# Cisco Videoscape Control Suite Management Console

## User Guide

# Please Read

## Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

# Notices

## Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

## Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

## Copyright

# Contents

# About This Guide

## Purpose

This document provides user instructions regarding the Videoscape Control Suite management console, which is a network management tool that provides a web user interface and a command-line interface (CLI).

## Audience

This document is written for system operators. Our engineers may also find this document to be useful.

## Document Version

This is the first formal release of this document.

# 1

# Introducing Cisco Videoscape Control Suite Management Console

## Introduction

This chapter provides general information about the Cisco Videoscape Control Suite (VCS) management console, including browsers supported, navigating the user interface (UI), account-based views, and common tasks.

Use this chapter for instructions to configure mail server settings, set up user roles, and learn about events and alarms.

## In This Chapter

# Introducing Cisco VCS Management Console

The management console is a network management tool that adds to the capabilities of the web user interface and the command-line interface (CLI).

**Note**: To receive the expected results with management console, you should run no more than 3 concurrent management console setups for standard server use (4 GB memory and 3 GHz CPU speed) and no more than 5 concurrent management console setups for high-end server use (8 GB memory and 3 GHz CPU speed).

The management console runs as a service on Red Hat Linux Enterprise Server 5.X 64-bit installations. As Linux service, the management console runs continuously and resumes running after a reboot.

## Supported Browsers

The management console is supported on the following browsers:

- Microsoft Internet Explorer 9.0(IE8 compatibility mode)
- Mozilla Firefox 5.0

**Important:** We strongly advise you to disable third-party browser extensions. In Internet Explorer, you can disable third-party browser extensions by choosing **Tools > Internet Options** and de-selecting the **Enable third-party browser extensions** check box on the **Advanced tab**.

## Understanding the User Interface

The management console web interface is organized in a life-cycle workflow that includes the following high-level task areas:

**Home**—When you log into the management console, a list of nodes appears with general information provided for all of the nodes. If you select the radio button for a specific node, you can then click the **Statistics**, **Logs**, or **Services** options to view more details for that node. Anytime you navigate away from the home page, you can click the home icon in the main menu bar to return.

**Note**: The Main Menu Bar displays only the functions associated with the user that is currently logged in to the management console. For example, a user that is not enabled for Administration functions will not see the Administration menu option.

**Services**—The Services menu options include links to tasks for the services associated with the user role. For example, a user assigned to only the user-group EAS-Mgr will be able to access only the EAS service.

**Operate**— The Operate menu options provide links to activities for monitoring, troubleshooting, and day-to-day maintenance of the network. Software download, COP installation, and upgrades are also performed from this option.

**Configure—**The Configure menu options provide links to configure nodes and NTP servers. Select the nodes view to see a list of the nodes in the current operators domain. You then have the option to select a specific node and add or delete servers to that node. From the NTP servers view, you can configure NTP server settings. You can add up to five servers, and delete as necessary.

**Administration—**The Administration menu options provide links to manage system configuration settings, manage access control, and specify data collection settings.

**Message Infrastructure—**The Message Infrastructure menu options include Deployment, Message Fabric, Service Infrastructure, and External SASL Plugin.

# Getting Started

After you install the VCS management console and launch the browser, complete the following tasks to get started:

- Configuring Mail Server Settings
- Setting Up User Roles

## Configuring Mail Server Settings

By configuring mail server settings, you will receive email notification when the management console has received any alarms in the managed nodes.

1. Select **Administration > Settings**.
2. From the sidebar menu, click **Mail Server Configuration**.
3. Enter the host name of the primary SMTP server.
4. Optionally, you may enter a username.
5. Enter a password for logging on to the SMTP server and confirm it.
6. If a secondary mail server is available, provide the information for the secondary SMTP server.
7. In the **Sender and Receivers** area, the **From** text box is pre-populated with CMC@<CMC server IP address>. You can change it to a different sender.
8. Enter the recipient's e-mail addresses in the **To** text box. The e-mail address you provide serves as the default value for other functional areas, such as alarms or reports. You can add multiple e-mail addresses separated by commas.

   **Note**: Global changes you make to the recipient e-mail addresses in Step 7 are disregarded if e-mail notifications were set.
9. If you want the email recipient list applied to the existing email notifications, select the **Apply recipient list to existing email notifications** check box.
10. Enter the text you want appended to the email subject line in the **Subject** field.
11. Click **Test** to send a test email to verify the settings you entered are correct.
12. Click **Save** to save the mail server settings, or click **Cancel** to cancel your entries without saving.

### Deleting the Mail Server Configuration

1. Select **Administration > Settings**.
2. From the sidebar menu, click **Mail Server Configuration**.
3. Click **Delete** to delete the saved configuration. A confirmation prompt appears.
4. Click **Ok** or **Cancel**.

## Setting Up User Roles

When you add users to the management console, you can specify their privileges by assigning them to a user group and to virtual domains. The user groups are predefined by the VCS, however, you can edit the permissions for the tasks in each user group.

### Add New User

1. Select **Administration > Users, Roles & AAA**.
2. From the sidebar menu, click **Users**.
3. From the command tool drop-down menu, select **Add User**; then, click **Go**.
4. Enter the username and password for the new user, and confirm the password.
   **Note**: Entries are case sensitive. The password must contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits and special characters.
5. Select the groups applicable for this user.
   **Note**: Use the scroll bar view all of the user groups.
6. Click **Save**, and then **OK**.

From the User Groups view, you can verify that the user has been added to the groups intended.

1. Click **User Groups** from the left sidebar menu. The default groups are displayed with the members listed for each.
2. Verify that the username for the new user appears in the appropriate groups.

#### Default User Groups

| Group Name | Privileges |
|---|---|
| AM-Mgr | Monitor and configure Alert Manager Service operations. |
| Admin | Monitor and configure management console operations and perform all system administration tasks except administering management console user accounts and passwords. |
| BOA-Mgr | Monitor and configure BOA operations. |
| Client-Directory-Mgr | Monitor and configure Client Directory operations. |
| Cloud-DVR Management | Monitor and configure Cloud-DVR operations. |
| ECSOperator | Monitor and configure ECS Operator operations. |
| ECSUser | Monitor and configure ECS User operations. |
| EPM-Mgr | Monitor and configure Endpoint Management. |

| Group Name | Privileges |
|---|---|
| Event-Mgr | Monitor and configure Event Manager Service operations. |
| Message-infra-Mgr | Monitor and configure Message Infra (XCP) operations. |
| Operator | Read Only access only. This user can Monitor node status and statistics. |
| Operator-Messaging-Mgr | Monitor and configure OMS operations. |
| Platform-Mgr | Monitor and configure platform management operations on management and managed nodes. For example, NTP configurations etc. |
| Resource-Mgr | Monitor and configure Resource Manager Service operations. |
| Root | Monitor and configure management console operations and perform all system administration tasks including changing any passwords. Only one user can be assigned to this group and is determined upon installation. It cannot be removed from the system, and no task changes can be made for this user. |
| Super Users | Monitor and configure management console operations and perform all system administration tasks including administering management console user accounts and passwords. Superusers tasks can be changed. |
| UHE-Mgr | Monitor and configure UHE operations. |
| UNG-Mgr | Monitor and configure UNG operations. |
| UPM-Adaptor-Mgr | Monitor and configure UPM operations. |
| wfe-user | Monitor and configure workflow engine operations. |

Details for managing permissions are provided in ***Administration*** (on page 17).

# Common Tasks

You can perform the following actions from nearly any management console screen:

- Changing Your Password
- Monitoring Alarms
- Launching Help

## Changing Your Password

1. Hover your cursor over your username (at the top of the window, to the left of the search box) and click **Change Password**.
2. To view the password policy, click the link beside the text box.
3. Enter a new password and confirm it as directed.
4. Click **Save**.

## Monitoring Alarms

At the bottom of the window, hover over Alarm Summary or Alarm Browser to see the latest active alarms.

## Launching Help

You can access online help using the following methods:

- Click the question mark icon at the top right of any screen.
- Select **Help > Online Help** from the **Help** menu on the bottom left of any screen.

# Searching

The management console provides a search tool at the top right of the screen. Methods for searching for events and alarms include:

- **Quick Search**—Uses a partial or complete IP address, node name, or node ID.
- **Advanced Search**—Provides filter criteria and allows you to save the search.
- **Saved Search**—Allows you to select from a list of saved searches to invokes an advanced search without having to define the criteria.

## Quick Search

To quickly search for an alarm or event, follow these steps:

1. In the **Search** text box, enter the complete or partial IP address, node name, or node ID.
2. Press **Enter**. The search results display the matching item type, the number of items that match your search parameter, and links to the list of matching results.
3. Click **View List** to view the alarms from the **Alarms and Events** pages.

## Advanced Search

To perform a more specific search for an alarm in the management console, follow these steps:

1. Click **Advanced Search** from the search tool menu.
2. In the **New Search** dialog, select a category from the **Search Category** drop-down list.
3. Select the applicable filters or parameters for your search.
   **Note**: Search parameters change depending on the category you select.
4. To search for acknowledged or unacknowledged alarms, select the **Acknowledged State** check box, and select **Acknowledged** or **Unacknowledged** from the drop-down list.
5. To search for alarms with a specific assigned status, select the **Assigned State** check box and select **Assigned**, **Unassigned**, or **Owner Name** from the drop-down list. If you selected Owner Name, enter the name of the alarm owner in the **Enter Owner Name** field.
6. To save this search, select the **Save Search** check box and enter a unique name for the search in the text box.
7. Click **Go**. The results page appears.

## Saved Search

To access and run a saved search, follow these steps:

1. Click **Saved Search** from the search tool menu.
2. Choose a category from the **Search Category** drop-down list.
3. Choose a saved search from the **Saved Search List** drop-down list.
4. If necessary, change the current parameters for the saved search.
5. Click **Go**. The results page appears.

**Note**: Saved searches apply only to the current partition.

# Monitoring Alarms and Events

The Alarms and Events page can be accessed from **Operate > Alarms & Events**.

You can adjust the default view by selecting filter criteria from the **Show** drop-down menu.

Custom filters can be defined and saved. For pattern searches, the underscore character (_) is reserved to match against any character.

**Note**: Alarms and Events are loaded into pages part by part to improve the application performance. When you scroll down the page, the next set of data is retrieved and shown.

## Understanding Alarms

An alarm is a Cisco VCS response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), Cisco VCS raises an alarm until the resulting condition no longer occurs.

One or more events can result in a single alarm being raised. An alarm is created in the following sequence:

1. A notification is triggered when a fault occurs in the network.
2. An event is created, based on the notification.
3. An alarm is created after checking if there is no active alarm corresponding to this event.

An alarm is associated with two types of events:

- Active events: Events that have not been cleared. An alarm remains in this state until the fault is resolved in a network.
- Historical events: Events that have been cleared. An event changes its state to an historical event when the fault is resolved in a network.

After an alarm is cleared, it indicates the end of an alarm life cycle. A cleared alarm can be revived if the same fault reoccurs within a preset period of time. The present period is set to 5 minutes in Cisco VCS.

### Event and Alarm Association

Cisco VCS management console maintains a catalog of events and alarms. The catalog contains the list of events managed by the management console, and the relationship among the events and alarms. Events of different types can be attached to the same alarm type.

When a notification is received:

1. The management console compares an incoming notification against the event and alarm catalog.
2. The management console decides whether an event has to be raised.
3. If an event is raised, the management console decides whether the event triggers a new alarm or associates it to an existing alarm.

A new event is associated with an existing alarm, if the new event triggered is of the same type and occurs on the same source.

For example, an active interface error alarm. The interface error events that occur at the same interface, are all associated to the same alarm.

### Alarm Status

The following are the supported statuses for an alarm:

- Not Acknowledged—When an event triggers a new alarm or an event is associated with an existing alarm.
- Acknowledged—When you acknowledge an alarm, the status changes from New to Acknowledged.
- Cleared—An alarm can be in these statuses:
  - Auto-clear from the node—The fault is resolved on the node and an event is triggered for the same. For example, a node-reachable event clears the node-unreachable event. This in-turn, clears the node-unreachable alarm.
  - Manual-clear from management console users—You can manually clear an active alarm without resolving the fault in the network. A clearing event is triggered and this event clears the alarm.

