabled.
Port	Indicates the base port of the Broker Server.
Protocol	Indicates the protocol used by the Broker Server.
Type	Indicates the type of Broker Server port.

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 to **Paused**. 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**.

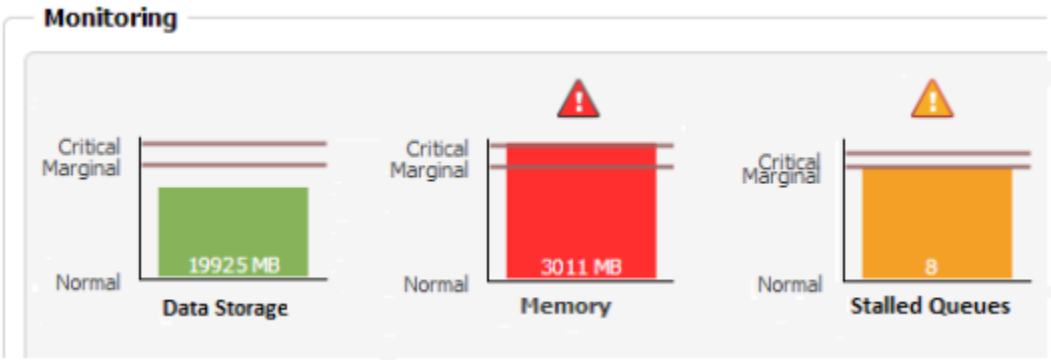
21 Monitoring webMethods Broker KPIs

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:

KPI	Description
Data Storage or Configuration Storage	Indicates the utilization of either the run-time data storage or the configuration data storage of Broker Server.
Memory	Indicates the utilization of Broker Server memory.
Stalled queues	Indicates the performance of the message queues.



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.

Marginal Value	Critical Value	Maximum Value
60% of the Broker Server's maximum storage size.	80% of the Broker Server's maximum storage size.	Broker Server's maximum storage size.

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.

Storage UtilizationBroker Server Data	Storage UtilizationConfiguration Data	Storage Value Displayed
Less than marginal value	Less than marginal value	Broker Server Data
Less than marginal value	More than marginal value, but less than critical value	Configuration Data
Less than marginal value	More than critical value, but less than maximum value	Configuration Data

Storage UtilizationBroker Server Data	Storage UtilizationConfiguration Data	Storage Value Displayed
More than marginal value, but less than critical value	Less than marginal value	Broker Server Data
More than marginal value, but less than critical value	More than marginal value, but less than critical value	Broker Server Data
More than marginal value, but less than critical value	More than critical value, but less than maximum value	Configuration Data
More than critical value, but less than maximum value	Less than marginal value	Broker Server Data
more than critical value, but less than maximum value	more than marginal value, but less than critical value	Broker Server Data
more than critical value, but less than maximum value	more than critical value, but less than maximum value	Broker Server Data

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).

Marginal Value	Critical Value	Maximum Value
80% of the `max-memory-size` parameter value.	95% of the `max-memory-size` parameter value.	Broker Server's memory limit defined in the `max-memory-size` parameter.

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

Marginal Value	Critical Value	Maximum Value
1 queue.	50% of the maximum value.	Defined by whichever of these values is greater: - 1 queue. - 5% of the total number of client queues or forward queues in Brokers. - Current number of stalled queues. 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.

22 Monitoring KPIs of Software AG Platform Manager Instances

Software AG Platform Manager returns the following three KPIs:

Name	Marginal Value	Critical Value	Maximum Value	Limitation Description
Used machine physical memory (in MB)	80%	95%	Physical memory of machine.	On hosts running a 32-bit JRE on a 32-bit operating system with more than 2GB RAM, this KPI shows a value that is too low. This is due to a known issue in the Java SE Runtime Environment.
Used machine disk space (in MB)	80%	95%	Physical disk space of machine.	
CPU Utilization	80%	90%	100%	■ This KPI is *only* displayed, if you use Java 7. ■ This KPI is *not* displayed when running on HP-UX.

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.

23 Configuring My webMethods Server Ports

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 depricated.
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.

24 Configuring My webMethods Server Email

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.

Field	Specify
Server Name	The SMTP server's host name. For example: smtp.server.com.
Port	The SMTP server's port number.
Sender Name	The default name to use in the **From** field of the email messages sent by the server.
Sender Email	The default email address to use in the **From** field of the email messages sent by the server.

