



# **User Guide for CiscoView Device Manager for the Cisco Content Switching Module**

## **Corporate Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

Text Part Number: OL-6013-02



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0502R)

*User Guide for CiscoView Device Manager for the Cisco Content Switching Module*  
Copyright © 2003-2005 Cisco Systems, Inc. All rights reserved.



<b>Preface</b>	<b>xiii</b>
Audience	xiii
Conventions	xiii
Product Documentation	xiv
Related Documentation	xv
Obtaining Documentation	xvi
Cisco.com	xvi
Documentation DVD	xvi
Ordering Documentation	xvii
Documentation Feedback	xvii
Cisco Product Security Overview	xvii
Reporting Security Problems in Cisco Products	xviii
Obtaining Technical Assistance	xix
Cisco Technical Support Website	xix
Submitting a Service Request	xx
Definitions of Service Request Severity	xx
Obtaining Additional Publications and Information	xxi

---

**CHAPTER 1**

<b>Getting Started With CVDM-CSM</b>	<b>1-1</b>
Before You Begin	1-2
What's New	1-3
Key Features in CVDM-CSM	1-5
Starting CVDM-CSM	1-8
Navigating in CVDM-CSM	1-13

- Understanding the CVDM-CSM Desktop 1-14
  - Selector 1-17
- Understanding the Action Buttons 1-19
- What Does the Home Page Show Me? 1-20
- What are My Virtual Servers? 1-24
- What Does the Setup Page Show Me? 1-25
- Configuring SSL Credentials 1-29
- Editing Preferences 1-30
- Viewing the Running Configuration Information for a Device 1-31
- Viewing the Device Transport Log 1-31
- Refreshing CVDM-CSM 1-32
- Delivering CLI Commands to the Switch/Module 1-32

**CHAPTER 2**

**Configuring CVDM-CSM 2-1**

- Understanding Wizards 2-2
- Basic Setup Wizard 2-3
  - Welcome Page of the Basic Setup Wizard 2-4
  - Configuring Client and Server Side VLANs 2-4
    - Adding Static Routes 2-8
  - Configuring a Virtual Server 2-9
  - Configuring the Default Policy 2-11
  - Summary 2-12
- Advanced Setup Wizard 2-13
  - Welcome Page of the Advanced Setup Wizard 2-14
  - Configuring Layer 7 Policies 2-14
- FAQ 2-15
  - How Do I Set Up a Virtual Server with Default Policy using Wizards? 2-16
  - How Do I Set Up a Virtual Server with Layer 7 Policy using Wizards? 2-17

## How Do I Set Up a Virtual Server with Default Policy and Layer 7 Policies? 2-18

- General 2-19
- Policies 2-21
- Default Policy 2-22
- Client Restriction 2-24
- Sticky Connections 2-25
- Other 2-28

---

### CHAPTER 3

## Managing VLANs 3-1

- Viewing a VLAN 3-2
- Adding a VLAN 3-4
- Editing a VLAN 3-6
- Viewing VLAN Clients 3-7
- Viewing a VLAN Server 3-8

---

### CHAPTER 4

## Managing Virtual Servers 4-1

- Viewing Virtual Servers 4-3
- Adding a Virtual Server 4-5
  - General 4-6
  - Policies 4-8
  - Default Policy 4-9
  - Client Restriction 4-11
  - Sticky Connections 4-12
  - Other 4-14
- Editing a Virtual Server 4-17
  - General 4-18
  - Policies 4-20
  - Default Policy 4-20

- Client Restriction 4-22
- Sticky Connections 4-23
- Other 4-24
- Viewing an Individual Virtual Server 4-26
  - Policies 4-29
  - Default Policy 4-30
  - Backup Server Farm 4-31
  - Client and Sticky Connections 4-32
  - Other Parameters 4-33
- Viewing a Policy 4-34
- Viewing a Default Policy 4-36
  - Server Farms 4-37
  - Backup Server Farms 4-39
  - Client Restrictions 4-40
  - Sticky Connections 4-41

**CHAPTER 5**

**Managing Server Farms 5-1**

- Server Farms 5-2
  - Viewing Server Farms 5-3
  - Adding Server Farms 5-5
    - General 5-6
    - Real Servers 5-8
    - Health Checkup 5-9
    - Redirect Virtual Server 5-10
  - Adding Multiple Real Servers 5-11
  - Editing Server Farms 5-12
    - General 5-13
    - Real Server 5-15
    - Health Checkup 5-16
    - Redirect Virtual Server 5-18

Viewing a Server Farm Node	5-19
Adding a Named Real Server	5-23
Adding an Unnamed Real Server	5-27
Editing a Real Server	5-30
Redirect Virtual Servers	5-34
Adding a Redirect Virtual Server	5-35
Editing Redirect Virtual Servers	5-37
NAT Pools	5-39
Viewing NAT Pools	5-40
Adding NAT Pools	5-42
Editing NAT Pools	5-43

---

**CHAPTER 6****Managing Real Servers** 6-1

Viewing Named Real Servers	6-2
Viewing an Individual Named Real Server	6-4
Viewing Unnamed Real Servers	6-6
Viewing an Individual Unnamed Real Server	6-7
Adding a Real Server	6-9
Editing a Real Server	6-10

---

**CHAPTER 7****Managing Policies** 7-1

Viewing Policies	7-3
Adding Policies	7-5
Editing Policies	7-11
Viewing Policy Nodes	7-16
Conditions and Action	7-17
Cookie Maps	7-18
Header Maps	7-19

- URL Maps 7-20
- Client Group 7-21
- Action 7-21
- Server Farms and Backup Server Farms 7-22
- Sticky Group 7-23
- Reverse Sticky Group 7-24
- Virtual Servers 7-24

**CHAPTER 8**

**Managing Maps 8-1**

- Viewing Maps 8-2
- Adding a Map 8-7
- Viewing Cookie Maps 8-8
- Adding a Cookie Map 8-9
- Viewing Return Code Maps 8-11
- Adding a Return Code Map 8-13
- Adding and Editing Match Conditions for a Return Code Map 8-16
- Viewing URL Maps 8-18
- Adding a URL Map 8-19
- Viewing Header Maps 8-20
  - HTTP Header Insert 8-22
- Adding a Header Map 8-23

**CHAPTER 9**

**Managing Sticky Groups 9-1**

- Viewing Sticky Groups 9-3
  - Adding a Sticky Group 9-6
  - Editing a Sticky Group 9-7
- Viewing Cookie Sticky Groups 9-8
  - Adding a Cookie Sticky Group 9-10



Editing a Cookie Sticky Group	9-11
Viewing Header Sticky Groups	9-13
Adding a Header Sticky Group	9-15
Editing a Header Sticky Group	9-16
Viewing Netmask Sticky Groups	9-18
Adding a Netmask Sticky Group	9-20
Editing a Netmask Sticky Group	9-21
Viewing SSL Sticky Groups	9-22
Adding an SSL Sticky Group	9-23
Editing an SSL Sticky Group	9-24

---

**CHAPTER 10**

<b>Managing Probes</b>	<b>10-1</b>
Viewing Probes	10-3
Adding Probes	10-5
Editing Probes	10-6
Viewing HTTP Probes	10-7
General Tab	10-8
Expected Status Tab	10-10
Header Details Tab	10-11
Adding HTTP Probes	10-12
Editing HTTP Probes	10-15
Viewing FTP Probes	10-18
General Tab	10-18
Expected Status Tab	10-19
Adding FTP Probes	10-20
Editing FTP Probes	10-22
Viewing SMTP Probes	10-23
General Tab	10-24

- Expected Status Tab 10-25
- Adding SMTP Probes 10-26
- Editing SMTP Probes 10-28
- Viewing TELNET Probes 10-29
  - General Tab 10-30
  - Expected Status Tab 10-31
- Adding TELNET Probes 10-32
- Editing TELNET Probes 10-34
- Viewing TCP Probes 10-36
- Adding TCP Probes 10-38
- Editing TCP Probes 10-39
- Viewing UDP Probes 10-40
- Adding UDP Probes 10-42
- Editing UDP Probes 10-43
- Viewing ICMP Probes 10-44
- Adding ICMP Probes 10-46
- Editing ICMP Probes 10-47
- Viewing Script Probes 10-48
- Adding Script Probes 10-50
- Editing Script Probes 10-52

**CHAPTER 11**

**Managing Other Features in CVDM-CSM 11-1**

- Understanding Fault Tolerance 11-1
- Configuring Fault Tolerance 11-3
- Editing Fault Tolerance Configuration 11-5
- Understanding Scripts 11-6
  - Viewing Scripts 11-7

Loading Scripts	11-9
Switch Tab	11-10
Network	11-11
FTP	11-11
TFTP	11-12
RCP	11-12
Viewing Environment Variables	11-13
Understanding XML Configuration	11-19
Viewing XML Configuration	11-20
Editing XML Configuration	11-21

---

**INDEX**





# Preface

---

This guide describes CiscoView Device Manager for the Cisco Content Switching Module (CVDM-CSM) and describes common tasks you can accomplish with CVDM-CSM.