  If the fault continues to exist in the network, a new event and alarm are created subsequently based on the event notification.

### Event and Alarm Severity

Each event has an assigned severity. Events fall broadly into the following severity categories, each with their associated color in the VCS management console:

- Flagging—Indicates a fault: Critical (red), Major (orange), Minor (yellow), or Warning (sky blue).
- Informational—Info (blue). Some of the Informational events clear the flagging events.

For example, a Link Down event might be assigned a Critical severity, while its corresponding Link Up event will be an Informational severity.

In a sequence of events, the event with the highest severity determines the severity of the alarm.

### Event and Alarm Persisted

All events and alarms, including active and cleared, are persisted in the management console database.

The relationships between the events are retained. The content of the database can be reviewed, using the Alarm and Event Browser pages.

**Note**: Events are stored in the form of the management console event object. The original notification structure of incoming event notifications (trap or syslog) is not maintained.

## Understanding Events

An event is an occurrence or detection of some condition in and around the network. An event is a distinct incident that occurs at a specific point in time. Examples of events include:

- Port status change
- Node reset
- Node becomes unreachable by the management station

An event can also be a:

- Possible symptom of a fault that is an error, failure, or exceptional condition in the network. For example, when a node becomes unreachable, an unreachable event is triggered
- Possible symptom of a fault clearing. For example, when a node state changes from unreachable to reachable, a reachable event is triggered

One or more events may generate an abnormal state or alarm. The alarm can be cleared, but the event remains. You can view the list of events using the Event Browser.

Select **Operate > Alarms & Events**, then click **Events** to access the Events Browser page. The following table lists the details that are displayed in the Event Browser. To get the latest information, click the **Refresh** icon (see Toolbar Icons).

**Event Browser**

| Field | Description |
|---|---|
| Description | Description of the event |
| Source | Affected node IP address |
| Time | Date and time when the event was generated |
| Severity | Event severities include: Critical, Major, Minor, Warning, Clear, Info. Color coded. Click the title to sort the events list by severity (ascending or descending order) |
| Name | |
| Category | Displays the alarm assigned category |

# Working with Alarms

### Acknowledging Alarms

The Acknowledge feature helps eliminate duplicate alarms. If you are continuously receiving an alarm from a particular node, you can stop that node from being counted as an active alarm. If the node generates a new violation on the same criteria, the management console will not create a new alarm. However, if the node violation is created on another criteria, a new alarm is created. Also, no emails are generated for these alarms after you have marked them as acknowledged.

To manage the rules for displaying alarms and generating associated emails, go to the **Administration > Settings > Alarms & Events** page to select your preferences.

### Changing Alarm Status

1. Select **Operate > Alarms & Events**.
2. Select the alarms for whose status you want to change, then click **Change Status**.
3. Select a status from the following options that applies to all of the items you have selected:
   - **Acknowledge**—This option pertains only to alarms with a current status of Not Acknowledged. When you select this option, the status for the selected items changes to Acknowledged.
   - **Unacknowledge**—This option pertains only to alarms with a current status of Acknowledged. When you select this option, the status for the selected items changes to Not Acknowledged.

- **Clear**—This option can be applied to alarms with a status of either Acknowledged or Not Acknowledged. When you request to clear an alarm, you are prompted to confirm the action.

4 To view the details of an alarm, click the pointer icon associated an alarm.

**Note**: Status can also be entered from the details view by clicking the Change Status icon in the General Info window.

### Assigning an Alarm

1 Select **Operate > Alarms & Events**.

2 Select the alarms you want to assign, then click **Assign**.

3 Select an action from the following options:

- **Assign to me**—This option assigns all of the selected alarms to the user currently logged in. The Owner column displays the user ID of the new owner.
- **Select Owner**—This option prompts you to select an owner from a list of users, and to provide the user's name and email address. An option is provided to send an email to the user when the assignment is made. When the user information is submitted, all selected alarms are assigned to that user. The Owner column displays the user ID of the new owner.
- **Unassign**—This option removes the Owner information from all selected alarms. The Owner column appears empty.

4 To view the details of an alarm, click the pointer icon associated an alarm.

**Note**: Assignments can also be entered from the details view by clicking the Assignments icon in the General Info window.

### Using the Annotation Feature

Use the annotation feature to add comments to the alarm details.

1 Select **Operate > Alarms & Events**.

2 Select the alarms you want to assign, then click **Annotation**. A text entry box appears.

3 Type a comment in the text box; then, click **Post**. The comment is added to the details of each alarm selected.

4 To view the details of an alarm, click the pointer icon associated an alarm.

**Note**: Comments can also be entered from the details view by clicking the clipboard icon in the Annotations window.

### Deleting an Alarm

1. Select **Operate > Alarms & Events**.
2. Select the alarms you want to delete, then click **Delete**.
3. When a prompt appears to confirm the action, click **Ok**.

# 2

# Administration

**Introduction**

The Administration area of the management console is where you specify system configuration settings, manage access control, and specify data collection settings.

## In This Chapter

# Defining Users, Roles, and Access

## Permissions for User Groups

The User Groups feature allows you to set permissions for tasks based on user roles.

When you select a group, the permissions associated with that group appear. Each task has a check box option to enable or disable for that group.

## Managing Users

### Adding a New User

You can add a user and assign predefined static roles. Besides complete access, you can give administrative access with differentiated privileges to certain user groups. The management console supports external user authentication using these access restrictions and authenticates the users against the TACACS+ and RADIUS servers.

1. Select **Administration > Users, Roles & AAA**, then click **Users**.
2. From the sidebar menu, click **Users**.
3. From the command tool drop-down menu, select **Add User**, then click **Go**.
4. Enter the username and password for the new user.
   **Note**: Entries are case sensitive. The password must contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits and special characters.
5. Select the groups applicable for this user.
   **Note**: Use the scroll bar view all of the user groups.
6. Click **Save**, and then **OK**.

From the **User Groups** view, you can verify that the user has been added to the groups intended.

1. Click **User Groups** from the left sidebar menu. The default groups are displayed with the members listed for each.
2. Verify that the username for the new user appears in the appropriate groups.

### Resetting and Changing the Password

As an administrator, you can reset the password for other users. You cannot reset your own password. You must use the Change Password option to reset your password,

To reset the password for the other users:

1. Select **Administration > Users, Roles & AAA**, then click **Users**.
2. Click on the username for the user whose password you want to change.

3 Enter a new password and confirm in, then click:
   - **Save** to save your changes.
   - **Cancel** to exit without saving your changes.

To reset your own password:

1 Click **Change Password**.
2 Enter the old password, new password and confirm password.
3 Click **Save** to save your changes. A confirmation message appears.

### Deleting Users

As an administrator, you can delete users from the database.

You cannot delete the web client default administrator admin.

To delete users:

1 Select **Administration > Users, Roles & AAA**, then click **Users**.
2 From the drop-down menu in the upper right, select the user you want to delete, select **Delete User(s)**, then click **Go**. A message appears to confirm the deletion.
3 Click **OK**. The users are removed from the User Management page. If there are any jobs scheduled in the deleted user's name, the job will continue to run until the job is cancelled.

### Default User Groups

Cisco VCS management console has the following predefined groups with the following default privileges:

- AM-Mgr—Allows users to perform tasks on Alert Manager functionality in the VCS platform.
- Event-Mgr—Allows users to configure and perform tasks on Event functionality in the VCS platform.
- Admin—Allows users to monitor and configure management console operations and perform all system administration tasks except administering management console user accounts and passwords.

  **Note**: If you choose admin account and log in as such on the controller, you can also see the guest users under Local Net Admin.
- SuperUsers—Allows users to monitor and configure management console operations and perform all system administration tasks including administering management console user accounts and passwords. Superusers tasks can be changed.
- Message-infra-Mgr—Allows user to configure the Message Infrastructure related functionality.

- Platform-Mgr—Allows users to configure the platform services in the VCS platform.
- Resource-Mgr—Allows users to configure the resources in the VCS platform.
- Root—Allows users to monitor and configure management console operations and perform all system administration tasks including changing any passwords. Only one user can be assigned to this group and is determined upon installation. It cannot be removed from the system, and no task changes can be made for this user.
- Client-Directory-Mgr—Allows users to configure the client directory in the VCS platform.
- EPM-Mgr—Allows users to configure the end point management in the VCS platform.

### Modifying User Group Permissions

1. Select **Administration > Users, Roles & AAA**, then click **User Groups**.
2. Click on the group name for the user group you want to modify. The Group Detail page appears listing the group's permitted operations.
3. Make any desired changes by selecting or deselecting the appropriate check boxes for task permissions and members.

   **Note**: Any changes you make will affect all members of this user group.
4. Click:
   - **Submit** to save and apply your changes.
   - **Cancel** to exit without saving your changes.

## Changing User Passwords

To change the password for a user:

1. Choose **Administration > Users, Roles & AAA**, then click **Users**.
2. Select the user name whose password you want to change.
3. Complete password fields, then click **Save**.

## Changing User Privileges

The management console uses a list of tasks to control which area of the management console users can access and the functions they can perform in those areas. You change user privileges by changing the User Group to which each user belongs. You use the User Group Task List to change what users in each group are authorized to do and the screens they can access.

To edit the task list for a user group:

1. Choose **Administration > Users, Roles & AAA**, then click **User Groups**.

2 Click on a group name to change the tasks this group is allowed to perform.

3 Click the **Members** tab to view the users of this group.

## Changing Password Policy

The management console supports various password policy controls, such as minimum length, repeated characters, etc.

To change password policies:

1 Choose **Administration > Users, Roles & AAA**, then click **Local Password Policy**.

2 Choose the necessary policies, then click **Save**.

## Setting the AAA Mode

CMC supports local as well as TACACS+ and RADIUS, but you must specify a TACACS+ or RADIUS server first.

To specify a TACACS+ server and then change the AAA mode to TACACS+:

1 Choose **Administration > Users, Roles & AAA**, then click **TACACS+**.

2 From the command pull-down menu, choose **Add TACACS+ Server**, then click **Go**.

3 Enter the TACACS+ server parameters, then click **Save**.

4 Click **AAA Mode**.

5 Select TACACS+ and specify whether to enable fallback to the local condition.

6 Click **Save**.

## Auditing Access

The management console maintains an audit record of user access.

To access the audit trail for a user or user's active sessions:

1 Choose **Administration > Users, Roles & AAA**, then click **Active Sessions**.

2 Click the **Audit Trail** icon to for the username for which you want to see the following data:

- User—User login name
- Operation—Type of operation audited
- Time—Time operation was audited

- Status—Success or failure
- Configuration Changes—This field provides a Details link if there are any configuration changes. Click on the Details link for more information on the configuration changes done by an individual user.

**Note**: The audit trail entries could be logged for individual node changes.

To access the audit trail for a user group:

1. Choose Administration > Users, Roles & AAA, then click User Groups.
2. Click the Audit Trail icon to for the username for which you want to see the following data:
   - User—User login name
   - Operation—Type of operation audited
   - Time—Time operation was audited
   - Status—Success or failure
   - Configuration Changes—This field provides a Details link if there are any configuration changes. Click on the Details link for more information on the configuration changes done by an individual user.

   **Note**: The audit trail entries could be logged for individual node changes.

## Viewing Audit Logs

The management console provides application audit logs, which log events that pertain to VCS features. For example, you can view the application audit log to see when a particular user logged in and what actions were taken.

1. Choose **Administration > Audit Logs**.
2. Click the **Application Audit** tab.

   **Note**: For Application Audit, the User Group column is blank for TACACS+/RADIUS users.
3. To view details about the log, click to expand the row for which you want to view details.

## Adding a TACACS+ Server

To configure the management console so it can communicate with the TACACS+ server:

1. Choose **Administration > Users, Roles & AAA**, then click **TACACS+**.
2. From the dropdown menu in the upper right, select **Add TACACS+ Server**, and then click **Go**.

3 Enter the TACACS+ server information, then click **Save**.

**Note**: For the management console to communicate with the TACACS+ server, the shared secret you enter on this page must match the shared secret configured on the TACACS+ server.