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

Field	Description
SMTP Username	Optional. The user name that My webMethods Server has to supply for authentication. If the SMTP server requires authentication, specify the user name.
SMTP Password	Optional. The password associated with the **SMTP Username**. If the SMTP server requires authentication, specify the appropriate password.

7. Click **Test** and **Save** the email settings.

25 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.

Name	Marginal Value	Critical Value	Maximum Value
Number of user sessions	80% of maximum	95% of maximum	At least 100, or high water mark. (High water mark is the highest value ever reached.)
JDBC connection pool size (maximum number of connections to JDBC)	80% of maximum	95% of maximum	As configured.
Average response time (in milliseconds)	50% of maximum	90% of maximum	At least 10 seconds, or high water mark.

26 Administering Universal Messaging

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 172.

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.

Configure this...	To specify...
Port Type	Which protocol, the port (interface) must use: ■ Socket protocol (nsp) ■ HTTP protocol (nhp) ■ HTTPS protocol (nhps) ■ SSL protocol (nsps) You cannot change this attribute after you create the port.
Port Number	The number of the port. You cannot change this attribute after you create the port.
Bind Address	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. You cannot change this attribute after you create the port.

Configure this...	To specify...
Backlog	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.
Enabled	Whether the port is enabled or disabled. **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.

Configure this...	To specify...
Client Authentication	Whether or not Universal Messaging requires client certificates for all requests. Select: - **None** if Universal Messaging does not require client certificates for all requests. - **REQUIRE_CERTIFICAT** if you want Universal Messaging to require client certificates for all requests.
SSL Enabled	Whether the port is SSL enabled or not. This attribute is always set to true for nhps and nsps port.
Keystore Type	File type of the keystore file. Universal Messaging supports only the JKS file type.
Server Location of Keystore	Location of the keystore file.
Keystore Password	Password required to access the SSL certificate in the keystore file.
Keystore Key Password	Password required to access a specific private key in the keystore file.

Configure this...	To specify...
Truststore Type	File type of the truststore file. Universal Messaging supports only the JKS file type.
Server Location of Truststore	Location of the truststore file.
Truststore Password	Password required to access the SSL certificate in the truststore file.

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 172.

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 172 and "Port Security Attributes" on page 173. 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:

KPI	Description
JVM Memory	Indicates the utilization of JVM memory. The marginal, critical, and maximum values for this KPI depend on the maximum memory size of the JVM. ■ Marginal is 80% of the maximum JVM memory. ■ Critical is 95% of the maximum JVM memory. ■ Maximum is 100% of the maximum JVM memory.
Fanout Backlog	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.

KPI	Description
	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 fanout backlog. Default is 100.
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.

27 Administering CentraSite

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.

Log File...	Stores...
Registry.log (CentraSite.AAB.log.1.xml CentraSite.AAB.log.0.xml)	The request logs (middle level information).
A file with type "2X0"	The data store request logs (low level information).

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**.

28 Configuring Cloud Factory Accounts

Adding an Amazon Elastic Compute Cloud Account

You add an Amazon Elastic Compute Cloud (Amazon EC2) account that you use with the Cloud Factory API using the Command Central web user interface.

To add an Amazon EC2 account

1. Select the Command Central environment from the Environment pane, then click the instance from the **Instances** tab.
2. Select the Cloud Factory component.
3. Click the **Configuration** tab.
4. Select **Accounts** in the drop-down list.

   Command Central displays the Cloud Factory account configuration page.
5. Click  to add an account.

   Command Central displays the Select Configuration dialog box.
6. Select **EC2** from the drop-down list and click **OK**.
7. Complete the following fields:

Field	Specify
Account Name	The name for the Amazon EC2 account. Do not use spaces in the account name.
Vendor	The name of the account vendor. Command Central generates the name automatically based on the configuration type you selected.
Region	The geographic region for which the account is created.
Availability Zone	Optional. The Amazon EC2 location for which the account is created.
Secret Key	The secret key provided by Amazon EC2.
Access Key	The access key provided by Amazon EC2.
Proxy Host	Optional. The proxy host name if the operating system uses a proxy.

Field	Specify
Proxy Port	Optional. The number of the proxy port if the operating system uses a proxy.

8. Click **Test** to test the account.
9. Click **Save**.

Adding a VMware vSphere Account

You add a VMware vSphere account that you use with the Cloud Factory API using the Command Central web user interface.

To add a VMware vSphere account

1. Select the Command Central environment from the Environment pane, then click the instance from the **Instances** tab.
2. Select the Cloud Factory component.
3. Click the **Configuration** tab.
4. Select **Accounts** in the drop-down list.

