Videoscape Control Suite Operators XCP

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

Chapter 14 Service Virtualization Manager 97

Chapter 15 Service Viewer 103

Chapter 16 HTTP Gateway 107

Chapter 17 Customer Information 111

Appendix A Standard Port Assignments 113

About This Guide

Introduction

The Videoscape Control Suite Message Infrastructure (MsgInfra) XCP controller is the web-based administration console that is used to configure the MsgInfra Server. This guide provides instructions for configuring and using the MsgInfra Server.

Audience

The audience for this document includes system administrators, operators, and installation engineers who deploy Videoscape Control Suite systems.

Document Version

This is the first formal release of this document.

1

Using the MsgInfra XCP Controller

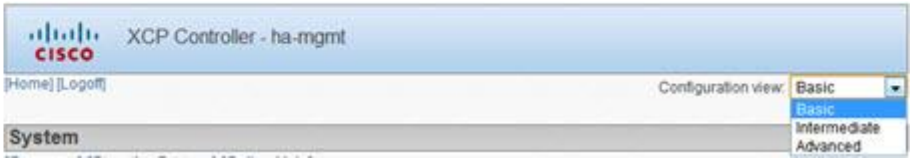
Introduction

The Videoscape Control Suite Message Infrastructure (MsgInfra) XCP controller is the web-based administration console that is used to configure the MsgInfra Server. From the controller's main page, you can access information about the server's core router, and about all of the plugins and components associated with the MsgInfra Server. You can start and stop the server and its components from this location. You can also view an XML summary of your server configuration.

In This Chapter

Configuration Views

The Videoscape Control Suite MsgInfra XCP controller offers three levels of configuration, called configuration views: **Basic**, **Intermediate**, and **Advanced**. The following figure shows the Configuration view menu, which is located in the top right corner of every controller configuration page. When you select a particular view, it remains in effect on all pages until you change it.



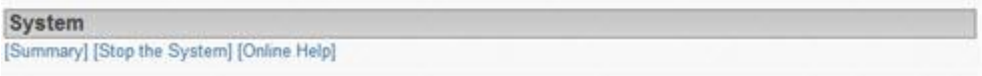
- The **Basic** configuration view displays the fewest configuration options and primarily uses the server's default values. Configuring your system using this view is sufficient for most server components, and enables you to get your Videoscape Control Suite system up and running in the shortest amount of time.
- The **Intermediate** configuration view displays all of the options that are available in the Basic view, in addition to some other options, such as those used for host name and command configurations, and for logging. It also includes many of the options for components that are installed with the Videoscape Control Suite extras installation package.
- The **Advanced** configuration view displays all of the options that are contained in the Basic and Intermediate views, in addition to a number of fine-tuning options such as buffer size, run level, and thread count. These options require a more advanced level of MsgInfra Server knowledge, and you can use them to adjust the performance of your Videoscape Control Suite system.

Areas on the Main Page

The System, Router, and Components areas on the controller's main page are described in the following sections.

The System Area

The controller's System area is shown in the following figure.



System

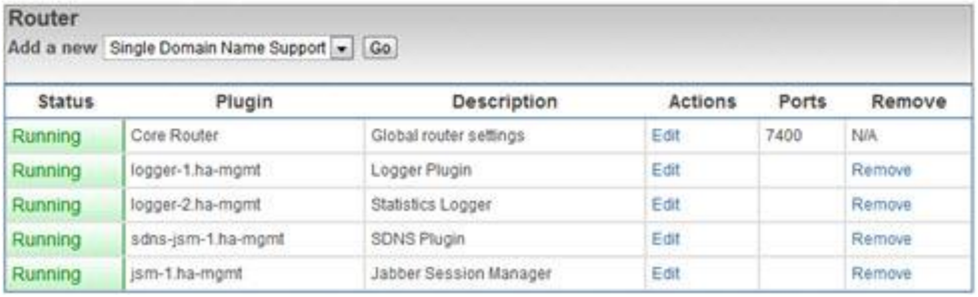
[Summary] [Stop the System] [Online Help]

The links in the System area perform the following functions:

- **Summary** — Displays the complete jabber.xml file, which contains your configuration settings.
- **Stop the System** — Stops the MsgInfra Server and all of its plugins and components. The Videoscape Control Suite Node Controller would monitor the MsgInfra Server state and start it automatically per Videoscape Control Suite policy.
- **Online Help** — Opens the controller's online help system.

The Router Area

Router plugins are extensions of the MsgInfra Server's core router, and always start and stop with the system. Each plugin on your system is listed in the controller's Router area, as shown in the following figure.



Router

Add a new Single Domain Name Support ▾ Go

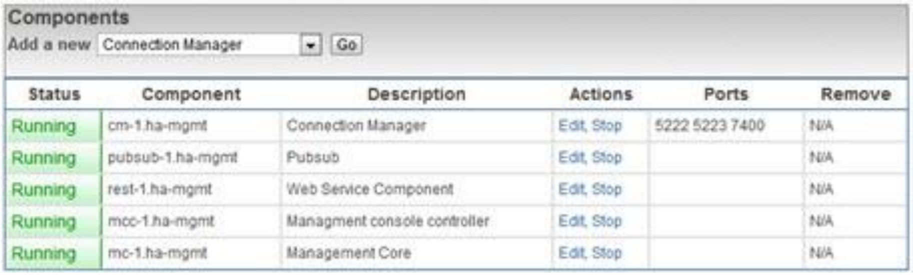
Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	logger-1.ha-mgmt	Logger Plugin	Edit		Remove
Running	logger-2.ha-mgmt	Statistics Logger	Edit		Remove
Running	sdns-jsm-1.ha-mgmt	SDNS Plugin	Edit		Remove
Running	jsm-1.ha-mgmt	Jabber Session Manager	Edit		Remove

You can add a new plugin by selecting it in the list and clicking **Go** to display its configuration page. You can also modify an existing plugin's configuration by clicking the corresponding **Edit** link, or remove a plugin (except for the core router) by clicking its **Remove** link.

Note: You cannot remove the Core Router, because it is the core of the MsgInfra Server.

The Components Area

Components are extensions of the MsgInfra Server that can be started and stopped independent of the server. The Components area, shown in the following figure, is where you add, modify, start, stop, or remove server components.



Add a new: Connection Manager

Status	Component	Description	Actions	Ports	Remove
Running	cm-1.ha-mgmt	Connection Manager	Edit, Stop	5222 5223 7400	N/A
Running	pubsub-1.ha-mgmt	Pubsub	Edit, Stop		N/A
Running	rest-1.ha-mgmt	Web Service Component	Edit, Stop		N/A
Running	mcc-1.ha-mgmt	Managment console controller	Edit, Stop		N/A
Running	mc-1.ha-mgmt	Management Core	Edit, Stop		N/A

You add a new component by selecting it in the list and clicking **Go** to access its configuration page. You can start and stop individual components if needed by clicking the **Start** and **Stop** links. You can also modify an existing component's configuration by clicking the corresponding **Edit** link, or remove a stopped component by clicking its Remove link. (You must stop a component before you can remove it.)

Online Help

You can click the **Online Help** link on the controller's main page to open the entire help system. Each configuration page also has a Help link that opens the online help topic just for that page, which contains descriptions of the configuration parameters.

2

Global Router Settings

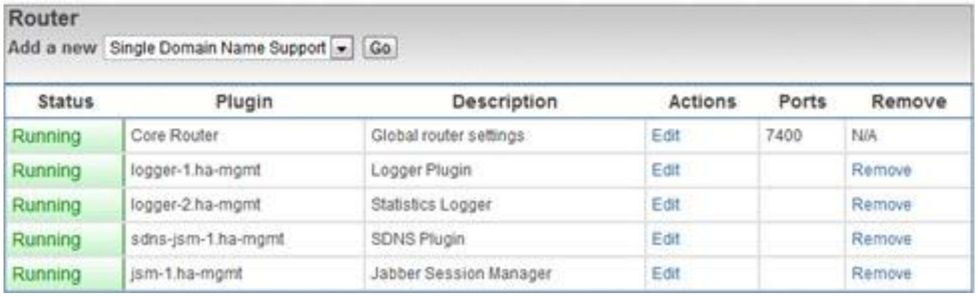
Introduction

The Videoscape Control Suite MsgInfra core router, which provides the MsgInfra Server's core communication functionality, is installed and configured with default settings when you install the server. The core router's configuration page contains global settings, which allow you to configure features that affect your entire server environment. For example, you can configure database settings that will be used by all components that require a database. You can override the core router's global settings in any individual component's configuration page if needed

In This Chapter

Global Router Configuration

To open the Global Router Configuration page, click **Edit** beside **Global router settings** in the **Router** area on the controller's main page.

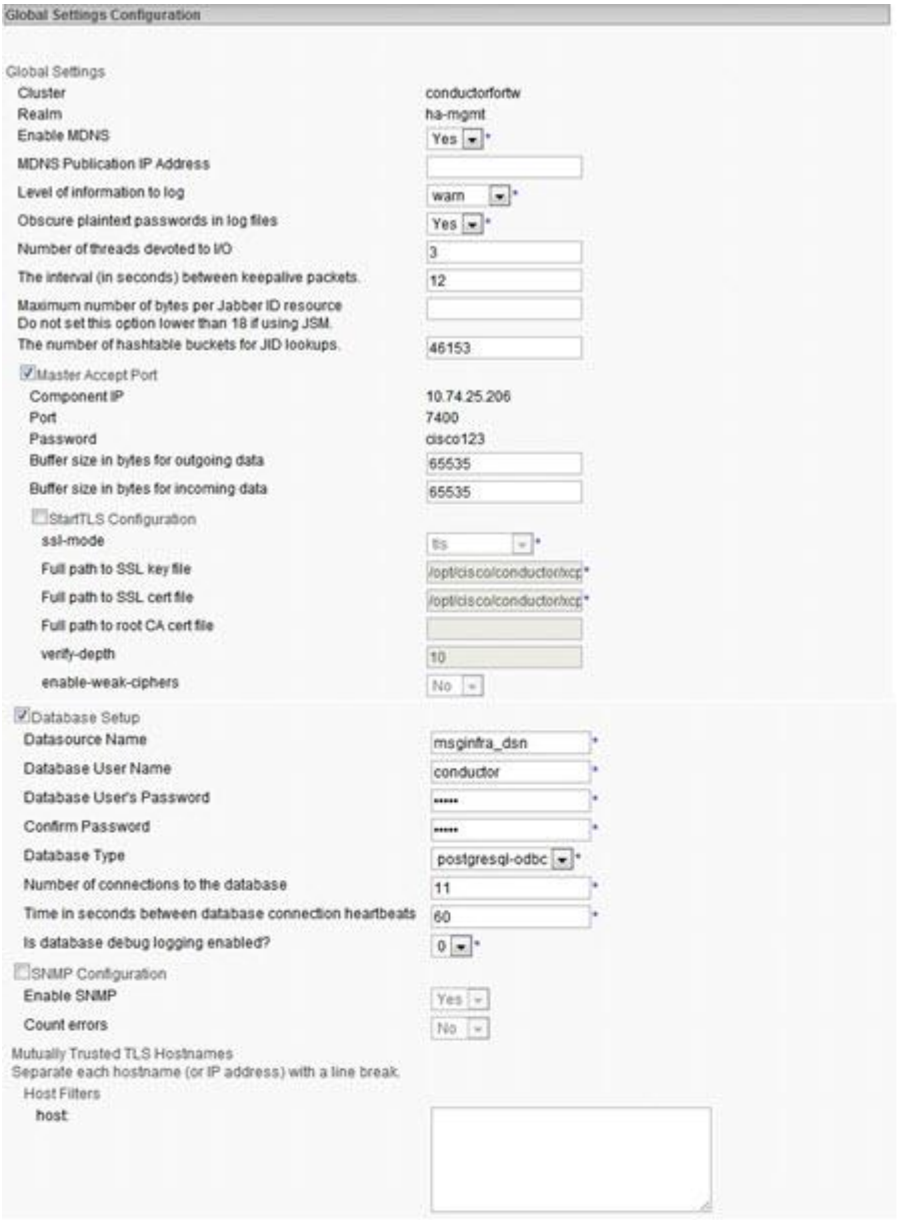


Router

Add a new Single Domain Name Support Go

Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	logger-1.ha-mgmt	Logger Plugin	Edit		Remove
Running	logger-2.ha-mgmt	Statistics Logger	Edit		Remove
Running	sdns-jsm-1.ha-mgmt	SDNS Plugin	Edit		Remove
Running	jsm-1.ha-mgmt	Jabber Session Manager	Edit		Remove

The Global Settings Configuration page is shown in the following illustration in the controller's Advanced configuration view so that you can see all of the options.



Global Settings Configuration

Global Settings

Cluster	conductorfortw
Realm	ha-mgmt
Enable MDNS	Yes *
MDNS Publication IP Address	
Level of information to log	warn *
Obscure plaintext passwords in log files	Yes *
Number of threads devoted to I/O	3
The interval (in seconds) between keepalive packets.	12
Maximum number of bytes per Jabber ID resource Do not set this option lower than 18 if using JSM.	
The number of hashtable buckets for JID lookups.	46153

☑ Master Accept Port

Component IP	10.74.25.206
Port	7400
Password	cisco123
Buffer size in bytes for outgoing data	65535
Buffer size in bytes for incoming data	65535

□ StartTLS Configuration

ssl-mode	tls *
Full path to SSL key file	/opt/cisco/conductor/xcp *
Full path to SSL cert file	/opt/cisco/conductor/xcp *
Full path to root CA cert file	
verify-depth	10
enable-weak-ciphers	No

☑ Database Setup

Datasource Name	msginfra_dsn *
Database User Name	conductor *
Database User's Password	••••• *
Confirm Password	••••• *
Database Type	postgresql-odbc *
Number of connections to the database	11 *
Time in seconds between database connection heartbeats	60 *
Is database debug logging enabled?	0 *

□ SNMP Configuration

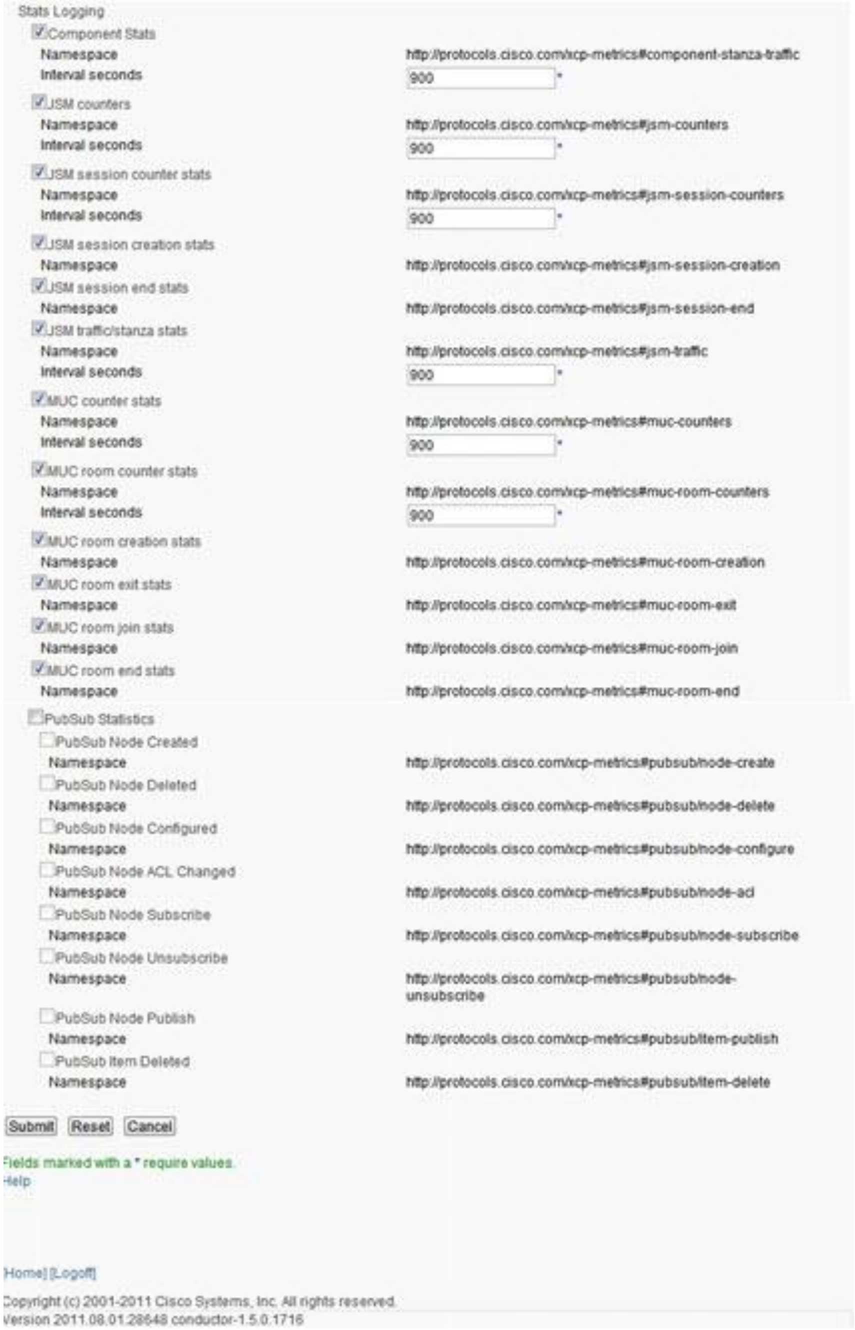
Enable SNMP	Yes
Count errors	No

Mutually Trusted TLS Hostnames
Separate each hostname (or IP address) with a line break.

Host Filters

host	

The page continues.



Stats Logging

☑ Component Stats	
Namespace	http://protocols.cisco.com/xcp-metrics#component-stanza-traffic
Interval seconds	900 *
☑ JSM counters	
Namespace	http://protocols.cisco.com/xcp-metrics#jsm-counters
Interval seconds	900 *
☑ JSM session counter stats	
Namespace	http://protocols.cisco.com/xcp-metrics#jsm-session-counters
Interval seconds	900 *
☑ JSM session creation stats	
Namespace	http://protocols.cisco.com/xcp-metrics#jsm-session-creation
☑ JSM session end stats	
Namespace	http://protocols.cisco.com/xcp-metrics#jsm-session-end
☑ JSM traffic/stanza stats	
Namespace	http://protocols.cisco.com/xcp-metrics#jsm-traffic
Interval seconds	900 *
☑ MUC counter stats	
Namespace	http://protocols.cisco.com/xcp-metrics#muc-counters
Interval seconds	900 *
☑ MUC room counter stats	
Namespace	http://protocols.cisco.com/xcp-metrics#muc-room-counters
Interval seconds	900 *
☑ MUC room creation stats	
Namespace	http://protocols.cisco.com/xcp-metrics#muc-room-creation
☑ MUC room exit stats	
Namespace	http://protocols.cisco.com/xcp-metrics#muc-room-exit
☑ MUC room join stats	
Namespace	http://protocols.cisco.com/xcp-metrics#muc-room-join
☑ MUC room end stats	
Namespace	http://protocols.cisco.com/xcp-metrics#muc-room-end
□ PubSub Statistics	
□ PubSub Node Created	
Namespace	http://protocols.cisco.com/xcp-metrics#pubsub/node-create
□ PubSub Node Deleted	
Namespace	http://protocols.cisco.com/xcp-metrics#pubsub/node-delete
□ PubSub Node Configured	
Namespace	http://protocols.cisco.com/xcp-metrics#pubsub/node-configure
□ PubSub Node ACL Changed	
Namespace	http://protocols.cisco.com/xcp-metrics#pubsub/node-acl
□ PubSub Node Subscribe	
Namespace	http://protocols.cisco.com/xcp-metrics#pubsub/node-subscribe
□ PubSub Node Unsubscribe	
Namespace	http://protocols.cisco.com/xcp-metrics#pubsub/node-unsubscribe
□ PubSub Node Publish	
Namespace	http://protocols.cisco.com/xcp-metrics#pubsub/item-publish
□ PubSub Item Deleted	
Namespace	http://protocols.cisco.com/xcp-metrics#pubsub/item-delete

Fields marked with a * require values.

Copyright (c) 2001-2011 Cisco Systems, Inc. All rights reserved.
Version 2011.08.01.28648 conductor-1.5.0.1716

The following sections describe the features that are contained in the Global Settings Configuration page.

The Cluster

The Cluster is a unique string that identifies your Videoscape Control Suite MsgInfra Server installation. Clusters enable the server to use dynamic routing in high-scale installations where multiple MsgInfra core routers are required. All of the routers that need to interact must have the same cluster name, and must be installed on the same network subnet.

The Realm

The Realm is a unique string that identifies the Videoscape Control Suite MsgInfra core router and all of its components.

MDNS

The MDNS (multicast DNS) option is configured by cluster.xml when you install the Videoscape Control Suite MsgInfra Server. MDNS allows the server to use its dynamic clustering feature, which provides automatic router-to-router functionality when you have multiple core routers installed in the same network subnet.

The Log Level

The **Level of information to log** option lets you specify the level at which the Videoscape Control Suite MsgInfra Server logs messages to the Jabberd Logger. This log level acts as a high-level filter for the types of messages that the server will log. Log messages that are less severe than the level you specify will not be sent to the logger. For example, if you set this level to warn, warning and error messages are sent to the logger, but info, verbose, and debug messages are not sent.

The log level is set to warn by default for system performance consideration, which means that log messages at the warn and error levels will be sent to the Jabberd Logger.

The log levels from which you can choose are described in the following table. Each log level specifies the severity of the data that is logged and determines the amount of data that the Conductor MsgInfra Server records: the lower the severity level, the more verbose the log. The levels are listed from highest severity to lowest.

Log Level	Description
error	System-generated errors, such as the inability to create listen ports, server configuration errors, failure to create the log files, etc.

Log Level	Description
warn	Non-fatal errors, such as bounced packets, nonexistent user logging in, invalid recipient for a message, etc., plus all data logged at the error level.
info	Data about socket connections and all JSM logs (packet, session, and message) plus all data logged at the error and warn levels. The server logs at this level by default.
verbose	Every packet that is processed by the server and JSM, plus all data logged at the error, warn, and info levels.
debug	Information from all other log levels in addition to debug data.

Obscure Plaintext Passwords

The **Obscure plaintext passwords in log files** option is enabled by default when you install the Videoscape Control Suite MsgInfra Server. This feature obscures passwords in log files. If you disable this option, passwords will be displayed in the log files using plaintext.

Advanced Performance Tuning Options

The following four options are displayed only in the controller's Advanced configuration view, and are used for router performance tuning.

Parameter	Description
Number of threads devoted to I/O	Enter the number of threads dedicated to I/O between the router and external components. These threads handle all traffic from external components. This option is used primarily for performance tuning. The value should be adequate in most circumstances. The default value is 3.
The interval (in seconds) between keepalive packets	Enter the number of seconds between keepalives that are sent over the network to ensure that the connection doesn't close at the TCP socket layer. When two keepalives are missed, the connection is closed and then restarted, if possible. The default value is 12.
Maximum number of bytes per Jabber ID resource	You may want to set a maximum resource if you are using a custom client that has a restriction. This value is the maximum number of bytes (18 or greater) that your users can specify for the resource portion of their Jabber ID. Resources allow users to log on to multiple client sessions using the same Jabber ID. For example, a user can log on as jane@corp.com/one in one location and as jane@corp.com/two in another location. One and two are the resource portions of the Jabber ID.

Parameter	Description
The number of hashtable buckets for JID lookups	Enter the number of hashtable buckets used for cashing Jabber IDs. The setting of this parameter affects the core router's memory usage and performance. The higher this number is set, the more memory the router uses, but the higher its performance. The default value is 46153.

The Master Accept Port

The core router uses the Master Accept Port to accept connection requests from Videoscape Control Suite MsgInfra components that run behind your firewall. The Master Accept Port is ideal for internal components that connect to the router, since it removes the necessity of configuring router connections for each individual component.

Note: Components that run outside the firewall can be configured to allow the core router to connect to them. This configuration mitigates the security risks that would exist if these components were to connect to the router.

Enabling StartTLS

The StartTLS Configuration option lets you configure secure socket layer settings to establish a secure connection with the server.

Important: The Videoscape Control Suite MsgInfra Server does not support private keys for SSL certificates that have pass phrases. If you have a pass phrase or encrypt your private key, your private key/public certificate pair will not load into the MsgInfra Server.

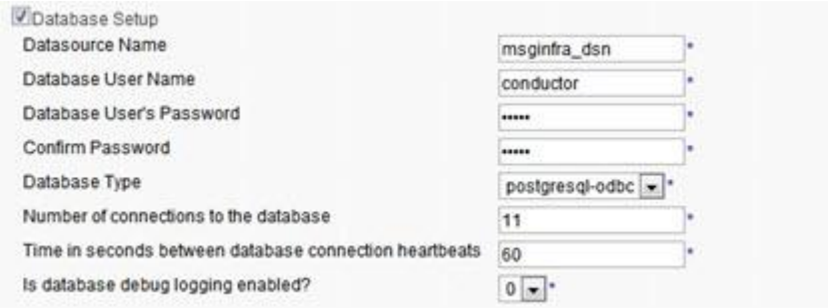
Follow these instructions to enable TLS.