The CHAP based authentication is not supported with Cisco Secure ACS 5.2 and lower versions in TACACS+. Hence setting CHAP as authentication type with Cisco Secure ACS 5.2 and lower version will lead to authentication failure to the management console.

## Deleting a TACACS+ Server

Complete the steps below to remove a TACACS+ server from the management console:

1 Choose **Administration > Users, Roles & AAA**, then click **TACACS+**.

2 Select the server or servers that you want to delete.

3 From the dropdown menu in the upper right, select **Delete TACACS+ Server(s)**, and then click **Go**.

4 Click **OK** to confirm that you want to delete the server. The server is removed from the management console.

## Adding a RADIUS Server

To configure the management console so it can communicate with the RADIUS server:

1 Choose **Administration > Users, Roles & AAA**, then click **RADIUS Servers**.

2 From the drop-down menu in the upper right, select **Add RADIUS Server**, and then click **Go**.

3 Enter the RADIUS server information, then click **Save**.

**Note**: For the management console to communicate with the RADIUS server, the shared secret you enter on this page must match the shared secret configured on the RADIUS server.

## Deleting a RADIUS Server

Complete the steps below to remove a RADIUS server from the management console:

1 Choose **Administration > Users, Roles & AAA**, then click **RADIUS**.

2 Select the server or servers that you want to delete.

3 From the drop-down menu in the upper right, select **Delete RADIUS Server(s)**, and then click **Go**.

4 Click **OK** to confirm that you want to delete the server. The server is removed from the management console.

## SFTP User Account

An SFTP user account has already been added to the management console. To remove this account:

1 Choose **Administration > Users, Roles & AAA**, then click **SFTP User Account**.

2 Click **Delete**.

## Service Account

A service account has already been added to the management console. To modify this account:

1 Choose **Administration > Users, Roles & AAA**, then click **Service Account**.

2 Click the radio button for the existing service account.

3 Click **Modify**.

4 Enter the password to validate this change, then click **OK**.

# Log File Configuration and Settings

1. Select **Administration > Logging**. The General Logging Options Screen appears.
2. Select an option for **Message Level**:
   - Error
   - Information
   - Trace
3. Select the check boxes within the Enable Log Module option to enable various administration modules:
   - **Log Modules**—Select this option to select all the modules.
   - **SNMP**—Captures logs for all SNMP communication between the management console and controllers.
   - **AAA**—Captures AAA related logs for the management console.
   - **Admin**—Contains Administration based logs, where all the configuration changes performed using the administration console is logged.
   - **Database**—Contains logs to debug important database-related operations in the management console.
   - **Faults**—Used by the event and alert subsystem.
   - **GUI**—Contains generic UI validation logs.
   - **Inventory**—Captures all Inventory-related logs.
   - **System**—Captures all System-related logs.
4. In the **Log File Settings** portion, enter the following settings. These settings will be effective after restarting the management console.
   - **Max. file size**—Maximum number of MBs allowed per log file.
   - **Number of files**—Maximum number of log files allowed.
   - **File prefix**—Log file prefix, which can include the characters "%g" to sequentially number of files.
5. Click the **Download** button to download the Log File to your local machine.

   **Note**: The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the zip file is an html file that documents the log files.
6. Click **Save**.

# Managing the Management Console

Within the Settings page, you can change the management console settings such as Alarms, Login disclaimer, Mail server Configuration, Notification receivers, and Audit Log Purge settings.

## Setting Alarms

You can specify clean-up options, display options, and email options for alarms by following these steps:

1 Select Administration > Settings, then click Alarms and Events.

2 Add or modify the necessary alarms parameters, then click **Save**.

**Notes**:

- Data cleanup tasks run nightly to delete old alarms. In addition to the data cleanup task, The management console has an hourly task to check alarm table size. When the alarm table size exceeds 300 K, the task deletes the oldest cleared alarms until the alarm table size is within 300 K.
- The Alarm Display Options apply to the Alarm Summary page only. Quick searches or alarms for any entity display all alarms regardless of the acknowledged or assigned state.
- E-mails are not generated for acknowledged alarms regardless of severity change.

## Setting Login Disclaimer

You can enter disclaimer text at the top of the Login page for all users.

1 Select **Administration** > Settings, then click **Login Disclaimer**.

2 Enter your Login Disclaimer text in the available text box, then click **Save**.

## Setting Mail Server Configuration

You can configure global e-mail parameters for sending e-mails from management console reports and alarm notifications. You can set the primary and secondary SMTP server host and port, the sender's e-mail address, and the recipient's e-mail addresses.

You must configure the global SMTP server before setting global e-mail parameters.

1 Select **Administration** > **Settings**, then click Mail Server Configuration.

2 Enter the necessary parameters.

**Notes**:

- The From text box in the Sender and Receivers portion of the page is populated with CMC@<CMC server IP address>. You can change it to a different sender.
- The e-mail address you enter serves as the default value for other functional areas, such as alarms or reports. However, changes you make to the recipient e-mail addresses are disregarded if e-mail notifications were set.

3 Click the **Configure email notification for individual alarm categories** link to specify the alarm categories and severity levels you want to enable. Email notifications are sent when an alarm occurs that matches categories and the severity levels you select.

4 Click the **Test** button to send a test e-mail using the parameters you configured. The test feature checks the connectivity to both primary and secondary mail servers by sending a test email.

5 If the test results were satisfactory, click **Save**.

## Setting Notification Receivers

You can view current or add additional notification receivers. Alerts and events are sent as SNMPv2 notifications to configured notification receivers.

1 Select **Administration > Settings**, then click **Notification Receivers**.

2 Select one of the following commands, then click **Go**:

- Add Notification Receiver
- Add EPM Notification Receiver
- Remove Notification Receiver

**Notes**:

- If you are adding a notification receiver with the notification type UDP, the receiver you add should be listening to UDP on the same port on which it is configured.
- If you are adding an EPM notification receiver, all the traps processed will be forwarded in EPM format to the destination.
- By default only Critical level events are processed as alarms of selected category.
- SNMPv1 traps are considered for Non EPM and both SNMPv1 and SNMPv2 traps are considered for EPM northbound notification.

3 Click **Save** or **Cancel**.

## Audit Log Purge Settings

You can define how long to keep logs before the system moves them to the trash or to a directory of your choosing.

1. Select **Administration > Settings**, then click **Audit Log Purge Settings**.
2. Click in the **Keep logs younger than days** field and enter the number of days that you want the system to keep logs before purging them.
3. To send logs to the trash after the specified number of days has passed, click the **Trash** radio button, or to send logs to a specific directory after the specified number of days has passed, click the **Directory** radio button and enter the directory path in the Directory field. For example, you might enter /opt/CSCOcmc/conf/ifm/ in the Directory field.
4. Click **Save**.

## Monitor Nodes from the Dashboard

You can view the status of nodes.

1. Select **Operate > Monitoring Dashboard**, then click **Overview**. The Videoscape Control Suite Nodes list window opens and lists all nodes set up in the management console.

   The high-level information provided in the list includes the information below:

   - **Node ID**
   - **Node State**
   - **Node Name**
   - **IP Address**
   - **Memory Usage %**
   - **Disk Usage %**
   - **CPU Utilization %**
   - **RAM Size(KB)**
   - **Disk Size (KB)**
   - **SysUpTime**
   - **Platform Version**
   - **Message Infra Version**

# 3

# Message Infrastructure

This chapter describes how to use the Msginfra Deployment option to deploy VCS on a single service node and on multiple service nodes.

## In This Chapter

# Deployment

From the Deployment menu item, you can access the Msginfra Deployment option. This option allows you to deploy VCS on a single service node and on multiple service nodes.

## Deploy Msginfra on a Single Service Node

1. Select **Message Infrastructure > Msginfra Deployment**, then click **Cluster Deploy**.
2. Click **Single Msginfra Mode** and then click **Next**. The Single Msginfra Node Deployment window opens.
3. Enter the **Service Domain Name**, **Client Domain Name**, **Pubsub Domain**, and click **Deploy**. The window closes and the Msginfra Deployment window appears with updated Deploy statuses.

   **Notes:**

   - Each field accepts alpha-numeric characters and some special characters with a character length from 4 to 32 characters.
   - The first and last characters must be alphanumeric characters.

## Deploy Msginfra on Multiple Service Nodes

1. Select **Message Infrastructure > Msginfra Deployment**, then click **Cluster Deploy**.
2. Click **Multiple Msginfra Nodes** and then click **Next**. The Multiple Msginfra Nodes Deployment window opens.
3. From the Available Nodes list, select the node you want to deploy as an Msginfra Node and click **Add**. The node moves to the Selected Node list.

   Note: The IP will be set on the Eth4 node. To change this, clear the Use Node IP for Router checkbox. Only IPv4 is supported.
4. Click **Next** to select the Service Connection Manager nodes.
5. From the Available Nodes list, select the node you want to deploy as a Service Connection Manager Node and click **Add**. The node moves to the Selected Node list.

   **Note:** The IP will be set on the Eth4 node. To change this, clear the **Use Router IP** checkbox. Only IPv4 is supported.
6. Click **Next** to select the Service Session Manager nodes.
7. Click in the **Domain Name** field and enter a name for the Service Session Manager domain name.

8 From the Available Nodes list, select the node you want to deploy as a Service Session Manager Node and click **Add**. The node moves to the Selected Node list.

**Note**: If Enable HA is selected, make certain that you have an even number of nodes in the Selected Nodes list.

9 Click **Next** to select the Client Connection Manager Nodes.

10 From the Available Nodes list, select the node you want to deploy as a Client Connection Manager Node and click **Add**. The node moves to the Selected Node list.

**Notes**:

- The IP will be set on the Eth4 node. To change this, clear the **Use Router IP for CM** checkbox.
- Client Connection Manager supports IPv4 and IPv6. The default is IPv4. To use IPv6, select **Use IPv6**.
- To set the Client Connection Manager router to use different IP sections, select **Use Specific IP for Router**. This feature supports only IPv4.

11 Click **Next** to select Client Session Manager nodes.

12 Click in the **Domain Name** field and enter a name for the Client Session Manager domain name.

13 From the Available Nodes list, select the node you want to deploy as a Client Session Manager Node and click **Add**. The node moves to the Selected Node list.

**Note**: If **Enable HA** is selected, make certain that you have an even number of nodes in the Selected Nodes list.

14 Click **Next** to set the Pubsub domain name.

15 Click in the **Pubsub Domain Name** field and enter a name for the Pubsub domain.

16 Click **Next** to view the Overview nodes configuration details window, which shows a summary of the nodes you have configured.

17 Click **Deploy**. The Overview nodes configuration details window closes and the Msginfra Deployment window appears with updated Deploy statuses.

# Message Fabric

From the Deployment menu item you can access the Msginfra Deployment option.

## Node/Router/Component

To view the Node/Router/Component main page, click **Message Infrastructure > Node/Router/Component**.

### Node List

The Node/Router/Component page displays the Node List, which includes all nodes setup in the management console.

The high-level information provided in the list includes the information below:

- **Node Name**—The name of the node is created manually during setup.
- **Node State**—The state of the node can be **Running**, **Offline**, or **Unknown**.
- **Node Type**—The type of the node can be **Management**, **Service,** or **Infra**.

#### Refresh List

The node list will automatically refresh every 30 seconds, or, you can click the refresh button to immediately refresh the list.

#### Node Details

Click the radio button for a node to view the router list and details for a specific node. You can then select an item under Router Realms to enable the task options, such as **Update XCP Access IP**. See the ***Router List*** (on page 32) section for more information.

### Router List

The Router List includes all routers for a selected node. Complete the steps below to view the routers associated with a specific node.

1. Click the radio button or the row of the node desired. All routers of the selected node will appear. The router list will be automatically refreshed every 30 seconds.
2. Click the **Refresh** button to refresh the router list immediately. The details provided in the list include the information below:
   - **Router Realm**—Indicates the router realm name.
   - **Router State**—Values can be **Running**, **Offline**, **Failure**, Adding, Unknown
     - Running

- Offline
- Adding — Indicates the router is in the install progress
- Failure — Indicates that the router encountered an error during installation.