   Command Central displays the Cloud Factory account configuration page.
5. Click  to add an account.

   Command Central displays the Select Configuration dialog box.
6. Select **VSphere** from the drop-down list and click **OK**.
7. Complete the following fields:

Field	Specify
Account Name	The name for the of the VMware vSphere account. Do not use spaces in the account name.
Vendor	The name of the account vendor. Command Central generates the name automatically based on the configuration type you selected.
Endpoint	The endpoint URL for the VMware vSphere SDK.
Region	The name of the data center accessed by this account. If you do not specify a value, the account connects to all machines to which you are granted access.

Field	Specify
Username	The user name for logging on the VMware vSphere account.
Password	The password for logging on the VMware vSphere account.

8. Click **Test** to test the account.
9. Click **Save**.

Editing Accounts

You can update the details for an account registered with the Cloud Factory API using the Command Central user interface.

To edit an account registered with the Cloud Factory API

1. Select the Command Central environment from the Environment pane, then click the instance from the **Instances** tab.
2. Select the Cloud Factory component.
3. Click the **Configuration** tab.
4. Select **Accounts** in the drop-down list.

   Command Central displays the Cloud Factory account configuration page.
5. Click the name of the account that you want to update.
6. On the Configuration details page for the account, click **Edit**.
7. Update the required fields.
8. Click **Save**.

Deleting Accounts

You can use the Command Central web user interface to delete a registered Cloud Factory account.

To delete a Cloud Factory account

1. Select the Command Central environment from the Environment pane, then click the instance from the **Instances** tab.
2. Select the Cloud Factory component.
3. Click the **Configuration** tab.
4. Select **Accounts** from the drop-down list.

Command Central displays the Cloud Factory account configuration page.

5. Select an account and click  to delete the account.

A 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:

Interface	Where to Find More Information
Web user interface	*webMethods Command Central Help*
Command line interface	*webMethods Command Central and webMethods Platform Manager Command Reference*

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

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Authentication Mode (select an **Environment**, click the **Instances** tab, select an **Instance**, click the **Overview** tab, click the  **Authentication Edit** button)
Command line interface	`cc add security credentials`

Working with Environments

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

Searching for an Environment

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Environments pane (type search criteria in the **Search Environments** box)
Command line interface	`cc list landscape environments`

Viewing Details about an Environment

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Environments pane (select an environment)
Command line interface	`cc get landscape environments` `cc list landscape environments`

Adding an Environment

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Environments pane (click the  **Add Environment** button)
Command line interface	`cc create landscape environments`

Editing Environment Details

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Environments pane (select an environment, click the  **Options** button in the Environments pane, select **Edit Environment**)
Command line interface	`cc update landscape environments`

Deleting an Environment

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Environments pane (select an environment, click the **Delete Environment** button)
Command line interface	`cc delete landscape environments`

Working with Installations

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

Searching for an Installation

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Installations tab (select an **Environment**, click the **Installations** tab, type search criteria in the **Search Installations** box)
Command line interface	`cc list landscape nodes`

Viewing Details about an Installation

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Installations tab (select an **Environment**, click the **Installations** tab, select an **Installation**)
Command line interface	`cc get landscape nodes` `cc list landscape nodes`

Viewing Products Installed in an Installation

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Installation Products tab (select an **Environment**, click the **Installations** tab, select an **Installation**, click the **Products** tab)
Command line interface	`cc get inventory products` `cc list inventory products`

Viewing Fixes Installed in an Installation

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Installation Fixes tab (select an **Environment**, click the **Installations** tab, select an **Installation**, click the **Fixes** tab)
Command line interface	`cc list inventory fixes`

Adding an Installation

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Installations tab (select an **Environment**, click the **Installations** tab, click the  **Add Installation** button)
Command line interface	`cc create landscape nodes`

Updating the Properties of an Installation

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Installation Overview tab (select an **Environment**, click the **Installations** tab, select an **Installation**, click the **Overview** tab)

If you are using this interface...	Use these navigation steps or commands...
Command line interface	`cc update landscape nodes`

Monitoring the Status of Product Instances in an Installation

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Installation Overview tab (select an **Environment**, click the **Installations** tab, select an **Installation**, click the **Overview** tab)
Command line interface	`cc get monitoring`

Linking an Installation to Multiple Environments

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Installations tab (select an **Environment**, click the **Installations** tab, drag an installation to the desired environment)
Command line interface	`cc add landscape environments nodes`

Creating a Unique ID for an Existing Installation

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Not supported
Command line interface	`cc exec landscape nodes generateNodeId`

Removing an Installation from an Environment

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Installations tab (select an **Environment**, click the **Installations** tab, select the installation to remove, click the  **Remove Installations** button)
Command line interface	`cc remove landscape environments nodes`

Working with Templates

This section provides a quick reference to the Command Central tasks that pertain to template-based provisioning of products.