1 Change to the controller's **Intermediate** configuration view.
2 Select the **StartTLS Configuration** option.
3 Configure the parameters as follows.
   - **ssl-mode** — Select **tls** or **tls-required** from the list.
     - **tls** - Enables TLS (transport layer security). Clients that support TLS can connect to the server securely over 5222. Clients that do not support TLS can still connect to the server. This mode does not require a secure connection.
     - **tls-required** - The same as the tls option, except that the client must support TLS. Clients that do not support TLS cannot connect to the server.
   - **Full path to SSL key file** — Enter the full path to the location of the private key that is used to establish a secure server connection. By default, this is set to *xcpInstallDir/certs/host-key.pem*. If you want to use a different key, place the key in the xcpInstallDir/certs directory, and enter its full path here. You can also use the *ip-key.pem* file if preferred, which is located in the same directory.

- **Full path to SSL cert file —** Enter the full path to the location of the certificate file. By default, this path is set to the same value as the SSL Key, *xcpInstallDir/certs/host-key.pem*. If you want to use a different certificate file, place the file in the xcpInstallDir/certs directory, and enter its full path here. You can also use the ip-key.pem file if preferred, which is located in the same directory.
- **Full path to root CA cert file** — Optionally, enter the full path to the CA certificate that is used to verify incoming client certificates.
- **verify-depth** — Enter the maximum depth for the certificate chain verification to allow for incoming client connections.
- **enable-weak-ciphers** — Select **Yes** if you want to allow SSL connections to use cryptographically weak ciphers.

Database Setup

The Database Setup option in the Global Settings Configuration page contains information about the database that you are using to store Videoscape Control Suite MsgInfra Server data. This database will be used globally by all components that use a database; however, if necessary, you can override the database settings in any component's configuration.



☑ Database Setup

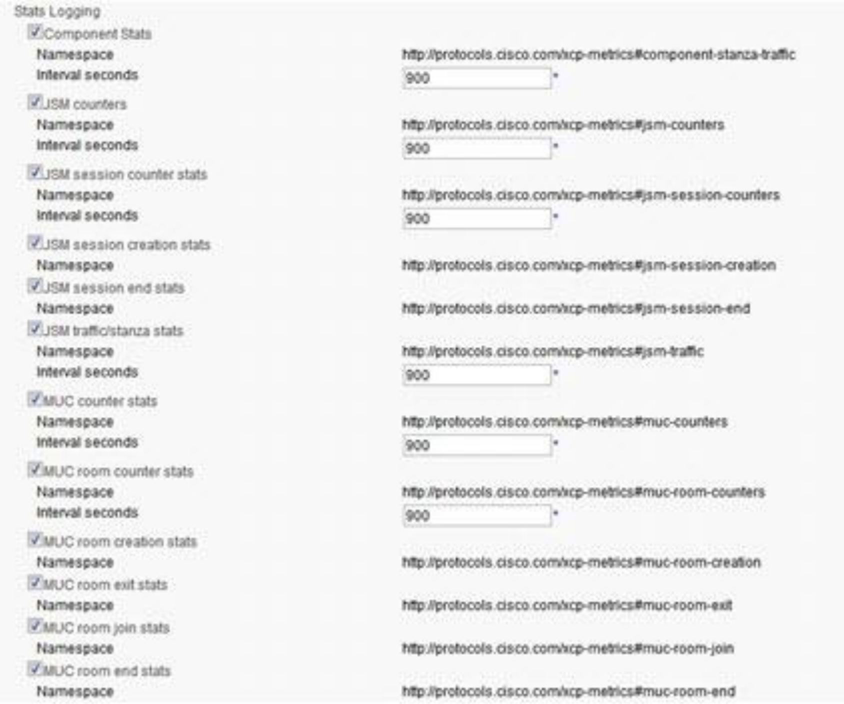
Datasource Name	msginfra_dsn *
Database User Name	conductor *
Database User's Password	••••• *
Confirm Password	••••• *
Database Type	postgresql-odbc ▾ *
Number of connections to the database	11 *
Time in seconds between database connection heartbeats	60 *
Is database debug logging enabled?	0 ▾ *

The basic Database Setup parameters are described in the following table.

Parameter	Description
Datasource Name	This is the name of the component's datasource as specified in the .odbc.ini file. The default value is MsgInfra_dsn.
Database User Name	Enter the username used to connect to the database. The default value is conductor.
Database User's Password	Enter the password used to connect to the database.
Confirm Password	Enter the password again to confirm it.
Database Type	Select the type of database you are using from the list. The MsgInfra Server selects PostgreSQL as its DB server and the default value is postgresql-odbc.

Stats Logging

The Stats Logging option in the Global Settings Configuration page contains configuration about the statistics associated with the Videoscape Control Suite MsgInfra Server. This option would split into several parts by different namespaces to trace different statistics in specified interval seconds. The default value is 900.



Stats Logging

☑ Component Stats	
Namespace	http://protocols.cisco.com/xcp-metrics#component-stanza-traffic
Interval seconds	900 *
☑ JSM counters	
Namespace	http://protocols.cisco.com/xcp-metrics#jsm-counters
Interval seconds	900 *
☑ JSM session counter stats	
Namespace	http://protocols.cisco.com/xcp-metrics#jsm-session-counters
Interval seconds	900 *
☑ JSM session creation stats	
Namespace	http://protocols.cisco.com/xcp-metrics#jsm-session-creation
☑ JSM session end stats	
Namespace	http://protocols.cisco.com/xcp-metrics#jsm-session-end
☑ JSM traffic/stanza stats	
Namespace	http://protocols.cisco.com/xcp-metrics#jsm-traffic
Interval seconds	900 *
☑ MUC counter stats	
Namespace	http://protocols.cisco.com/xcp-metrics#muc-counters
Interval seconds	900 *
☑ MUC room counter stats	
Namespace	http://protocols.cisco.com/xcp-metrics#muc-room-counters
Interval seconds	900 *
☑ MUC room creation stats	
Namespace	http://protocols.cisco.com/xcp-metrics#muc-room-creation
☑ MUC room exit stats	
Namespace	http://protocols.cisco.com/xcp-metrics#muc-room-exit
☑ MUC room join stats	
Namespace	http://protocols.cisco.com/xcp-metrics#muc-room-join
☑ MUC room end stats	
Namespace	http://protocols.cisco.com/xcp-metrics#muc-room-end

3

Logging

Introduction

The Videoscape Control Suite MsgInfra Server provides a number of different logging options. By default, the server's core router is configured to log JSM and router data to syslog at the warn log level. You can change this default level as needed. Any level that you choose logs data at that level, in addition to all the levels above it. For example, when the log level is set to info, data is logged at the warn and error levels as well.

If you require more logging than what occurs by default, you can configure the server to log statistics and other types of JSM data, and to use file and stderr loggers, in addition to syslog. You can also configure syslog and stream loggers for each component.

Note: Logging is an intermediate, and sometimes advanced, feature in the MsgInfra XCP controller. When you configure Logging, make sure you are using the controller's Intermediate or Advanced configuration view.

In This Chapter

Setting the Log Level for Router-Generated Packets

The log level specifies the severity of the data that is logged and determines the amount of data that the server records; the lower the severity level, the more verbose the log. The core router is configured by default to log packets at the warn level and above, which means that log packets are generated only for data that comes into the router at the warn and error levels.

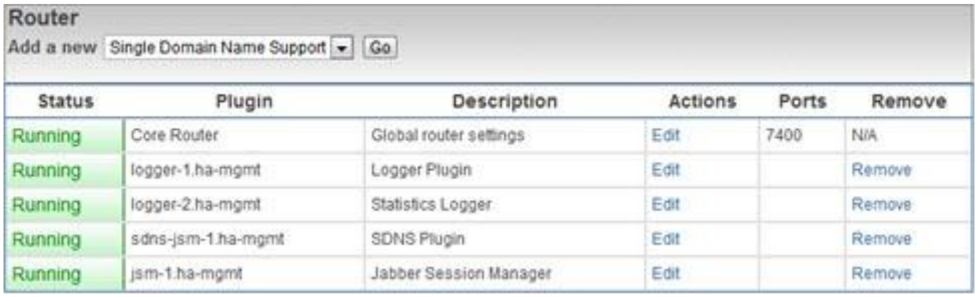
Log levels are described in the following table, and are listed in the order of decreasing severity. For example, the warn log level is less severe than the error log level. The lower the severity level, the higher the log's level of verbosity.

Severity Level	Information Logged
error	System-generated errors, such as the inability to create listen ports, server configuration errors, failure to create the log files, etc.
warn	All error level data plus non-fatal errors, such as bounced packets, nonexistent user logging in, invalid recipient for a message.
info	All error and warn level data, plus information about socket connections and all JSM logs (packet, session, and message).
verbose	All error, warn, and info level data, plus every packet that is processed by the server and JSM.
debug	All log-level data, plus debug data.

Note: The log level must be set to info or higher for the Jabber Session Manager (JSM) log types (message, packet, and session) to function properly. In addition, statistics data is not available if the log's verbosity level is set below info.

Changing the Router's Default Log Level

1 In the **Router** area on the controller's main page, click **Edit**, beside **Global Router Settings**.

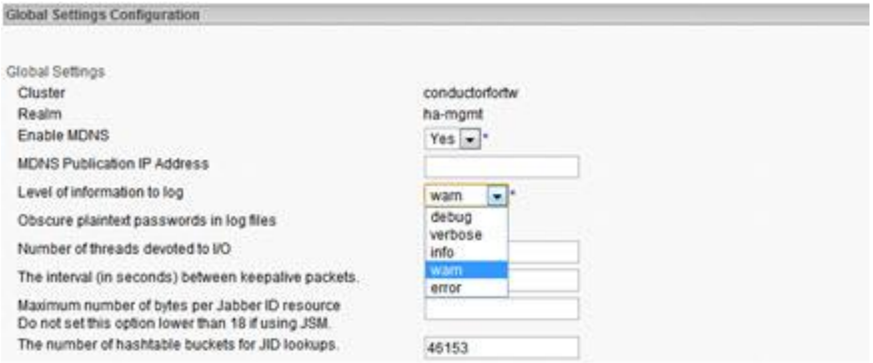


Router

Add a new Single Domain Name Support ▾ Go

Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	logger-1.ha-mgmt	Logger Plugin	Edit		Remove
Running	logger-2.ha-mgmt	Statistics Logger	Edit		Remove
Running	sdns-jsm-1.ha-mgmt	SDNS Plugin	Edit		Remove
Running	jsm-1.ha-mgmt	Jabber Session Manager	Edit		Remove

2 In the Global Settings Configuration page, select the preferred level in the Level of information to log list.



Global Settings Configuration

Global Settings

Cluster	conductorfortw
Realm	ha-mgmt
Enable MDNS	Yes *
MDNS Publication IP Address	
Level of information to log	warn *
Obscure plaintext passwords in log files	
Number of threads devoted to I/O	
The interval (in seconds) between keepalive packets.	
Maximum number of bytes per Jabber ID resource Do not set this option lower than 18 if using JSM.	
The number of hashtable buckets for JID lookups.	46153

3 Scroll to the bottom of the page and click **Submit** to save your configuration.

Jabberd Logger Configuration

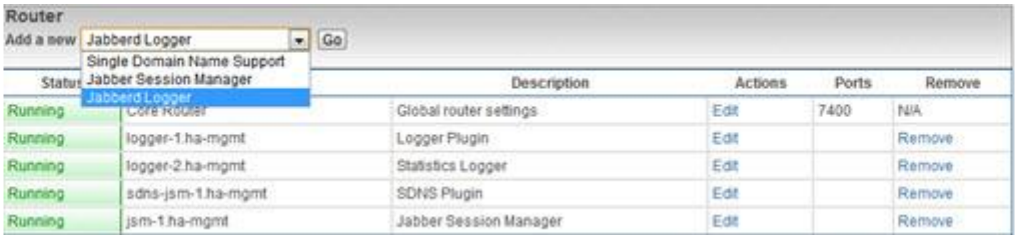
The Jabberd Logger receives packets that are generated by the core router, by JSM, and by any other plugin, and logs them to syslog, file, and/or stderr. The Jabberd Logger that is installed by default is configured to capture information generated in the generic namespace, jcs:log:default, and to log the information to syslog. You can edit the default logger, or you can add new ones. In the Jabberd Logger Configuration page, you can select the namespaces for other types of information that you want to log, and you can specify the names of the hosts from which you want to log the information. You can also select the types of loggers that you want to use, and the log level(s) used to log the information.

You can configure multiple Jabberd Loggers depending on how specific you want your logging to be. For example, if you want to log presence and session packets for host alpha.example.com to a file logger, and message packets for host beta.example.com to syslog, you would need to configure two Jabberd Loggers to handle the logging.

Adding a Jabberd Logger

1 Change to the controller's Intermediate configuration view.

2 In the **Router** area on the controller's main page, select **Jabberd Logger** from the list, and then click **Go**.

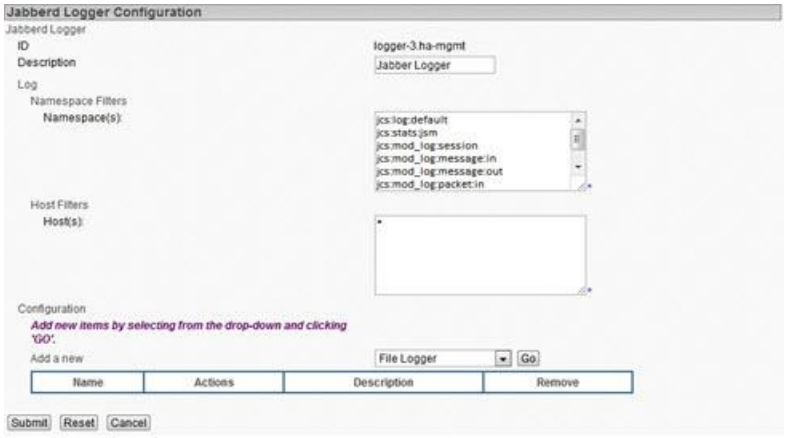


Router

Add a new: Jabberd Logger

Statu		Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	logger-1.ha-mgmt	Logger Plugin	Edit		Remove
Running	logger-2.ha-mgmt	Statistics Logger	Edit		Remove
Running	sdns-jsm-1.ha-mgmt	SDNS Plugin	Edit		Remove
Running	jsm-1.ha-mgmt	Jabber Session Manager	Edit		Remove

Result: The Jabberd Logger Configuration page appears.



Jabberd Logger Configuration

Jabberd Logger

ID: logger-3.ha-mgmt

Description: Jabber Logger

Log

Namespace Filters

Namespace(s):

```
jcs:log:default
jcs:stats:jsm
jcs:mod_log:session
jcs:mod_log:message:in
jcs:mod_log:message:out
jcs:mod_log:packet:in
```

Host Filters

Host(s): *

Configuration

Add new items by selecting from the drop-down and clicking 'GO'.

Add a new: File Logger

Name	Actions	Description	Remove

Note: The remaining sections in this chapter describe how to configure the Jabberd Logger.

Selecting Namespaces

Namespaces are used to capture specific types of log packets that are generated by JSM (mod_log) or the core router. When these packets are generated, they are sent to the Jabberd Logger. If they match the namespaces that are in the **Namespace Filters** list in the Jabberd Logger Configuration page, the Jabberd Logger logs the information to the configured log types (syslog, file, or stderr).

The namespaces that Jabber provides for logging are described in the following table.

Namespace	This Log Captures ...
jcs:log:default	Information from the router and from JSM. This namespace is selected by default.
jcs:stats:jsm	System statistic information. You must select this namespace if you plan to enable Statistics logging in the JSM configuration.
jcs:mod_log:session	Information about each user session that occurs on the server. You must select this namespace if you plan to enable session packet logging in the JSM configuration.
jcs:mod_log:message:in	Incoming messages and file transfer requests as they are received by the server. You must select this namespace if you plan to enable incoming message logging in the JSM configuration, and you want the Jabberd Logger to handle the logging.
jcs:mod_log:message:out	Outgoing messages and file transfer requests as they are sent by the server. You must select this namespace if you plan to enable outgoing message logging in the JSM configuration, and you want the Jabberd Logger to handle the logging.
jcs:mod_log:packet:in	Information about packets going into JSM. **Note:** Logging incoming and outgoing packets is not recommended because of the massive load it places on the router. This type of logging is usually reserved for debugging purposes.
jcs:mod_log:packet:out	Information about packets coming out of JSM.
jcs:mod_log:presence	Information about client users' presence. You must select this namespace if you plan to enable presence packet logging in the JSM configuration.

Specifying Host Filters

In the **Host Filters** box, you can specify the names of hosts from which you want to log the selected packet types. For jcs:log:default packets, you should leave the asterisk (*), which will log packets in that namespace from all hosts. However, for other namespace filters, you can either use the asterisk to indicate that you want to log these packet types from all hosts, or you can list specific hosts only.

Configuring Loggers and Log Levels

In addition to the Syslog logger, which is enabled by default, you can configure a file logger and a standard error logger. In addition, you can select one or more log levels at which to log the information to these log types.

Syslog Logger

The Syslog logger is enabled by default when you install the server. This logger logs information from the router, and from JSM and other plugins to syslog. Syslog refers to the logging daemon used to log messages generated by your operating system components. Syslog also provides log rotation based on file age and size. It can be run locally or remotely and does not require any additional hardware or software.

1 Under **Configuration** on the Jabberd Logger Configuration page, click **Details** beside the **Syslog Logger**. The Syslog Logger Configuration page is displayed. (If you prefer, you can add a new Syslog logger rather than modifying the existing one.)

2 Configure the Syslog Logger parameters as follows.

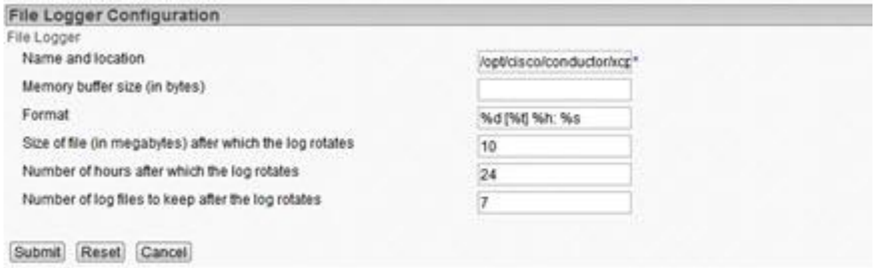
- **Identity** — Identifies where the log information came from. The identity is displayed in syslog next to the associated data. You can change the default value, if preferred.
- **Facility** — Select the facility that you want to use from the list.
- **Format** — Enter the formatters for the information that you want to log to syslog. See ***Formatting Logs*** (on page 24) for more information.

3 Click **Submit** to save your configuration.

File Logger

The File Logger lets you specify the name and location of a log file and various parameters for the information that you want to log to it.

1 Under **Configuration** on the Jabberd Logger Configuration page, select **File Logger** in the list, and then click **Go**. The File Logger Configuration page is displayed.



File Logger Configuration

File Logger

Name and location	/opt/cisco/conductor/xcp *
Memory buffer size (in bytes)	
Format	%d [%t] %h: %s
Size of file (in megabytes) after which the log rotates	10
Number of hours after which the log rotates	24
Number of log files to keep after the log rotates	7

2 Configure the File Logger parameters as follows.

- **Name and location** — Enter the name and location of the log file.
- **Memory buffer size (in bytes)** — Enter the number of bytes in the memory buffer used to store log information. When the size limit is reached, the logs are written to the current log file. If you enter 0, the messages are written to a log file continuously.
- **Format** — Enter the type of information that you want to log to the file using any or all of the log formatters. See ***Formatting Logs*** (on page 24) for more information.
- **Size of file (in megabytes) after which the log rotates** — Enter the size of the log file in megabytes after which the log rotates. For example, if you enter 24, the log rotates out every time the file reaches a size of 24 megabytes. If you enter a value both for this option and the next, the log rotates when it reaches either the size or the age limit.
- **Number of hours after which the log rotates** — Enter the number of hours after which you want the log to rotate. For example, if you enter 24, the log rotates out every 24 hours.
- **Number of log files to keep after the log rotates** — Enter the number of log files to keep after they have been rotated. When this number is reached, the oldest rotated log file is deleted.

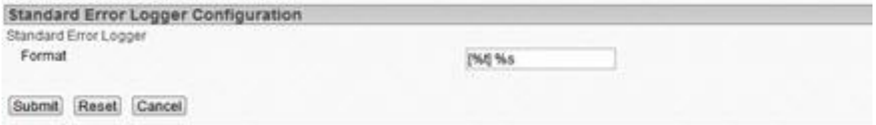
3 Click **Submit** to save your configuration.

Standard Error Logger

The Standard Error Logger lets you format information that is logged to stderr.

1 Under **Configuration** on the Jabberd Logger Configuration page, select **Standard Error Logger** in the list, and then click **Go**.

2 In the Standard Error Logger Configuration page, enter the log formatters for the type of information that you want to log. See ***Formatting Logs*** (on page 24) for more information.



Standard Error Logger Configuration

Standard Error Logger

Format: [%t] %s

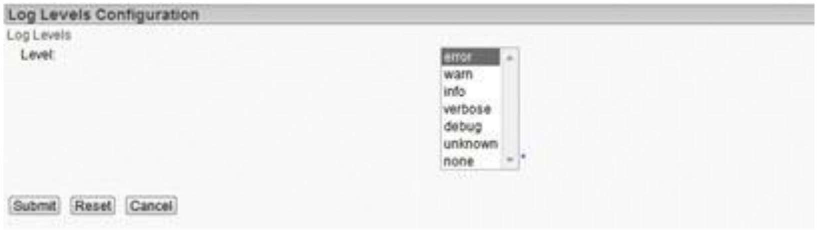
3 Click **Submit** to save your configuration.

Log Levels

You can select one or more log levels, which pertain to all of the loggers configured in this particular instance of the Jabberd Logger plugin.

1 Under **Configuration** on the Jabberd Logger Configuration page, select **Log Levels** in the list, and then click **Go**.

2 In the Log Levels Configuration page, select one or more log levels in the list; hold down the **Ctrl** key to select more than one. The logs that you select for this particular Jabberd Logger configuration will each log at these levels.



3 Click **Submit** to save your configuration.

Formatting Logs

You can modify how log information is formatted using a number of attribute codes. Add any or all of the attribute codes listed in the following table in a logger's **Format** box to capture the desired data in your log.

Format Tag	Description
%h	The point in the code where the log message was generated. In general, this information is useful in debugging the server. It is usually not useful when used with message and session logs.
%i	The thread number inside the server that generates the log message; used for debugging.
%s	The information being logged.
%d	The Greenwich Mean Time and date when the log message was generated.
%t	The log level of the message; for example, none, error, info, warn, verbose, debug. This attribute does not work with message, packet, or session logs.

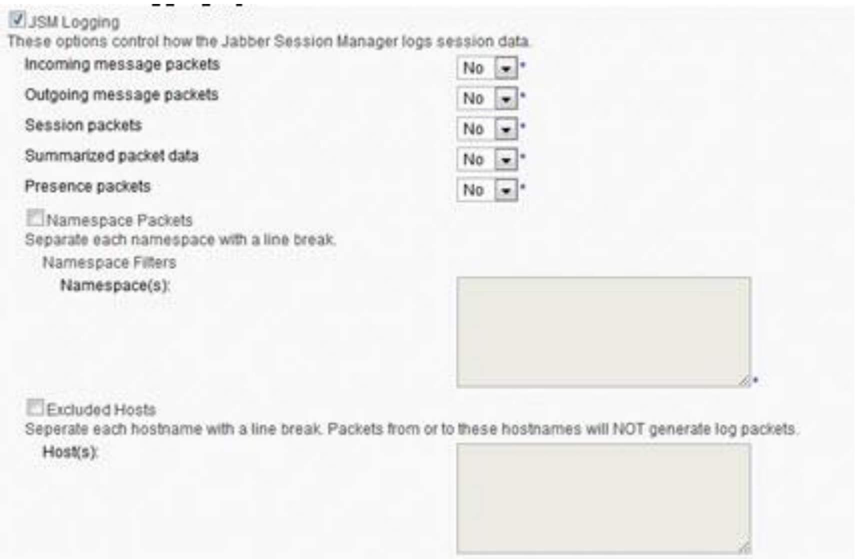
JSM Logging

You can configure the logging of message, session, and presence packets in the Jabber Session Manager. These packets will be logged, in addition to the JSM-generated packets that are logged by default.

1 Change to the controller's Advanced configuration view.

2 In the **Router** area on the controller's main page, click **Edit**, beside **Jabber Session Manager**.

3 In the Jabber Session Manager Configuration page, scroll down toward the bottom of the page, and select the **JSM Logging** option.



☑ JSM Logging

These options control how the Jabber Session Manager logs session data.

Incoming message packets	No
Outgoing message packets	No
Session packets	No
Summarized packet data	No
Presence packets	No

□ Namespace Packets

Separate each namespace with a line break.