– **Router Failure Reason** — Values can be:

- Realm conflicted
- IP address conflicted
- Provision mismatch
- BOOT failure
- Redundant router
- Adding timeout failure
- Unknown

**Note**: If the Router State is not Failure, the Router Failure Reason field will be empty.

– **Router Type** — Values can be **BOOT**, **NONE-HA**, or **HA**.

– **HA State** — This field is only applicable when the Router Type supports high-availability (HA). Values can be **Active** or **Standby**.

– **HA Switch Mode** — This field is only applicable when the Router Type is HA. Values can be **Auto** or **Manual**.

– **Router IP** — The field shows the IP address of the router.

– **Router Port** — This field shows the router port number.

– **Administration IP** — This field shows the administration IP address.

– **Administration Port** — This field shows the administration port number.

– **Router Software** — This field shows the version of software installed on the router.

### Remove Node

Complete the steps below to remove a node.

**Note**: A node must be offline to be removed.

1 Select the offline node you want to remove from the node list.

2 Click the **Remove** button.

3 Click **Ok** when the confirmation message appears. When the operation is complete, a message indicating success appears at the right bottom screen. Click the **X** to close the window or wait 15 seconds for it to close automatically. If an error occurs during the operation, an error message will appear at the top of the window.

### Add Router

Complete the steps below to add a router to a node.

**Note**: The Router Type must be NONE-HA to add router.

1 Select the node where the router is to be added; then, click the **Add** button.

2 Follow the guidelines provided to enter values for the fields below:

- **Realm**—Enter a value that is unique within the whole cluster. Only alphanumeric and the dash (-) characters are acceptable; however, do not use a dash (-) for the first or last character in the value. The length must be 4 to 32 characters.
- **Router Multi-Accept-IO IP**—Enter the host IP address.

  **Notes**:

  – The Router Multi-Accept-IO IP and the associated Router Multi-Accept IO Port must be unique in the cluster.

  – The Router Multi-Accept-IO IP associated with the Administration Port should be unique in the cluster.
- **Router Multi-Accept IO Port**—Enter the host port. The valid range is 1025-60000. The default is 7400.
- **Administration IP**—Enter the IP address of the XCP web controller to be used. The router XCP Access IP address is used as the redirect IP address of the current router's web controller.
- **Administration Port**—Enter the port that XCP web controller "listens to." The valid range is 1025-60000. The default is 7300.

3 Click the **Save** button. When the operation is complete, a message indicating success appears at the right bottom screen. Click the **X** to close the window or wait 15 seconds for it to close automatically. If an error occurs during the operation, an error message will appear at the top of the window.

**Notes**:

- All fields must contain values for the **Save** button to be enabled.
- The **Reset** button clears unsaved values from the fields.
- The **Back** button returns to the Router List page.

### Remove Router

Complete the steps below to remove a router.

**Note**: A router must be in an offline or failure state to be removed.

1. From the Router List, select the router to be removed; then, click the **Remove** button.
2. Click **Ok** when the confirmation message appears. When the operation is complete, a message indicating success appears at the right bottom screen. Click the **X** to close the window or wait 15 seconds for it to close automatically. If an error occurs during the operation, an error message will appear at the top of the window.

### Stop Router

Complete the steps below to perform the Stop operation for a router.

**Notes**:

- Two methods of stop are supported, **Gracefully stop** and **Force stop**. The Gracefully stop option invokes the normal stop progress. The Force stop option interrupts any running processes to expedite the stop operation.
- The stop operation is applicable only to routers that are in a Running state.

1. From the Router List, select the router to be stopped; then, click **Stop** and select **Gracefully Stop** or **Force Stop**.
2. Click **Ok** when the confirmation message appears. When the operation is complete, a message indicating success appears at the right bottom screen. Click the **X** to close the window or wait 15 seconds for it to close automatically. If an error occurs during the operation, an error message will appear at the top of the window.

**Note**: If the success message appears, the stopped router state may not immediately change to offline. Click the refresh button or waiting for the next automatic refresh for the router state to change to offline.

### Start Router

To perform the start operation for a router, select the router to be started from the Router List; then, click the **Start** button.

**Notes**:

- The start operation is applicable only to routers that are in an offline or bootfailure state.
- If the success message appears, the router state may not immediately change to running. Click the refresh button or waiting for the next automatic refresh for the router state to change to running.

### Update XCP Access IP

Complete the steps below to update the XCP Access IP address associated with the router.

1. From the Router List, select the router to be updated; then, click the **Update XCP Access IP** button.
2. Enter the correct IP address.
3. Click the **Save** button. When the operation is complete, a message indicating success appears at the right bottom screen. Click the **X** to close the window or wait 15 seconds for it to close automatically. If an error occurs during the operation, an error message will appear at the top of the window.

   **Notes**:

   - All fields must contain values for the **Save** button to be enabled.
   - The **Reset** button clears unsaved values from the fields.
   - The **Back** button returns to the Router List page.

### XCP Web Controller

Complete the steps below to access the Extensible Communications Platform (XCP) Web controller to configure and view the current state of your XCP server.

1. From the Router List, select the router to be updated; then, click the **XCP Web Controller** button.
2. Click **Enter the XCP Controller now**. For information on how to use the XCP Controller, refer to one of the following documents:

   - Videoscape Control Suite Operators XCP User Guide (part number OL-29289)
   - COP Files for Cisco Videoscape Control Suite Services Installation Guide (part number OL-27753)

### Switch HA Mode

Complete the steps below to change the HA mode of a router.

1 From the Router List, select the router to be updated; then, click the **Switch HA Mode** drop-down menu.

**Note**: The Router Type for the router must be **HA** for the **Switch HA Mode** drop-down menu to be enabled.

2 Select the appropriate mode:

- **Auto**—This setting enables the system to switch traffic between paired routers. The paired routers are in different nodes within the same realm.
- **Manual**—The setting requires an operator to manually switch routers.

When the operation is complete, a message indicating success appears at the right bottom screen. Click the **X** to close the window or wait 15 seconds for it to close automatically. If an error occurs during the operation, an error message will appear at the top of the window.

### Switch Standby Router

Complete the steps below to change the HA mode of a router.

1 From the Router List, select the router to be updated.

**Note**: To enable the Switch Standby Mode button, the following fields must be set to the values below for the router selected:

- Router Type: **HA**
- HA State: **Standby**
- HA Switch Mode: **Manual**

2 Click the **Switch Standby Mode** button. When the operation is complete, a message indicating success appears at the right bottom screen. Click the **X** to close the window or wait 15 seconds for it to close automatically. If an error occurs during the operation, an error message will appear at the top of the window.

### Component List

1 From the Router List , select a router; then, click the **Component List** button. The Component List page appears.

**Note**: If the router status is Offline or Failure, the component fields display Offline. If the router status is Unknown, the fields are empty.

2 Click the **Back** button to return to the previous Node list and Router List page.

# Publish Subscribe

To view the Publish Subscribe page, click **Message Infrastructure > Publish Subscribe**.

### Pubsub Service List

The PubSub Service List appears on the Publish Subscribe page. The list refreshes automatically every 30 seconds.

### Pubsub Node List

Complete the steps below to view the Pubsub Node List for an existing pubsub service.

1. Click **Message Infrastructure > Publish Subscribe**.
2. Select the pubsub service from the PubSub Service List. The Pubsub Node List appears below the PubSub Service List.
3. If necessary, use the filter options to find the pubsub node desired.

### Add Pubsub Node

Complete the steps below to add a pubsub node.

1. Click **Message Infrastructure > Publish Subscribe**.
2. If necessary, use the filter options to find the pubsub service desired.
3. Select the pubsub service from the PubSub Service List. The Pubsub Node List appears below the PubSub Service List.
4. Click **Add**. The Add Pubsub Node page appears.
5. Provide values for the required fields, indicated by asterisk (*).

   **Note**: Click the help icon (**?**) by each field to see the current rules for that parameter.
6. Enter information, if desired, into the optional fields.
7. Click **Save** to complete the add operation, or, click **Reset** to clear the fields.
8. Click **Back** to return to the Publish Subscribe page. The new node will appear in the Pubsub Node List on the Publish Subscribe page next time you select that pubsub service.

### Edit Pubsub Node

Complete the steps below to edit a pubsub node.

1. Click **Message Infrastructure > Publish Subscribe**.
2. If necessary, use the filter options to find the pubsub service desired.
3. Select the pubsub service from the PubSub Service List. The Pubsub Node List appears below the PubSub Service List.
4. Select a pubsub node.
5. Click **Edit**. The Edit Pubsub Node page appears.
6. Update the values as needed.

   **Note**: Neither the node name nor the multicast node can be changed.
7. Click **Save** to complete the edit operation, or, click **Reset** to clear the fields.
8. Click **Back** to return to the Pubsub Management page.

### Remove Pubsub Node

Complete the steps below to remove a pubsub node.

1. Click **Message Infrastructure > Publish Subscribe**.
2. If necessary, use the filter options to find the pubsub service desired.
3. Select the pubsub service from the PubSub Service List. The Pubsub Node List appears below the PubSub Service List.
4. Select a pubsub node.
5. Click **Remove**. The pubsub node is removed.

### Subscription List

Complete the steps below to manage a subscription list for a pubsub node.

1. Click **Message Infrastructure > Publish Subscribe**.
2. If necessary, use the filter options to find the pubsub service desired.
3. Select the pubsub service from the PubSub Service List. The Pubsub Node List appears below the PubSub Service List.
4. Select a pubsub node.
5. Click **Subscription List**. The Subscription page appears.
6. Select a subscription list and then invoke one of the operations.
   - **Edit Subscription List**—The Edit Subscription page appears. Continue with step 7.
   - **Unsubscribe**—The items selected are removed from the list.

     **Note**: You select multiple subscriptions to remove them in a single operation.
   - **Back**—The Pubsub Service List appears.

7 Provide values for all fields.

**Note**: Click the help icon (**?**) by each field to see the current rules for that parameter.

8 Click the **Add** to move to add the subscription to the Modified Subscription List field.

9 Repeat steps 7 and 8 to build the subscription list. The **Remove** option allows you to remove items from the Modified Subscription List field.

10 Click **Save** to complete the edit operation.

11 Click **Back** to return to the Subscription List page.

### Affiliation List

Complete the steps below to manage an affiliation list for a pubsub node.

1 Click **Message Infrastructure > Publish Subscribe**.

2 If necessary, use the filter options to find the pubsub service desired.

3 Select the pubsub service from the PubSub Service List. The Pubsub Node List appears below the PubSub Service List.

4 Select a pubsub node.

5 Click **Affiliation List**. The Affiliation page appears.

6 Select an affiliation list and then invoke one of the operations.

- **Edit Affiliation List**—The Edit Subscription page appears. Continue with step 7.
- **Remove**—The items selected are removed from the list.

  **Note**: You select multiple affiliations to remove them in a single operation.
- **Back**—The Pubsub Service List appears.

7 Provide values for all fields.

**Note**: Click the help icon (**?**) by each field to see the current rules for that parameter.

8 Click the **Add** to move to add the affiliation to the Modified Affiliation List field.

9 Repeat steps 7 and 8 to build the affiliation list. The **Remove** option allows you to remove items from the Modified Affiliation List field.

10 Click **Save** to complete the edit operation.

11 Click **Back** to return to the Affiliation List page.

# Account JID

To view the Account JID page, click **Message Infrastructure > Account (JID)**.

### Add User JID

Complete the steps below to add a new user ID.

1. Click **Message Infrastructure >Account (JID)**.
2. Click **Add**.
3. Provide values for all fields.

   **Note**: Click the help icon (**?**) by each field to see the current rules for that parameter.
4. Click **Save** to complete the add operation, or click **Reset** to clear the fields.
5. Click **Back** to return to the Service Instance Management page. The service instance will appear in the Service Instance List on the Service Instance Management page.

### Remove User JID

Complete the steps below to remove an existing User JID.

1. Click **Message Infrastructure > Account (JID)**.
2. If necessary, use the filter options to find the User JID you need to remove.
3. Select the User JID from the User JID List.
4. Click **Remove**. The User JID is removed.