Creating a Template from an Existing Installation

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Installations tab (select an **Environment**, click the **Installations** tab, select the installation to provision, c lick  and select **Save as template**.
Command line interface	`cc create templates`

Applying a Template to a New Node

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Installations tab (select an **Environment**, click the **Installations** tab, select the installation to provision, c lick  and select **Apply template**.
Command line interface	`cc exec templates apply`

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

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Instances tab (select an **Environment**, click the **Instances** tab)
Command line interface	`cc list inventory components`

Viewing Details about an Instance

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Instances tab (select an **Environment**, click the **Instances** tab, select an **Instance**)
Command line interface	`cc get monitoring` `cc get inventory components`

Changing the Display Name of an Instance

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Instance Overview tab (select an **Environment**, click the **Instances** tab, select an **Instance**, click the **Overview** tab, update the **Display Name** field, press Enter)
Command line interface	`cc update inventory components`

Changing the Icon Representing an Instance

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Instance Overview tab (select an **Environment**, click the **Instances** tab, select an **Instance**, click the **Overview** tab, click the arrow next to the display name icon in the Details section)
Command line interface	`cc list resources icons` `cc update inventory components`

Viewing or Clearing Instance Alerts

If you are using this interface...	Use these navigation steps or commands...
Web user interface	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)
Command line interface	`cc list monitoring alerts` `cc delete monitoring alerts`

Starting an Instance

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Instances tab (select an **Environment**, click the **Instances** tab, click the **Status** button next to the instance, select **Start**)
Command line interface	`cc exec lifecycle`

Stopping an Instance

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Instances tab (select an **Environment**, click the **Instances** tab, click the **Status** button next to the instance, select **Stop**)
Command line interface	`cc exec lifecycle`

Restarting an Instance

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Instances tab (select an **Environment**, click the **Instances** tab, click the **Status** button next to the instance, select **Restart**)
Command line interface	`cc exec lifecycle`

Pausing an Instance

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Instances tab (select an **Environment**, click the **Instances** tab, click the **Status** button next to the instance, select **Pause**)
Command line interface	`cc exec lifecycle`

Resuming an Instance

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Instances tab (select an **Environment**, click the **Instances** tab, click the **Status** button next to the instance, select **Resume**)

If you are using this interface...	Use these navigation steps or commands...
Command line interface	`cc exec lifecycle`

Debugging an Instance

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Instances tab (select an **Environment**, click the **Instances** tab, click the **Status** button next to the instance, select **Debug**)
Command line interface	`cc exec lifecycle`

Working with Logs

This section provides a quick reference to the Command Central tasks that pertain to viewing and downloading product logs.

Viewing Product Logs

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Select an environment in the Environments pane, select the **Instances** tab, click the name of a product instance, select the **Logs** tab
Command line interface	`cc list diagnostics logs`

Viewing the Contents of a Log

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Select an environment in the Environments pane, select the **Instances** tab, click the name of a product instance, select the **Logs** tab, click the log alias for a log in the Alias column

If you are using this interface...	Use these navigation steps or commands...
Command line interface	`cc get diagnostics logs`

Downloading Logs

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Select an environment in the Environments pane, select the **Instances** tab, click the name of a product instance, select the **Logs** tab, select the logs you want to download, click  , click **Download selected logs**
Command line interface	`cc get diagnostic logs export file`

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

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Compare Products page (select an **Environment**, click the **Installations** tab, select two or more **Installations**, click the  **Options** button, select **Compare Products**)
Command line interface	`cc get inventory products compare`

Comparing Fix Levels

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Compare Fixes page (select an **Environment**, click the **Installations** tab, select two or more **Installations**, click the  **Options** button, select **Compare Fixes**)
Command line interface	`cc get inventory fixes compare`

Comparing Configuration Settings

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Compare Configurations page (select an **Environment**, click the **Instances** tab, select two or more **Instances**, click the  **Options** button, select **Compare Configuration**)
Command line interface	`cc get configuration compare`

Working with Product Inventory

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

Viewing Component Inventory

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Instances tab (select an **Environment**, click the **Instances** tab, click the arrow to the left of an instance name)
Command line interface	`cc get inventory components` `cc list inventory components`