## Audience

This document is for the experienced Network Operations, Security Operations, or Super Admin user managing Cisco Catalyst 6500 Series of switches.

## Conventions

This document uses the following conventions:

<b>Item</b>	<b>Convention</b>
Commands and keywords	<b>boldface font</b>
Variables for which you supply values	<i>italic font</i>
Displayed session and system information	screen font
Information you enter	<b>boldface screen font</b>
Variables you enter	<i>italic screen font</i>

Item	Convention
Menu items and button names	boldface font
Selecting a menu item	Option > Network Preferences

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

# Product Documentation

**Note**

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 1](#) describes the product documentation that is available.

**Table 1**      **Product Documentation**

Document Title	Available Formats
<i>Release Notes for CiscoView Device Manager for the Cisco Content Switching Module</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a>
<i>User Guide for CiscoView Device Manager for the Cisco Content Switching Module</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a>
Context Sensitive Online Help	<ul style="list-style-type: none"> <li>Click <b>Help</b> from the top right corner of the CVDM-CSM desktop.</li> <li>Click the <b>Help</b> button in any dialog box.</li> </ul>

# Related Documentation


**Note**

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 2](#) describes the additional documentation that is available.

**Table 2**      **Related Documentation**

Document Title	Available Formats
<i>Release Notes for CiscoView Device Manager for the Cisco Catalyst 6500 Series Switch</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a>
<i>User Guide for CiscoView Device Manager for the Cisco Catalyst 6500 Series Switch</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a>
<i>User Guide for CiscoView Device Manager for the Cisco Catalyst 6500 Series Switch SSL Services Module</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a>
<i>Catalyst 6500 Series Switch Content Switching Module Configuration Note, 4.2</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/csm/csm_4_2/config/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/csm/csm_4_2/config/index.htm</a>
<i>Catalyst 6500 Series Switch Content Switching Module Configuration Note, 4.1(1)</i>	On Cisco.com at this URL: <a href="http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/csm/csm_4_1/icn/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/csm/csm_4_1/icn/index.htm</a>

# Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

## Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>



## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpkc/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpkc/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.

- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)
- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)



### Tip

---

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

---

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

# Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



### Note

---

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

---

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



# Getting Started With CVDM-CSM

---

CiscoView Device Manager for the Cisco Content Switching Module (CVDM-CSM) enables users easily to configure content load-balancing services on their CSMs. CVDM-CSM is a task-based tool that allows users to control the versatility of their CSM by offering configuration, such as setting up virtual servers, creating server farms, and applying advanced policies. CiscoView Device Manager is a free embedded manager that resides in the Cisco Catalyst 6500 Series supervisor engine flash memory.

CiscoView Device Manager for the CSM (CVDM-CSM) supports server load balancing configuration on the CSM, including:

- Configuring virtual servers.
- Configuring server farms and attaching real servers to them.
- Configuring client and server VLANs.
- Configuring Layer 4 through Layer 7 policies, including maps and sticky groups.



---

**Note**

---

CVDM-CSM supports the deployment of native Cisco IOS commands only.

---

For enterprises and service providers to offer accelerated content delivery services in their data centers, an easy-to-use, web based, device-management GUI is required for CVDM-CSM.

This section contains the following topics:

- [Before You Begin, page 1-2](#)
- [What's New, page 1-3](#)
- [Key Features in CVDM-CSM, page 1-5](#)
- [Starting CVDM-CSM, page 1-8](#)
- [Navigating in CVDM-CSM, page 1-13](#)
- [Configuring SSL Credentials, page 1-29](#)
- [Editing Preferences, page 1-30](#)
- [Viewing the Running Configuration Information for a Device, page 1-31](#)
- [Viewing the Device Transport Log, page 1-31](#)
- [Refreshing CVDM-CSM, page 1-32](#)
- [Delivering CLI Commands to the Switch/Module, page 1-32](#)

## Before You Begin

Before you begin using CVDM-CSM:

- Make sure you have gone through the CVDM-CSM Readme and Release Notes before installation.

CVDM-CSM Readme contains important information regarding the following topics:

- Hardware and software Requirements
  - Installing CVDM-CSM
  - Launching CVDM-CSM
  - Uninstalling CVDM-CSM
  - Troubleshooting notes
- Make sure you have necessary privileges. Privilege level 15 is ideal.
  - Install the necessary Java Plug-in.



# What's New

CVDM-CSM 1.1 provides support for Content Switching Module with SSL (CSM-S). CSM-S can look at decrypted data and make flow routing decisions. CSM-S allows you to launch CiscoView Device Manager for the SSL Services Module (CVDM-SSLSM). To do this, click on the **SSL** button in the homepage and configure the credentials for the CVDM-SSLSM. After they are validated CVDM-SSLSM launches. CVDM-SSLSM uses the Secure Socket Layer (SSL) protocol to enable secure transactions of data through privacy, authentication, and data integrity.

The new features in this release are:

- Launching CVDM-SSLSM from the CVDM-CSM application.
- Saving the running configuration of the SSL daughter card. For more details, see [Viewing the Running Configuration Information for a Device, page 1-31](#)
- Directing the connection to the server, so that the CSM-S can be configured to forward the packets directly to the SSL daughter card and not to the real server.
- Wizards allow you to easily configure create client-side VLAN and server-side VLAN in router mode (different subnets) or bridge mode (single subnet). For more details, see [Understanding Wizards, page 2-2](#).
- Configuring the real server within a server farm with the **local** option to direct the traffic to the SSL daughter card.
- Scripts—Allows you to view and load health-monitoring and standalone scripts. For more details, see [Understanding Scripts, page 11-6](#).
- Environment variables—Allows you to configure CVDM-CSM environment variables. For more details, see [Viewing Environment Variables, page 11-13](#).
- URL learning—Allows CVDM-CSM to get information such as session ID from a URL. This ensures persistence when clients disable cookies on their browsers.
- Cookie sticky, offset and length—Allows you to configure a specific cookie name and automatically learn its value either from the client request HTTP header or from the server Set Cookie message. For more details, see [Adding a Cookie Sticky Group, page 9-10](#).

- **Cookie insert**—Allows the CVDM-CSM to insert a cookie in the Set-Cookie header of the HTTP response. This enables cookie sticky even when servers are not configured to set cookies. The cookie contains information that the CVDM-CSM uses to ensure persistence to a specific real server. For more details, see [Adding a Cookie Sticky Group, page 9-10](#).
- **Header insert**—Allows you to insert a header value and name in the HTTP header. This is useful in client NAT where backend servers require client information. For more details, see [HTTP Header Insert, page 8-22](#).
- **Header Sticky**—Allows you to configure the CVDM-CSM to perform stickiness based on the contents of a specified HTTP header. For more details, see [Adding a Header Sticky Group, page 9-15](#).
- **Backend encryption**—Supports network-based SSL acceleration. CVDM-CSM load balances data to a real server through CSM-S for encryption.
- **Partial Server Farm Failover**—Allows you to define the threshold number of real servers to be out of service before the backup server farm takes over. You can also define the number of real servers to be in service for the server farm to be considered operational. For more details, see the Default Policy section in [Adding a Virtual Server, page 4-5](#).
- **Probe scripts**—The CVDM-CSM now enables you to upload and execute Toolkit Command Language (TCL) scripts on the CSM. Using this feature you can write customized TCL scripts to develop customized health probes or standalone tasks. For more details, see [Understanding Scripts, page 11-6](#).