Namespace Filters

Namespace(s):

□ Excluded Hosts

Seperate each hostname with a line break. Packets from or to these hostnames will NOT generate log packets.

Host(s):

4 Select **Yes** beside any of the packets that you want to log.

5 Select the **Namespace Packets** option if you want to log IQ packets for specific namespaces. Enter the namespaces in the Namespace(s) box.

Example:

```
jabber:iq:roster
jabber:iq:last
```

6 Select the **Excluded Hosts** option if you want to exclude specific hosts from packet log generation. Enter the host names for each host in the **Host(s)** box. Host name exclusions apply to all logging parameters.

7 Click **Submit** to save your configuration. You are returned to the controller's main page.

8 In the **Router** area, click **Edit**, beside **Logger Plugin**.

9 In the Jabberd Logger Configuration page, select or type the namespaces in the **Namespace Filters** list that correspond to the packet types that you selected for JSM logging. The namespaces correspond to the Jabber Session Manager packets as described in the following list. Packets generated by JSM in these namespaces will be logged to the loggers that you have configured for the Jabberd Logger.

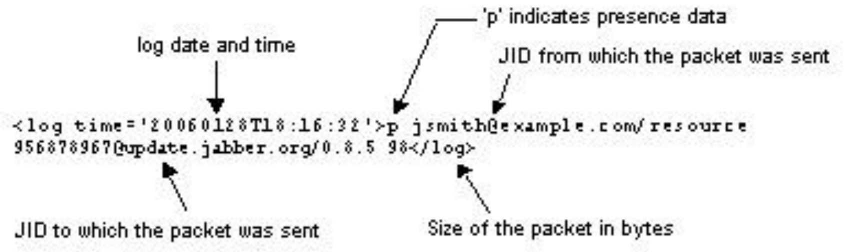
- **jcs:mod_log:session** — Session Packets
- **jcs:mod_log:message:in** — Incoming message packets
- **jcs:mod_log:message:out** — Outgoing message packets
- **jcs:mod_log:packet:in** — Summarized packet data
- **jcs:mod_log:packet:out** — Summarized packet data
- **jcs:mod_log:presence** — Presence packets

10 Click **Submit** to save your configuration.

11 Restart your Videoscape Control Suite MsgInfra system.

Packet Logs

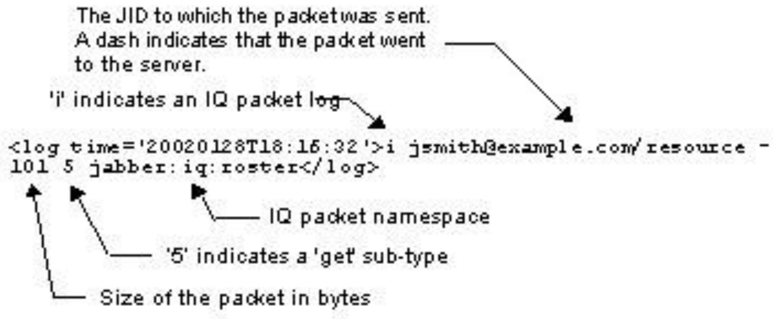
Packet logs contain two types of data: **non-IQ packets** and **IQ packets**. A non-IQ packet records whether the packet contained an IQ packet (designated by i), presence information (designated by p), or subscription information (designated by s). Non-IQ packet information resembles the following:



```
<log time='20060128T18:16:32'>p jsmith@example.com/resource
956878967@update.jabber.org/0.8.5 98</log>
```

'p' indicates presence data
log date and time
JID from which the packet was sent
JID to which the packet was sent
Size of the packet in bytes

An IQ packet contains all of the information that is saved for the non-IQ packet. It also includes a numeric sub-type for the packet and the namespace from which the data came. Numeric sub-types include: 5 for get; 6 for set, and 7 for result. IQ packet log information resembles the following:



```
<log time='20020128T18:16:32'>i jsmith@example.com/resource -
101 5 jabber:iq:roster</log>
```

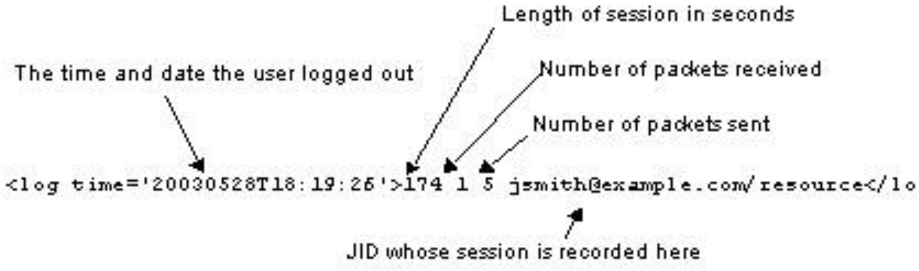
The JID to which the packet was sent.
A dash indicates that the packet went
to the server.
'i' indicates an IQ packet log
IQ packet namespace
'5' indicates a 'get' sub-type
Size of the packet in bytes

Session Logs

Session logs contain information about each user session that occurs on the server. When the user logs off or is disconnected, the server logs the timestamp of when the session ended, the number of seconds the session lasted, and the full Jabber ID of the user associated with the session (for example, user@host/resource). It also records the number of packets sent and received.

The session log provides information only after a session has ended, and therefore does not provide information about a user’s session while that user is logged in.

Session log information resembles the following:



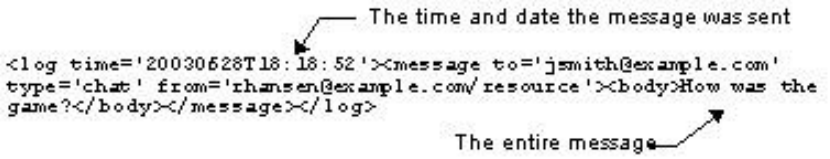
Length of session in seconds
The time and date the user logged out
Number of packets received
Number of packets sent
JID whose session is recorded here

```
<log time='20030528T18:19:26'>174 1 5 jsmith@example.com/resource</lo
```

Message Logs

Message logs contain all messages. You may want to use the message log feature to archive your message traffic. You may archive traffic through the server by writing the message logs to a file and backing them up outside of the server.

Message log information resembles the following:


The time and date the message was sent
The entire message

```
<log time='20030628T18:18:52'><message to='jsmith@example.com'
type='chat' from='rhansen@example.com/resource'><body>How was the
game?</body></message></log>
```

Statistics Logging

Statistics logging captures server statistics and logs the data to log types that are configured for the Jabberd Logger. The **Stats** option in the JSM has also been configured by default to capture data every 60 seconds.

Server statistics data includes the number of:

- Users who are currently online
- Successful logins in the last time-slice interval
- Successful logins since server startup
- Failed logins since server startup
- Offline messages stored in the last time-slice interval
- Total messages since server startup
- Presence packets since server startup
- IQ packets since server startup

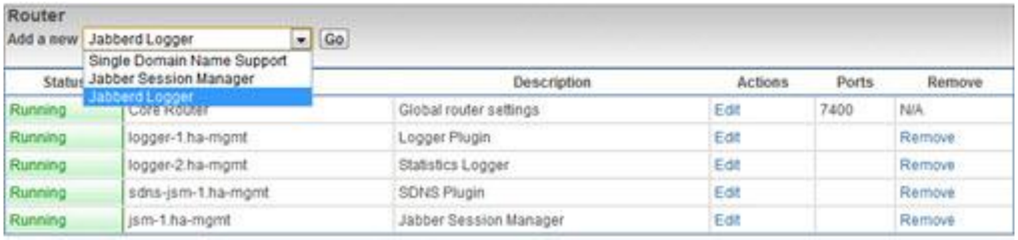
Statistics data also includes information about:

- The length of time, in seconds, that the server has been running
- The average message size in the last time-slice interval
- The number of messages in the last time-slice interval

Adding a New Statistics Logger

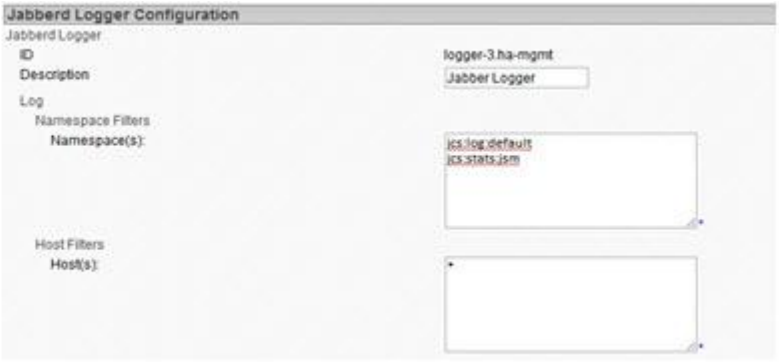
1 Change to the controller's Intermediate configuration view.

2 In the **Router** area on the controller's main page, select **Jabberd Logger** in the list, and then click **Go**.



Statu		Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	logger-1.ha-mgmt	Logger Plugin	Edit		Remove
Running	logger-2.ha-mgmt	Statistics Logger	Edit		Remove
Running	sdns-jsm-1.ha-mgmt	SDNS Plugin	Edit		Remove
Running	jsm-1.ha-mgmt	Jabber Session Manager	Edit		Remove

3 In the Jabberd Logger Configuration page, in the **Namespace Filters** list, remove all of the namespaces except for **`jcs:log:default`** and **`jcs:stats:jsm`**.



Jabberd Logger Configuration

Jabberd Logger

ID: logger-3.ha-mgmt

Description: Jabber Logger

Log

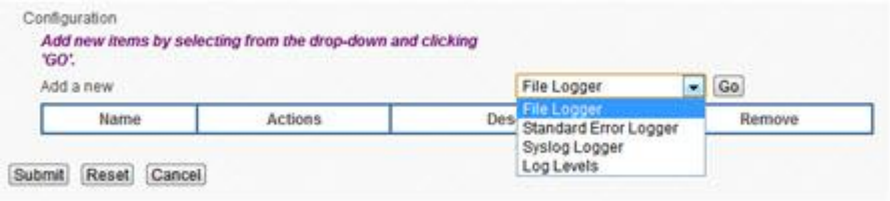
Namespace Filters

Namespace(s): jcs:log:default
jcs:stats:jsm

Host Filters

Host(s): *

4 Add and configure one or more loggers that you want to use for capturing statistic data.



Configuration

Add new items by selecting from the drop-down and clicking 'GO'.

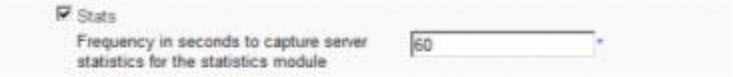
Add a new: File Logger

Name	Actions	Des	Remove

5 Click **Submit** to save your configuration. You are returned to the controller's main page.

6 In the **Router** area, click **Edit**, beside **Jabber Session Manager**.

7 In the Jabber Session Manager Configuration page, under **Stats**, the frequency for capturing server statistics is set to 60 seconds. Change this value if preferred.



☑ Stats

Frequency in seconds to capture server statistics for the statistics module: 60 *

8 Scroll to the bottom of the Jabber Session Manager Configuration page, and click **Submit** to save your configuration.

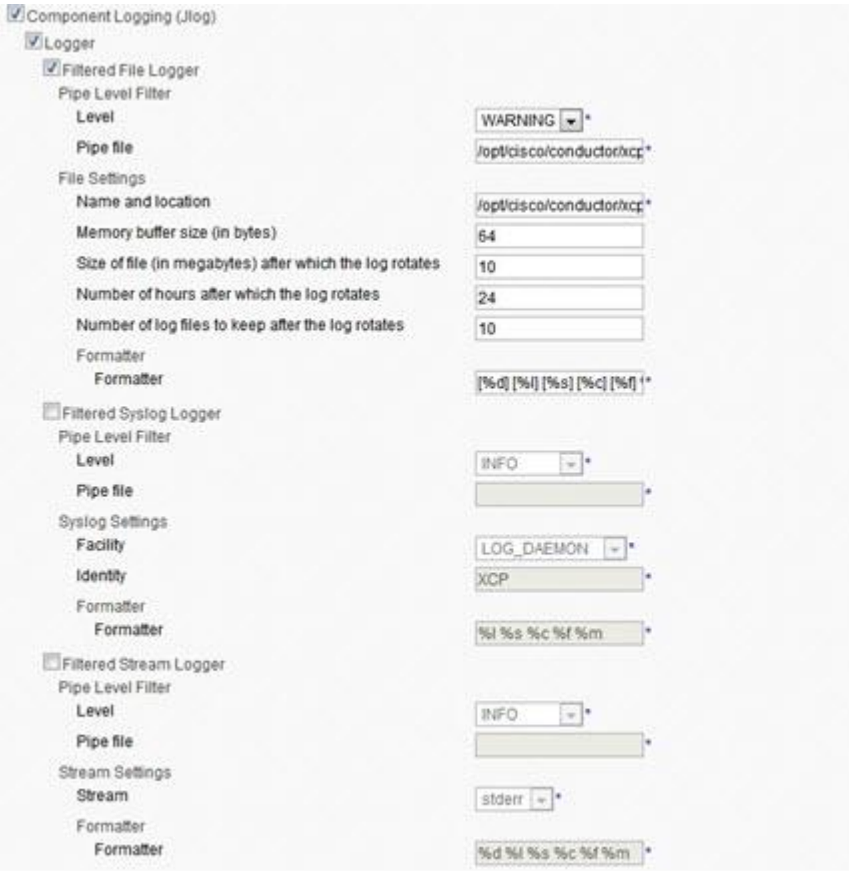
Component Logging - Jlog

All Videoscape Control Suite MsgInfra components can log to the Jabber Logging Library, Jlog. Each component (CM/Pubsub/SASL) configuration page has a **Component Logging** (Jlog) section, in which you can configure Syslog and stream loggers that filter the information based on the selected log level. The information that is logged varies by component.

The Syslog and stream loggers log information that is generated at or above the selected severity level and drops messages that are below that level. For example, if you select the warning level, warning and error messages are logged, and messages at the debug, verbose, and info levels are dropped.

1 Change to the controller's Intermediate or Advanced configuration view.

2 Select the check boxes beside **Component Logging** (Jlog) and **Logger**.



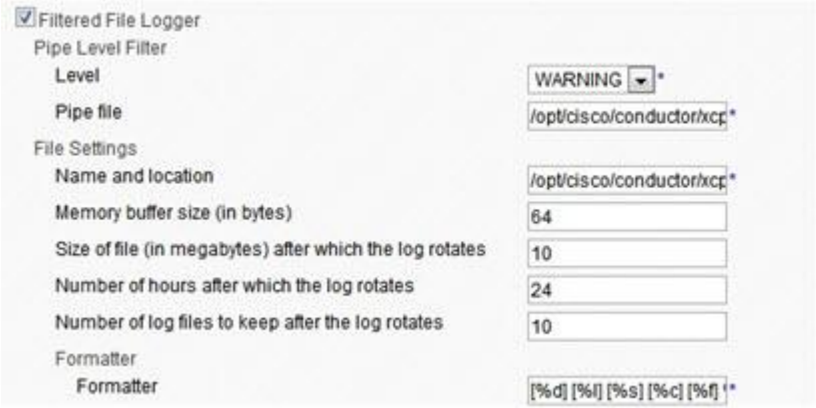
☑ Component Logging (Jlog)
☑ Logger
☑ Filtered File Logger
Pipe Level Filter
Level: WARNING *
Pipe file: /opt/cisco/conductor/xcp *
File Settings
Name and location: /opt/cisco/conductor/xcp *
Memory buffer size (in bytes): 64
Size of file (in megabytes) after which the log rotates: 10
Number of hours after which the log rotates: 24
Number of log files to keep after the log rotates: 10
Formatter
Formatter: [%d] [%l] [%s] [%c] [%f] *
□ Filtered Syslog Logger
Pipe Level Filter
Level: INFO *
Pipe file: *
Syslog Settings
Facility: LOG_DAEMON *
Identity: XCP *
Formatter
Formatter: %l %s %c %f %m *
□ Filtered Stream Logger
Pipe Level Filter
Level: INFO *
Pipe file: *
Stream Settings
Stream: stderr *
Formatter
Formatter: %d %l %s %c %f %m *

3 Select one or other filtered logger types and configure them as described in the following sections.

Configuring the Filtered File Logger

The Filtered File Logger logs component information to file at the selected level.

1 Select the Filtered file Logger option.



☑ Filtered File Logger

Pipe Level Filter

Level	WARNING *
Pipe file	/opt/cisco/conductor/xcp *

File Settings

Name and location	/opt/cisco/conductor/xcp *
Memory buffer size (in bytes)	64
Size of file (in megabytes) after which the log rotates	10
Number of hours after which the log rotates	24
Number of log files to keep after the log rotates	10

Formatter

Formatter	[%d] [%l] [%s] [%c] [%f] *

2 In the **Level** list, select the preferred severity level.

3 In the **Pipe file** box, enter the full path to a pipe file for this component.

Note: If you are running the Videoscape Control Suite MsgInfra Server for Solaris or Linux, we suggest naming the file **`$JABBER_HOME/var/log/comp-id`**, where comp-id is the component's ID. If you are running the Windows version of the server, we suggest naming the file **`\\.\pipe\comp-id`**, where comp-id is the component's ID. If the pipe file does not already exist on your system, it will be created.

You can send the file a pipe command of U (up) or D (down) to increase or decrease the amount of data being logged from the component. For example, if your log level is set to verbose and you send a pipe command of D, the log's level of verbosity is decreased to info.

You can also use the echo C > pipe_file command to create an entry in syslog indicating the current log level for the component. For pipe_file, enter the full or relative path (including the pipe file's name) to the location of the component's pipe file.

4 Select the **File Setting** option.

5 In the **Name and location** box, enter the full path to a log file for this component.

6 In the **Memory buffer size (in bytes)** box, enter a number to define memory buffer size for this component.

7 In the **Size of file (in megabytes) after which the log rotates** box, enter the size of the log file in megabytes after which the log rotates.

8 In the **Number of hours after which the log rotates** box, enter the number of hours after which you want the log to rotate.

9 In the Number of log files to keep after the log rotates box, enter the number of log files to keep after they have been rotated.

10 In the Formatter box, enter the formatters for the information that you want to log. See *Formatting Logs* (on page 24).

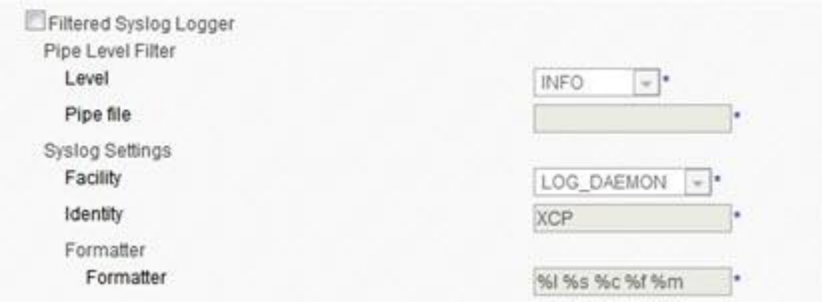
11 When you have finished configuring the loggers, click **Submit** to save your configuration.

12 Restart your MsgInfra system.

Configuring the Filtered Syslog Logger

The **Filtered Syslog Logger** logs component information to syslog at the selected level.

1 Select the **Filtered Syslog Logger** option.



□ Filtered Syslog Logger

Pipe Level Filter

Level: INFO *

Pipe file: *

Syslog Settings

Facility: LOG_DAEMON *

Identity: XCP *

Formatter

Formatter: %l %s %c %f %m *

2 In the **Level** list, select the preferred severity level.

3 In the **Pipe file** box, enter the full path to a pipe file for this component.

Note: If you are running the MsgInfra Server for Solaris or Linux, we suggest naming the file **`$JABBER_HOME/var/log/comp-id`**, where comp-id is the component's ID. If you are running the Windows version of the server, we suggest naming the file **`\\.\pipe\comp-id`**, where comp-id is the component's ID. If the pipe file does not already exist on your system, it will be created.

You can send the file a pipe command of U (up) or D (down) to increase or decrease the amount of data being logged from the component. For example, if your log level is set to verbose and you send a pipe command of D, the log's level of verbosity is decreased to info.

You can also use the **`echo C > pipe_file`** command to create an entry in syslog indicating the current log level for the component. For pipe_file, enter the full or relative path (including the pipe file's name) to the location of the component's pipe file.

4 In the **Facility** list, select the facility that you want to use. Facilities are defined on the syslog(3) manpage.

5 In the **Identity** box, enter a term that identifies where the log information is coming from. The identity is displayed in syslog next to the associated data. You can change the default value as needed.

6 In the **Formatter** box, enter the formatters for the information that you want to log. See *Formatting Logs* (on page 24).

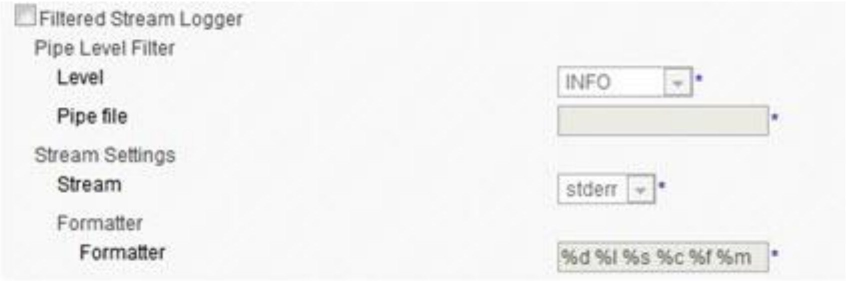
7 When you have finished configuring the loggers, click **Submit** to save your configuration.

8 Restart your MsgInfra system.

Configuring the Filtered Stream Logger

The Filtered Stream Logger logs information to stdout or to stderr at the selected level.

1 Select the **Filtered Stream Logger** option.



□ Filtered Stream Logger

Pipe Level Filter

Level: INFO *

Pipe file: *

Stream Settings

Stream: stderr *

Formatter

Formatter: %d %l %s %c %f %m *

2 In the **Level** list, select the preferred severity level.

3 In the **Pipe File** box, enter the full path to a pipe file for this component.

Note: If you are running the MsgInfra Server for Solaris or Linux, we suggest naming the file **`$JABBER_HOME/var/log/comp-id`**, where comp-id is the component's ID. If you are running the Windows version of the server, we suggest naming the file **`\\.\pipe\comp-id`**, where comp-id is the component's ID. If the pipe file does not already exist on your system, it will be created.

4 In the **Stream** list, select **stderr** or **stdout**.

5 In the **Formatter** box, enter the formatters for the information that you want to log. See ***Formatting Logs*** (on page 24).

6 When you have finished configuring the loggers, click **Submit** to save your configuration.

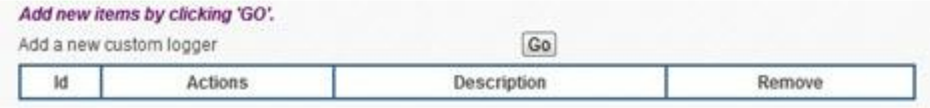
7 Restart your MsgInfra system.

Adding a New Custom Logger

If you have created a custom logger for logging component information using the libjcore library, you can add it to your Videoscape Control Suite MsgInfra Server configuration.

1 Change to the controller's Advanced configuration view.

2 Click **Go** beside **Add a new custom logger**.

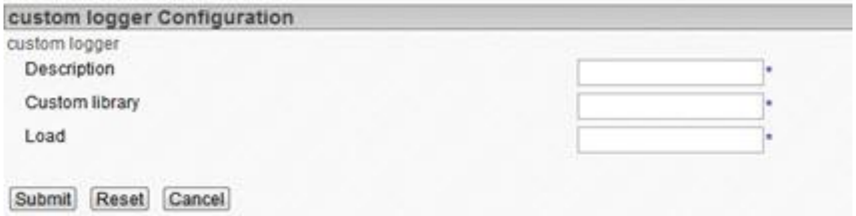


Add new items by clicking 'GO'.

Add a new custom logger

Id	Actions	Description	Remove

Result: The Custom Logger Configuration page is displayed.



custom logger Configuration

custom logger

Description *

Custom library *

Load *

3 Configure the parameters as follows.

- **Description** — Enter a description for the custom logger.
- **Custom Library** — Enter the library used for this logger.
- **Load** — Enter the library entry point function.

4 Click **Submit** to save your custom logger configuration. You are returned to the component's configuration page.

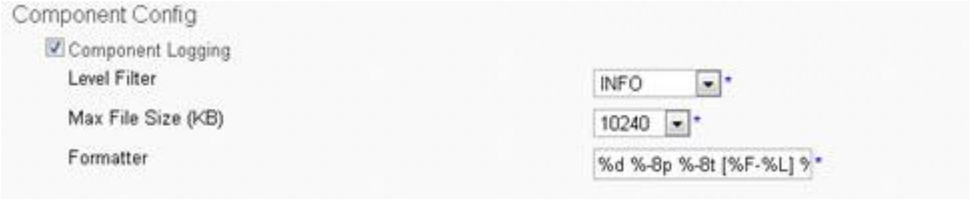
5 Click **Submit** again to return to the controller's main page.