# Service Infrastructure

From the Message Infrastructure menu, you can access the Service Infrastructure options. These options allow you to manage virtual services and service instances.

## Virtual Service

To view the Virtual Service page, click **Message Infrastructure > Virtual Service**.

### Virtual Service List

The Virtual Service page displays a list of current virtual services and allows the user to create, edit, or remove virtual services.

### Virtual Service List Filter

1. In the upper right corner of the Virtual Service page, select **Quick Filter** to display the following filter options:
   - **Namespace**
   - **Name**
   - **Category**
   - **Access Point**
   - **Admin User**
2. Enter partial or complete information in one or more of the fields. The results are returned automatically.

### Create Dynamic Virtual Service

Complete the steps below to add a new dynamic virtual service.

1. Click **Message Infrastructure > Virtual Service**.
2. Click **Create Dynamic VS**.
3. Provide values for the following required fields.

   **Note**: Click the help icon (**?**) by each field to see the current rules for that parameter.
   - **Category**—Select **HTTP**, **HTTPS**, **RMI**, or **XMPP**.
   - **Name**—Enter a unique value.
   - **Namespace**—Enter a unique value.
   - **Admin State**—Select **Enable** or **Disable**.
   - **KeepAlive Interval**—Enter a value from 1 through 30.

4 Enter information, if desired, into the following optional fields.
   - **Algorithm**—Select **hash_from**, **roundrobin**, or **consistent_hash_from**.
   - **Admin JID**—Enter a value if you want the client to be able to discover that status of the selected instances for this virtual service.
   - **Access Point**—Enter a unique value that begins with a character or digit.
5 Click **Save** to complete the add operation for the new virtual service, or, click **Reset** to clear the fields.
6 Click **Back** to return to the Virtual Service Management page. The virtual service will appear in the Virtual Service List on the Virtual Service Management page.

### Create Static Virtual Service

Complete the steps below to add a new static virtual service.

1 Click **MsgInfra Infrastructure > Virtual Service**.
2 Click **Create Static VS**.
3 Provide values for the following required fields.

   **Note**: Click the help icon (**?**) by each field to see the current rules for that parameter.
   - **Name**—Enter a unique value.
   - **Namespace**—Enter a unique value.
   - **Admin State**—Select **Enable** or **Disable**.
   - **KeepAlive Interval**—Enter a value from 1 through 30.
   - **Algorithm**—Select **hash_from**, **roundrobin**, or **consistent_hash_from**.
4 Enter information, if desired, into the following optional fields.
   - **Admin JID**—Enter a value if you want the client to be able to discover the status of the selected instances for this virtual service.
   - **Access Point**—Enter a unique value that begins with a character or digit.
5 Click **Save** to complete the add operation for the new virtual service, or, click **Reset** to clear the fields.
6 Click **Back** to return to the Virtual Service Management page. The virtual service will appear in the Virtual Service List on the Virtual Service Management page.

### Edit Virtual Service

Complete the steps below to edit an existing virtual service.

1 Click **Message Infrastructure > Virtual Service**.
2 If necessary, use the filter options to find the virtual service you need to edit.
3 Select a virtual service from the Virtual Service List. The Edit, Remove and Modify Admin State operations become active.

4 Click **Edit**. The Edit Virtual Service page appears with the current values pre-populated.

5 Update the values as needed.

6 Click **Save** to complete the edit operation for the virtual service, or, click **Reset** to clear the fields.

7 Click **Back** to return to the Virtual Service Management page.

#### Remove Virtual Service

Complete the steps below to remove an existing virtual service.

1 Click **Message Infrastructure > Virtual Service**.

2 If necessary, use the filter options to find the virtual service you need to remove.

3 Select the virtual service from the Virtual Service List. The Edit, Remove and Modify Admin State operations become active.

4 Click **Remove**. The virtual service is removed.

#### Modify Virtual Service Admin State

Complete the steps below to modify the Admin State of an existing virtual service.

1 Click **Message Infrastructure > Virtual Service**.

2 If necessary, use the filter options to find the virtual service you need to modify.

3 Select a virtual service from the Virtual Service List. The Edit, Remove and Modify Admin State operations become active.

**Note**: If the virtual service is currently Enabled, the Disable Admin State option appears. If the virtual service is currently Disabled, the Enable Admin State option appears.

4 Click **Enable/Disable Admin State**. The Admin State is modified.

#### Show Service Instance List for Selected Virtual Service

Complete the steps below to view a list of the Service Instances for an existing virtual service.

1 Click **Message Infrastructure > Virtual Service**.

2 If necessary, use the filter options to find the virtual service you need to modify.

3 Select a virtual service from the Virtual Service List. The Service Instance List appears below the Virtual Service List.

#### Modify SI Admin State for Selected Virtual Service

Complete the steps below to modify the Admin State of an existing Service Instance.

1 Click **Message Infrastructure > Virtual Service**.

2 If necessary, use the filter options to find the virtual service you need to modify.

3 Select a virtual service from the Virtual Service List. The Service Instance List appears below the Virtual Service List.

4 Select the service instance you would like to change from the list of services.

5 Click **Enable/Disable Admin State**. The Admin State is modified.

### Edit SI for Selected Virtual Service

Complete the steps below to edit the SI of an existing Service Instance.

1 Click **Message Infrastructure > Virtual Service**.

2 If necessary, use the filter options to find the virtual service you need to modify.

3 Select a virtual service from the Virtual Service List. The Service Instance List appears below the Virtual Service List.

4 Select the service instance you want to edit from the Service Instance List.

5 Click **Edit SI**. The SI fields appear.

**Note**: Click the help icon (**?**) by each field to see the current rules for that parameter.

6 Update the editable fields.

7 Click **Save** to save the changes, or click **Back** to cancel the changes and close the Edit SI view.

## Service Instance

To view the Service Instance Management page, click **Message Infrastructure > Service Instance**.

### Service Instance List

The Service Instance Management page displays a list of current service instances and allows the user to create, edit, or remove service instances.

### Service Instance List Filter

1 Use the filter icon on the far right of the Service Instance Management page to display the following filter options:

- **JID**
- **Namespace**
- **AccessPoint**
- **Binding JSM**

2 Enter partial or complete information in one or more of the fields. The results are returned automatically.

### Create SI

Complete the steps below to add a new service instance.

1. Click **Message Infrastructure > Service Instance**.
2. Click **Create SI**.
3. Provide values for all fields.

   **Note**: Click the help icon (**?**) by each field to see the current rules for that parameter.
4. Click **Save** to complete the add operation, or click **Reset** to clear the fields.
5. Click **Back** to return to the Service Instance page. The service instance will appear in the Service Instance List on the Service Instance page.

### Edit SI

Complete the steps below to edit an existing service instance.

**Notes**:

- Only service instances with an Admin State of OOS can be edited.
- The Namespace value for service instances associated with a static virtual service cannot be edited.

1. Click **Message Infrastructure > Service Instance**.
2. If necessary, use the filter options to find the service instance you need to edit.
3. Select a service instance from the Service Instance List. The Edit, Remove and Modify Admin State operations become active.
4. Click **Edit SI**. The Edit SI page appears with the current values pre-populated.
5. Update the values as needed.
6. Click **Save** to complete the edit operation, or, click **Reset** to clear the fields.
7. Click **Back** to return to the Service Instance Management page.

### Remove SI

Complete the steps below to remove an existing virtual service.

**Notes:**

- A service instance must have an Admin State of OOS to be removed.
- If you want to remove the service instance from the system you must also remove the entry from Account JID.

1. Click **Message Infrastructure > Service Instance**.
2. If necessary, use the filter options to find the service instance you need to remove.
3. Select the service instance from the Service Instance List. The Edit, Remove and Modify Admin State operations become active.

4 Click **Remove**. The service instance is removed from the Service Instance List.

5 If you want to remove the service instance from the system database, you must remove the associated User JID by completing the steps below:

   **a** Click **Message Infrastructure >Account JID**.

   **b** If necessary, use the filter options to find the User JID you need to remove.

   **c** Select the User JID from the User JID List.

   **d** Click **Remove**. The User JID is removed.

### Modify SI Admin State

Complete the steps below to modify the Admin State of an existing service instance.

1 Click **Message Infrastructure > Service Instance**.

2 If necessary, use the filter options to find the service instance you need to modify.

3 Select a service instance from the Service Instance List. The Edit SI, Remove, and Modify Admin State operations become active.

   **Note**: If the service instance is currently Enabled, the Disable Admin State option appears. If the service instance is currently Disabled, the Enable Admin State option appears.

4 Click **Enable/Disable Admin State**. The Admin State is modified.

# External SASL Plugin

The Simple Authentication and Security Layer(SASL) component that supports the Cisco Videoscape Control Suite Message Infrastructure product. It also describes how to create and deploy a SASL plug in.

**Note**: SASL software is included in the core Videoscape Control Suite software and does not require separate installation.

## SASL Authentication Framework

The SASL component is the default authentication component in the Conductor system that processes all authentication requests coming from a client via the Connection Manager (CM).

The following steps describe the authentication process:

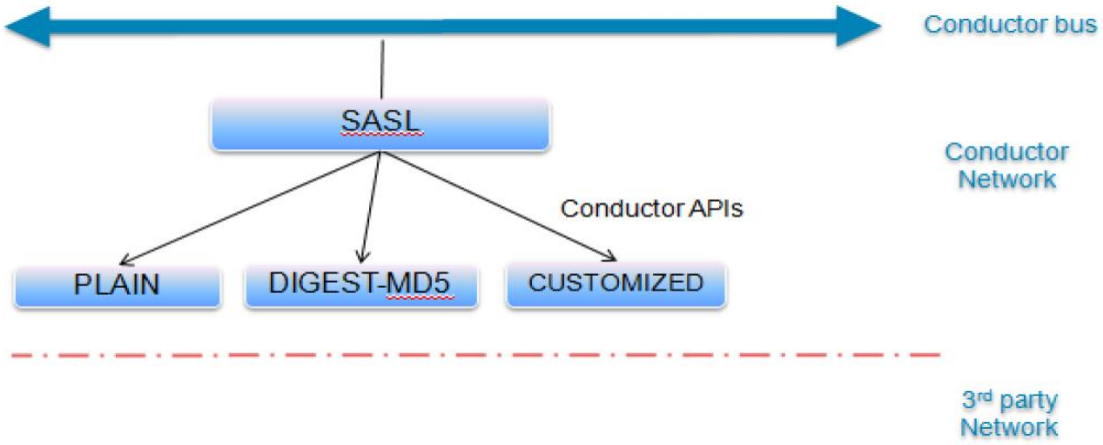
1. CM forwards the authentication request to the SASL component.
2. SASL processes the request and returns a response to CM.
3. CM interprets the response and sends back the result to the client to complete a single iteration.

   **Note**: Multiple iterations can occur to complete the authentication process.
4. After the client has been successfully authenticated, CM sends a request to the Jabber Session Manager (JSM) to create a client session using the client's Jabber ID (JID).

The features of the Conductor authentication framework include:

- Allow multiple mechanisms to co-exist in the single user domain
- Support the PLAIN and DIGEST-MD5 authentication mechanisms in the default installation
- Allow third-party developers to customize mechanisms with Conductor SDK

- Support **Add**, **Remove**, and **Update** functions from the UI management interface




## Set Up Overview

In summary:

1. You should create customized plug-ins by utilizing Conductor SDK APIs.
2. You need to integrate your plug-in into the Conductor system. Conductor SDK comes with a sample plug-in. 'Chapter 2 Quick Start' gives a step-by-step introduction of how to deploy your plug-ins.

## Create and Deploy a SASL Plug-In

This section provides instructions to create a new SASL plug-in from source code and deploy it in the management console.

### About the Sample Plug-In

Videoscape Control Suite Message Infrastructure SASL SDK provides a sample plug-in under conductor_sasl_sdk/sample.

It is a sample implementation of standard PLAIN mechanism defined in RFC4422.