# Key Features in CVDM-CSM

The following table describes the key features of CVDM-CSM.

Feature	Description
Dual Mode setup Wizard	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Configure and manage client and server VLANs and virtual servers, and associate default policies using the Basic Virtual Server Setup wizard.</li> </ul> <p>For more information, see <a href="#">Basic Setup Wizard, page 2-3</a>.</p> <ul style="list-style-type: none"> <li>• Configure the Layer 7 policies along with the above configurations using the Advanced Virtual Server Setup wizard.</li> </ul> <p>For more information, see <a href="#">Advanced Setup Wizard, page 2-13</a>.</p>
VLAN setup	<p>Allows you to configure client-side and server-side VLANs.</p> <p>See, <a href="#">Chapter 3, “Managing VLANs”</a>.</p>
Virtual Server setup	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Create and delete virtual servers.</li> <li>• Enable and disable virtual service.</li> <li>• Associate virtual servers with a server farm or policy.</li> <li>• Restrict client access to virtual servers.</li> <li>• Configure performance, load, connection, and traffic parameters.</li> <li>• Configure sticky connections.</li> <li>• Enable partial server farm failover.</li> </ul> <p>See, <a href="#">Chapter 4, “Managing Virtual Servers”</a>.</p>

Feature	Description
Server Farm configuration	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Configure server farms.</li> <li>• Specify load-balancing algorithm, and monitor in-band health for each server farm.</li> <li>• Configure a set of real servers and their attributes.</li> <li>• Configure client NAT pools.</li> <li>• Configure redirect virtual servers and their attributes.</li> <li>• Configure health monitoring probes, and enable inband health checkup.</li> <li>• Direct the traffic to the SSL daughter card.</li> </ul> <p>See, <a href="#">Chapter 5, “Managing Server Farms”</a>.</p>
Real Server configuration	<p>Allows you to configure the named real servers by their IP address and location. See, <a href="#">Chapter 6, “Managing Real Servers”</a>.</p>
Policy configuration	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Configure access rules such as maps (cookie map, header map, URL map), client groups (access control lists), sticky group (cookie, header, netmask. and SSL).</li> <li>• Associate server farm and backup server farm with a particular policy.</li> </ul> <p>See, <a href="#">Chapter 7, “Managing Policies”</a>.</p>
Map configuration	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Configure maps to define multiple URLs, cookies, HTTP headers, and return codes into groups that can be associated with a policy.</li> <li>• Insert information such as the client’s IP address into the HTTP header using HTTP header insert feature. This feature is particularly useful when the CVDM-CSM performs source NAT and the application on the server side still requires visibility to the original source IP.</li> </ul> <p>See, <a href="#">Chapter 8, “Managing Maps”</a>.</p>

Feature	Description
Sticky Group configuration	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Configure sticky groups such as cookie, header, SSL, netmask.</li> </ul> <p>See, <a href="#">Chapter 9, “Managing Sticky Groups”</a>.</p>
Health Monitoring Probes configuration	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Configure specific types of health probes, such as FTP, HTTP, ICMP, SMTP, TCP, Telnet, UDP, and Script health probes to administer your network.</li> </ul> <p>See, <a href="#">Chapter 10, “Managing Probes”</a>.</p>
Fault Tolerant Group configuration	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Configure active and standby CVDM-CSMs, fault tolerant VLANs, and parameters like failover time and heartbeat time.</li> <li>• Set priority for any CVDM-CSM.</li> </ul> <p>See, <a href="#">Understanding Fault Tolerance, page 11-1</a>.</p>
Load Scripts	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Upload and execute Toolkit Command Language (TCL) scripts.</li> <li>• Customize scripts to develop health probes or standalone tasks.</li> </ul> <p>See, <a href="#">Understanding Scripts, page 11-6</a>.</p>
View Environment Variables	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Configure CVDM-CSM environment variables and see the values of the configured variables.</li> </ul> <p>See, <a href="#">Viewing Environment Variables, page 11-13</a>.</p>
XML Configuration	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Configure the CVDM-CSM using a Document Type Definition (DTD).</li> </ul> <p>See, <a href="#">Understanding XML Configuration, page 11-19</a>.</p>

# Starting CVDM-CSM

- Step 1** In your browser, enter the IP address or DNS hostname of the device. The Enter Network Password dialog box appears (see [Figure 1-1](#)), prompting you for your level 15 credentials.



**Note**

If you are using a Cisco IOS 12.1.(13)E image, enter the following in your web browser:

```
http://<ip-address>/flash/cv/applet.html?dynarchives=cvdm-csm-1.1.sgz&slotNo=<slot-number>
```

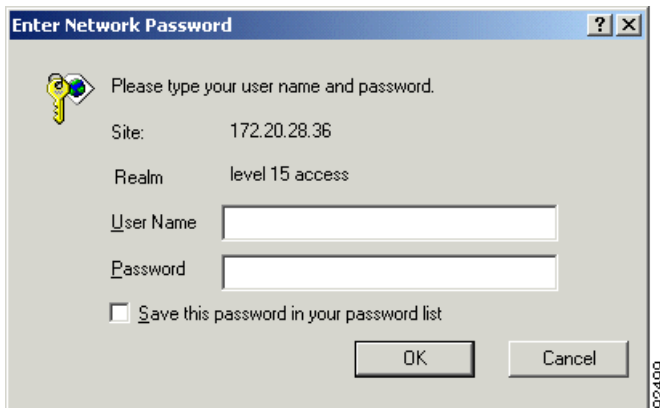
or

```
http://<ip-address>/flash/cv/applet.html?dynarchives=cvdm-csm-1.1_K9.sgz&slotNo=<slot-number>
```

(if you installed Cisco IOS Cryptographic software)

where *<ip-address>* is the IP address of the switch and *<slot-number>* is the slot number where CVDM-CSM resides.. It may be useful to bookmark this URL for future use.

**Figure 1-1** Enter Network Password Dialog Box



- Step 2** Enter your username and password for level 15 access. If you do not have level 15 access to the device, CVDM-CSM will not start.



**Note** If enable password is used for HTTP authentication, use enable password only.

- Step 3** Click **OK**. The device home page appears.
- Step 4** Click the CSM: Slot <slot-number> (CVDM-CSM) link under Device Managers > Service Module section (where <slot-number> is the slot number where CSM resides).
- Step 5** The CVDM-CSM splash screen appears, and the Password Needed - Networking dialog box appears (see [Figure 1-2](#)).

**Figure 1-2** *Splash Screen and Password Needed - Networking Dialog box*





**Note** If you do not have Java Plug-in version 1.4.2\_06, you will be prompted to install it. If you are not prompted, go to [http://java.sun.com/products/archive/j2se/1.4.2\\_06/index.html](http://java.sun.com/products/archive/j2se/1.4.2_06/index.html) and install the Java Plug-in. This website is Copyright © 1995-2004, Sun Microsystems, Inc.

The CVDM-CSM splash screen must remain open in order for the application to function properly. Do not close this window until you log out. CVDM-CSM will appear in a separate window.



**Note** It may take some time before CVDM-CSM appears.

**Step 6** In the Password Needed- Networking dialog box, enter your username and password.



**Note** If an enable password is used for HTTP authentication, use the enable password only.

**Step 7** Click **Yes**. The Warning- Security dialog box appears. (see [Figure 1-3](#))

**Figure 1-3** Warning - Security Dialog Box



92496



- Step 8** To accept the security certificate and continue, click **Yes**. A dialog box appears (see [Figure 1-4](#)), prompting you for your username and password

**Figure 1-4** *.Enter Credentials for <IP Address> Dialog Box (Username and Password)*

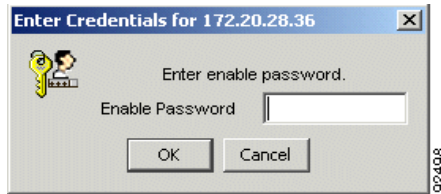


- Step 9** If you are using a Cisco IOS Cryptographic image, proceed to [Step 10](#). If you are not using a Cisco IOS Cryptographic image, proceed to [Step 13](#).
- Step 10** If Secure Shell Protocol (SSH) is enabled on the device but is not activated, the SSH Activation dialog box appears. Modify the appropriate values.