6 Restart your MsgInfra system.

Component Logging – MC/MCC/Web Service Component

Logs of Management Core component, Management Console Controller component, and Web Service component are outputted to one log file. You can configure log attributes of these components, as needed, for debugging.

1. Change to the controller's Advance configuration view.
2. Click **Edit** of the Management Core component, Management Console Controller component, or Web Service component in the **Components** area.



Component Config

☑ Component Logging

Level Filter	INFO *
Max File Size (KB)	10240 *
Formatter	%d %-8p %-8t [%F-%L] % *

3. Configure the Component Config window, as follows:
   - **Level Filter** — Enter the log level as needed. Six levels are supported; they are ERROR, WARNING, INFO, VERBOSE, DEBUG, and ALL. Their priorities are as follows: ERROR > WARNING > INFO> VERBOSE > DEBUG > ALL.

     Note: The default log level is INFO. This means that the log info with INFO, WARNING, and ERROR level will be recorded.
   - **Max File Size** — Enter the maximum log file size. Five options are provided; they are 10M, 20M, 30M, 50M, and 100M.
   - **Formatter** — Enter the output log format as needed. Refer to following formatter table for details.

Conversion Character	Description
%l	Used to output location information of the caller which generated the logging event.
%L	Used to output the line number from where the logging request was issued.
%c	Used to output the category of the logging event. The category conversion specifier can be optionally followed by precision specifier, which is a decimal constant in brackets. If a precision specifier is given, then only the corresponding number of right-most components of the category name will be printed. By default, the category name is printed in full. For example, for the category name "a.b.c" the pattern %c{2} will output "b.c".

Conversion Character	Description
%d	Used to output the date of the logging event. The date conversion specifier may be followed by a date format specifier enclosed between braces. For example, %d{HH:mm:ss,SSS} or %d{dd MMM yyyy HH:mm:ss,SSS}. If no date format specifier is given, then ISO 8601 format is assumed.
%m	Used to output the application-supplied message associated with the logging event.
%p	Used to output the level of the logging event, such as verbose, info, debug, error, etc.
%t	Used to output the name of the thread that generated the logging event.
%n	Outputs the platform-dependent line separator character or characters.

4 Edit the logging configuration and click **Submit**.

4

Jabber Session Manager

Introduction

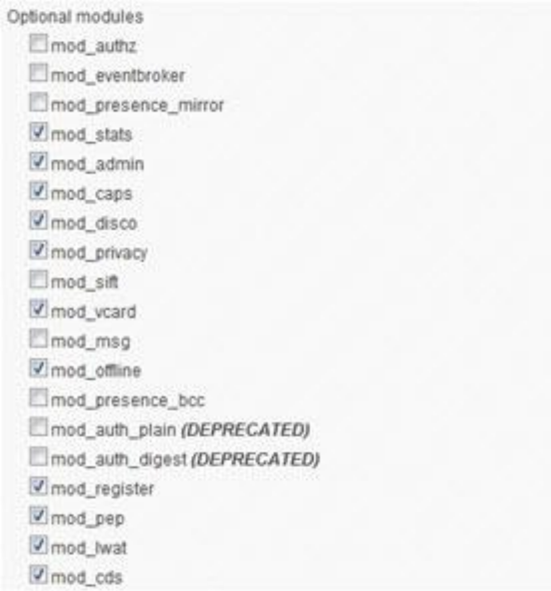
The Jabber Session Manager (JSM) controls all sessions on the Videoscape Control Suite MsgInfra Server. Each time a client connects to the server, a new session is started; one session is opened for every client logged onto the system. An operational Jabber Session Manager is provided by default when you install the Videoscape Control Suite MsgInfra Server. You can modify the configuration, enabling the JSM to handle additional MsgInfra features, as needed.

In This Chapter

Optional Modules

The optional modules are used by the Videoscape Control Suite MsgInfra Server to enable specific features. Many of the modules, once you enable them, must be configured in more detail further down in the JSM configuration, or in a different component.

The **Optional modules** section in the Jabber Session Manager Configuration page is shown in the following figure in the Advanced configuration view so that all of the modules are visible. As shown, some of the modules are selected by default.



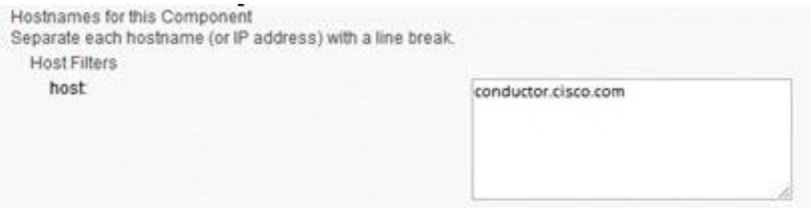
Optional modules

☐ mod_authz
☐ mod_eventbroker
☐ mod_presence_mirror
☑ mod_stats
☑ mod_admin
☑ mod_caps
☑ mod_disco
☑ mod_privacy
☐ mod_sift
☑ mod_vcard
☐ mod_msg
☑ mod_offline
☐ mod_presence_bcc
☐ mod_auth_plain *(DEPRECATED)*
☐ mod_auth_digest *(DEPRECATED)*
☑ mod_register
☑ mod_pep
☑ mod_lwat
☑ mod_cds

See the online help for the Jabber Messenger Configuration page for descriptions of the modules that display in each configuration view.

Hostnames for this Component

The **Hostnames for this Component** configuration section is available in the controller's Intermediate configuration view. JSM will handle packets from all of the hosts listed here.



Hostnames for this Component
Separate each hostname (or IP address) with a line break.
Host Filters
host: conductor.cisco.com

By default, the hostname in the **Host Filters** box belongs to the server on which MsgInfra is installed. You can enter the names or IP addresses of other hosts for which you want this JSM to handle packets, as well. To enable the JSM to handle packets from any host, enter an asterisk (*).

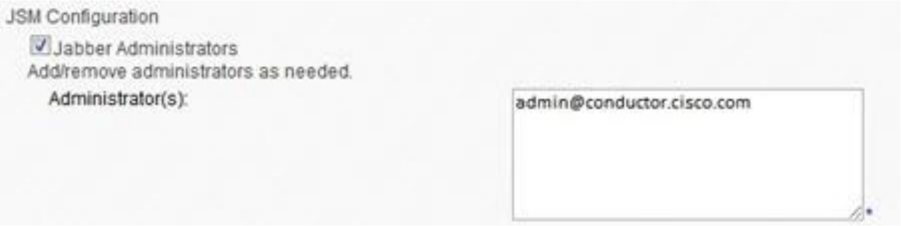
A host filter must be a host name, or an IPv4 or IPv6 address.

Important: If you configure SDNS to run in front of this JSM, leave the **Host Filters** box blank. Since the hostname for which this JSM handles packets must be specified in the SDNS component's configuration, if you add the hostname in the JSM configuration as well, the same packets will be sent to the host twice.

Jabber Administrators

To use the Jabber Administrator feature, select **mod_admin** under **Optional modules**.

The Jabber Administrators configuration section is available in the controller's Intermediate configuration view. You can add and delete Jabber administrators as needed.



JSM Configuration

☑ Jabber Administrators

Add/remove administrators as needed.

Administrator(s): admin@conductor.cisco.com

By default, the **Administrator(s)** box contains the Jabber ID of the person who installed the MsgInfra Server. You can add other Jabber IDs as necessary; separate each Jabber ID with a line break.

The following sections describe tasks that Jabber administrators can perform.

Receiving License Notifications

Jabber administrators receive IM notifications when the MsgInfra Server license is about to expire. The notifications start one week before the license is due to expire, and are repeated with increasing frequency until the expiration occurs.

Unregistering Users

Jabber administrators can unregister any user who has an account on the MsgInfra Server. To do this, the administrator must use a client that is capable of sending raw XML to the server. Once a user has been unregistered, his or her account is deactivated, and the Jabber ID is marked unavailable. Unregistered users are automatically removed from the rosters of contacts on the same server who are subscribed to their presence. (They may not be removed from the rosters of people who are on other Jabber servers.)

Deleting Offline Messages

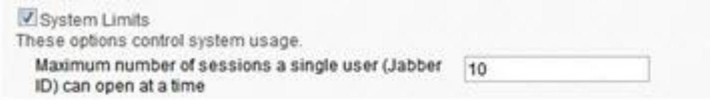
When a Jabber user is unregistered, the user's persistent data, such as preferences, v-card, JID, and off-line messages, remains stored in the system.

Broadcasting Messages to All Users

Jabber administrators can broadcast messages through a Videoscape Control Suite client to all users who are connected to a specific Connection Manager.

System Limits

The **System Limits** configuration section is available in the controller's Advanced configuration view. This setting controls the usage of your Videoscape Control Suite MsgInfra system.



☑ System Limits

These options control system usage.

Maximum number of sessions a single user (Jabber ID) can open at a time: 10

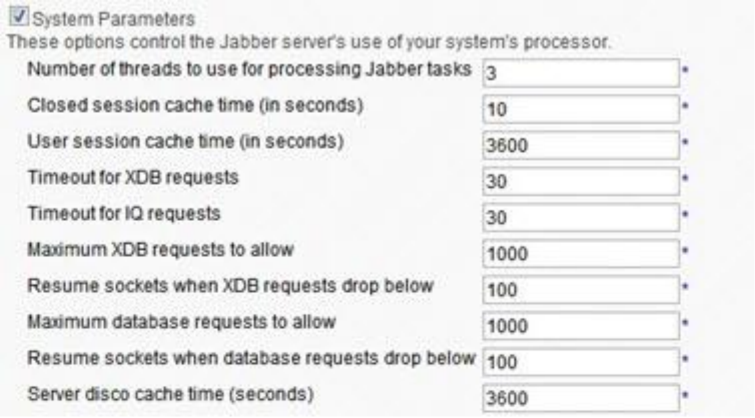
The **System Limits** parameter is described, as follows:

- **Maximum number of sessions a single user (Jabber ID) can open at a time** — Enter the maximum number of sessions a Jabber user can have on the server using the same Jabber ID and different resources. Each time a Jabber user logs into the server, a session is created. If the same user logs on from two locations, that user has two sessions active on the server.

  Users may define a number of concurrent sessions in cluster.xml by JSM's **maxsession** attribute. The default value is 10.

System Parameters

The **System Parameters** configuration section is available in the controller’s Advanced configuration view. These parameters control the MsgInfra Server’s use of your system’s processor, and default values have been supplied based on average server usage. If you want to change these values, we recommend that you call Jabber Support for help.



☑ System Parameters

These options control the Jabber server's use of your system's processor.

Number of threads to use for processing Jabber tasks	3 *
Closed session cache time (in seconds)	10 *
User session cache time (in seconds)	3600 *
Timeout for XDB requests	30 *
Timeout for IQ requests	30 *
Maximum XDB requests to allow	1000 *
Resume sockets when XDB requests drop below	100 *
Maximum database requests to allow	1000 *
Resume sockets when database requests drop below	100 *
Server disco cache time (seconds)	3600 *

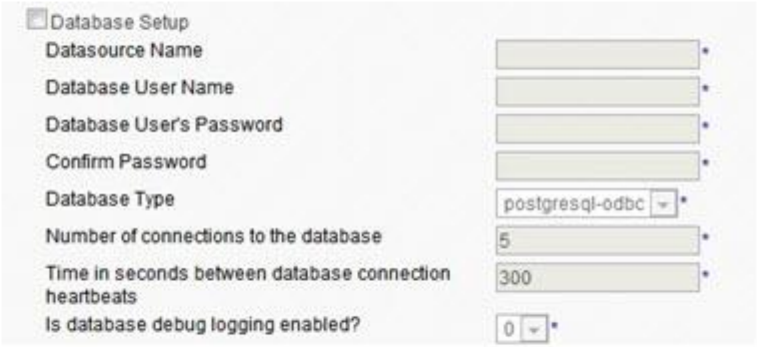
The System Parameters are described in the following table.

Parameter	Description
Number of threads to use for processing Jabber tasks	The number of threads that the MsgInfra Server should create to process Jabber tasks. We recommend that you use the number of CPUs plus 1. Creating more threads enables the MsgInfra Server to process Jabber tasks more quickly, but uses more of your system’s processor. The default value is 3.
Closed session cache time (in seconds)	The number of seconds that a user’s session is cached in memory after he or she logs out. The lower the number of seconds, the more time JSM must spend trying to free memory. The higher the number of seconds, the fewer times cleanup occurs. The default value is 10.
User session cache time (in seconds)	The number of seconds that a user’s session resources are cached after he or she has logged out from all sessions. The lower the number of seconds, the more time JSM must spend trying to free memory. The higher the number of seconds, the fewer times cleanup occurs. The default value is 3600.

Parameter	Description
Timeout for XDB requests	The number of seconds to wait before an XDB request that has been sent to the router times out. This setting affects users; the higher the setting, the slower the system runs. If you are configuring JSM for the **Redirect Events to External Component** feature, set this value to something greater than 0. The default value is 30.
Timeout for IQ requests	The number of seconds to wait before an IQ request that has been sent to the router times out. This item is used only during the discovery of other components, and its setting has no effect on users. The default value is 30.
Maximum XDB requests to allow	The number of XDB requests that can be sent to the JSM from the Connection Manager (CM) at one time. When this number is reached, the MsgInfra core router tells the CM to stop listening on its socket. The default value is 1000.
Resume sockets when XDB requests drop below	The number of XDB requests that JSM still must handle before accepting them again from the CM. When this number is reached, the MsgInfra core router tells the CM to resume listening on its socket. The default value is 100.
Maximum database requests to allow	The number of database requests that can be sent to the JSM at one time. When this number is reached, the MsgInfra core router tells the CM to stop listening on its socket. The default value is 1000.
Resume sockets when database requests drop below	The number of database requests that JSM still must handle before accepting them again. When this number is reached, the MsgInfra core router tells the CM to resume listening on its socket. The default value is 100.
Server disco cache time (seconds)	The number of Videoscape Control Suite Server caches the service discovery data timeout. The default value is 3600.

Database Setup

The **Database Setup** configuration section is available in the controller’s Intermediate and Advanced configuration views. If you selected one of the other databases, this option is dimmed.



□ Database Setup

Datasource Name	*
Database User Name	*
Database User's Password	*
Confirm Password	*
Database Type	postgresql-odbc *
Number of connections to the database	5 *
Time in seconds between database connection heartbeats	300 *
Is database debug logging enabled?	0 *

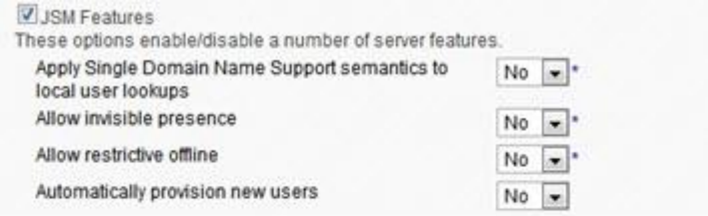
Any database configured in this section is used only to store basic Jabber IM data such as usernames, passwords, rosters, vCard information, and offline messages.

The Database Setup parameters are described in the following table.

Parameter	**Description**
Datasource Name	Enter the name of the database’s datasource.
Database User Name	Enter the username used to connect to the database.
Database User’s Password	Enter the password used to connect to the database.
Confirm Password	Enter the password again to confirm it.
Database Type	Select the type of database you are using from the list.
Number of connections to the database	Enter the number of connections that you want the component to use for processing requests.
Time in seconds between database connection heartbeats	Enter the number of seconds after which the database connection should refresh. Do not set this value to zero without contacting Jabber support.
Is database debug logging enabled? (Advanced view only)	Select 1 to log database debug information. Database logging uses the Conductor MsgInfra router’s logging facility, the Jabberd Logger. The log level must be set to debug for database logging to occur.

JSM Features

The **JSM Features** configuration section is available in the controller's Advanced configuration view. These parameters are used to enable and disable a number of miscellaneous server features.



☑ JSM Features

These options enable/disable a number of server features.

Apply Single Domain Name Support semantics to local user lookups: No *

Allow invisible presence: No *

Allow restrictive offline: No *

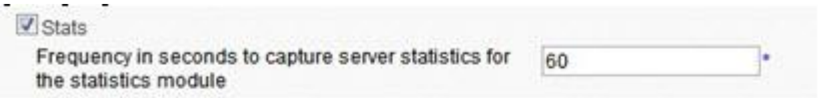
Automatically provision new users: No

The JSM feature parameters are described in the following table.

Parameter	Description
Apply Single Domain Name Support semantics to local user lookups	Select **Yes** if you are using Single Domain Name Support (SDNS) for multiple JSMs. SDNS determines if a particular Jabber ID is a local user when users are spread across multiple domains.
Allow invisible presence	Select **Yes** if you want to allow users to set their presence to **Invisible** so that they can be online with the MsgInfra Server, but show up in their contacts' rosters as offline.
Allow restrictive offline	Select **Yes** if you want to prevent the server from off-lining bounced messages that are empty. This setting affects message packets only.
Automatically provision new users	Select **Yes** if you want users who authenticate via SASL or x509 to be created automatically in the JSM database when they create a new session. With the **Yes** setting, you will no longer have to provision users in the JSM database as part of your new employee provisioning process.

Stats

The **Stats** feature, available in the controller's Intermediate configuration view, logs server statistics to the log types that are configured for the statistics logger. A Statistics logger has been set up by default in the MsgInfra Server configuration and logs info-level data to **`$JABBER_HOME/var/log/stats-logger.log`**. The Stats feature has been configured by default to capture data every 60 seconds. You can change the frequency if preferred.

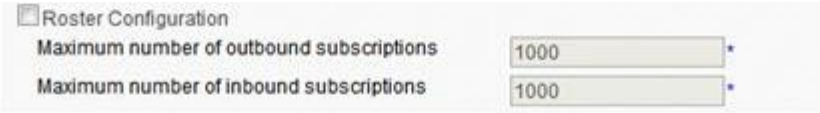


☑ Stats

Frequency in seconds to capture server statistics for the statistics module: 60 *

Roster Configuration

The **Roster Configuration** section is available in the controller's Advanced configuration view.



□ Roster Configuration

Maximum number of outbound subscriptions 1000 *

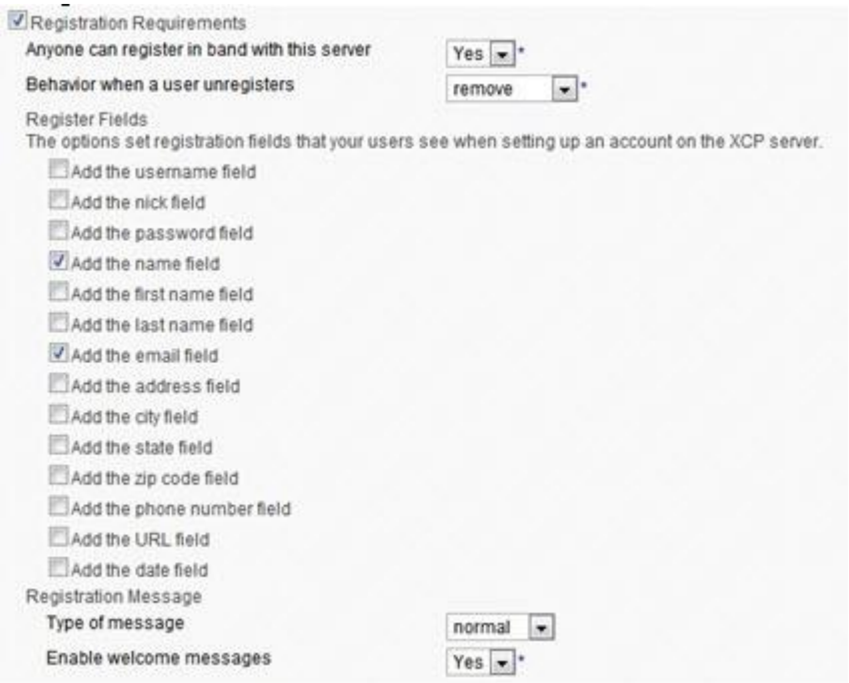
Maximum number of inbound subscriptions 1000 *

Select the **Roster Configuration option** if you want to change the default setting (150) for the maximum number of items that users can have in their rosters. This feature limits how much space rosters require on your Videoscape Control Suite MsgInfra Server. Roster items include contacts, pending contacts, and any other item that appears in the roster.

Registration Requirements

The **Registration Requirements** feature, which is enabled by default, lets client users create accounts on the MsgInfra Server. It also lets you configure the information and prompts that display in the client interface when users register.

The **Registration Requirements** configuration section is available in the controller's Basic and Intermediate configuration views.



☑ Registration Requirements

Anyone can register in band with this server: Yes *

Behavior when a user unregisters: remove *

Register Fields

The options set registration fields that your users see when setting up an account on the XCP server.

- □ Add the username field
- □ Add the nick field
- □ Add the password field
- ☑ Add the name field
- □ Add the first name field
- □ Add the last name field
- ☑ Add the email field
- □ Add the address field
- □ Add the city field
- □ Add the state field
- □ Add the zip code field
- □ Add the phone number field
- □ Add the URL field
- □ Add the date field

Registration Message

Type of message: normal

Enable welcome messages: Yes *

1 Change to the controller's Intermediate configuration view.

2 Select **mod_register** under **Optional** modules.

3 Under **Registration Requirements**, select the registration fields that you want to display on the client.

4 Configure the following parameters as needed.

- **Anyone can register in band with this server** — When set to **Yes**, anyone can create an account on this server using Jabber (pre-XMPP) protocol. If you select **No**, users cannot register in-band.
- **Behavior when a user unregisters** — Select to determine the action the server should take when a user unregisters. The default setting is **remove**, which removes the user from the database. The **disable** option disables the user's account without removing them from the database. The **not-allowed** option prevents users from unregistering.
- **Registration Message** — The server uses these parameters to send an instant welcome message to newly created accounts. If you want to change the wording of a message, you must modify your dictionary file.

- **Type of message** — Select **normal**, **chat**, or **headline** for the type of registration message you want sent. The Jabber clients always use the chat type, which sends welcome messages in a chat window.

  You can select another message type if you are using a custom client. For example, a **headline** type could be a pop-up message, and a **normal** type could be a message sent in a window containing a **Reply** button. You must define these types as you plan to use them with your custom client.
- **Enable welcome messages** — Select **Yes** if you want the server to send a welcome message to users after they register.

JSM Logging

The **JSM Logging** feature lets you log message, session, and presence packets in addition to the JSM-generated packets that are logged by the server by default.

5

Connection Managers

Introduction

The Connection Manager (CM) enables Videoscape Control Suite clients to connect to the MsgInfra Server. You can configure multiple instances of the CM to increase the number of connections your server can handle and to enable communication over different protocols.

Cisco Systems, Inc. strongly recommends that you configure a separate CM to handle each different communication task rather than configuring one CM to do everything. The reasons for this include:

- **Scalability** — Each CM has a maximum number of connections that it can handle. For example, the client CM can handle only 20,000 concurrent client connections. Your system can handle more client connections if you add additional client CMs.
- **Different communication protocols** — Cisco Systems, Inc. recommends that you configure a separate CM to handle each communication protocol that you plan to use.
- **Redundancy** — Configuring separate CMs also helps to ensure that you experience as few communication problems as possible. If the system on which one CM is installed fails, other systems can pick up the slack.

In This Chapter

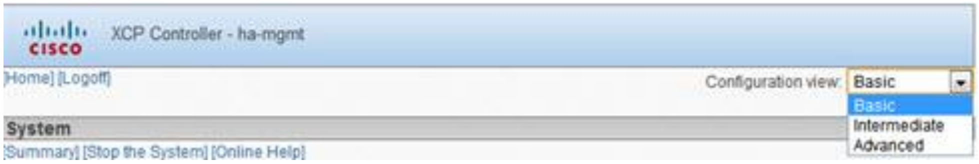
Configure the Basic Connection Manager

This section describes how to configure the Connection Manager component. The command processors that you can configure within the Connection Manager are described in separate chapters.

The following instructions describe how to configure the Connection Manager using the parameters provided in the controller's Basic configuration view. These parameters are sufficient to configure an operational CM. For descriptions of all of the CM parameters, see the Connection Manager Configuration page's online help.