The sample plug-in executes the following process:

1. Decodes the authentication string passed from SASL component
   **Note**: This step of the process uses the Base64 algorithm.
2. Parses the username and password from the decoded string.
3. Retrieves the user's password from the database by user and domain.
4. Validates the password and returns the result of authentication.

### Build the Sample SASL Plug-In

The sample source code can be found in **conductor_sasl_sdk/sample**.

Type **make** to build **sample.so**.

**Example**:

```
$ ls sample

Makefile Mechanism.cpp Mechanism.hpp sample.cpp sample.hpp
SaslContext.cpp SaslContext.hpp

$ make

g++ -m32 -c -o Mechanism.o Mechanism.cpp -O0 -g2 -Wall -fPIC

g++ -m32 -c -o SaslContext.o SaslContext.cpp -O0 -g2 -Wall -fPIC

g++ -m32 -c -o Base64.o Base64.cpp -O0 -g2 -Wall -fPIC

g++ -m32 -c -o sample.o sample.cpp -O0 -g2 -Wall -fPIC

g++ -m32 -o sample.so Mechanism.o SaslContext.o Base64.o sample.o
-O0 -g2 -Wall -fPIC -shared
```

**Note**: The plug-in must support a 32-bit shared library to integrate with the Videoscape Control Suite Message Infrastructure.

### Deploy the Sample SASL Plug-In

Complete the following steps to deploy the sample SASL plug-in using the command line interface (CLI).

1. Import the plug-in from VSOS command line.

   **Example**:

   ```
   admin:file transfer secure-import
   root@172.17.6.32:/tmp/sample.so

   Valid entry

   The authenticity of host '172.17.6.32 (172.17.6.32)' can't be
   established.

   RSA key fingerprint is
   2a:ea:86:df:bc:7c:04:89:28:6a:dd:8a:19:b1:2d:7d.

   Are you sure you want to continue connecting (yes/no)? yes

   Warning: Permanently added '172.17.6.32' (RSA) to the list of
   known hosts.

   root@172.17.6.32's password:

   sample.so
   100%   89KB  89.3KB/s   00:00
   ```

2. Verify the plug-in has been imported.

   **Example**:

   ```
   admin:file list activelog ftpdir
   ```

```
sample.so
dir count = 0, file count = 1
```

3 Follow the steps below to open the XCP Web Controller UI.

   **a** Log in to the CMC Web Portal.

   **b** From the menu bar, select **Message Infrastructure > Infrastructure Management**.

   **c** Select one service node from the node list; then, choose one router from the router list.

   **d** Click the **XCP Web Controller** button to open the Web Controller GUI.
   **Note**: You may be prompted to confirm this request.

4 The XCP Web Controller offers three levels of configuration view: Basic, Intermediate, and Advanced. From the drop-down menu associated with **Configuration View**, select **Advanced** to see detailed configuration.

5 Click the **Edit** option associated with **Sasl Auth Component** in the Components area on the main page to open the SASL configuration page.

6 Follow the steps below to add an Sasl Auth Mechanism.

   **a** **From the Sasl Auth Configuration** section, click the **Remove** option associated with the existing two mechanisms, **PLAIN** and **DIGEST-MD5**.

   **b** Click the **Go** button to add a new mechanism. The Mechanism Configuration view appears.

   **c** Complete the fields using the guidelines below.

   **Note**: To verify this sample plug-in against the XMPP client, such as Pidgin or Psi, follow the steps in the ***Verify Sample Plug-in with the XMPP client*** (on page 54) section.

   - **Name** (Required)—The name of the mechanism that is listed in server's available mechanisms to the client when a client initiates the login request. According to RFC4422, SASL mechanisms are named by character strings, from 1 to 20 characters in length, consisting of ASCII uppercase letters, digits, hyphens, and/or underscores.
   - **Description** (Optional)—The text of mechanism description shows in the Sasl Auth configuration page.
   - **Library** (Required)—The full path of mechanism plug-in. By default, the path should look like /common/log/taos-log-a/ftpdir/<your plug-in name>.

     **Notes**:

     – This plug-in is loaded when SASL component starts next time.

     – For the sample (default) plug-in use:
     **/common/log/taos-log-a/ftpdir/sample.so**

– **Load** (Required)—The name of entry function of mechanism plug-in. SASL component calls this function to load mechanism during SASL component starts up. This function must assign the mechanism name that is identical with the Name entered in the management interface above.

**d** Click the **Submit** button to save your changes and return to the **Sasl Auth Configuration** page.

**e** Click **Submit** at the bottom of the page to save all SASL changes and return to the main page. Once you submit your changes, the SASL configuration file, e.g. 'etc/sasl_auth-1.xml', will be updated to reflect your changes.

**Example:**

```
<sasl_auth:config
xmlns="http://www.jabber.com/config/sasl_auth">
    <mechanisms
xmlns="http://www.jabber.com/config/sasl_auth">
      <mechanism description="SAMPLE mechanism"
library="/common/log/taos-log-a/ftpdir/sample.so"
load="sasl_sample" name="SAMPLE"
xmlns="http://www.jabber.com/config/sasl_auth"/>
</mechanisms>
…
</sasl_auth:config>
```

**7** Follow the steps below to turn on SASL Component Logging feature to debug the SASL component run-time behavior.

**a** From the SASL component configuration page, select Logger > Filtered File Logger.

**b** Complete the fields to configure the parameters.

Example: The parameters in the example below will turn on DEBUG level and output the log file to `/common/log/taos-log-a/conductor/b200-cm1/sasl-1.log`.

**Note**: The following parameters are used to configure the log level.

- **Level**—Conductor offers five logging levels: DEBUG, VERBOSE, INFO, WARN and ERROR. Suggest turning on a lower level (like DEBUG) for debugging, and setting a higher (like WARN or ERROR) level for production environment.
- **Pipe file**—The full path of the pipe file. You can send the file a pipe command of U(up) or D(down) to increase or decrease the logging level.
- **Name and location**—The full path of the log file.

**a** Click **submit** at the bottom of the page to save all SASL changes and return to the main page. The SASL configuration file will be updated to reflect your changes.

**Example**: etc/sasl_auth-1.xm

```
<sasl_auth:config xmlns="http://www.jabber.com/config/sasl_auth">
…
<logging xmlns="http://www.jabber.com/config/logging">
    <logger xmlns="http://www.jabber.com/config/logging/logger/composite"
type="composite">
        <std-file:logger xmlns:std-
file="http://www.jabber.com/config/logging/logger/std-file" type="std-
file" xmlns="http://www.jabber.com/config/logging/logger/std-file">
          <filter xmlns="http://www.jabber.com/config/logging/filter/pipe"
level="DEBUG" pipe-name="/common/log/taos-log-a/conductor/b200-cm1/sasl-
1.pipe" type="pipe"/>
          <logger xmlns="http://www.jabber.com/config/logging/logger/file"
backup-log-count="10" buffer-size="0" name="/common/log/taos-log-
a/conductor/b200-cm1/sasl-1.log" rotate-age-hours="0" rotate-size-megs="0"
type="file">
            <bf:formatter
xmlns:bf="http://www.jabber.com/config/logging/basic_formatter"
type="basic">[%d] [%l] [%s] [%c] [%f] %m</bf:formatter>
          </logger>
        </std-file:logger>
    </logger>
</logging>
</sasl_auth:config>
```

8. (Optional) Follow the steps below to turn on the JSM auto-provision feature.

   Note: If your system is configured to provision users outside of the Conductor system, the interfacing system must perform authentication for that user and return a result of either <success/> or </fail/>, to the Conductor system. With this configuration, Conductor has no account information the first time the user attempts to access the system. Turn on the Jabber Session Manager (JSM) auto-provision feature to synchronize the account with the Conductor database.

   The Jabber Session Manager (JSM) auto-provision feature allows JSM to automatically create a new user when the SASL component authenticates the client successfully for an account that does not exist in the Conductor database. The default password for the account will be a single dash (-). If the account already exists in the database, JSM will not provision the user again.

   a. To turn on this feature, click **Edit** beside Jabber Session Manager in the Router area of the main page.

   b. Find JSM Features section, change "Automatically provision new users" to Yes.

   c. Click **Submit** at the bottom of the page to save the change and return to the main page.

9. Save your changes.

10. Click **Restart the system** to make the changes take effect.

### Verify Sample Plug-in with the XMPP client

To verify this sample plug-in against the XMPP client, such as Pidgin or Psi, rename this mechanism to **PLAIN** and change **SampleMech::name** in the sample code. Then, build and import the plug-in.

### Monitor the Sample SASL Plug-In

You can view the plug-in log from the VCS CLI.

1. List the file and directory for the active log.

   **Example:**

```
admin:file list activelog conductor/*
<dir>   new1boot349
<dir>   new1jsm349
<dir>   nodectl
dir count = 3, file count = 0
admin:file list activelog conductor/new1jsm349/*
jabberd.log                              sasl-1.log
stats.log
dir count = 0, file count = 3
```

2. Use the **file view/dump/tail activelog [filename]** command to view the content.

   **Example:**

```
admin:file view activelog conductor/new1jsm349/sasl-1.log
[2012-03-28T03:30:39Z] [ERROR] [no-subject] [sasl-
1.new1jsm349] [] jax::Component::onClose[2012-03-28T03:30:42Z]
[INFO ] [no-subject] [SaslComponent.cpp:726] [] loading
mechanism PLAIN, module libsasl_plain.so entry sasl_plain.
[2012-03-28T03:30:42Z] [INFO ] [no-subject]
[SaslComponent.cpp:777] [] mechanism PLAIN is loaded
successfully.
[2012-03-28T03:30:42Z] [INFO ] [no-subject]
[SaslComponent.cpp:726] [] loading mechanism DIGEST-MD5,
module libsasl_md5.so entry sasl_md5.
[2012-03-28T03:30:42Z] [INFO ] [no-subject]
[SaslComponent.cpp:777] [] mechanism DIGEST-MD5 is loaded
successfully.
[2012-03-28T03:30:42Z] [INFO ] [no-subject] [sasl-
1.new1jsm349] [] Component is connected to the Jabber router.


end of the file reached
options: q=quit, n=next, p=prev, b=begin, e=end (lines 1 - 5
of 5) : q
```

### Download the Sample SASL Plug-In from the CMC

1. Log into CMC.
2. Click **Services** on the top-right corner. Then, select a node and click the **Logs** button to download the logs.
3. Unzip the log file and locate the SASL logs under **/common/log/taos-log-a/conductor/<router name>**.

```
[2011-06-09T01:10:12Z] [INFO ] [no-subject] [SaslComponent.cpp:689] []
loading mechanism PLAIN, module sample.so entry sasl_sample.
[2011-06-09T01:10:12Z] [INFO ] [no-subject] [SaslComponent.cpp:741] []
mechanism PLAIN is loaded successfully.
[2011-06-09T01:10:12Z] [INFO ] [no-subject] [sasl_auth-1.jabber] []
Component is connected to the Jabber router.
```

**Note**: The log contains the output to load the sample plug-in during its startup.

**Example:**

```
[2012-02-06T08:38:03Z] [VBOSE] [no-subject] [SaslComponent.cpp:232] []
onPacket: <xdb from='cm-1_jsmcp-1.jabber' id='jtx_b277081a-59ec-4780-
8674-d788909e1f0' ns='http://jabber.com/protocol/sasl' to='localhost'
type='set'><auth ga:client-uses-full-bind-result='true' mechanism='PLAIN'
xmlns='urn:ietf:params:xml:ns:xmpp-sasl'
xmlns:ga='http://www.google.com/talk/protocol/auth'>AHRlc3QAdGVzdA==</aut
h></xdb>
[2012-02-06T08:38:03Z] [DEBUG] [no-subject] [SaslComponent.cpp:245] []
hashkey 2
[2012-02-06T08:38:03Z] [DEBUG] [no-subject] [SaslComponent.cpp:444] []
[PLAIN] start: AHRlc3QAdGVzdA==
[2012-02-06T08:38:03Z] [INFO ] [no-subject] [ODBCConnection.cpp:202] []
connect dsn:msginfra_pg username:conductor type:1
```