GUI Element	Description
Hostname	Hostname of the device.
Domain Name	Name of the domain to which the host belongs.
Key Length	SSH key length.

- Step 11** Click **OK**. The Enter Credentials for <IP Address> dialog box appears.
- Step 12** Enter your SSH username, password, and enable password.
- Step 13** If SSH is not available, a dialog box appears and asks if you want to authenticate using Telnet instead. To proceed, click **Yes**.  
The Enter Credentials for <IP Address> dialog box appears (see [Figure 1-5](#)). Enter your device user name and password.
- Step 14** Click **OK**. If enable is configured, the Enter Credentials for <IP Address> dialog box appears.

**Figure 1-5** *Enter Credentials for <IP Address> Dialog Box (Enable Password)*



- Step 15** Enter the enable password.
- Step 16** Click **OK**. The CVDM-CSM home page appears.
-

# Navigating in CVDM-CSM

Before you begin using CVDM-CSM, you must understand the basic operation of the user interface, including the login procedure and user interface elements.

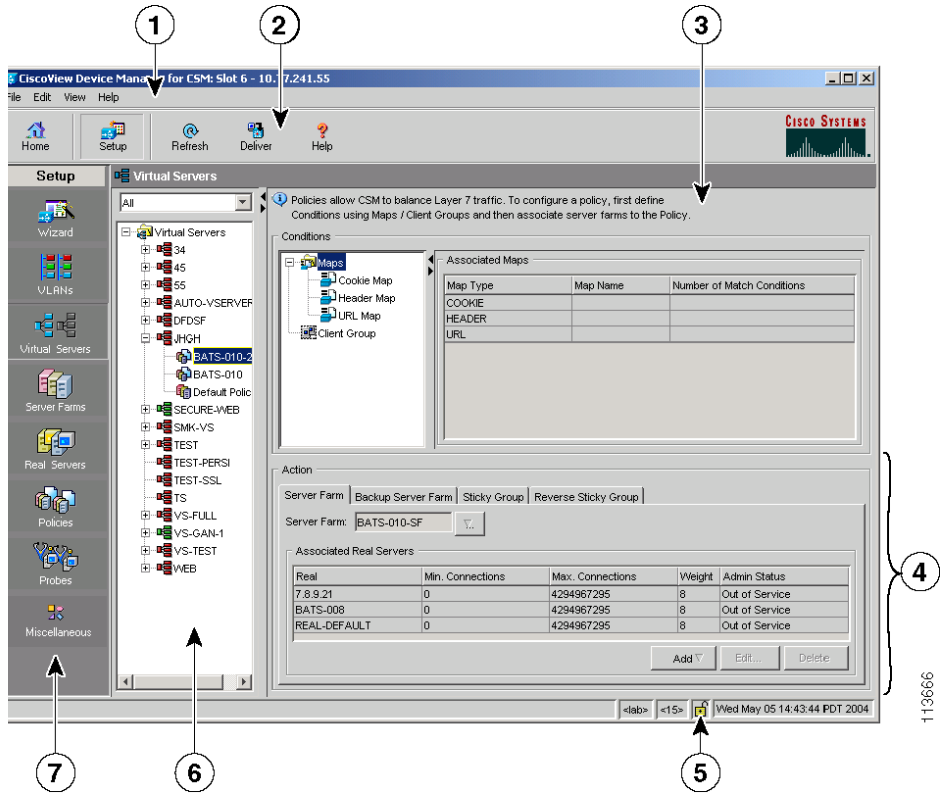
See the following sections for more information:

- [Understanding the CVDM-CSM Desktop, page 1-14](#)
- [Understanding the Action Buttons, page 1-19](#)
- [What Does the Home Page Show Me?, page 1-20](#)
- [What are My Virtual Servers?, page 1-24](#)
- [What Does the Setup Page Show Me?, page 1-25](#)

# Understanding the CVDM-CSM Desktop

This section describes the main GUI elements of the CVDM-CSM application.

**Figure 1-6** CVDM-CSM GUI Elements



113666

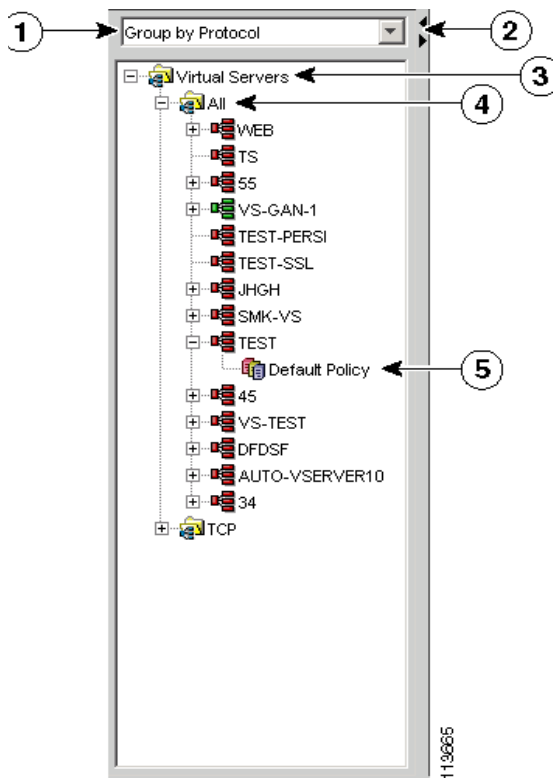
Figure 1-6 Reference	Location	Description
1	Menu bar	<p>Provides File, Edit, View, and Help buttons.</p> <ul style="list-style-type: none"> <li>• File           <ul style="list-style-type: none"> <li>– File &gt; Save to Startup—Saves the configuration running on the device as the startup configuration. You can also save the running configuration of the SSL daughter card to the startup configuration of CVDM-CSM.</li> <li>– Deliver to Device—Sends the configuration to the device.</li> <li>– File &gt; Exit—Logs you out of CVDM-CSM and closes the window. A warning appears if any configurations have not been applied. Based on your preference, the configurations are either applied or discarded before the application closes.</li> </ul> </li> <li>• Edit           <ul style="list-style-type: none"> <li>– Edit &gt; Preferences—Displays the Preferences dialog box, from which you can edit your global user preferences. For more information, see <a href="#">Editing Preferences, page 1-30</a>.</li> <li>– Edit &gt; Credentials—Displays the Enter SSL Credentials dialog box. For more information, see <a href="#">Configuring SSL Credentials, page 1-29</a>.</li> </ul> </li> <li>• View           <ul style="list-style-type: none"> <li>– View &gt; Home—Displays the home page.</li> <li>– View &gt; Setup—Displays the features page.</li> <li>– View &gt; Running Configuration—Displays the configuration running on the <b>Supervisor</b>, the <b>CSM</b>, and the <b>SSL</b>. You can view the running configuration of the SSL only when you give the correct credentials.</li> <li>– View &gt; Refresh—Collects the most recent device information and updates the CVDM-CSM data. For more information, see <a href="#">Refreshing CVDM-CSM, page 1-32</a>.</li> <li>– View &gt; Transport Log—Displays the transport log of the device. For more information, see <a href="#">Viewing the Device Transport Log, page 1-31</a>.</li> </ul> </li> </ul>

<b>Figure 1-6 Reference</b>	<b>Location</b>	<b>Description</b>
1	Menu bar	<ul style="list-style-type: none"> <li>• Help               <ul style="list-style-type: none"> <li>– Help &gt; Help Topics—Displays online help.</li> <li>– Help &gt; About—Displays CVDM-CSM version information.</li> </ul> </li> </ul>
2	Task bar	<p>Provides access to CVDM-CSM functionality.</p> <ul style="list-style-type: none"> <li>• Home—Displays the home page.</li> <li>• Setup—Displays the features page.</li> <li>• Refresh—Collects the most recent device information and updates CVDM-CSM with it.</li> <li>• Deliver—Opens the Deliver Configuration to Switch/Module(s) dialog box, from which you can send accumulated CVDM-CSM CLI commands to the device. For more information, see <a href="#">Delivering CLI Commands to the Switch/Module, page 1-32</a>.</li> <li>• Help—Displays context-sensitive help.</li> </ul>
3	Page	CVDM-CSM working area in which you perform tasks.
4	Pane	One part of a divided page or dialog box.
5	Status bar	<p>Provides the following information:</p> <ul style="list-style-type: none"> <li>• Message describing the current status of the application.</li> <li>• Icon showing a table of users logged in to the device.</li> <li>• Application user and privilege level.</li> <li>• Icon showing the list of pending CLIs to be delivered to the device.</li> <li>• Icon showing the security level of the connection.</li> <li>• Time stamp showing the application startup time.</li> </ul>
6	Selector	Hierarchy of the groups and objects available in the Switch or Services page that allows you to access specific functions for a Switch or Service object. See <a href="#">Selector, page 1-17</a> for more information.
7	Setup pane	Contains buttons, under the Switch or Services page, that allow you to access switch or services functions.