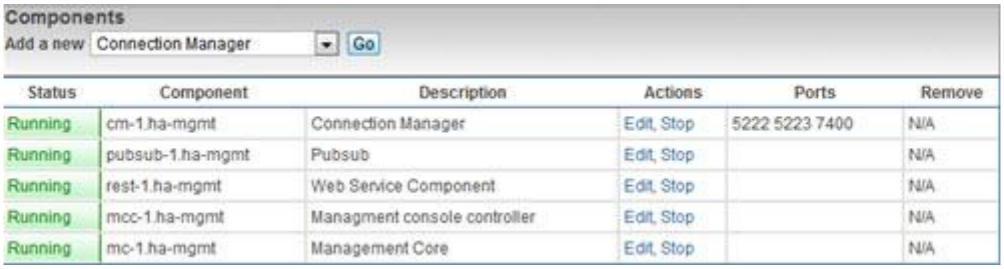
Configuring a Basic Connection Manager

1 Change to the controller's Basic configuration view.



Configuration view: Basic

2 In the **Components** area on the controller's main page, click **Go** to add a Connection Manager.

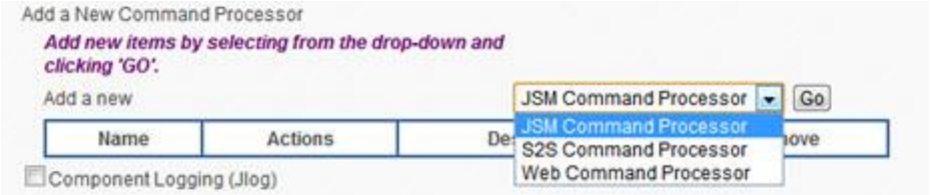


Add a new Connection Manager

Status	Component	Description	Actions	Ports	Remove
Running	cm-1.ha-mgmt	Connection Manager	Edit, Stop	5222 5223 7400	N/A
Running	pubsub-1.ha-mgmt	Pubsub	Edit, Stop		N/A
Running	rest-1.ha-mgmt	Web Service Component	Edit, Stop		N/A
Running	mcc-1.ha-mgmt	Managment console controller	Edit, Stop		N/A
Running	mc-1.ha-mgmt	Management Core	Edit, Stop		N/A

3 On the Connection Manager Configuration page, change the **Description** so that it describes this particular CM.

4 Under **Add a New Command Processor**, select a command processor in the list, and then click **Go**.



Add new items by selecting from the drop-down and clicking 'GO'.

Add a new JSM Command Processor

□ Component Logging (Jlog)

Note: The command processors are described as follows.

- **JSM Command Processor** — Connects the MsgInfra Server to Videoscape Control Suite clients. Configuration instructions for this command processor are provided in *Client Connections* (on page 57).
- **S2S Command Processor** — Enables MsgInfra Servers to communicate with each other across domains.

- **Web Command Processor** — Handles HTTP requests, and translates and transfers data between Videoscape Control Suite clients and the MsgInfra router over the Web.

5 When you have finished configuring the command processor and have returned to the Connection Manager Configuration page, click **Submit** to save your configuration.

6

Client Connections

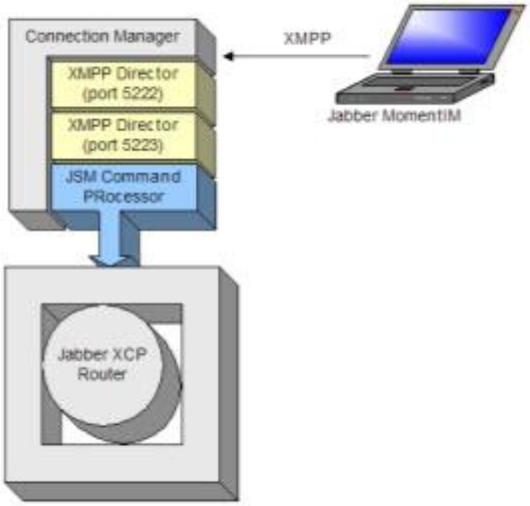
Introduction

When you install the Videoscape Control Suite MsgInfra Server, there may be two types of Connection Managers in a default installation. The first CM (**`cm-1.ha-cmps, cm-2.ha-cmps`**), is configured to work with Videoscape Control Suite clients that use XMPP connections. The second CM (**`cmw-1.ha-cmps`**) is configured for Videoscape Control Suite clients that use HTTP Binding connections (BOSH).

In This Chapter

XMPP Connection Manager

The XMPP Connection Manager that is set up by default (**`cm-1.ha-cmps, cm-2.ha-cmps`**) is configured with a JSM Command Processor and two XMPP directors.

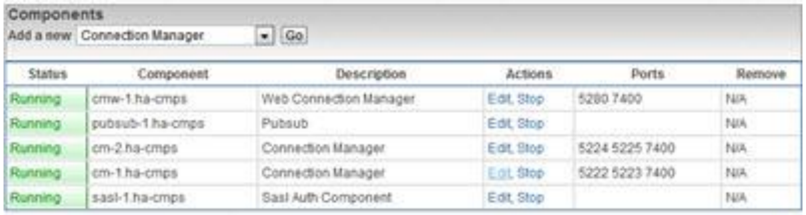


JSM Command Processor Configuration

Important: If you want to add a new JSM Command Processor, Cisco recommends that you configure it in a separate Connection Manager in order to maximize the efficiency with which the MsgInfra Server can handle client communication.

Viewing the Configuration

1. Change to the controller's Intermediate configuration view.
2. In the **Components** area on the controller's main page, click **Edit** beside the first Connection Manager.

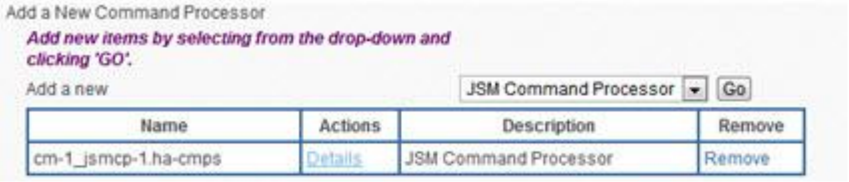


Components

Add a new Connection Manager Go

Status	Component	Description	Actions	Ports	Remove
Running	cmw-1.ha-cmps	Web Connection Manager	Edit, Stop	5280 7400	N/A
Running	pubsub-1.ha-cmps	Pubsub	Edit, Stop		N/A
Running	cm-2.ha-cmps	Connection Manager	Edit, Stop	5224 5225 7400	N/A
Running	cm-1.ha-cmps	Connection Manager	Edit, Stop	5222 5223 7400	N/A
Running	sasl-1.ha-cmps	Sasl Auth Component	Edit, Stop		N/A

3. In the Connection Manager Configuration page under **Add a New Command Processor**, click **Details** beside the JSM command processor.



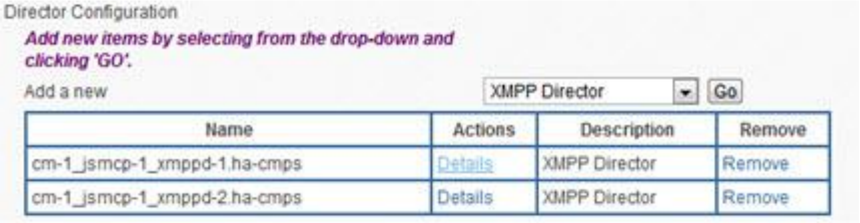
Add a New Command Processor

Add new items by selecting from the drop-down and clicking 'GO'.

Add a new JSM Command Processor Go

Name	Actions	Description	Remove
cm-1_jsmcp-1.ha-cmps	Details	JSM Command Processor	Remove

4 In the JSM Command Processor Configuration page, click **Details** beside the **XMPP Directors** if you want to view their configurations.



Director Configuration

Add new items by selecting from the drop-down and clicking 'GO'.

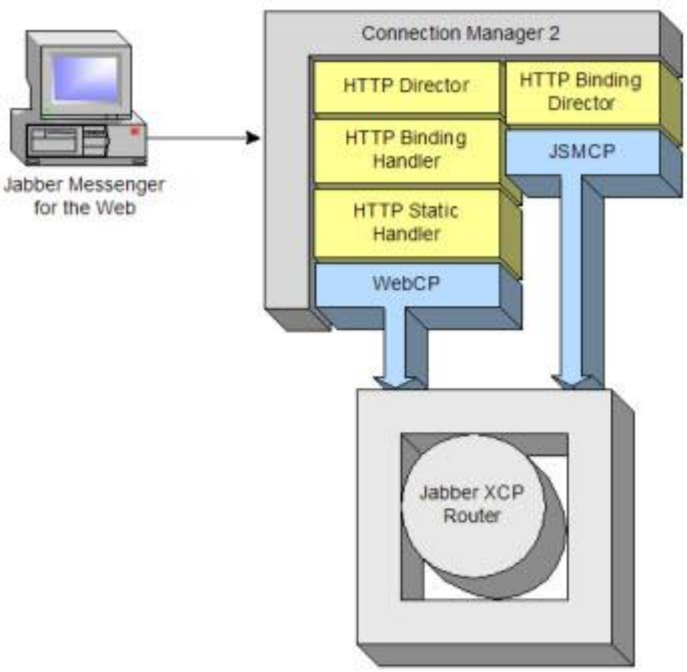
Add a new XMPP Director

Name	Actions	Description	Remove
cm-1_jsmcp-1_xmppd-1.ha-cmps	Details	XMPP Director	Remove
cm-1_jsmcp-1_xmppd-2.ha-cmps	Details	XMPP Director	Remove

HTTP Binding (BOSH) Connection Manager

The HTTP Binding (BOSH) Connection Manager that is set up by default (**`cmw-1.ha-cmps`**) is illustrated in the following figure. It is configured with a JSM Command Processor containing an HTTP Binding Director, and a Web Command Processor containing an HTTP Director, an HTTP Binding Handler, and an HTTP Static Handler.

HTTP binding connections wrap XMPP traffic in HTML, enabling XEP-0124-compliant, web-based clients to access the MsgInfra Server without requiring any changes to network or firewall settings. The HTTP binding feature complies with **XEP-0124: HTTP Binding**.



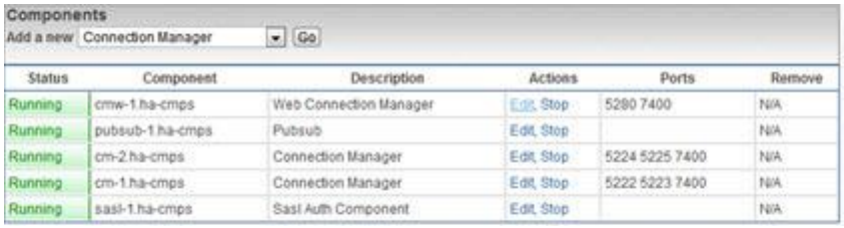
JSM Command Processor Configuration (BOSH)

The JSM Command Processor is configured with an HTTP Binding Director, which interprets HTTP-wrapped XMPP packets, strips off the HTTP wrapper, and forwards the packets to the JSM.

Viewing the Configuration

1 Change to the controllers Basic configuration view.

2 In the **Components** area on the controller's main page, click **Edit** beside the second Connection Manager.

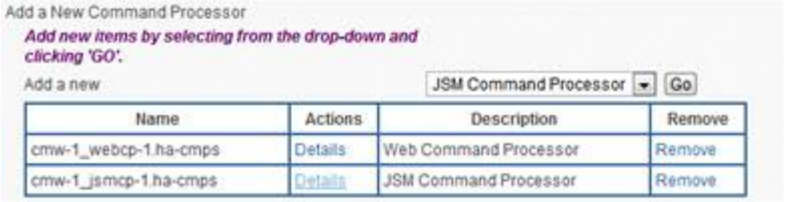


Components

Add a new Connection Manager Go

Status	Component	Description	Actions	Ports	Remove
Running	cmw-1.ha-cmps	Web Connection Manager	Edit, Stop	5280 7400	N/A
Running	pubsub-1.ha-cmps	Pubsub	Edit, Stop		N/A
Running	cm-2.ha-cmps	Connection Manager	Edit, Stop	5224 5225 7400	N/A
Running	cm-1.ha-cmps	Connection Manager	Edit, Stop	5222 5223 7400	N/A
Running	sasl-1.ha-cmps	Sasl Auth Component	Edit, Stop		N/A

3 In the Connection Manager Configuration page, in the table of configured command processors, click **Details** beside JSM Command Processor.



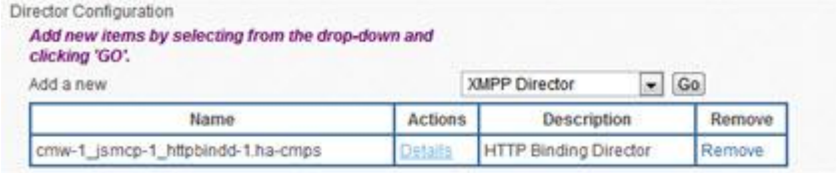
Add a New Command Processor

Add new items by selecting from the drop-down and clicking 'GO'.

Add a new JSM Command Processor Go

Name	Actions	Description	Remove
cmw-1_webcp-1.ha-cmps	Details	Web Command Processor	Remove
cmw-1_jsmcp-1.ha-cmps	Details	JSM Command Processor	Remove

4 In the JSM Command Processor Configuration page, under **Director Configuration**, click **Details** beside HTTP Binding Director.



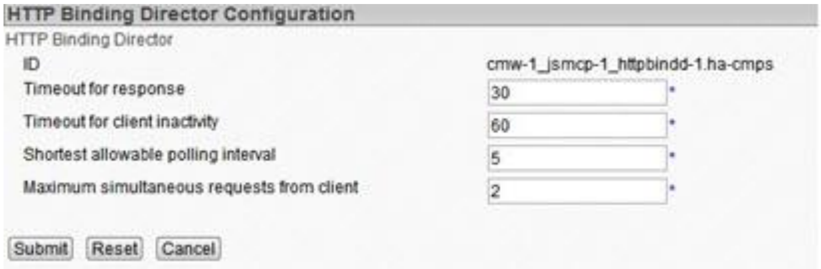
Director Configuration

Add new items by selecting from the drop-down and clicking 'GO'.

Add a new XMPP Director Go

Name	Actions	Description	Remove
cmw-1_jsmcp-1_httpbindd-1.ha-cmps	Details	HTTP Binding Director	Remove

5 In the HTTP Binding Director Configuration page, default values have been provided. They are described in the following table. You can change them if you prefer.



HTTP Binding Director Configuration

HTTP Binding Director

ID	cmw-1_jsmcp-1_httpbindd-1.ha-cmps
Timeout for response	30 *
Timeout for client inactivity	60 *
Shortest allowable polling interval	5 *
Maximum simultaneous requests from client	2 *

Parameter	Description
Timeout for response	The maximum number of seconds that the HTTP binding director will wait to respond to a request from the client. The default value is 30.
Timeout for client inactivity	The maximum number of seconds that a client can be inactive before the HTTP connection is shut down. The default value is 60.

Parameter	Description
Shortest allowable polling interval	The shortest allowable polling interval (in seconds) after which the client may send a polling request. If polling requests are sent in shorter time intervals, the HTTP connection is shut down. The default value is 5.
Maximum simultaneous requests from client	The number of simultaneous requests that the client can make with the requests attribute. The recommended value is 2, which is the default setting. If a client makes more simultaneous requests than the number specified here, the HTTP connection shuts down. The default value is 2.

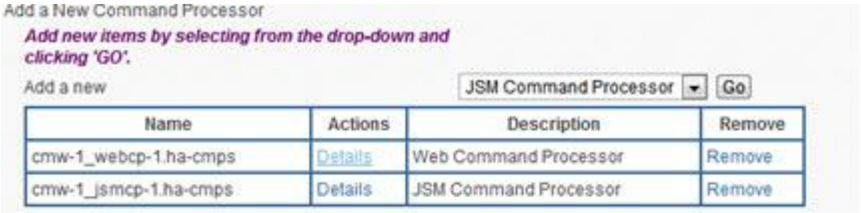
Web Command Processor Configuration

The Web Command Processor is configured with an HTTP Director, an HTTP Binding Handler, and an HTTP Static Handler. The HTTP binding handler intercepts XEP-124-compliant packets, and forwards them to the HTTP binding director.

Viewing the Configuration

1 Change to the controller's Advanced configuration view.

2 In the Connection Manager Configuration page, in the table of configured command processors, click **Details** beside Web Command Processor.



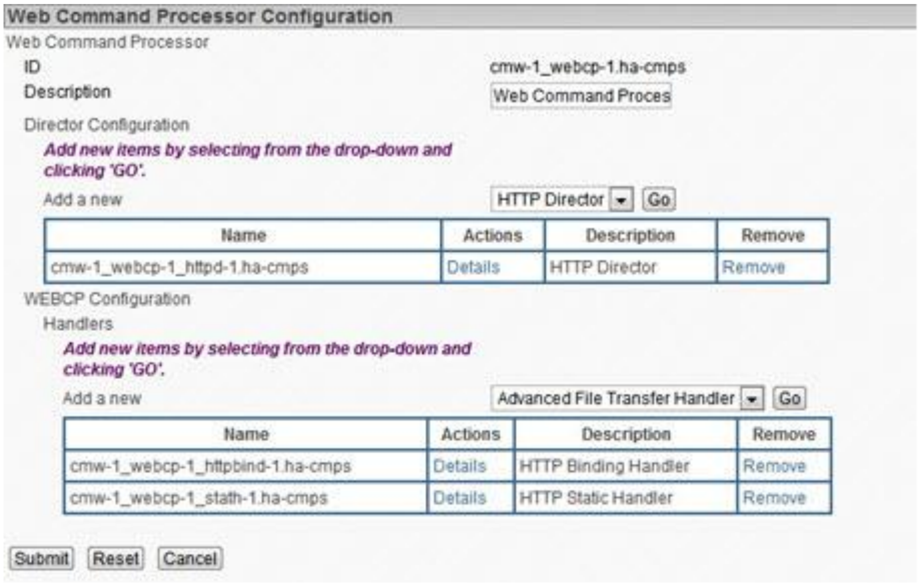
Add a New Command Processor

Add new items by selecting from the drop-down and clicking 'GO'.

Add a new JSM Command Processor

Name	Actions	Description	Remove
cmw-1_webcp-1.ha-cmps	Details	Web Command Processor	Remove
cmw-1_jsmcp-1.ha-cmps	Details	JSM Command Processor	Remove

3 In the Web Command Processor Configuration page, click **Details** beside the HTTP Director or the handlers, if you want to see their configurations.



Web Command Processor Configuration

Web Command Processor

ID: cmw-1_webcp-1.ha-cmps

Description: Web Command Proces

Director Configuration

Add new items by selecting from the drop-down and clicking 'GO'.

Add a new: HTTP Director

Name	Actions	Description	Remove
cmw-1_webcp-1_httpd-1.ha-cmps	Details	HTTP Director	Remove

WEBCP Configuration

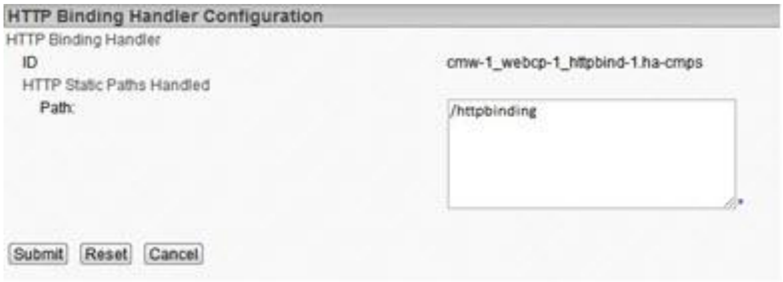
Handlers

Add new items by selecting from the drop-down and clicking 'GO'.

Add a new: Advanced File Transfer Handler

Name	Actions	Description	Remove
cmw-1_webcp-1_httpbind-1.ha-cmps	Details	HTTP Binding Handler	Remove
cmw-1_webcp-1_stath-1.ha-cmps	Details	HTTP Static Handler	Remove

4 On the HTTP Binding Handler Configuration page, the **Path** has been configured as **`/httpbinding`**. You can change this setting, if needed. The Path is the HTTP URI path on which this handler listens for HTTP binding traffic. For example, in the URI, **`http://www.example.com:7300/httpbinding`**, the path is /httpbinding.



HTTP Binding Handler Configuration

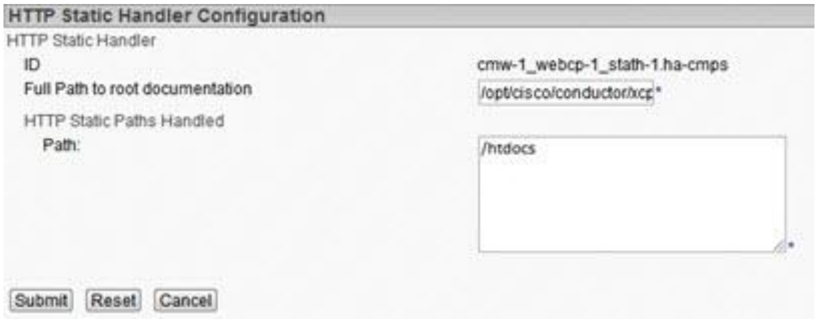
HTTP Binding Handler

ID: cmw-1_webcp-1_httpbind-1.ha-cmps

HTTP Static Paths Handled

Path: /httpbinding

5 On the HTTP Static Handler Configuration page, you can change the values if needed. They are described in the following table.



HTTP Static Handler Configuration

HTTP Static Handler

ID cmw-1_webcp-1_stath-1.ha-cmps

Full Path to root documentation /opt/cisco/conductor/xcp *

HTTP Static Paths Handled

Path: /htdocs *

Parameter	Description
Full Path to root documentation	The full path to the location where the files being served by the handler are stored.
HTTP Static Paths Handled	The prefix that the Web Command Processor uses to determine which handler to use. In the following URL, the file index.html is served to the client by this handler using the default path, htdocs: `http://corp.example.com:5280/htdocs/index.html`

7

Single Domain Name Support

Introduction

This chapter provides instructions for configuring the Single Domain Name Support (SDNS) plugin.

In This Chapter

Overview of SDNS Support

Single Domain Name Support (SDNS) provides a method for distributing the load for a single domain over multiple, equivalent components or plugins. The SDNS plugin accomplishes this by allowing you to deploy a single domain name across a network of Videoscape Control Suite MsgInfra routers and components on different computers, even at different locations or with different subdomain names. SDNS allows two components with equivalent capabilities to act side by side, thereby reducing performance bottlenecks and increasing the number of concurrent users that are supported on each system.

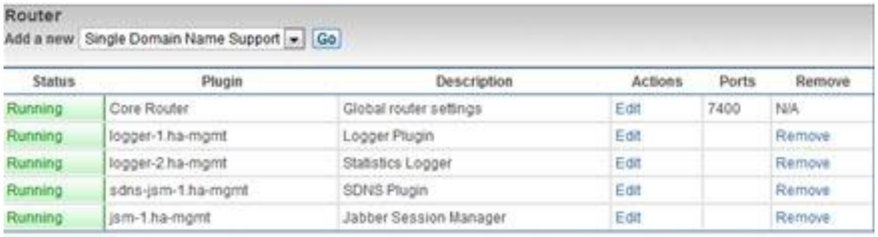
The MsgInfra components and plugins that make the most effective use of SDNS are JSM and Pubsub. When you use SDNS to front for one or more of these components or plugins, you can configure an SDNS plugin on each router for each component or plugin.

Note: SDNS is limited with regards to disco searches. When multiple, equivalent components are configured for SDNS, only one of the components will be searched when a disco request is received. For example, when multiple Pubsub components are configured for SDNS and a user searches for existing categories, only one of the Pubsub components will be searched.

Configuring the SDNS Plugin

1 Change to the controller's Advanced configuration view.

2 In the **Router** area on the controller's main page, click **Go** to add an Single Domain Name Support.

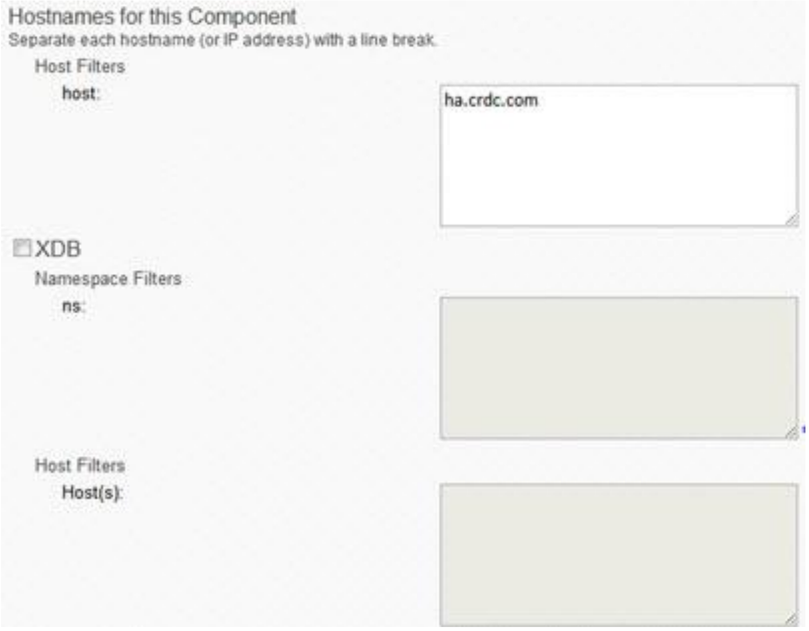


Router

Add a new Single Domain Name Support ▾ Go

Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	logger-1.ha-mgmt	Logger Plugin	Edit		Remove
Running	logger-2.ha-mgmt	Statistics Logger	Edit		Remove
Running	sdns-jsm-1.ha-mgmt	SDNS Plugin	Edit		Remove
Running	jsm-1.ha-mgmt	Jabber Session Manager	Edit		Remove

3 Choose **Hostnames** for this Component configuration. Enter the hostname with which you want to use the SDNS plugin.



Hostnames for this Component

Separate each hostname (or IP address) with a line break.