Viewing Product Inventory

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Installations tab (select an **Environment**, click the **Installations** tab, click the arrow to the left of an installation name)
Command line interface	`cc get inventory products` `cc list inventory products`

Viewing Fix Inventory

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Installation Fixes tab (select an **Environment**, click the **Installations** tab, select an **Installation**, click the **Fixes** tab)
Command line interface	`cc list inventory fixes`

Working with Repositories

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

Creating an Image Repository

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Go to **Views > Repositories**, click  , select **Image**, specify values for the fields in the Create image repository dialog box
Command line interface	`cc create repository`

Registering a Master Repository

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Go to **Views > Repositories**, click  , select **Master**, specify values for the fields in the Register master repository dialog box
Command line interface	`cc create repository`

Deleting a Repository

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Go to **Views > Repositories**, select the repository to delete, click 

Command line interface	`cc delete repository`
	`cc delete repository with node alias`
	`cc delete repositories`

Editing Image Repository Details

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Go to **Views > Repositories**, click the name of the repository you want to edit, edit the fields that allow modifying
Command line interface	`cc update repository` `cc update repository details`

Editing Master Repository Details

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Go to **Views > Repositories**, click the name of the repository you want to edit, edit the fields that allow modifying
Command line interface	`cc update repository` `cc update repository details`

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

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/tabs on the left, select Email from the list at the top of the page, click the **Edit** button)

Command line interface	`cc get configuration common`
	`cc list configuration types`
	`cc get 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`

Working with Ports

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

Adding 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, select a component from the list/tabs on the left, select **Port** from the list at the top of the page, click the **Add Port** button)

Command line interface	`cc 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

If you are using this interface...	Use these navigation steps or commands...
	`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)

Command line interface	`cc update configuration data`
	`cc list configuration types`
	`cc list configuration instances`
	`cc delete configuration instance`
	`cc create configuration data`
	`cc get configuration data`
	`cc add configuration data`
	`cc update configuration data`

Viewing Configuration Details for 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)

Command line interface	`cc get configuration common`
	`cc get configuration data`
	`cc get configuration types`
	`cc list configuration types`

Deleting 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, select the row of the port you want to delete, click the **Delete Port** button)

Command line interface	`cc exec configuration validation delete`
	and then
	`cc delete configuration data`

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

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Instance Overview tab, Monitoring section (select an **Environment**, click the **Instances** tab, select an **Instance**, click the **Overview** tab)
Command line interface	`cc get monitoring`

Working with Security Credentials

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

Retrieving Security Credentials

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Authentication Mode (select an **Environment**, click the **Instances** tab, select an **Instance**, click the **Overview** tab, click the  **Authentication Edit** button)
Command line interface	`cc get security credentials`

Adding Security Credentials

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Authentication Mode (select an **Environment**, click the **Instances** tab, select an **Instance**, click the **Overview** tab, click the  **Authentication Edit** button)
Command line interface	`cc add security credentials`

Deleting Security Credentials

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Not supported
Command line interface	`cc delete security credentials`

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

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Licenses (select an **Environment**, click the **Instances** tab, select an **Instance**, click the **Configuration** tab, select **Licenses** from the list at the top of the page, select a license type)

Command line interface	`cc get configuration common`
	`cc get configuration types`
	`cc list configuration types`
	`cc get configuration data`

Selecting a New License or Changing the Server License Location

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Licenses (select an **Environment**, click the **Instances** tab, select an **Instance**, click the **Configuration** tab, select **Licenses** from the list at the top of the page, select a license type, click **Edit**)
Command line interface	`cc get data`

If you are using this interface...	Use these navigation steps or commands...
	`cc exec configuration validation update` `cc update configuration data`

Creating a License Report Snapshot

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Go to **Views > Licenses**, click 
Command line interface	`cc create license-tools reports snapshot`

Viewing Details About License Reports

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Go to **Views > Licenses**, use the report ID to search for a specific report
Command line interface	`cc license-tools reports snapshot` `cc get license-tools reports snapshot reportid`

Downloading License Reports

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Go to **Views > Licenses**, select the license report you want to download, click  , select the appropriate format for download
Command line interface	`cc get license-tools reports snapshot output PDF` `cc get license-tools reports snapshot output XML`

Deleting License Reports

If you are using this interface...	Use these navigation steps or commands...
Web user interface	Go to **Views > Licenses**, select the license report you want to delete, click 
Command line interface	`cc delete license-tools reports snapshot` `cc delete license-tools reports snapshot reportid`