## Selector

Figure 1-7 shows the selector; Table 1-1 describes the selector elements.

**Figure 1-7 Selector**



**Table 1-1 Selector Elements**

Figure 1-7 Reference	Location	Description
1	Group folder	Displays a group of objects. Click the plus (+) symbol to see the contents of this folder.
2	Selector handle	Click the handle to open and close the selector, or click the handle and drag it to resize it.

**Table 1-1** *Selector Elements (continued)*

<b>Figure 1-7 Reference</b>	<b>Location</b>	<b>Description</b>
3	Subgroup folder	Displays a subgroup of objects. Click the plus (+) symbol to see the contents of this folder.
4	Object	Displays the individual entity contained in the group or subgroup. Click an object to open the page for that object.

**Note**

[Figure 1-7](#) shows what the selector looks like when there are folders, subfolders, and objects displayed. Some selectors do not contain all of these elements.



## Understanding the Action Buttons

This section describes the action buttons that appear in CVDM-CSM dialog boxes and wizards.

- For a description of the wizard action buttons, see [Table 1-2 on page 1-19](#).
- For a description of the dialog box action buttons, see [Table 1-3 on page 1-19](#).

**Table 1-2** *Wizard Action Buttons*

<b>Button</b>	<b>Action</b>
Back	Takes you to the previous page.
Next	Takes you to the next page.
Finish	Takes you to the wizard summary page.
Cancel	Exits the wizard without making any changes.
Help	Displays context-sensitive online help.

**Table 1-3** *Dialog Box Action Buttons*

<b>Button</b>	<b>Action</b>
OK	Saves your changes.
Cancel	Exits the dialog box without making any changes.
Help	Displays context-sensitive online help.

## What Does the Home Page Show Me?

The home page is the first screen that comes up when you start CVDM-CSM. It provides an overview of CVDM-CSM (see [Figure 1-8](#)).

**Figure 1-8** CVDM-CSM Home Page Components and Description

The screenshot shows the CVDM-CSM Home Page interface. The browser title bar indicates 'CiscoView Device Manager for CSM: Slot 6' and the IP address '172.26.196.195'. The interface includes a menu bar (File, Edit, View, Help) and a toolbar with icons for Home, Setup, SSL, Refresh, Deliver, and Help. The main content area is divided into several sections:

- System Overview:** Displays device information such as Model Type (WVS-X6066-SLB-S-K9), Serial Number (SAD074103EV), Slot Number (6), Software Version (1.1(1)), and Hardware Version (1.7). It also shows Network Processor Utilization for IXP1-Session, IXP2-TCP, IXP3-Layer 7, IXP4-Load Balancing, and IXP5-NAT, all at 0%. Additional metrics include Overflow Errors (0), Redundancy, Status (None), and FT VLAN ID.
- Services Dashboard:** Provides a summary of service status, including Inservice (1), Out of Service (13), Policy Associated (2), and Default Policy (8). It also lists Configured Policies (6), Policies Without Condition (1), and Policy Without Actions (3).
- Connection Dashboard:** Shows 'Current Connections: 0% of 1 Million Connections' and a note that all values are in units of Kilo connections. It includes a table for Cumulative Connections (Created, Destroyed, Failed, Timed Out) and L4 and L7 Connections (L4 Decisions, L7 Decisions, L4 Rejections, L7 Rejections), all showing 0 K.
- Server Dashboard:** Displays 'My Virtual Servers' with a table for Name, IP Address, Operations, and Status. It also shows Server Farms with Total (16) and Available (3) counts, and Real Servers with Named (15) and Unnamed (2) counts.
- FAQ:** A search bar with the text 'How do I setup a Virtual Server with Default Policy?' and a 'Go' button.

Five numbered callouts (1-5) point to specific elements: 1 points to the Home icon in the toolbar; 2 points to the SSL icon; 3 points to the Connection Dashboard; 4 points to the Services Dashboard; and 5 points to the Server Dashboard.

130081

<b>Figure 1-8 Reference</b>	<b>Location</b>	<b>Description</b>
1	SSL Button	<p>This button is visible only if you launch the CVDM-CSM for a CSM-S service module. It will not be visible if you launch CVDM-CSM.</p> <p>When you click this button:</p> <ol style="list-style-type: none"> <li>1. You must configure the credentials for CVDM-SSLSM, if they are not configured.</li> <li>2. After you enter the credentials, they are validated and CVDM-SSLSM launches.</li> </ol>
2	<p><b>System Overview tab</b></p> <p>Model Type</p> <p>Overflow Errors</p> <p>Serial Number</p> <p>Slot Number</p> <p>Software Version</p> <p>Hardware Version</p> <p><b>Redundancy pane</b></p> <p>Status</p> <p>FT VLAN ID</p> <p><b>Network Processor Utilization pane</b></p>	<p>Model type of the CSM.</p> <p>Number of overflow errors for the system.</p> <p>Serial number of the card.</p> <p>Slot number of the CSM for which the application is open.</p> <p>Software version of the CSM module.</p> <p>Hardware version of the CSM module.</p> <p>Displays if the module is Active or Standby mode.</p> <p>The VLAN over which heartbeat messages are sent. Both CSMs must have the same VLAN ID.</p> <p>The network processor utilization, in percentage, for IXP1-Session, IXP2-TCP, IXP3-Layer7, IXP4-Load-Balancing, and IXP5-NAT.</p>

<b>Figure 1-8 Reference</b>	<b>Location</b>	<b>Description</b>
3	<b>Connection Dashboard tab</b>	
	Graphs	Select this tab to view the Connection Dashboard details as graphs.  The graphs are indicated in units of kilo connections.
	Absolute Values	Select this tab to view all the actual counter values.
	<b>Cumulative Connections pane</b>	
	Created	Number of connections at the specified moment. The units are kilo connections.
	Destroyed	Number of connections destroyed. The units are kilo Connections.
	Failed	Number of connections that failed. The units are kilo connections.
	Timed Out	Number of connections that timed out. The units are kilo connections.
	<b>L4 and L7 Connections pane</b>	
	L4 Decisions	Number of Layer 4 load-balancing decisions made. The units are kilo connections.
	L7 Decisions	Number of Layer 7 load-balancing decisions made. The units are kilo connections.
	L4 Rejections	Number of Layer 4 load-balancing rejections made. The units are kilo connections.
	L7 Rejections	Number of Layer 7 load-balancing rejections made. The units are kilo connections.

<b>Figure 1-8 Reference</b>	<b>Location</b>	<b>Description</b>
4	<b>Services Dashboard tab</b>	
	<b>Virtual Servers</b>	
	In Service	Number of virtual servers that are operational.
	Out of Service	Number of virtual servers that are not operational.
	Policy Associated	Number of virtual servers that have associated policies.
	Default Policy	Number of virtual servers that have only the default policy.
	<b>Policies</b>	
	Configured Policies	Number of policies that are configured in the CSM module.
	Policies Without Conditions	Number of policies that do not have conditions.
	Policies Without Actions	Number of policies that do not have actions.
	<b>Server Farms</b>	
	Total	Number of server farms configured in the CSM module.
	Available	Number of server farms with at least one operational real server.
	<b>Real Servers</b>	Displays the administrative status of the real servers.
	Named Reals	Number of named real server configured on the CVDM-CSM.
	Unnamed Reals	Number of unnamed real server configured on the CVDM-CSM.
5	<b>Server Dashboard</b>	
	My Virtual Server	Selected virtual servers that are used in emergencies as critical servers. For more details, see <a href="#">What are My Virtual Servers?</a> , page 1-24.
	Name	Name of the virtual server.
	IP Address	IP address of the virtual server.
	Operational Status	Virtual servers that are out of service.