Host Filters

host: ha.crdc.com

□ XDB

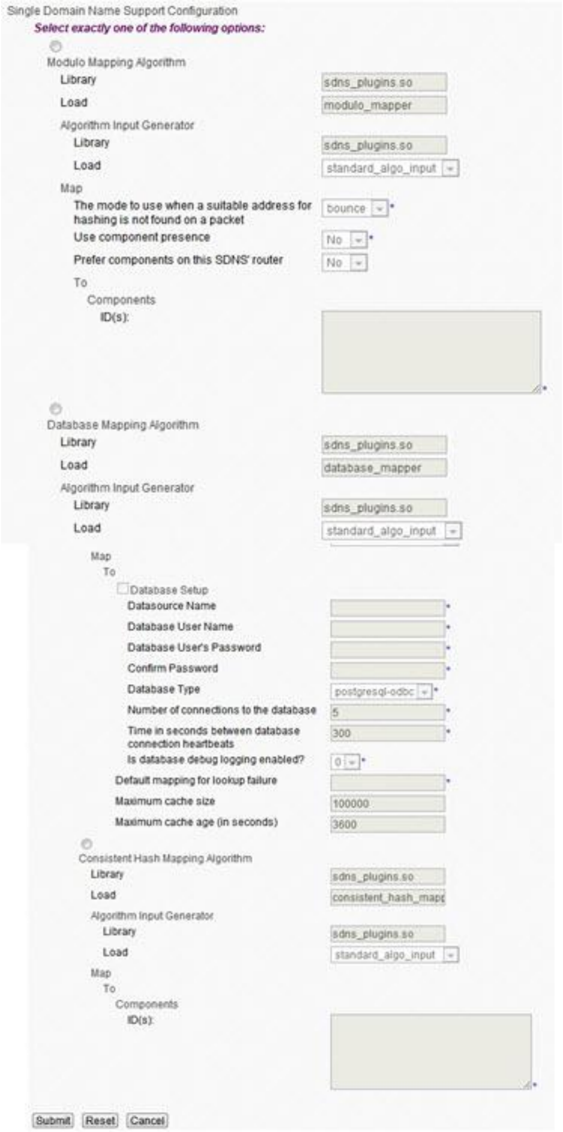
Namespace Filters

ns:

Host Filters

Host(s):

4 Choose one SDNS support configuration.



Single Domain Name Support Configuration

Select exactly one of the following options:

○ Modulo Mapping Algorithm

Library	sdns_plugins.so
Load	modulo_mapper
Algorithm Input Generator	
Library	sdns_plugins.so
Load	standard_algo_input
Map	
The mode to use when a suitable address for hashing is not found on a packet	bounce *
Use component presence	No *
Prefer components on this SDNS' router	No
To	
Components	
ID(s):	*

○ Database Mapping Algorithm

Library	sdns_plugins.so
Load	database_mapper
Algorithm Input Generator	
Library	sdns_plugins.so
Load	standard_algo_input
Map	
To	
□ Database Setup	
Datasource Name	*
Database User Name	*
Database User's Password	*
Confirm Password	*
Database Type	postgresql-odbc *
Number of connections to the database	5 *
Time in seconds between database connection heartbeats	300 *
Is database debug logging enabled?	0 *
Default mapping for lookup failure	*
Maximum cache size	100000
Maximum cache age (in seconds)	3600

○ Consistent Hash Mapping Algorithm

Library	sdns_plugins.so
Load	consistent_hash_mapp
Algorithm Input Generator	
Library	sdns_plugins.so
Load	standard_algo_input
Map	
To	
Components	
ID(s):	*

5 If you want to configure any other parameters, see their descriptions in the online help for the SDNS Plugin Configuration page.

6 Click **Submit** to save your configuration.

7 Restart your Videoscape Control Suite MsgInfra system.

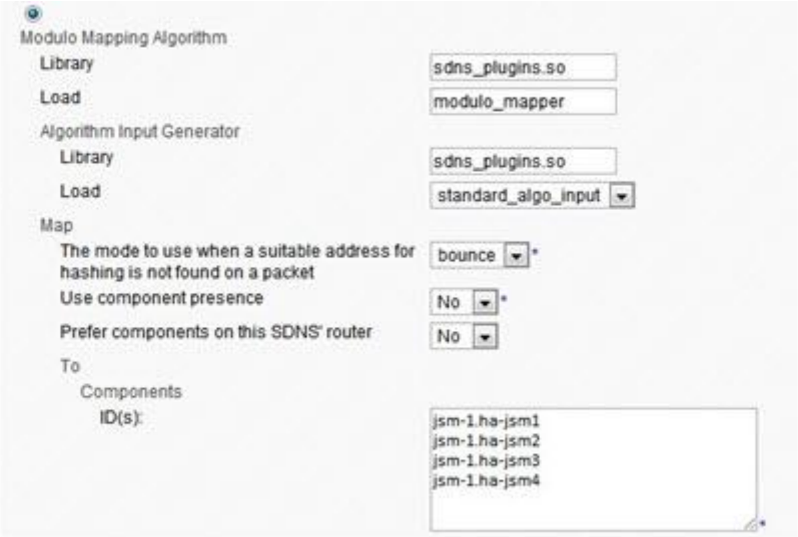
SDNS Mapping Algorithm

When you configure the SDNS plugin, you can choose between the **modulo** mapping algorithm and the **database** mapping algorithm (or you can write your own) to store the mapping between subdomains and the global domain in a supported database.

Modulo Mapping Algorithm

The modulo mapping algorithm algorithmically determines the mapping between the global domain and subdomains, and is particularly effective if your scalability needs are high. This algorithm is faster than the database mapping algorithm; however, it provides less control over where stanzas are rerouted. The modulo mapping algorithm uses the mathematical function *modulo* to map to the correct subdomain within the global domain by hashing the user/host Jabber ID and using the integral hash value modulo.

The following figure shows the **Modulo Mapping Algorithm** section in the SDNS Configuration page. **Use component presence** should be "NO" for the JSM-SDNS type plugin, and "YES" for the SDNS-Pubsub type plugin.



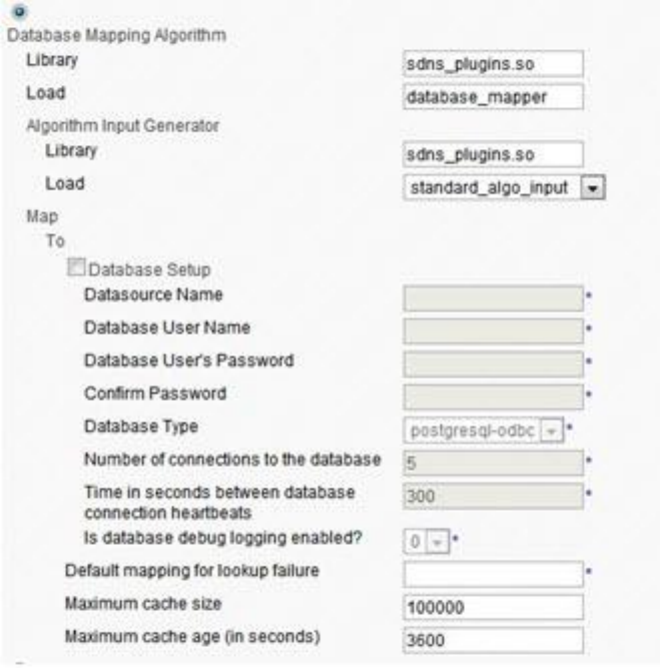
● Modulo Mapping Algorithm

Library	sdns_plugins.so
Load	modulo_mapper
Algorithm Input Generator	
Library	sdns_plugins.so
Load	standard_algo_input
Map	
The mode to use when a suitable address for hashing is not found on a packet	bounce *
Use component presence	No *
Prefer components on this SDNS' router	No
To	
Components	
ID(s):	jsm-1.ha-jsm1 jsm-1.ha-jsm2 jsm-1.ha-jsm3 jsm-1.ha-jsm4 *

Database Mapping Algorithm

The database mapping algorithm is recommended for distributed setups and is not as fast as the modulo mapping algorithm. However, it provides finer control over where stanzas are rerouted.

The following figure shows the **Database Mapping Algorithm** section in the SDNS Configuration page. SDNS will use the global database set up in the Core Router configuration if you do not configure the Database Setup option shown in the figure. If you prefer to use a database other than the one that is configured for the core router, you can configure another one here.

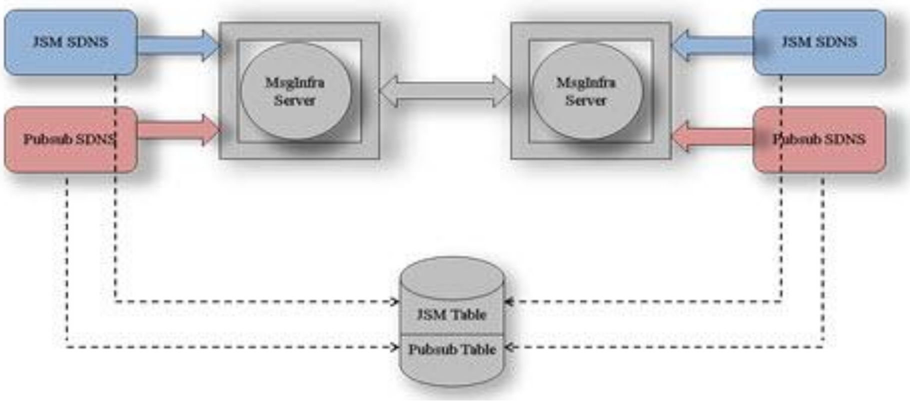


● Database Mapping Algorithm

Library	sdns_plugins.so
Load	database_mapper
Algorithm Input Generator	
Library	sdns_plugins.so
Load	standard_algo_input
Map	
To	
□ Database Setup	
Datasource Name	*
Database User Name	*
Database User's Password	*
Confirm Password	*
Database Type	postgresql-odbc *
Number of connections to the database	5 *
Time in seconds between database connection heartbeats	300 *
Is database debug logging enabled?	0 *
Default mapping for lookup failure	*
Maximum cache size	100000
Maximum cache age (in seconds)	3600

If you select the database mapping algorithm, you must insert mapping information (JID and MAPPED_HOST) into the SDNS_MAP table in your database.

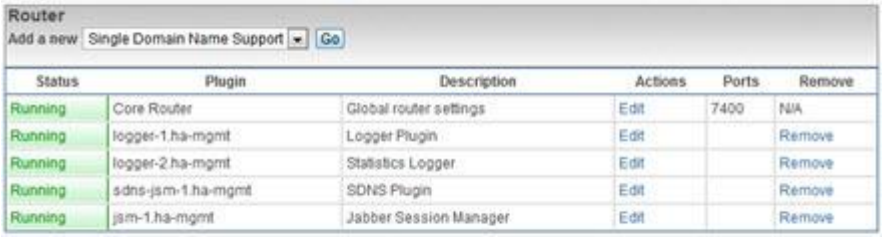
Note: If you have multiple SDNS plugins that use the database mapping algorithm, you must have a separate SDNS_MAP table for each component. The simplest way to give each SDNS plugin its own set of tables is to configure each component to connect to the database with a different database username.



Configuring JSM for SDNS

1 Change to the controller's Advanced configuration view.

2 In the **Router** area on the controller's main page, click **Edit** beside Jabber Session Manager.

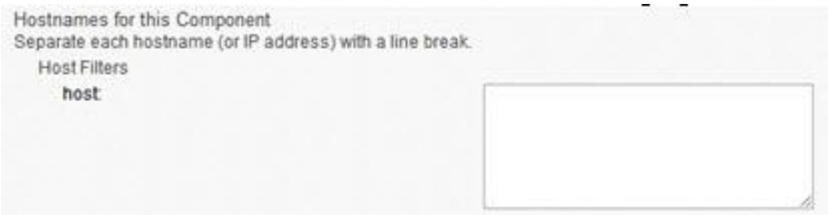


Router

Add a new Single Domain Name Support ▾ Go

Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	logger-1.ha-mgmt	Logger Plugin	Edit		Remove
Running	logger-2.ha-mgmt	Statistics Logger	Edit		Remove
Running	sdns-jsm-1.ha-mgmt	SDNS Plugin	Edit		Remove
Running	jsm-1.ha-mgmt	Jabber Session Manager	Edit		Remove

3 In the Jabber Session Manager Configuration page, scroll down to the **Hostnames for this Component** area and remove the host names as shown in the following figure.



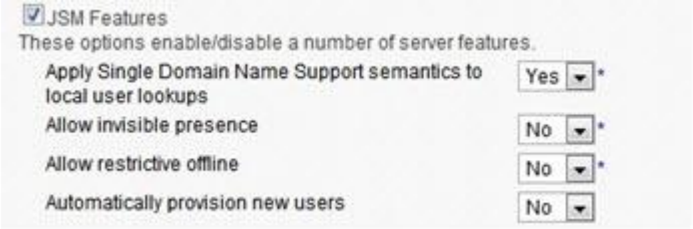
Hostnames for this Component

Separate each hostname (or IP address) with a line break.

Host Filters

host

4 Scroll down to the **JSM Features** area, and select **Yes** beside **Apply Single Domain Name Support semantics to local user lookups**.



☑ JSM Features

These options enable/disable a number of server features.

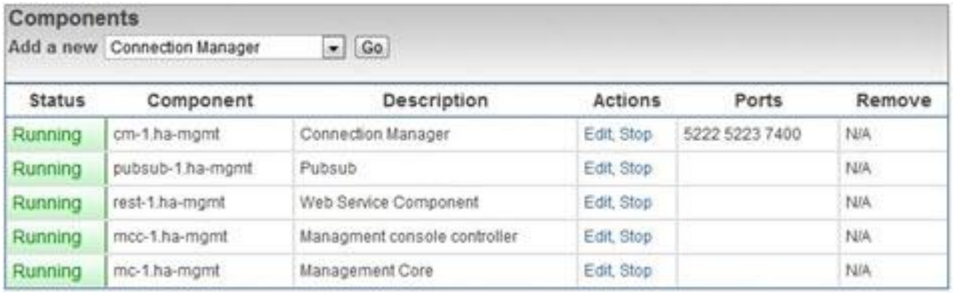
Apply Single Domain Name Support semantics to local user lookups	Yes ▾ *
Allow invisible presence	No ▾ *
Allow restrictive offline	No ▾ *
Automatically provision new users	No ▾

5 Click **Submit** to save your configuration.

6 Repeat this procedure for the JSM on the other router.

Configuring Pubsub for SDNS

1. Change to the controller's Advanced configuration view.
2. In the **Components** area on the controller's main page, click **Edit**, beside **Pubsub**.

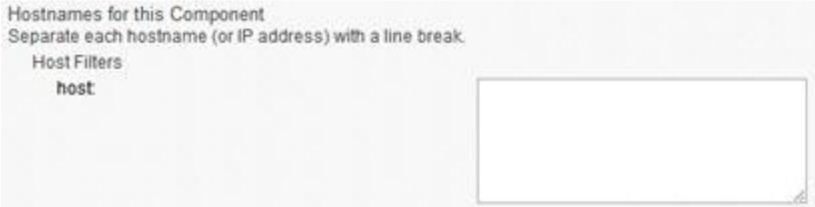


Components

Add a new Connection Manager Go

Status	Component	Description	Actions	Ports	Remove
Running	cm-1.ha-mgmt	Connection Manager	Edit, Stop	5222 5223 7400	N/A
Running	pubsub-1.ha-mgmt	Pubsub	Edit, Stop		N/A
Running	rest-1.ha-mgmt	Web Service Component	Edit, Stop		N/A
Running	mcc-1.ha-mgmt	Managment console controller	Edit, Stop		N/A
Running	mc-1.ha-mgmt	Management Core	Edit, Stop		N/A

3. In the Pubsub Configuration page, scroll down to the **Hostnames for this Component** area and remove the host names, as shown in the following figure.



Hostnames for this Component
Separate each hostname (or IP address) with a line break
Host Filters
host:

4. Click **Submit** to save your configuration.
5. Repeat this procedure for the Pubsub component on the other router.

8

Pubsub

Introduction

The Pubsub is an enabling technology, which means that you must write an application that uses its functionality. The Pubsub allows you to organize different types of information into categories that are accessible by users of your application. Users can create, publish to, and subscribe to nodes.

- The Pubsub is compliant with XEP 60: (**`www.xmpp.org/extensions/xep-0060.html`**)
- The Pubsub chapter in the MsgInfra Server Developer Guide provides information about XEP-60 compliance and suggestions for implementation.

In This Chapter

Planning Your Pubsub Deployment

If you have a small deployment, you can configure the Pubsub service as a single component. However, if your deployment is larger, you should add multiple Pubsub components using the Single Domain Name Support functionality to spread the load over multiple machines.

You can redirect Pubsub stanzas based on the node identifier. This means that any given Pubsub instance handles a subset of the total number of Pubsub nodes in the system. How large a subset it handles is determined by how many nodes are in the system and how many Pubsub instances are available to share the load.

Pubsub Configuration

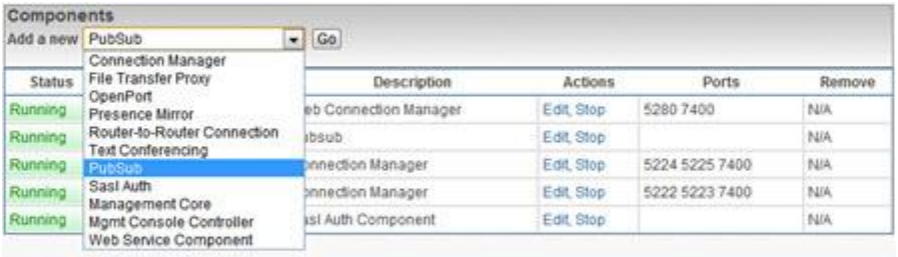
This section describes how to configure the Pubsub component and its associated categories.

Configuring the Pubsub Component

The following instructions describe only the intermediate parameters that are specific to the Pubsub component. For descriptions of all of the parameters associated with the component, see the Pubsub Configuration page's online help.

1 Change to the controller's Intermediate configuration view.

2 In the **Components** area on the controller's main page, select **Pubsub** in the list, and then click **Go**.



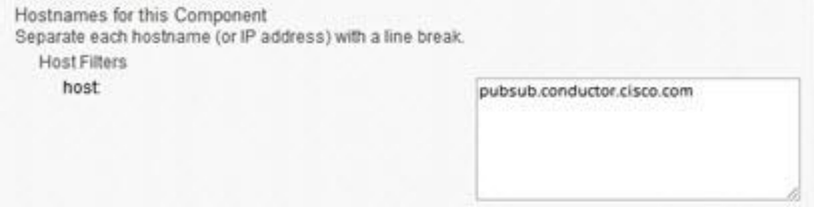
Components

Add a new PubSub

Status		Description	Actions	Ports	Remove
Running		eb Connection Manager	Edit, Stop	5280 7400	N/A
Running		ıbsub	Edit, Stop		N/A
Running		onnection Manager	Edit, Stop	5224 5225 7400	N/A
Running		onnection Manager	Edit, Stop	5222 5223 7400	N/A
Running		ısl Auth Component	Edit, Stop		N/A

3 In the **Hostnames for this Component** option, enter the hostname for the Pubsub component.

Note: The name "pubsub.service" is forbidden due to system internal usage.



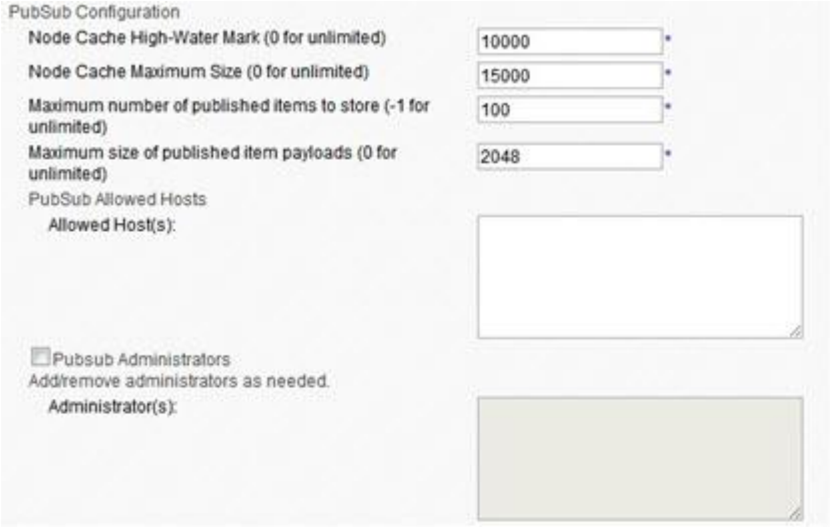
Hostnames for this Component

Separate each hostname (or IP address) with a line break.

Host Filters

host: pubsub.conductor.cisco.com

4 On the Pubsub Configuration page, scroll down to the **Pubsub Configuration** area.



PubSub Configuration

Node Cache High-Water Mark (0 for unlimited) 10000 *

Node Cache Maximum Size (0 for unlimited) 15000 *

Maximum number of published items to store (-1 for unlimited) 100 *

Maximum size of published item payloads (0 for unlimited) 2048 *

PubSub Allowed Hosts

Allowed Host(s):

□ Pubsub Administrators

Add/remove administrators as needed.

Administrator(s):

5 Configure the parameters, as follows.

Parameter	Description
Node Cache High-Water Mark	Enter the high-water mark for nodes that can be served. This is a load control parameter. If the **Nodes** number exceeds the high-water mark, when a new Pubsub stanza arrives, a delete operation will be put on the queue of least-recently-used node. ■ The suggested value is 10000. Use 0 for unlimited. The maximum value is 32767. ■ It must be less than **Node Cache maximum Size**.
Node Cache maximum Size	Enter the maximum nodes that can be served. This is a load control parameter. If the **Nodes** number exceeds the maximum size, no new node can be handled. ■ The suggested value is 15000. 0 for unlimited. The maximum value is 32767.
Maximum number of published items to store	Enter the maximum items a pubsub node can store if the node is configured as a persist node. ■ The suggested value is 100. Use -1 for unlimited.
Maximum mumber of published item payloads	Enter the maximum bytes of payload in a Pubsub publish message. ■ The suggested value is 2048. Use 0 for unlimited.
Pubsub Allowed Hosts	Not used
Pubsub Administrators	Enter the Jabber IDs of users who can administer nodes; for example, admin@example.com. Separate each ID with a line break.

6 The Pubsub requires a database access. If you configured one of these databases when you installed the MsgInfra Server, you do not have to configure one here. However, if you want to use a different database for the Pubsub, select the **Database Setup** option and configure the parameters.

7 Click **Submit** to save your configuration.

9

Simple Authentication and Security Layer

Introduction

The Simple Authentication and Security Layer (SASL) is a method for adding authentication support to connection-based protocols. SASL supports both Plaintext and Digest-MD5 authentication types.

The SASL component is the default authentication component in Videoscape Control Suite systems that process all authentication requests coming from clients via the Connection Manager. The Connection Manager (CM) responds by forwarding the authentication request to the SASL component. The SASL component processes the request and sends back the response to the CM. The CM interprets the response and sends back the result to the client to complete a single iteration. Multiple iterations can happen to complete the whole authentication process. After the client has been successfully authenticated, the CM sends requests to the Jabber Session Manager (JSM) to create a client session with the client's Jabber ID (JID).

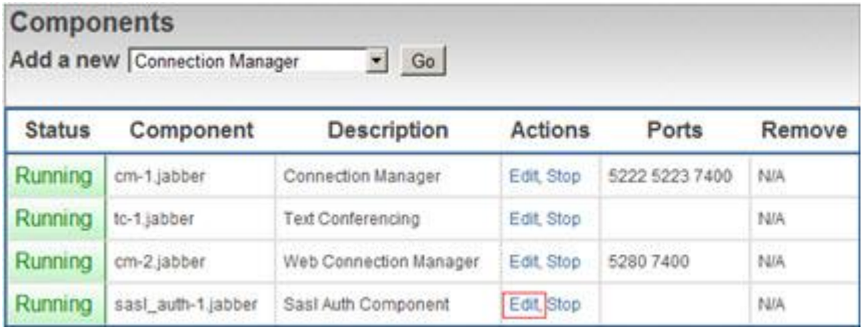
In This Chapter

SASL Management Interface

The Videoscape Control Suite provides the GUI management interface that allows the adding/removing/updating authentication mechanisms that exist in the Videoscape Control Suite system. These are the steps to configure the SASL mechanism from the management interface.

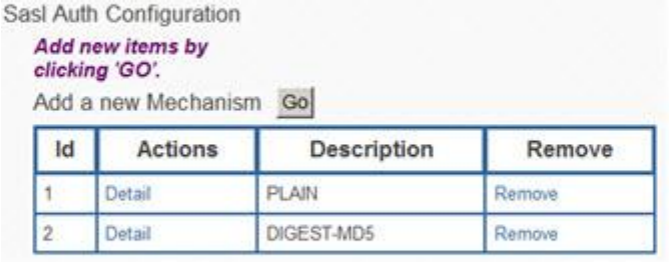
1 Switch to the Advanced view.

2 Open the SASL configuration page. Click **Edit** beside the **Sasl Auth Component** in the **Components** area on the main page.