4. Complete the parameters for any XMPP client to connect with the Conductor server.
5. Verify that the SASL component can invoke the sample plug-in to authenticate the client.

```
[2012-02-06T08:38:03Z] [DEBUG] [no-subject] [SaslComponent.cpp:629] []
getUsersPass test localhost
[2012-02-06T08:38:03Z] [DEBUG] [no-subject] [SaslComponent.cpp:659] []
getUsersPass successfully
[2012-02-06T08:38:03Z] [DEBUG] [no-subject] [SaslComponent.cpp:457] []
[PLAIN] return 0 errno 0 challenge
[2012-02-06T08:38:03Z] [DEBUG] [no-subject] [SaslComponent.cpp:492] []
[PLAIN] respond <xdb from='localhost' id='jtx_b277081a-59ec-4780-8674-
d788909e1f0' ns='http://jabber.com/protocol/sasl' to='cm-1_jsmcp-
1.jabber' type='result'><success jid='test@localhost'
xmlns='urn:ietf:params:xml:ns:xmpp-sasl'/><x type='submit'
xmlns='jabber:x:data'><field
var='FORM_TYPE'><value>http://www.jabber.com/schemas/saslprops.xsd</value
></field><field type='text-single' var='sasl-
service'><value>xmpp</value></field><field type='text-single' var='sasl-
server'><value>localhost</value></field><field type='text-single'
var='sasl-mechname'><value>PLAIN</value></field><field type='text-single'
var='sasl-username'><value>test</value></field><field type='text-single'
var='JID'><value>test@localhost</value></field></x></xdb>
[2012-02-06T08:38:03Z] [VBOSE] [no-subject] [SaslComponent.cpp:784] []
Sending: <xdb from='localhost' id='jtx_b277081a-59ec-4780-8674-
d788909e1f0' ns='http://jabber.com/protocol/sasl' to='cm-1_jsmcp-
1.jabber' type='result'><success jid='test@localhost'
xmlns='urn:ietf:params:xml:ns:xmpp-sasl'/><x type='submit'
xmlns='jabber:x:data'><field
var='FORM_TYPE'><value>http://www.jabber.com/schemas/saslprops.xsd</value
></field><field type='text-single' var='sasl-
service'><value>xmpp</value></field><field type='text-single' var='sasl-
server'><value>localhost</value></field><field type='text-single'
var='sasl-mechname'><value>PLAIN</value></field><field type='text-single'
var='sasl-username'><value>test</value></field><field type='text-single'
var='JID'><value>test@localhost</value></field></x></xdb>
[2012-02-06T08:38:03Z] [DEBUG] [no-subject] [metrics]
[BaseRecord.cpp:106] Added field to record: field name('mech')
[2012-02-06T08:38:03Z] [DEBUG] [no-subject] [metrics]
[BaseRecord.cpp:106] Added field to record: field name('jid')
[2012-02-06T08:38:03Z] [VBOSE] [no-subject] [SaslComponent.cpp:810] []
Sending payload: <log ns='http://protocols.cisco.com/xcp-metrics#sasl-
auth-success' timestamp='2012-02-06T08:38:03.151365Z' type='info'
from='sasl_auth-1.jabber'><element><record interval-sec='0'
xmlns='http://protocols.cisco.com/xcp-metrics#sasl-auth-
success'><jid>test@localhost</jid><mech>PLAIN</mech></record></element></
log>
```

# Upload, Deploy and Remove the SASL Plug-In from the Management Console

Follow the instructions in this section to upload, deploy, and remove the SASL plug-in from the management console.

### Upload the SASL Plug-In

Follow these instructions to upload the SASL plug-in from your desktop or from an sftp site.

1. From the management console, click **Message Infrastructure** and select **Upload**. The Upload window opens.
2. Click **Import**. The Import Images window opens.
3. Select the source where the SASL plug-in resides: **Desktop** or **SFTP**.
4. Complete the following tasks depending on your selection in the previous step:

   **Important**: The SASL plug-in must be packaged as a tar file with "SASL" as the prefix of the filename, for example **SASL<plugin name>.tar**.

   - **Desktop**: In the Collection Options area, click the **Browse** button and browse to where the plug-in resides on your desktop. Then click **Open**. The path to the file you selected shows in the Select File field.
   - **SFTP**: In the Collection Options area, enter the **user password** for the SFTP site where the plug-in resides, and leave the remaining fields with their pre-populated data.
5. Click **Submit**. The plug-in tar file is uploaded to the management console and appears in the plug-in list on the management console.

### Deploy the SASL Plug-In

Follow these instructions to upload the SASL plug-in from the management console.

1. From the management console, click **Message Infrastructure** and select **Deploy**. The Deploy window opens and lists all nodes that have the SASL plug-in installed on them.
2. Select the **Node** checkbox for the node that will deploy the tar file. The Sasl Plugin File List window opens and lists all the tar files that have been uploaded to the management console.
3. Select the tar file that you want to deploy on the node you have selected.
4. Click **Sasl Plugin Deploy**. A message prompts you to confirm your action.
5. Click **OK**. A message indicates that the deployment initiation was successful.
6. Click **OK**. The window updates and shows the tar file has now been deployed to the selected node and indicates that the plug-in has been successfully deployed.

   **Note**: The path of the SASL plug-in file deployed on the selected node is /opt/cisco/conductor/saslplugins/<tar file name>.

### Remove the SASL Plug-In

1. From the management console, click **Message Infrastructure** and select **Remove**. The Remove window opens. This window lists all of the nodes to which a plug-in file has been deployed.
2. Select the node whose plug-in file you want to remove. The Deployed Sasl Plugin File List area opens and shows all plug-in files that have been deployed on that node.
3. Select the file that you want to remove.
4. Click **Uninstall**. A message prompts you to confirm your action.

Click **OK**. The zip file is removed from the Deployed Sasl Plugin File List and the node status updates to indicate that the plug-in was successfully removed.

# 4

# Workflow Engine

The Cisco VCS Workflow Engine (WFE) allows complex tasks to be performed by executing "workflows." Each workflow defines a series of steps to perform when a specific URL is invoked. This chapter provides an overview of how to develop and deploy a workflow package using the WFE.

## In This Chapter

# Overview

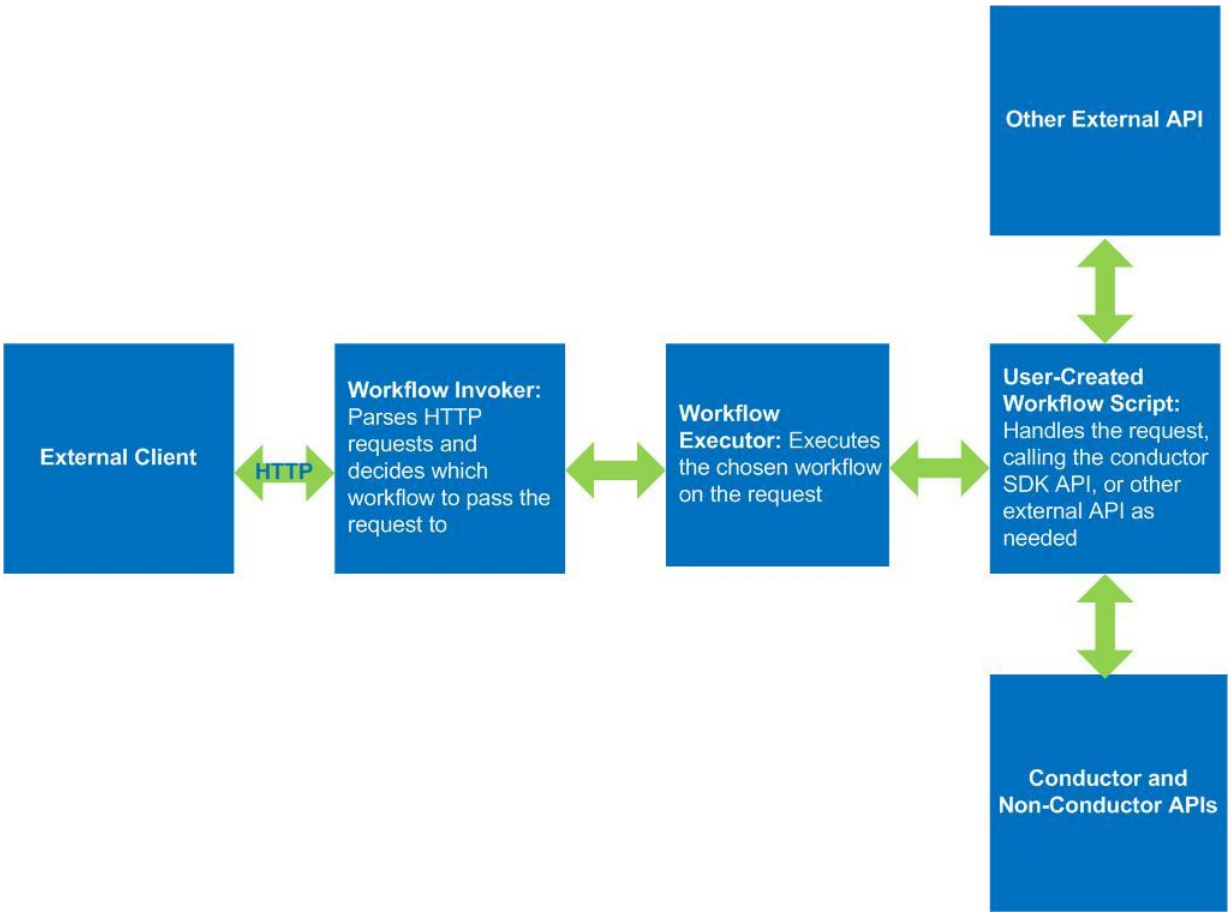
This section provides an overview of both the WFE components and the process for setting up the WFE.

## What Is the WFE?

From the VCS management console, users can perform complex operations or processes by executing "workflows." These workflows define a series of steps to perform when specific URLs are invoked. These workflows are completely customizable without requiring recompilation of code or any changes to the software.

All workflows are stored on a node for which the WFE COP has been installed. Nodes without the COP installation cannot support WFE. These workflows are defined as either a script that supports any JSR223 scripting language.

The following diagram shows the major components of the WFE.



## WFE Setup At a Glance

To set up a workflow for use from the management console, complete the following tasks which are described in detail later in this chapter:

1. Create a custom script and package it in a zip file.
2. Deploy the zip file from the management console.
3. Invoke the script from a command line (CLI).

# Create and Package a Custom Script

To use the WFE to automate a task, you'll first need to create a workflow that specifies an accessible endpoint, such as a URL, and the scripts to be run from the endpoint. To deploy the workflow, create a zip file that uses the structure shown below.

```
.zip
---------------------------------
   workflows/
   lib/
   deploy/
   workflowendpoints.csv
   WorkflowRoutingRules.js - Optional
   SubscriberServiceRules.js - Optional
```

## Workflow Zip File

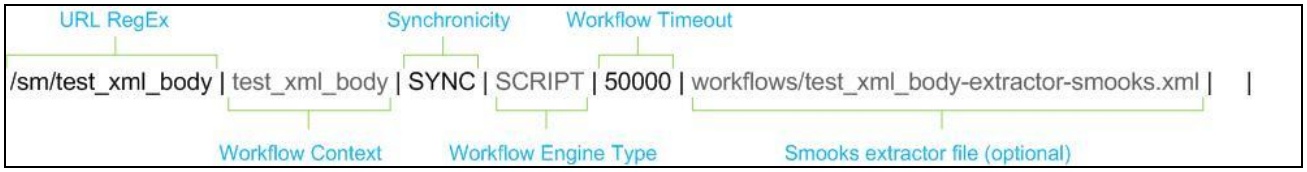
The following table shows the files and content contained in the workflow zip file.

| Zip Directory | WFE Location |
|---|---|
| workflows/ | Contains the workflow script file, such as xxxx.js<br>**WFE Location:** /opt/jboss/jboss-as-7.1.0.Final/standalone/configuration/bni/workflows |
| lib/ | Client stub jar files which should be imported when access VCS service. These files usually are generated by “wsdl2stub” command of ServiceSDK and then packed into jar files.<br>**Important:** Do not overwrite existing classes, for example, the Conductor SDK.<br>**WFE Location:** /opt/jboss/jboss-as-7.1.0.Final/standalone/deployments/Conductor-workflow-invoker.war/WEB-INF/lib |
| deploy/ | **WFE Location:** /opt/jboss/jboss-as-7.1.0.Final/standalone/deployments/ |
| workflowendpoints.csv | A line of workflow URL mapping configuration, as shown in the example in the following section on the Workflow Invoker.<br>**WFE Location:** /opt/jboss/jboss-as-7.1.0.Final/standalone/configuration/bni |
| **Optional Files** | |
| WorkflowRoutingRules.js | If this file exists, it will cover the same file under /opt/jboss/jboss-as-7.1.0.Final/standalone/configuration/bni |
| SubscriberServiceRules.js | If this file exists, it will cover the same file under /opt/jboss/jboss-as-7.1.0.Final/standalone/configuration/bni |

## Workflow Invoker

As mentioned earlier, the workflow invoker is the web application running on the WFE node that accepts the incoming HTTP requests, parses them, passes the parsed parameters to the workflow, and then converts the workflow's results into an HTTP response.