## What are My Virtual Servers?

My Virtual Servers is a page you can access through a link on the home page, under the **Server Dashboard**.

---

**Step 1** Click the **My Virtual Servers** link under the **Server Dashboard**.

The My Virtual Servers page appears, displaying the following fields:

Field	Description
<b>Virtual Server Name</b>	A list of virtual servers.
<b>Select</b>	Select the check box next to a virtual server to include it as a part of your user preferences.
<b>Select All</b>	Select this check box to select all the virtual servers.

## What Does the Setup Page Show Me?

The Setup page allows you to access the features in CVDM-CSM. You can launch wizards from this page or you can start working with VLANs, virtual servers, server farms, real servers, policies, fault tolerance, XML configuration, probe scripts from this page.

When you reach the Setup page, the following GUI elements appear in an outlook bar on the left side of the content window:

GUI Element	Description
Wizard	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Configure and manage client and server VLANs and virtual servers, and associate default policies using the Basic Virtual Server Setup wizard.</li> </ul> <p>For more information, see <a href="#">Basic Setup Wizard, page 2-3</a>.</p> <ul style="list-style-type: none"> <li>• Configure the Layer 7 policies along with the above configurations using the Advanced Virtual Server Setup wizard.</li> </ul> <p>For more information, see <a href="#">Advanced Setup Wizard, page 2-13</a>.</p>
VLANs	<p>Allows you to configure client-side and server-side VLANs.</p> <p>See, <a href="#">Chapter 3, “Managing VLANs”</a>.</p>
Virtual Servers	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Create and delete virtual servers.</li> <li>• Enable and disable virtual service.</li> <li>• Associate virtual servers with a server farm or policy.</li> <li>• Restrict client access to virtual servers.</li> <li>• Configure performance, load, connection, and traffic parameters.</li> <li>• Configure sticky connections.</li> <li>• Enable partial server farm failover.</li> </ul> <p>See, <a href="#">Chapter 4, “Managing Virtual Servers”</a>.</p>

GUI Element	Description
Server Farms	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Configure server farms.</li> <li>• Specify load-balancing algorithm, and monitor in-band health for each server farm.</li> <li>• Configure a set of real servers and their attributes.</li> <li>• Configure client NAT pools.</li> <li>• Configure redirect virtual servers and their attributes.</li> <li>• Configure health monitoring probes, and enable inband health checkup.</li> <li>• Direct the traffic to the SSL daughter card.</li> </ul> <p>See, <a href="#">Chapter 5, “Managing Server Farms”</a>.</p>
Real Servers	<p>Allows you to configure the named real servers by their IP address and location. See, <a href="#">Chapter 6, “Managing Real Servers”</a>.</p>



GUI Element	Description
Policies	<p>With the object selector, you can make the following selections:</p> <ul style="list-style-type: none"> <li>• <b>Policies</b>—When you select policies, you can: <ul style="list-style-type: none"> <li>– Configure access rules such as maps (cookie map, header map, URL map), client groups (access control lists), and sticky group (cookie, header, netmask, and SSL).</li> <li>– Associate a server farm and a backup server farm with a particular policy.</li> </ul> <p>See, <a href="#">Chapter 7, “Managing Policies”</a>.</p> </li> <li>• <b>Maps</b>—When you select maps, you can: <ul style="list-style-type: none"> <li>– Configure maps to define multiple URLs, cookies, HTTP headers, and return codes into groups that can be associated with a policy.</li> <li>– Insert information such as the client’s IP address into the HTTP header using HTTP header insert feature. This feature is particularly useful when the CVDM-CSM performs source NAT and the application on the server side still requires visibility to the original source IP.</li> <li>– Specify the name of the field and the corresponding value for the CVDM-CSM to match, when receiving an HTTP request.</li> </ul> <p>See, <a href="#">Chapter 8, “Managing Maps”</a>.</p> </li> <li>• <b>Sticky Groups</b>—When you select maps, you can configure Sticky groups such as Cookie, Header, SSL, Netmask.</li> </ul> <p>See, <a href="#">Chapter 9, “Managing Sticky Groups”</a>.</p>

GUI Element	Description
Probes	<p>Allows you to configure specific types of health probes, such as FTP, HTTP, ICMP, SMTP, TCP, Telnet, UDP, and Script health probes to administer your network.</p> <p>See, <a href="#">Chapter 10, “Managing Probes”</a>.</p>
Miscellaneous	<p>With the object selector, you can make the following selections:</p> <ul style="list-style-type: none"> <li>• <b>Fault Tolerance</b>—When you select policies, you can: <ul style="list-style-type: none"> <li>– Configure active and standby CVDM-CSMs, fault tolerant VLANs, and parameters like failover time and heartbeat time.</li> <li>– Set the priority for any CVDM-CSM.</li> </ul> <p>See, <a href="#">Understanding Fault Tolerance, page 11-1</a>.</p> </li> <li>• <b>Scripts</b>—When you select scripts, you can: <ul style="list-style-type: none"> <li>– Upload and execute Toolkit Command Language (TCL) scripts.</li> <li>– Customize scripts to develop health probes or standalone tasks.</li> </ul> <p>See, <a href="#">Understanding Scripts, page 11-6</a>.</p> </li> <li>• <b>Environment Variables</b>—When you select environment variables, you can configure CVDM-CSM environment variables and see the values of the configured variables. <p>See, <a href="#">Viewing Environment Variables, page 11-13</a>.</p> </li> <li>• <b>XML Config</b>—When you select XML config, you can configure the CVDM-CSM using a Document Type Definition (DTD). <p>See, <a href="#">Understanding XML Configuration, page 11-19</a>.</p> </li> </ul>

# Configuring SSL Credentials

CVDM-CSM uses the device credentials to log into the SSL daughter card and extract the details to launch the CiscoView Device Manager for the SSL Services Module (CVDM-SSLSM).

- To enter the SSL credentials, click **SSL** at the top of the window.

The Enter Credentials–SSL:*slot number* dialog box appears. Enter the appropriate values.

Field	Description
Username	Enter your CVDM-SSLSM username.
Password	Enter your CVDM-SSLSM password.
Enable Username	Enter your CVDM-SSLSM enable username.
Enable Password	Enter your CVDM-SSLSM enable password.

After you enter the credentials, they are validated and the CVDM-SSLSM launches. Once the credentials are validated you cannot edit them. When you select **Edit > Credentials** from the menu bar and invoke the Edit Credentials–SSL:*slot number* dialog box, you can only view the validated credentials.

# Editing Preferences

- Step 1** Select **Edit > Preferences** from the menu bar. The Preferences dialog box appears.
- Step 2** Modify the appropriate values:

GUI Element	Action
Show CLI Preview for Wizards check box	<p>Select this check box if you want CVDM-CSM to display the CLI commands to be delivered to the device after you have completed a wizard.</p> <p>When you select this check box and click <b>Finish</b> in a wizard, the Deliver Configuration to the Switch/Module(s) dialog box opens and displays the CLI commands.</p> <p>For more information, see <a href="#">Delivering CLI Commands to the Switch/Module, page 1-32</a>.</p>
Show CLI Preview on Delivery check box	<p>Select this check box if you want CVDM-CSM to display the CLI commands to be delivered to the device.</p> <p>When you select this check box and click <b>Deliver</b>, the Deliver Configuration to Switch/Module(s) dialog box opens and displays the CLI commands.</p> <p>For more information, see <a href="#">Delivering CLI Commands to the Switch/Module, page 1-32</a>.</p>
Confirm before exiting check box	<p>Select this check box if you want CVDM-CSM to confirm with you before exiting the application.</p> <p>Select the <b>Always display this dialog box before exiting</b> check box if you always want CVDM-CSM to confirm that you want to exit the application.</p>
Refresh after Delivery check box	<p>Select this check box to refresh CVDM-CSM after delivering accumulated CLI commands for the device.</p>

# Viewing the Running Configuration Information for a Device

---

**Step 1** Select **View > Running Config** from the menu bar, then select one of the following:

- **Supervisor...**
- **CSM: Slot X...**
- **SSL:Slot X...**



---

**Note** You can select options only for the installed service modules.

---

**Step 2** The Show Running Configuration dialog box appears. Information about the running configuration for the selected component appears.