Status	Component	Description	Actions	Ports	Remove
Running	cm-1.jabber	Connection Manager	Edit, Stop	5222 5223 7400	N/A
Running	tc-1.jabber	Text Conferencing	Edit, Stop		N/A
Running	cm-2.jabber	Web Connection Manager	Edit, Stop	5280 7400	N/A
Running	sasl_auth-1.jabber	Sasl Auth Component	Edit, Stop		N/A

3 To edit the Sasl Auth Configuration, locate the **Sasl Auth Configuration** section to add/update/remove mechanisms.

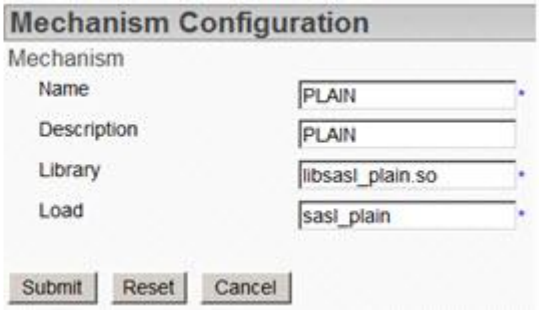


Id	Actions	Description	Remove
1	Detail	PLAIN	Remove
2	Detail	DIGEST-MD5	Remove

Notes:

- Click **Go** to add a new mechanism.
- Click **Remove** to remove an existing mechanism.
- Click **Detail** to show the detailed configuration of one mechanism.

4 Click **Detail** to edit a mechanism.



Name: PLAIN *

Description: PLAIN

Library: libsasl_plain.so *

Load: sasl_plain *

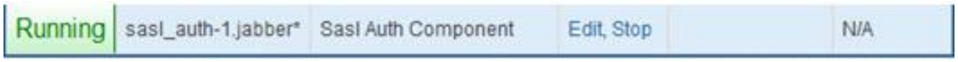
Note: The following parameters are used to configure an SASL mechanism.

Parameter	Attribute	Description
Name	Mandatory	The name of the mechanism that appears in the server's listing of 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 the mechanism description shows in the Sasl Auth Configuration page.
Library	Mandatory	The file name of the mechanism plugin. The default location of the plugin is **`$CONDUCTOR_HOME/lib`**. You can also specify the full path of the plugin. This plug-in is loaded when the SASL component starts.
Load	Mandatory	The name of the entry function of the mechanism plugin. The SASL component calls this function to load the mechanism during SASL component start-up. This function must assign the mechanism name that is identical with the **Name** entered in the management interface.

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

6 Click **Submit** at the bottom of the page to save all SASL changes and return to the main page.

7 Click **Restart** the system to implement the changes.



Running	sasl_auth-1.jabber*	Sasl Auth Component	Edit, Stop		N/A

Note: The asterisk to the right of sasl_auth-1.jabber indicates that the configuration has been modified, but that the system must be restarted to implement the changes.

10

Router-to-Router Connection

Introduction

This chapter provides instructions for configuring the Router-to-Router connection, which enable the Videoscape Control Suite Msginfra Servers to communicate with one another.

In This Chapter

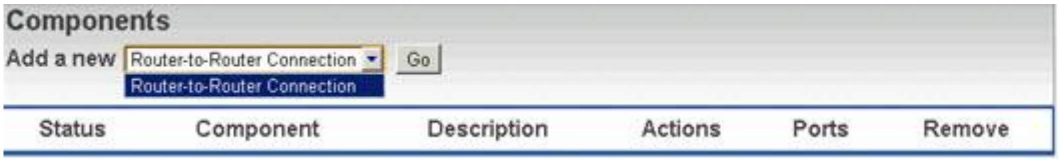
Overview of Router-to-Router Connection

The Router-to-Router Connection provides Msginfra Servers the ability to communicate with each other in a network environment without MDNS capability or a cross-VLAN network environment. Users could manually set up Router-to-Router Connections per network topology.

Configuring the Router-to-Router Connection

1 Change to the controller's Advanced configuration view.

2 In the **Component** area on the controller's main page, click **Go** to add a Router-to-Router Connection.

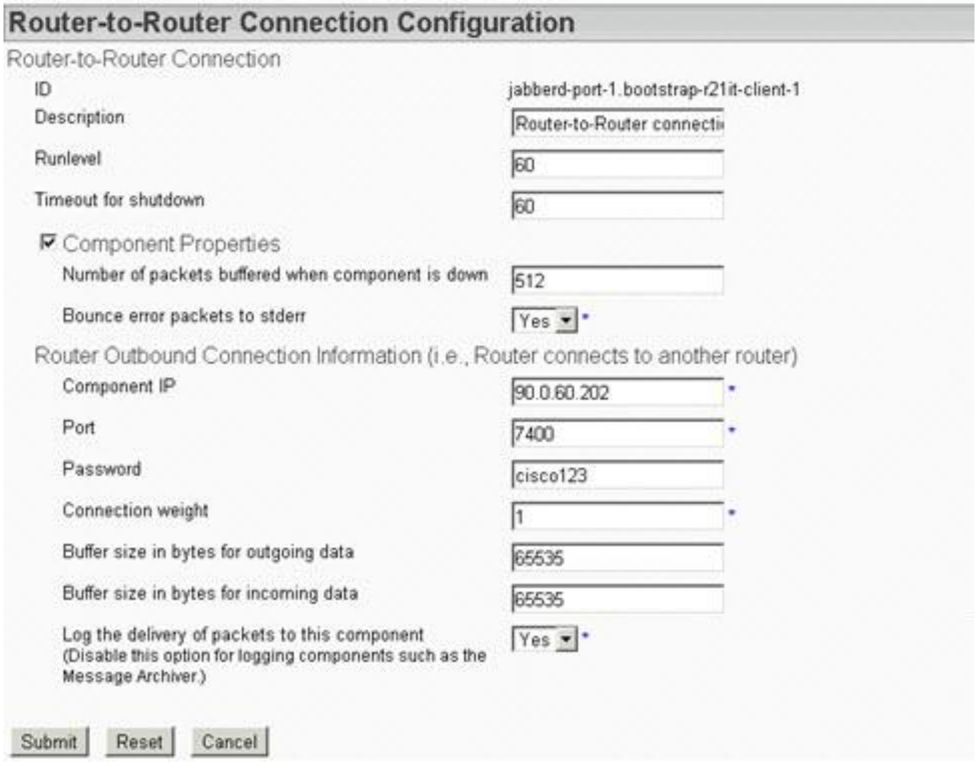


Components

Add a new: Router-to-Router Connection ▾ Go

Status	Component	Description	Actions	Ports	Remove

3 In the Router-to-Router Connection Configuration page, configure the following parameters.



Router-to-Router Connection Configuration

Router-to-Router Connection

ID	jabberd-port-1.bootstrap-r21it-client-1
Description	Router-to-Router connecti
Runlevel	60
Timeout for shutdown	60

☑ Component Properties

Number of packets buffered when component is down	512
Bounce error packets to stderr	Yes ▾ *

Router Outbound Connection Information (i.e., Router connects to another router)

Component IP	90.0.60.202 *
Port	7400 *
Password	cisco123
Connection weight	1 *
Buffer size in bytes for outgoing data	65535
Buffer size in bytes for incoming data	65535
Log the delivery of packets to this component (Disable this option for logging components such as the Message Archiver.)	Yes ▾ *

Submit Reset Cancel

Note: Refer to the following table for guidance.

Parameter	Description
Component IP	Enter the remote server's IP address.
Port	Enter the remote server's Master Accept Port (the default Master Accept Port is 7400).
Password	Enter the password specified for the remote server's Master Accept Port.
Connection Weight	Enter the weight for this particular router connection. A higher weight means the connection is less desirable, or lower priority. During route calculations, the weight of the path is taken into consideration, and packets travel along the path of least resistance.

11

Management Core

Introduction

The Management Core component works as the back-end of the Videoscape Control Suite Management Console. It cooperates with the Node Controller which resides on every Videoscape Control Suite node to provide a centralized management function for the whole Videoscape Control Suite system. Customers can easily monitor the status of an individual node, router, etc., and can operate their life-cycle from within the Management Console.

This chapter provides instructions for configuring the Management Core component.

In This Chapter

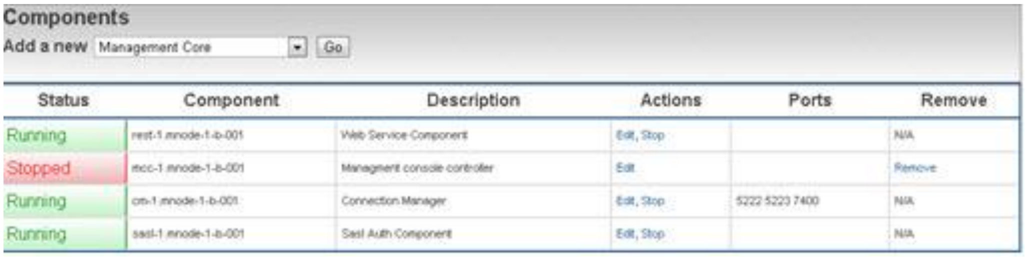
Configuring the Management Core Component

The default parameters provided in the controller's configuration view are sufficient for deploying the Management Core.

Adding a New Management Core Component

1 Change to the controller's Advanced configuration view.

2 In the **Components** area on the controller's main page, click **Go** to add a new Management Core.

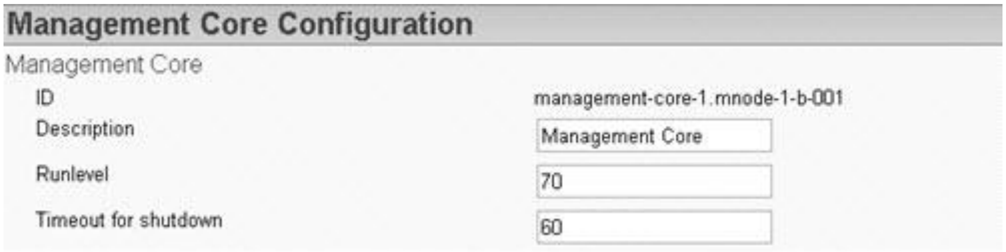


Components

Add a new Management Core ▾ Go

Status	Component	Description	Actions	Ports	Remove
Running	rest-1.mnode-1-b-001	Web Service Component	Edit, Stop		N/A
Stopped	mcc-1.mnode-1-b-001	Managment console controller	Edit		Remove
Running	cm-1.mnode-1-b-001	Connection Manager	Edit, Stop	5222 5223 7400	N/A
Running	sasl-1.mnode-1-b-001	Sasl Auth Component	Edit, Stop		N/A

3 Edit the **Description** of the Management Core component as you need.

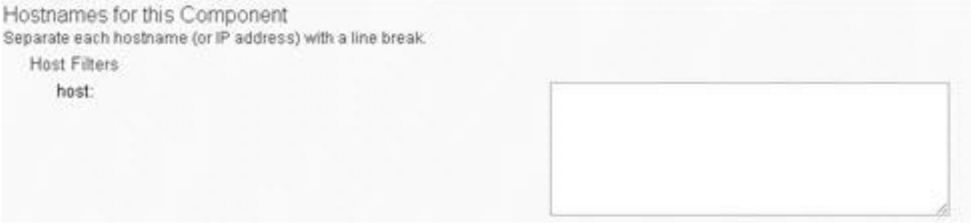


Management Core Configuration

Management Core

ID	management-core-1.mnode-1-b-001
Description	Management Core
Runlevel	70
Timeout for shutdown	60

4 Enter the **Hostname** value.



Hostnames for this Component

Separate each hostname (or IP address) with a line break.

Host Filters

host:

5 Click **Submit** to save the configuration.

6 Click **Restart** the system to apply the new configuration.

Important: Only one Management Core component is supported in the Videoscape Control Suite Management System, and it can only be deployed on the bootstrap router of the Management Node. Multiple Management Core components deployed in one system will result in management data confusion, which will introduce some unexpected results to the system.

12

Management Console Controller

Introduction

The Management Console Controller (MCC) component is the gateway between the Management GUI and the back-end service. It provides the following services:

- Accepts commands from the Management GUI and send them to their destination. It returns the results back to the GUI.
- Accepts service registration requests and provides registered service information.
- Accepts events and sends them as SNMP trap packets back out.
- Works as a signal of service status. If the MCC is inactive for a period of time, the whole managed node will be restarted or reloaded to recover.

In This Chapter

Architectural Overview

The MCC serves as a gateway between the GUI, MsgInfra, and other services, such as AlertManager, EventManager, and EAS.

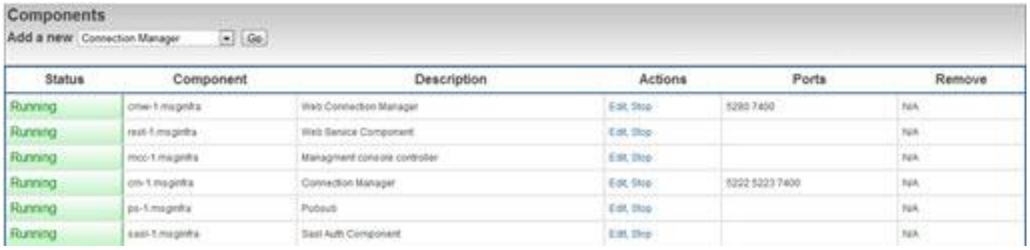
- When the user performs an operation on the management console GUI, the management console sends a command to the MCC. After it receives the command, the MCC sends it to its destination component and waits for a response. Execution results are returned back to the GUI.
- An SNMP event and service registration request is published through Pubsub. The MCC parses these message requests and performs the service registration or SNMP trap operation, in accordance with the message format.
- The ServM process manages the lifecycle of the MCC component and checks the status of the MCC. If the MCC has been inactive for a period of time, the ServM process will treat the current managed node as inactive. It then performs a restart or reload operation to initiate service recovery.

Configuring the MCC Component

You can configure the MCC component from the Videoscape Control Suite MsgInfra XCP controller page.

1 Change to the controller's Advanced configuration view.

2 In the **Components** area on the controller's main page, click **Edit** to edit the existing MCC component.

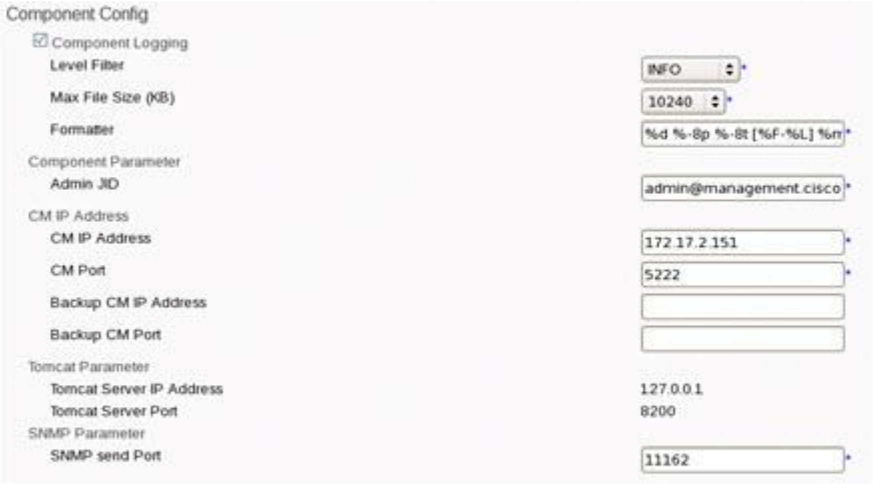


Components

Add a new Connection Manager ▾ Go

Status	Component	Description	Actions	Ports	Remove
Running	cmw-1.msginfra	Web Connection Manager	Edit, Stop	5280 7400	N/A
Running	rest-1.msginfra	Web Service Component	Edit, Stop		N/A
Running	mcc-1.msginfra	Managment console controller	Edit, Stop		N/A
Running	cm-1.msginfra	Connection Manager	Edit, Stop	5222 5223 7400	N/A
Running	ps-1.msginfra	Pubsub	Edit, Stop		N/A
Running	sasl-1.msginfra	Sasl Auth Component	Edit, Stop		N/A

3 Configure the MCC parameters in the **Component Config** section.



Component Config

☑ Component Logging

Level Filter	INFO ⬍ *
Max File Size (KB)	10240 ⬍ *
Formatter	%d %-8p %-8t [%F-%L] %m *
Component Parameter	
Admin JID	admin@management.cisco *
CM IP Address	
CM IP Address	172.17.2.151 *
CM Port	5222 *
Backup CM IP Address	
Backup CM Port	
Tomcat Parameter	
Tomcat Server IP Address	127.0.0.1
Tomcat Server Port	8200
SNMP Parameter	
SNMP send Port	11162 *

Note: Use the information in the following table for guidance.

Parameter	Description
Level Filter	Log level filter. Options are **ALL**, **INFO**, **DEBUG**, **VERBOSE**, **WARNING**, and **ERROR.**
Max Filter Size	Sets the maximum logger file size.
Formatter	Log content format.
Admin JID	Administrator JID.
SNMP send Port	The UDP port used by the MCC to send SNMP traps.

4 Click **Submit** to save the configuration.

13

Service Mapping Manager

Introduction

The Service Mapping Manager (SMM) is one of the components of Service Virtualization, which provides the service request mapping functionalities. The SMM is implemented as a plugin of the core router, jabberd. It shares the same design idea of the existing SDNS, and has more enhancements to enable a client-based service instance, as well as a more robust load-balancing algorithm.

In This Chapter

Deployment Strategy of the Service Mapping Manager

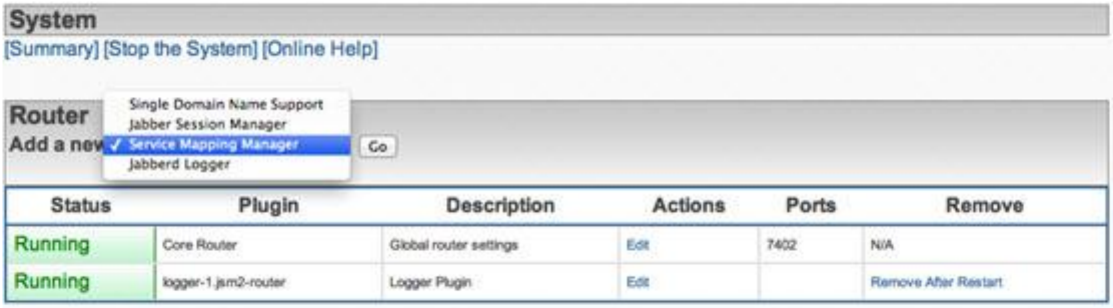
The SMM is the entry point of all service requests which are to be delivered to the Virtual Service. The SMM selects a proper service instance and assigns the request to it. Although we can install just one SMM for all service requests, a better strategy is that each jabberd, where there will be request packets requiring delivery, be equipped with an SMM to reduce hops-to-destination. More SMMs provide the high availability and the load balancing functions.

Configure the Service Mapping Manager Plugin

Normally, the SMM will be installed on your system automatically upon the initial configuration of the cluster. An SMM is also configured and installed whenever required, such as when adding more nodes. To add/configure a new SMM, the following steps apply.

1 Switch to Advanced view.

2 In the **Router** area on the controller's main page, click **Go** to add a new SMM.


[Summary] [Stop the System] [Online Help]
Single Domain Name Support
Jabber Session Manager
✓ Service Mapping Manager
Jabberd Logger
Go

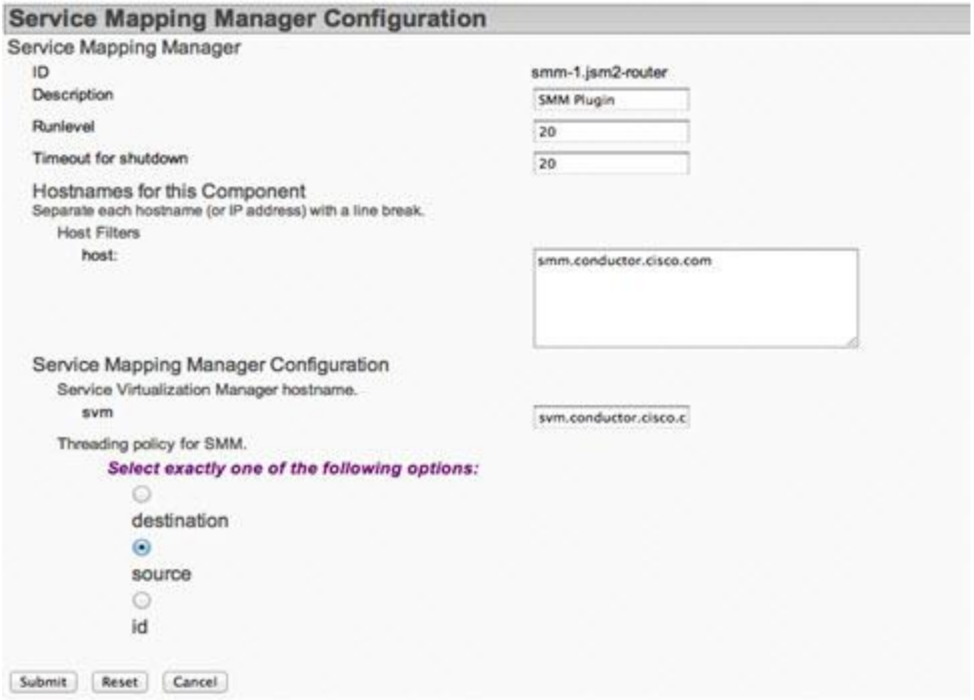
System

Router

Add a new

Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7402	N/A
Running	logger-1.jsm2-router	Logger Plugin	Edit		Remove After Restart

3 Configure the Service Mapping Manager.



Service Mapping Manager Configuration

Service Mapping Manager

ID	smm-1.jsm2-router
Description	SMM Plugin
Runlevel	20
Timeout for shutdown	20

Hostnames for this Component

Separate each hostname (or IP address) with a line break.

Host Filters

host: smm.conductor.cisco.com

Service Mapping Manager Configuration

Service Virtualization Manager hostname.

svm svm.conductor.cisco.c

Threading policy for SMM.

Select exactly one of the following options:

○ destination

● source

○ id

Notes:

- **Hostname for This Component** — Specify a hostname. All of the SMMs within the same cluster should have an identical hostname.
- **Service Virtualization Manager hostname** — Specify the hostname of the Service Virtualization Manager .

- **Threading policy for SMM** — Strategy determining how the SMM allocates task between its working threads. It is used to tune the performance of the SMM. The default value is *destination* and that setting works fine for most cases.

  Note: Refer to the following table when configuring the threading policy.

Threading policy	Mapping	Location
Destination	Based on the JID of the service request producer.	All SMM of the client JSM routers.
Source	Based on the JID of the service request producer.	Currently not used.
ID	Based on the ID of the service request IQ.	All SMMs of the service instance JSM routers, if there has been a performance bottleneck.

4 Click **Submit** to save the configuration.

14

Service Virtualization Manager

Introduction

The Service Virtualization Manager (SVM) is one of the components of Service Virtualization, which provides the service provisioning and service instance monitoring functionalities. The SVM is implemented as a component of the core router, jabberd. We can deploy SDNS for multiple SVMs in order to achieve SVM's load balancing and high availability.