The workflow invoker is primarily driven by a single configuration file (**workflowendpoints.csv**) that is found in /opt/jboss/jboss-as-7.1.0.Final/standalone/configuration/bni. This file contains a pipe separated configuration row per workflow/endpoint, as shown in the following example:




The following table provides details about configuration file contents.

| Name | Description |
|---|---|
| URL RegEx | The regular expression that should be applied to the incoming URL to determine if this entry should be executed for that incoming URL. |
| Workflow Context | A string passed to the Subscriber Selection Rules and Workflow Selection Rules that is used to determine which actual workflow script to execute. |
| Workflow Engine Type | The type (SCRIPT) of the workflow to invoke. By default, for SCRIPT engine types, the workflow selection rule will select the XXX.js file, where XXX is the workflow context column. |
| Synchronicity (Optional) | SYNC or ASYNC<br>Sync will wait until the workflow is completed to respond while Async will respond immediately. |
| smooks extractor file (Optional) | A smooks file which describes how to extract the inbound request body. The results of the smooks evaluation are passed to the workflow as global variables. |
| Workflow Timeout | The time in milliseconds before the invoker servlet should wait for the workflow before returning a failure HTTP response. In this case, the HTTP status code will be 500. |
| Parent Spring Context (Optional) | The parent of the spring context that the workflow should make available as global variables. |
| Spring Context (Optional) | A string that represents a path to the spring context whose beans will be made available as global variables within the workflow. This spring context should be available in the classpath of the application itself. |

# Deploy the Zip File

After you have created the zip file as described in the previous section, deploy the zip file using one of the following methods:

- Upload the zip file to the specified node from the management console
- Upload the zip file to the specified node using the CLI

## Deploy the Zip File to the Management Console

To deploy the zip file, first upload the zip file from your desktop to the management console, and then deploy the zip file to a specific WFE node so that it can be invoked.

### Upload the Zip File to the Management Console

1. From the management console, click **Services** and select **Workflow Download**. The Workflow Repository window opens. This window holds all of the workflow zip files that have been created and uploaded.
2. Click **Import**. The Import Images window opens.
3. In the Source area, select **Desktop** or **SFTP** if it is not already selected.
4. Click **Browse**. A browser window opens showing your desktop.
5. Navigate to where you have stored the zip file on your desktop and select the zip file.
6. Click **Open**. The browser window closes and the zip file you selected shows in the Select File field in the Import Images window.
7. Click **Submit**. A message prompts you to confirm that you want to upload the zip file.
8. Click **OK**. The zip file appears in the Workflow Repository.

### Deploy the Zip File to a WFE Node

1. From the management console, click **Services** and select **Deployment**. The Workflow Engine Deployment window opens and lists all nodes that have the WFE installed on them.

   Important: Only the nodes with WFE COP installed on them appear in the Workflow Engine Deployment window.
2. Select the Node checkbox for the node that will deploy the zip file. The Workflow Files to install window opens and lists all the workflow zip files that have been uploaded to the management console.
3. Select the zip file that you want to deploy on the node you have selected.
4. Click **Workflow Deploy**. A message prompts you to confirm your action.
5. Click **OK**. A message indicates that the deployment initiation was successful.

6 Click **OK**. The Workflow Engine Deployment window updates and shows the zip file has now been deployed to the selected node and indicates that the Workflow has been successfully deployed.

## Deploy the Workflows Using the CLI

To deploy the workflow files, first upload the files to the management console using the existing file transfer secure-import CLI. Then deploy the file to a specific WFE node as described in the following instructions.

### View Existing Workflow Files

Before you deploy a workflow file to a WFE node, you may want to view the files that already exist on the management console. To view the files, use the following commands:

- To view the files that have been uploaded but not deployed, use **file list activelog ftpdir**.
- To list files that are currently deployed, **file load wf list**.

### Upload a Workflow File to the Management Console

Upload script-based workflows to the management console by copying the unzipped workflows directory and lib directory to the following locations:

- **Workflows directory:** to /opt/jboss/jboss-as-7.1.0.Final/standalone/configuration/bni/workflows.
- **Lib directory:** /opt/jboss/jboss-as-7.1.0.Final/standalone/deployments/Conductor-workflow-invoker.war/WEB-INF/lib

You do not need to restart the system as the engine will reload any changed workflows.

### Deploy a Zip File to a WFE Node

Use the following CLI to deploy a zip file that has been uploaded into the node: **file load wf deploy**.

# Remove a Deployed Workflow File

Use one of the following methods to remove a workflow zip file after it has been deployed:

- Remove the zip file using the management console
- Remove the zip file using the CLI

## Use the Management Console to Remove the Zip File

1. From the management console, click **Services** and select **Update**. The Workflow Engine Update window opens. This window lists all of the nodes to which a workflow file has been deployed.
2. Select the node whose workflow file you want to remove. The List of Workflow Files Deployed area opens and shows all zip files that have been deployed on that node.
3. Select the zip file that you want to remove.
4. Click **Uninstall**. A message prompts you to confirm your action.
5. Click **OK**. The zip file is removed from the List of Workflow Files Deployed and the node status updates to indicate that the workflow was successfully removed.

## Use the CLI to Remove the Zip File

Use this CLI to remove a workflow zip that has been previously deployed: **file load wf remove**

# Invoke the Script

After the workflow has been deployed to specific nodes, you can invoke it using the CLI, similar to the following example:

```
echo
"<root><param1>AAAAA</param1><subparam><param2>22222</param2><param3>value33
3</param3><subparam><root>" | curl -X POST -H 'Content -type: text/xml' -d
@- http://10.20.30.40:8081/sm/test_xml_body
```

# 5

# User Profile Manager Adaptor

This chapter provides an overview of the Cisco VCS User Profile Manager (UPM) adaptor component that supports the Cisco Videoscape Control Suite Message Infrastructure product. It also describes how to configure UPM adaptor settings.

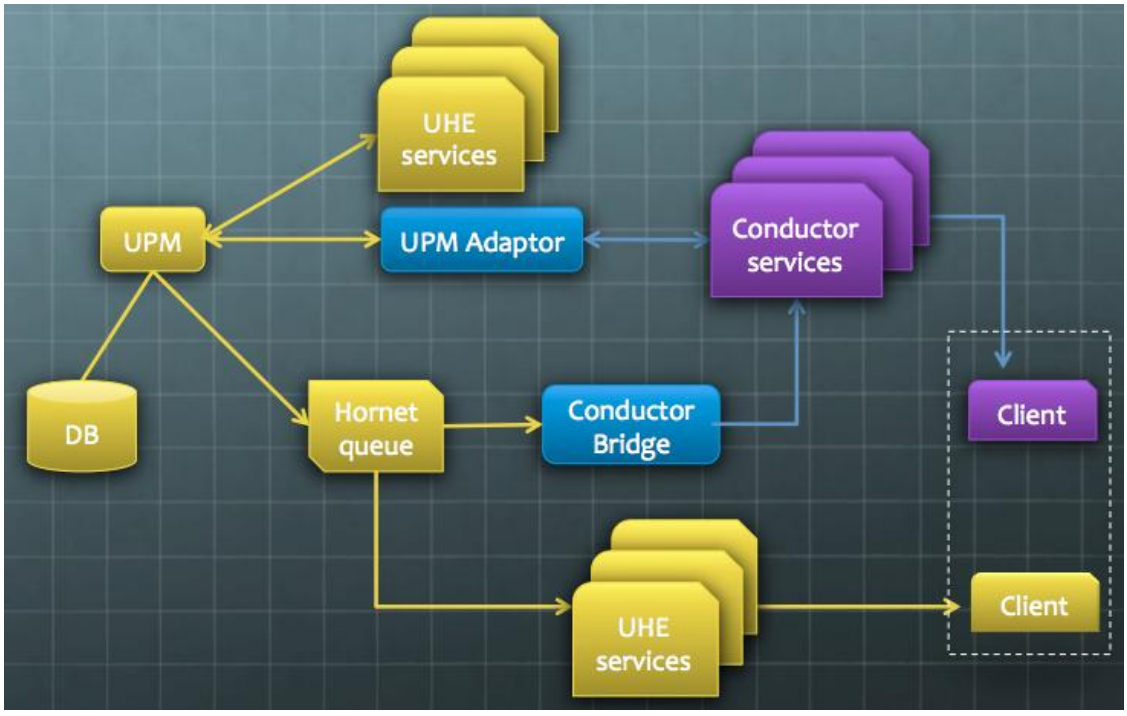
## In This Chapter

# Overview

UPM is a software component that is a central repository of user-related data in a multi-device TV system. It provides a comprehensive storage for household, user, and device-level settings, preferences, and associated data. UPM supplies this information to external systems in order to provide a personalized experience for end users.

The Client Directory (CD) component provides similar services to VCS applications. The UPM adaptor integrates the UPM and the CD to minimize changes for legacy applications following integration.

The following diagram, shows VCS 2.5 components in blue, existing VCS components are in purple, and NDS components are in yellow.



# Configure UPM Adaptor Settings

1. From the management console, click **Services** and select **UPM Adaptor Settings**. The UPM Adaptor Instance window opens.
2. Select the JID whose UPM adaptor settings you want to configure and click **Edit**. The Edit UPM Adaptor Instance Configuration window opens.
3. Enter data in the following fields:
   - UPM IP
   - HornetQ IP
   - Component Mode
   - Component Name
   - Component Password
   - Component Open Port IP
   - Component Port
   - Pubsub Enable
   - Pubssub JID
   - Debug flag
   - WFE Mode
   - WFE IP
   - WFE Create User URL
   - WFE Create Account URL
   - WFE Create Device URL
   - WFE Delete Device URL
   - WFE Delete Account URL
   - WFE Delete Device URL
4. Click **Save**. The message Operation Saved Successfully appears.
5. Click **Back** to close the Edit UPM Adaptor Instance Configuration window.

# 6

# Configure Nodes and NTP Servers

This chapter describes how to configure VCS nodes and network time protocol (NTP) servers.

## In This Chapter

# Configure VCS Nodes

The Configure menu options provide links to configure nodes. From the Configure Videoscape Controls Suite Nodes window, you can view the list of the nodes in the current operator's domain.

To view a list of modes in the current operator's domain, from the management console, click **Configure** and select **Videoscape Control Suite Nodes**. The Configure Videoscape Control Suite Nodes window opens and lists all nodes in the current operator's domain.

# Configure VCS NTP Servers

The Configure menu options provide links to NTP servers. From the NTP servers view, you can configure NTP server settings. You can add up to five servers, and delete as necessary.

Follow these instructions to configure VCS NTP servers.

1. From the management console, click **Configure** and select **Videoscape Control Suite NTP Servers**. The NTP Config window opens and lists all nodes in the current operator's domain.
2. Click in the **IPv4 Address** fields for the servers you want to configure and enter the IPv4 addresses that each server will use.
3. Click in the **Overwrite current configuration** box to replace the current NTP server configuration with the new configuration.
4. Click **Submit**.

# 7

# Customer Information

## If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883



May 2013

Part Number OL-26324-01