You can click the **Save to File** button to save this information as a text file.

---

## Viewing the Device Transport Log

---

**Step 1** Select **View > Transport Log** from the menu bar. A warning message appears.

**Step 2** To proceed, click **OK**. The Transport Log dialog box appears, displaying information about communication between CVDM-C6500 and CVDM-CSM.

You can do either of the following:

- Click **Clear Log** to clear the information in the transport log.
  - Click **Save to File** to save the transport log information as a text file.
-

## Refreshing CVDM-CSM

You can refresh CVDM-CSM at any time to obtain the latest service module information and update the CVDM-CSM data. You do not have to refresh the application after delivering accumulated CLI commands for the device; the application is automatically refreshed.

- 
- Step 1** Do one of the following:
- Click **Refresh** at the top of the window.
  - Or
  - Select **View > Refresh** from the menu bar.
- Step 2** A dialog box appears, asking if you want to proceed with the refresh. To proceed, click **Yes**. The most recent device information is collected and populated in CVDM-CSM.
- 

## Delivering CLI Commands to the Switch/Module

You must deliver accumulated CLI commands to the device before any changes you make in CVDM-CSM will be applied. The Deliver Configuration to Switch/Module(s) dialog box displays the accumulated CLI commands to be delivered to the device.

- 
- Step 1** Click the **Deliver** button in the taskbar.
- The Deliver Configuration to Switch/Module(s) dialog box appears if you have configured CVDM-CSM to display the accumulated CLI commands when you click the Deliver button.



- Note** The Deliver Configuration to Switch/Module(s) dialog box also appears when you click the **Finish** button in a wizard if you have configured CVDM-CSM to display the accumulated CLI commands after you have completed a wizard.
-

**Step 2** Edit the appropriate values:

GUI Element	Action/Description
Deliver button	Click to send the accumulated CLI commands to the device.
Save to File... button	Click to save the CLI commands as a text file.
Close button <sup>1</sup>	Close the dialog box without delivering any CLI commands.
Deliver Later button <sup>2</sup>	Click to deliver the wizard CLI commands to the device at a later time.
Refresh after Delivery check box	Select this check box to refresh CVDM-CSM after delivering accumulated CLI commands for the device.

1. This button is available only in the Deliver Configuration to Switch/Module(s) dialog box that is displayed after you click **Deliver** at the top of the window.
2. This button is available only in the Deliver Configuration to Switch/Module(s) dialog box that is displayed after you click **Finish** in a wizard.



**Note**

The Deliver Configuration to Switch/Module(s) dialog box displays *all* accumulated CLI commands that will be delivered to the device; therefore, any previous CLI commands that were not sent to the device are shown in this dialog box, as well as the CLI commands you have generated in this session.







## Configuring CVDM-CSM

---

CVDM-CSM allows user to setup the CSM module features with the help of wizards, which simplify the complex configuration.

This section includes the following topics:

- [Understanding Wizards, page 2-2](#)
- [Basic Setup Wizard, page 2-3](#)
- [Advanced Setup Wizard, page 2-13](#)
- [FAQ, page 2-15](#)

# Understanding Wizards

CVDM-CSM Manager allows you to choose between two types of setup wizards: basic and advanced.

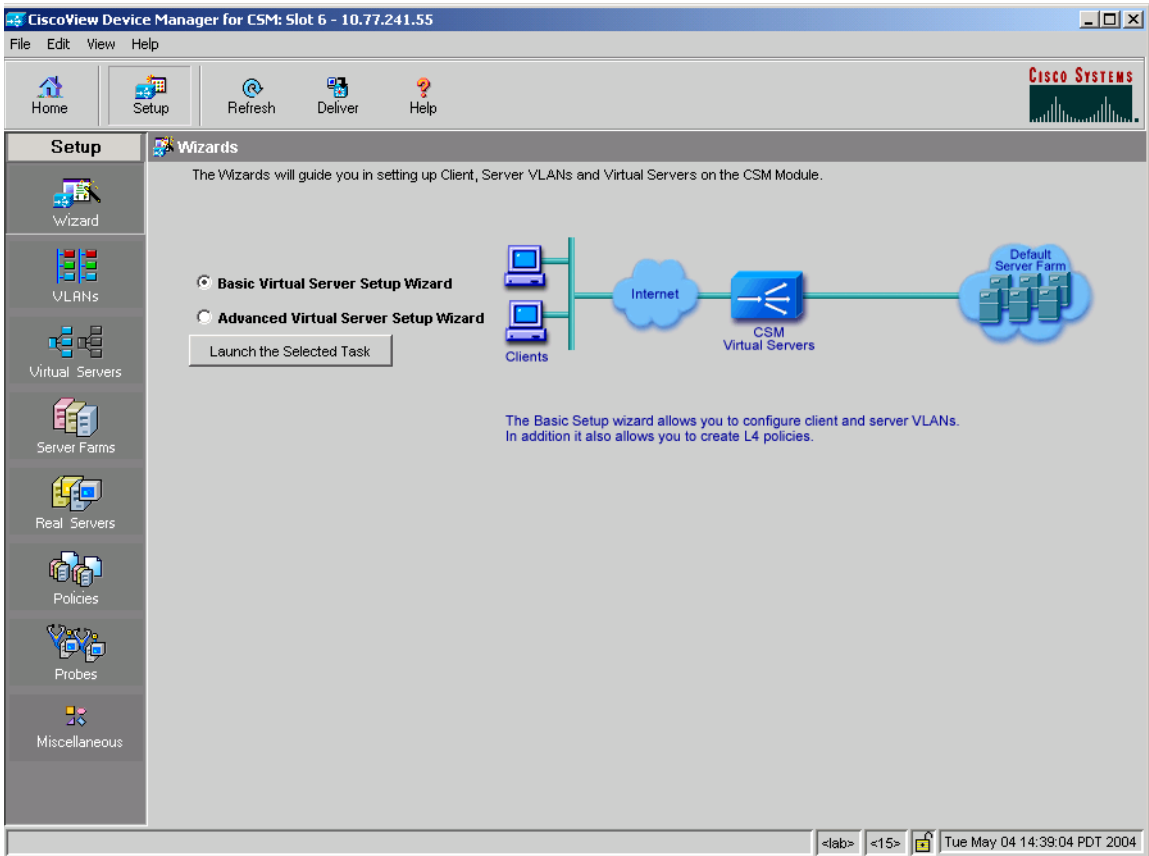
To choose between the two wizards:

- 
- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Wizards** in the Setup pane. The setup wizards information appears in the content area.
- Step 3** Select either of the two wizards:
- Basic Setup Wizard
  - Advanced Setup Wizard
- Step 4** Click **Launch Selected Task** to launch the corresponding wizard.
-

# Basic Setup Wizard

The Basic Setup Wizard allows you to configure and manage client and server VLANs and virtual servers, and associate Layer 4 policies. [Figure 2-1](#) shows the Basic Setup Wizard page.

**Figure 2-1** Basic Setup Wizard Page



115306

## Welcome Page of the Basic Setup Wizard

This wizard guides you to setup a virtual server with a default server farm and set of real servers. It also guides you to setup client-side or server side VLANs. You can also associate the VLAN to the Virtual Server.

The Welcome page lists the three basic configuration steps:

- Step 1: Configure Client and Server side VLANs in Route (different subnet) or Bridge (single subnet) Mode. For more information, see [Configuring Client and Server Side VLANs, page 2-4](#).
- Step 2: Configure a Virtual Server. For more information, see [Configuring a Virtual Server, page 2-9](#).
- Step 3: Configure a Default Policy. For more information, see, [Configuring the Default Policy, page 2-11](#).

## Configuring Client and Server Side VLANs

You can create client-side VLAN and server-side VLAN in route mode (different subnets) or bridge mode (single subnet), from this step. If you have configured at least one client-side or server-side VLAN, this step is optional.

In bridge mode configuration, the client-side and server-side VLANs are on the same subnets. Hence, the IP address and mask values of the client VLAN are populated for the server VLAN.

In route mode configuration, the client-side and server-side VLANs are on different subnets.