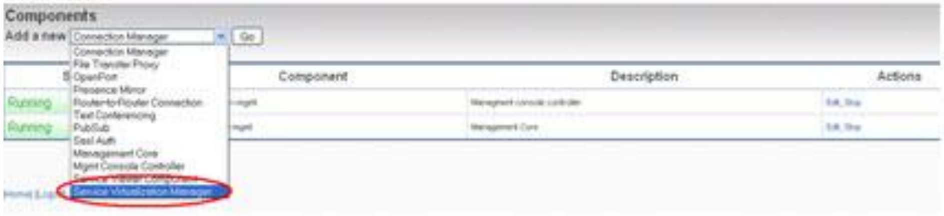
In This Chapter

Configure the Service Virtualization Manager Component

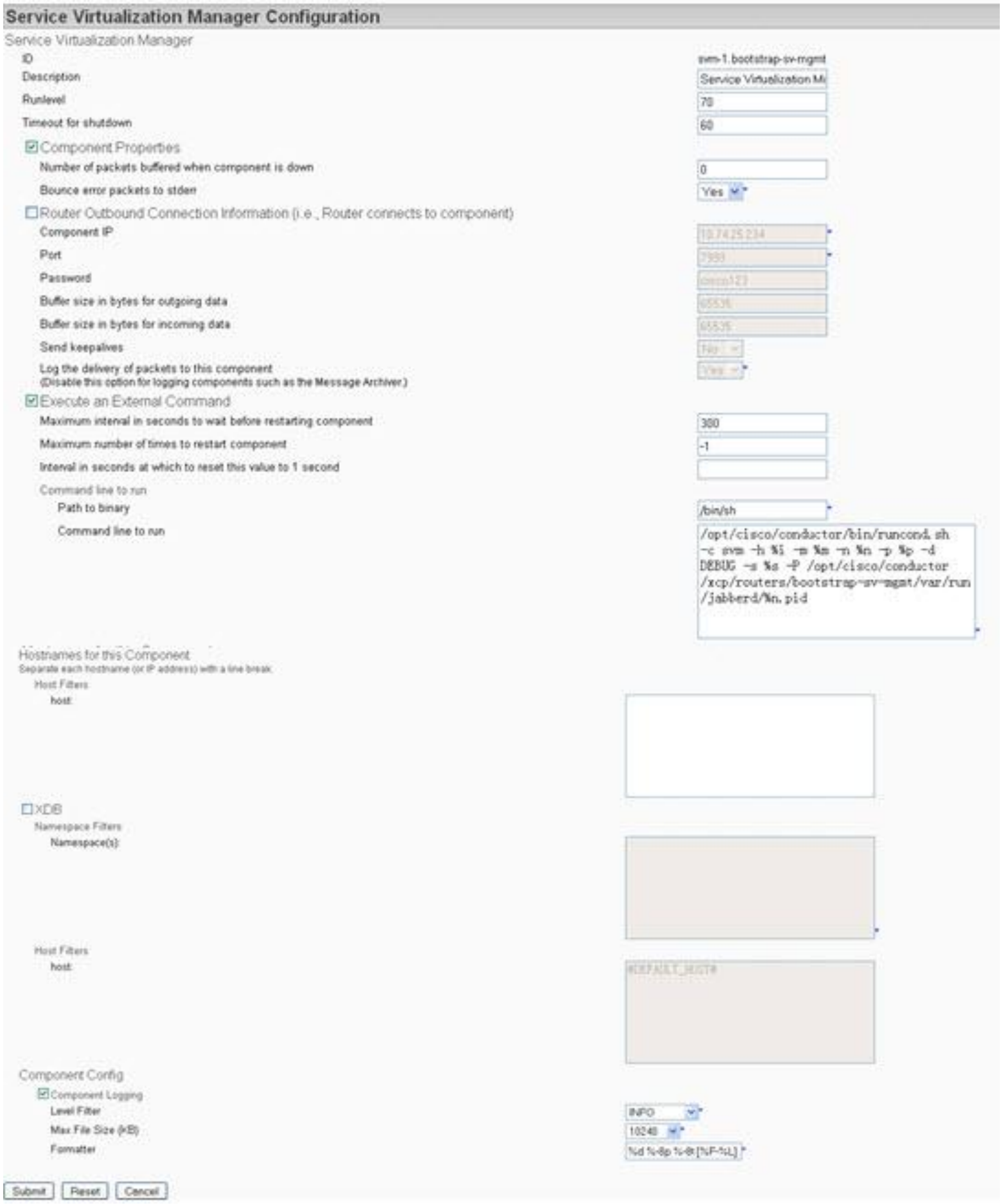
The Videoscape Control Suite provides the GUI management interface to allow for management of the SVM component in the Videoscape Control Suite system. The steps needed to add and manage the SVM component from the management interface, follow.

1 Switch to Advanced view.

2 In the **Components** area on the controller's main page, click **Go** to add a new SVM component.



3 Refer to the following image to configure the SVM.



Service Virtualization Manager Configuration

Service Virtualization Manager

ID	svm-1.bootstrap-sv-mgmt
Description	Service Virtualization M
Runlevel	70
Timeout for shutdown	60

☑ Component Properties

Number of packets buffered when component is down	0
Bounce error packets to stderr	Yes *

☐ Router Outbound Connection Information (i.e., Router connects to component)

Component IP	10.74.25.234 *
Port	7999 *
Password	cisco123
Buffer size in bytes for outgoing data	65535
Buffer size in bytes for incoming data	65535
Send keepalives	No
Log the delivery of packets to this component (Disable this option for logging components such as the Message Archiver.)	Yes *

☑ Execute an External Command

Maximum interval in seconds to wait before restarting component	300
Maximum number of times to restart component	-1
Interval in seconds at which to reset this value to 1 second	

Command line to run

Path to binary	/bin/sh *
Command line to run	/opt/cisco/conductor/bin/runcond.sh -c svm -h %i -m %m -n %n -p %p -d DEBUG -s %s -P /opt/cisco/conductor/xcp/routers/bootstrap-sv-mgmt/var/run/jabberd/%n.pid *

Hostnames for this Component

Separate each hostname (or IP address) with a line break.

Host Filters

host:

☐ XDB

Namespace Filters

Namespace(s): *

Host Filters

host: #DEFAULT_HOST#

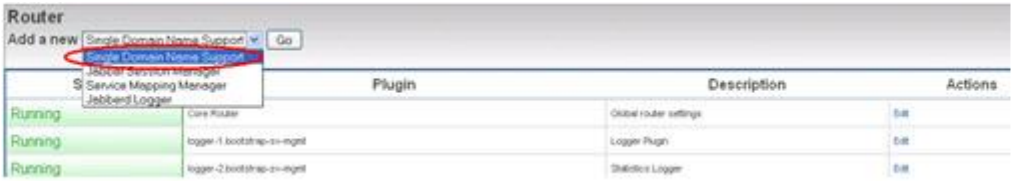
Component Config

☑ Component Logging

Level Filter	INFO *
Max File Size (kB)	10240 *
Formatter	%d %-8p %-8t [%F-%L] *

Note: If there is just one single SVM deployed in the cluster, you need to assign a hostname for this SVM. In most cases, you will deploy a SDNS on top of multiple SVMs for the high availability and load balancing purpose. For the SDNS case, there is no need to assign a hostname to the SVMs.

4 Add an SDNS plugin for the SVM component.

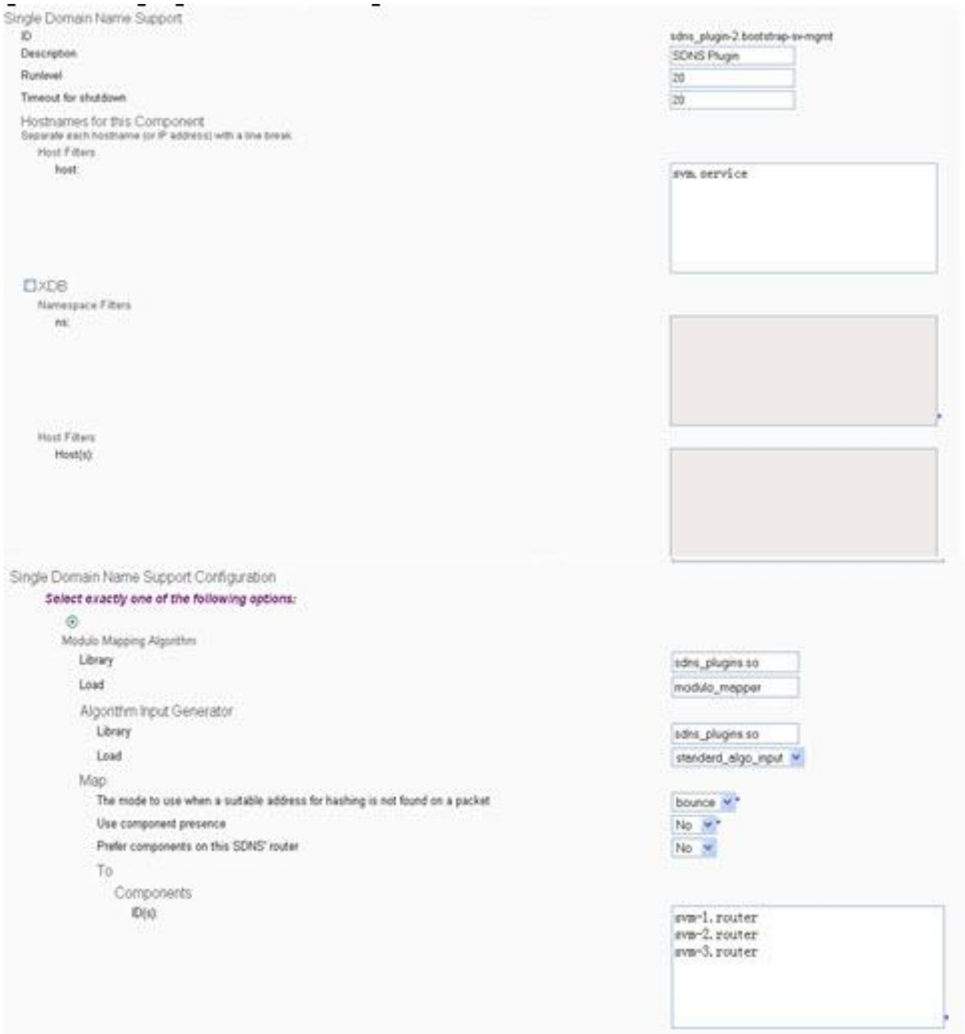


Router

Add a new Single Domain Name Support ▾ Go

S	Plugin	Description	Actions
Running	Core Router	Global router settings	Edit
Running	logger-1.bootstrap-sv-mgmt	Logger Plugin	Edit
Running	logger-2.bootstrap-sv-mgmt	Statistics Logger	Edit

5 Configure the SDNS plugin for the SVM component.



Single Domain Name Support

ID	sdns_plugin-2.bootstrap-sv-mgmt
Description	SDNS Plugin
Runlevel	20
Timeout for shutdown	20

Hostnames for this Component

Separate each hostname (or IP address) with a line break.

Host Filters

host: svm.service

☐ XDB

Namespace Filters

ns:

Host Filters

Host(s):

Single Domain Name Support Configuration

Select exactly one of the following options:

◉

Modulo Mapping Algorithm

Library	sdns_plugins.so
Load	modulo_mapper

Algorithm Input Generator

Library	sdns_plugins.so
Load	standard_algo_input ▾

Map

The mode to use when a suitable address for hashing is not found on a packet	bounce ▾ *
Use component presence	No ▾ *
Prefer components on this 'SDNS' router	No ▾

To

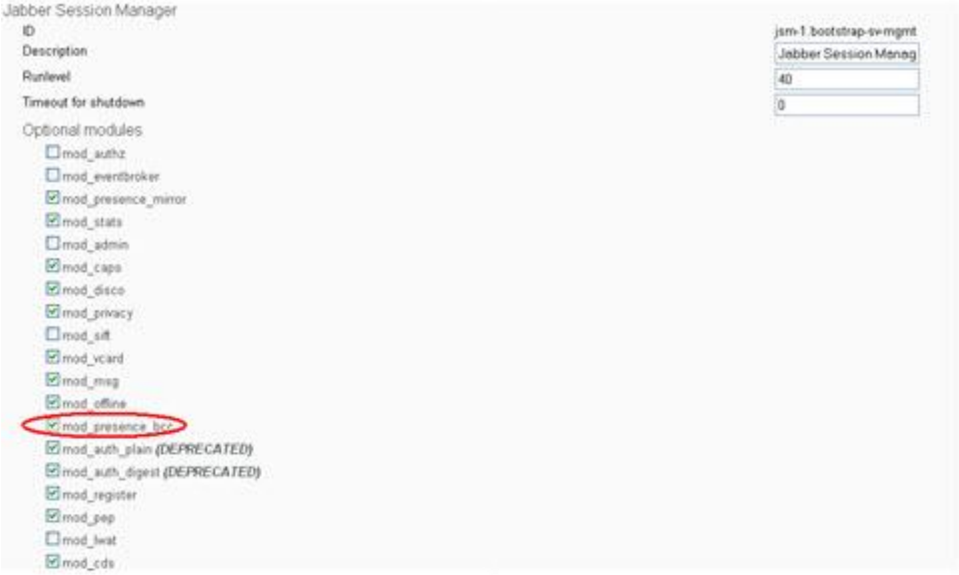
Components

ID(s):

```
svm-1.router
svm-2.router
svm-3.router
```

Note: Assign a hostname for this SDNS and list all the SVMs in the SDNS component lists.

6 Configure the JSM plugin for the SVM component.



Jabber Session Manager

ID jsm-1.bootstrap-sv-mgmt

Description Jabber Session Manag

Runlevel 40

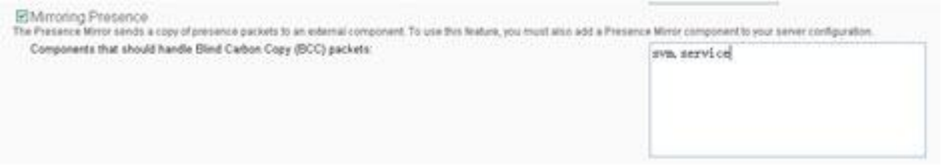
Timeout for shutdown 0

Optional modules

- ☐ mod_authz
- ☐ mod_eventbroker
- ☑ mod_presence_mirror
- ☑ mod_stats
- ☐ mod_admin
- ☑ mod_caps
- ☑ mod_disco
- ☑ mod_privacy
- ☐ mod_sift
- ☑ mod_vcard
- ☑ mod_msg
- ☑ mod_offline
- ☑ mod_presence_bcc
- ☑ mod_auth_plain *(DEPRECATED)*
- ☑ mod_auth_digest *(DEPRECATED)*
- ☑ mod_register
- ☑ mod_pep
- ☐ mod_iwat
- ☑ mod_cds

Note: The **mod_presence_bcc** module must be enabled.

7 Select **Mirroring Presence** and input the host of the SVM.



☑ Mirroring Presence

The Presence Mirror sends a copy of presence packets to an external component. To use this feature, you must also add a Presence Mirror component to your server configuration.

Components that should handle Blind Carbon Copy (BCC) packets: svm.service

15

Service Viewer

Introduction

The Service Viewer is one of the components of Service Virtualization, which provides a web portal to view and download service description files (WSDL or XSD).

In This Chapter

Deployment Strategy of the Service Viewer

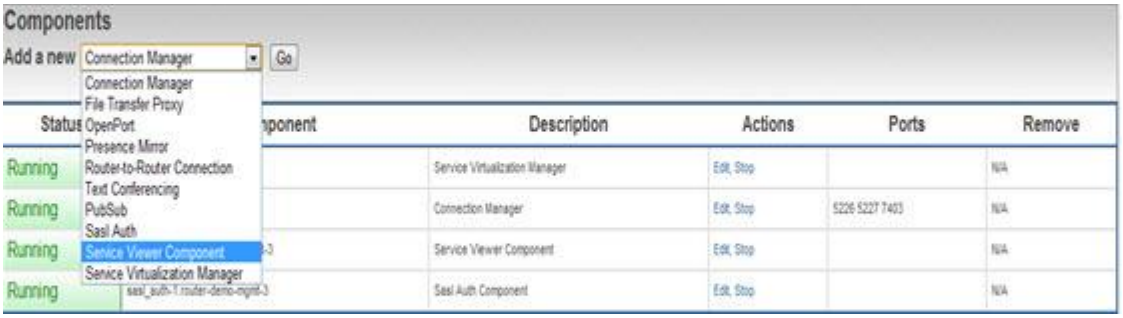
The Service Viewer is not a mandatory component because it simply provides a more convenient way for application developers to view and download service description files. It can be installed in a Service Node where the application developers can access it. Because there is no internal load balancer provided for the Service Viewer, an external load balancer should be used if load balancing and high availability are needed.

Configure the Service Viewer

Normally, the Service Viewer is installed on your system automatically upon the initial configuration of the cluster. A Service Viewer is also configured and installed whenever required, such as when adding more nodes. To add or configure a new Service Viewer, follow these steps.

1 Switch to Advanced view.

2 In the **Components** area on the controller's main page, click **Go** to add a new Service Viewer component.

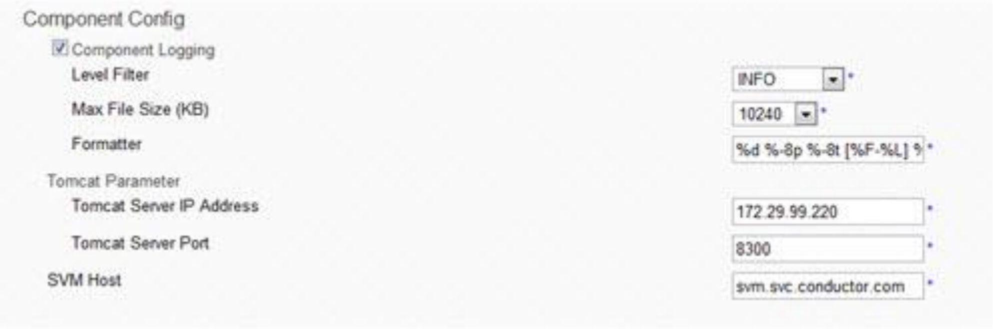


Components

Add a new: Connection Manager ▾ Go

Status	ponent	Description	Actions	Ports	Remove
Running		Service Virtualization Manager	Edit, Stop		N/A
Running		Connection Manager	Edit, Stop	5226 5227 7403	N/A
Running	-3	Service Viewer Component	Edit, Stop		N/A
Running	sasl_auth-1.router-demo-mgmt-3	Sasl Auth Component	Edit, Stop		N/A

3 Configure the Service Viewer by specifying these parameters.



Component Config

☑ Component Logging

Level Filter	INFO ▾ *
Max File Size (KB)	10240 ▾ *
Formatter	%d %-8p %-8t [%F-%L] % *
Tomcat Parameter	
Tomcat Server IP Address	172.29.99.220 *
Tomcat Server Port	8300 *
SVM Host	svm.svc.conductor.com *

Note: The **Component Logging** area is the same as for other components, where you can change the component's logging level or format. For the Service Viewer, focus on the **Tomcat** parameter and **SVM host** fields.

Parameter	Description
Tomcat Server IP Address	The IP address to which the Service Viewer binds.
Tomcat Server Port	The port number on which the Service Viewer listens.
SVM Host	The value of the SVM host depends on how SVM is configured and deployed. If there is no SDNS configured for SVM, then the value should be the hostname of SVM; otherwise, the value should be the hostname of the corresponding SDNS.

4 Click **Submit** to save the configuration.

16

HTTP Gateway

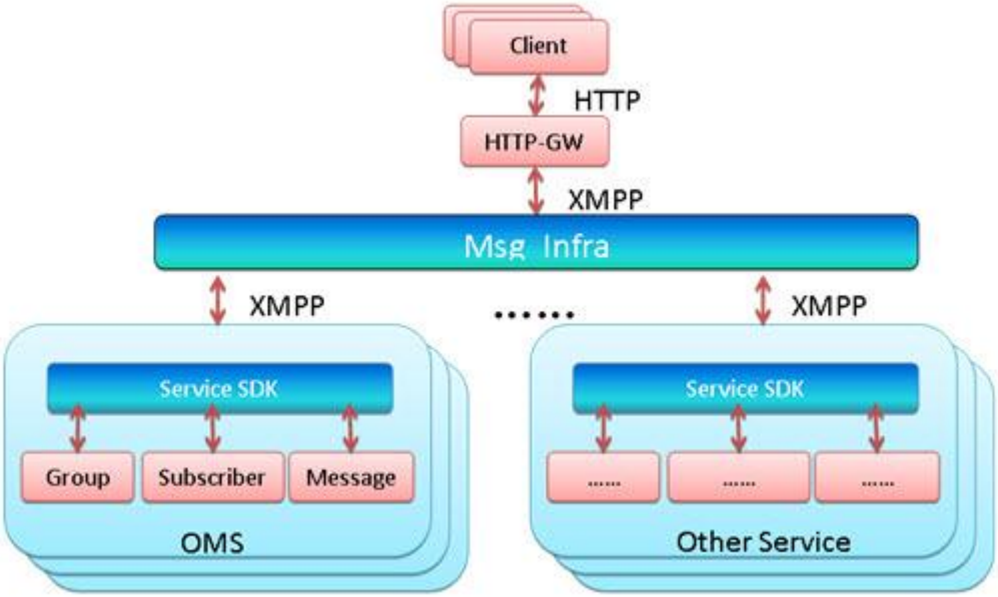
Introduction

The HTTP Gateway (HTTP-GW) component is provided as the bridge between the HTTP and XMPP services. It enables XMPP-based Videoscape Control Suite service HTTP capability. Normally, the HTTP-GW component should be installed at the Service Node. There can be multiple HTTP-GW components installed simultaneously. By default, the HTTP-GW will listen at port 8100.

In This Chapter

Architectural Overview

The HTTP-GW translates HTTP requests into XMPP messages and sends them to back-end XMPP-based Virtual Services. After invocation, the HTTP-GW will return the results back to the HTTP client.

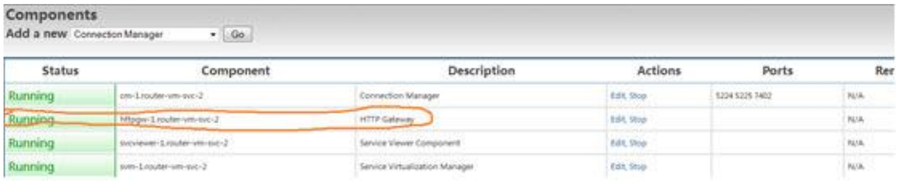


Configuring the HTTP-GW Component

You can configure the HTTP-GW component from the Videoscape Control Suite MsgInfra XCP controller page.

1 Change to the controller's Advanced configuration view.

2 In the **Components** area on the controller's main page, click **Edit** to edit the existing HTTP-GW component.

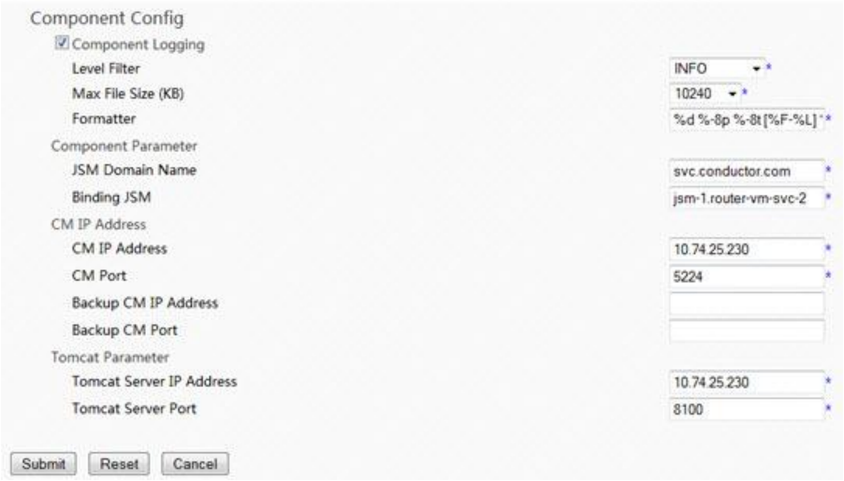


Components

Add a new Connection Manager ▾ Go

Status	Component	Description	Actions	Ports	Rer
Running	cm-1.router-vm-svc-2	Connection Manager	Edit, Stop	5224 5225 7402	N/A
Running	httpgw-1.router-vm-svc-2	HTTP Gateway	Edit, Stop		N/A
Running	svcviewer-1.router-vm-svc-2	Service Viewer Component	Edit, Stop		N/A
Running	svm-1.router-vm-svc-2	Service Virtualization Manager	Edit, Stop		N/A

3 In the **Component Config** area, configure the HTTP-GW parameters.



Component Config

☑ Component Logging

Level Filter	INFO ▾ *
Max File Size (KB)	10240 ▾ *
Formatter	%d %-8p %-8t [%F-%L] *

Component Parameter

JSM Domain Name	svc.conductor.com *
Binding JSM	jsm-1.router-vm-svc-2 *

CM IP Address

CM IP Address	10.74.25.230 *
CM Port	5224 *
Backup CM IP Address	
Backup CM Port	

Tomcat Parameter

Tomcat Server IP Address	10.74.25.230 *
Tomcat Server Port	8100 *

Note: The following table describes the parameters.

Parameter	Description
Level Filter	Log level filters: **ALL**, **INFO**, **DEBUG**, **VERBOSE**, **WARNING**, **ERROR**
Max Filter Size	Maximum logger file size
Formatter	Log content format
JSM Domain Name	Service JSM domain name
Binding JSM	Service JSM component ID
CM IP Address	CM IP address
CM Port	CM port number
Tomcat Server IP	Tomcat HTTP server listening IP address
Tomcat Server Port	Tomcat HTTP server listening port number

4 Click **Submit** to save the configuration.

17

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.

A

Standard Port Assignments

Introduction

This appendix lists the standard port assignments used by the Videoscape Control Suite MsgInfra Server and by the Jabber clients.

In This Appendix

Component Connection Port

By default, all components use port 7400 (the Master Accept Port) to connect to the Videoscape Control Suite MsgInfra core router. Port 7300 is the default listening port used by the controller. You can change both of these ports during server installation.

Client Connection Ports

These ports are used by Jabber clients to connect to components.

Connection Manager

- Port 5222 — Access for plaintext and TLS clients
- Port 5223 — Access for SSL clients
- Port 5280 — Access for WAP clients and HTTP binding (XEP-0124: BOSH)

HTTP Gateway

By default, the HTTP Gateway uses port 8100 to export the HTTP interface.

Management Console Controller

By default, the management console controller uses port 8200 to export the interface and port 11162 for sending trap messages.

Service Viewer

By default, the service viewer uses port 8300 to export the interface.

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

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc., trademarks used in this document.

Product and service availability are subject to change without notice.

June 2013 Part Number OL-28289-01