Select the radio button to configure in the **Route mode** or **Bridge mode**.

The fields in the table will vary according to the mode of configuration. In bridge mode configuration, you can configure only VLAN ID. The IP address and mask have to be the same for both client-side and server-side VLANs.

You can configure the following in the Configuring Client and Server Side VLANs dialog box.

Field	Action/Description
<b>Client VLAN</b>	
VLAN ID	<p>Specify the ID of the client-side VLAN. You can create a new VLAN or choose from a list of available VLANs.</p> <p>Click <input type="button" value="v..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select VLAN</b>—Allows you to select a VLAN from a list. If you choose <b>local</b>, CSM-S forwards the packets directly to the real server.</li> <li>• <b>Create VLAN</b>—Allows you to create a VLAN by entering the VLAN ID.</li> <li>• <b>Clear VLAN</b>—Allows you to clear the VLAN field.</li> </ul>
IP Address	<p>Enter the IP address of the client-side VLAN. You can configure only one management IP address per VLAN.</p>
Alias	<p>Click <input type="button" value="v..."/> and select <b>Add Alias</b>. The Add Alias dialog box appears. Enter the alias IP address. You can add an alias IP address only after you add a valid IP address.</p> <p>You can configure up to 255 aliases per VLAN. When more than one alias IP address is listed, they will appear serially, separated by a comma.</p>
Gateways	<p>Click <input type="button" value="v..."/> and select <b>Add Gateways</b>. The Add Gateways dialog box appears. From the list, select the gateway for the client-side VLAN.</p> <p>You can configure up to 7 gateways per VLAN, with a total of up to 255 gateways for the entire system.</p> <p>A gateway must be in the same network as specified in the IP address. When more than one gateway IP address is listed, they will appear serially, separated by a comma.</p>
Static Routes	<p>Specify the static route. When more than one static route is listed, they will appear serially, separated by a comma.</p> <p>Click <input type="button" value="v..."/> and select <b>Add Static Route</b> to add a static route from a list. For more information on adding static routes, see <a href="#">Adding Static Routes, page 2-8</a>.</p>

Field	Action/Description
Server VLAN	In bridge mode configuration, you can configure only VLAN ID. The IP address and mask have to be the same for both client-side and server-side VLANs.
VLAN ID	<p>Specify the ID of the server-side VLAN. You can create a new VLAN or choose from a list of available VLANs.</p> <p>Click <input type="button" value="▽..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select VLAN</b>—Allows you to select a VLAN from a list. If you choose <b>local</b>, CSM-S directly forwards the packets to the real server.</li> <li>• <b>Create VLAN</b>—Allows you to create a VLAN by entering the VLAN ID.</li> <li>• <b>Clear VLAN</b>—Allows you to clear the VLAN field.</li> </ul>
IP Address	(Disabled for bridge mode) Enter the IP address of the server-side VLAN. You can configure only one management IP address per VLAN.
Alias	<p>(Only in route mode) Click <input type="button" value="▽..."/> and select <b>Add Alias</b>. The Add Alias dialog box appears. Enter the alias IP address. You can add an alias IP address only after you add a valid IP address.</p> <p>When more than one alias IP address is listed, they will appear serially, separated by a comma.</p>
Mask	<p>(Disabled for bridge mode) From the list, select the IP mask to be applied. You can choose from Class A, Class B, Class A and Class D masks.</p> <p>If it is not specified, the default for network mask is 255.255.255.255.</p>

Field	Action/Description
Gateways	<p>(Only in route mode) Click <input type="button" value="▽..."/> and select <b>Add Gateways</b>. The Add Gateways dialog box appears. From the list, select the gateway for the server-side VLAN.</p> <p>You can configure up to seven gateways per VLAN, with a total of up to 255 gateways for the entire system. A gateway must be in the same network as specified in the IP address. When more than one gateway IP address is listed, they will appear serially, separated by a comma.</p>
Static Routes	<p>(Only in route mode) Specify the static route. When more than one static route is listed, they will appear serially, separated by a comma.</p> <p>Click <input type="button" value="▽..."/> and select <b>Add Static Route</b> to add a static route from a list. For more information on adding static routes, see <a href="#">Adding Static Routes, page 2-8</a>.</p>

## Adding Static Routes

- 
- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Wizards** in the Setup pane. The Setup Wizards information appears in the content area.
- Step 3** You can select either of the following two wizards:
- **Basic Setup Wizard**
  - **Advanced Setup Wizard**
- Step 4** Click **Launch Selected Task** to launch the corresponding wizard. The Welcome page appears.
- Step 5** Click **Next**. The Configure Client and Server Side VLAN dialog box appears.
- Step 6** In the Client and Server VLAN section, click  in the static route field. The Add Static Route dialog box appears, displaying the following columns.

Field	Description
Destination IP	Enter the IP address of the destination.
Mask	From the list, select the mask to be applied. You can choose from Class A, Class B, Class A and Class D masks. The default for network mask is 255.255.255.255.
Next Hop	Enter the IP address of the next hop.

---



## Configuring a Virtual Server

The Basic Setup Wizard allows you to configure the basic parameters of a virtual server. You can configure the IP address, mask, protocol, port, service type and also specify a VLAN to enable traffic from it.

The Advanced Setup Wizard allows you to configure client and server VLANs and also create layer 4 to layer 7 policies.

The Configure Virtual Server dialog box appears, displaying the following columns:

Column	Description
Virtual Server	Click <input type="button" value="v..."/> and select one of the following: <ul style="list-style-type: none"> <li>• <b>Select Virtual Server</b>—Allows you to select a virtual server from a list.</li> <li>• <b>Create Virtual Server</b>—Allows you to create a virtual server by entering its name.</li> </ul>
<b>Virtual IP Address</b>	
IP Address	Enter the IP address of the virtual server.
Mask	Enter the mask for the IP address, to allow connections for the entire network. The default IP mask is 255.255.255.255.
Protocol	From the list, select the load-balancing protocol.
Allow Traffic from VLAN	From the list, select a VLAN to enable traffic from it.

Column	Description
Port	<p>From the list, select the port.</p> <p>This field is enabled only when you choose TCP or UDP as the protocol.</p>
Service Type	<p>From the list, select the service type. You can combine connections associated with the same service. This allows all related connections from a client to use a particular real server.</p> <p>The options depend on the protocol you choose. You can choose from the following:</p> <ul style="list-style-type: none"> <li>• FTP—Combines connections to FTP port 21.</li> <li>• RTSP—Combines connections to Real Time Streaming Protocol (RTSP) TCP port 554.</li> <li>• Termination—Enables TCP termination for DoS attack protection.</li> <li>• Per-packet—Load balances each packet independently. This option is for non-TCP only.</li> </ul>

## Configuring the Default Policy

From this step, you can configure multiple real servers and associate them to the server farm, and delete the association of the existing real server.

The following columns appear in the Configure Default Policy dialog box:

Field	Description
Default Server Farm	Click <input type="text" value="▽..."/> and select one of the following: <ul style="list-style-type: none"> <li>• <b>Select Server Farm</b>—Allows you to select a server farm from a list.</li> <li>• <b>Create Server Farm</b>—Allows you to create a server farm by entering its name.</li> </ul>
<b>Associated Real Servers</b>	
Real	The real server associated to the server farms.
Local	Indicates if this real server is the SSL card.
Minimum Connections	Minimum number of connections for the real server.
Maximum Connections	Maximum number of connections for the real server.
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Lets you know the administrative status of the real server.



### Note

You can add, edit or delete named and unnamed real servers only after you add or select a server farm.

From the Configure Default Policy dialog box, you can do the following:

- Click **Add** and do either of the following:
  - **Select Named Real Server**—Opens the Add Named Real Server dialog box. For more information, see [Adding a Named Real Server, page 5-23](#).

- **Create Unnamed Real Server**—Opens the Add Unnamed Real Server dialog box. For more information, see [Adding an Unnamed Real Server, page 5-27](#).
- **Add Multiple Real Servers**—Opens the Real Server Selector and allows you to add multiple real servers. For more information, see [Adding Multiple Real Servers, page 5-11](#).
- Click **Edit** to edit the selected real server. For more information on editing real servers, see [Editing a Real Server, page 6-10](#).
- Click **Delete** to delete the selected real server.

## Summary

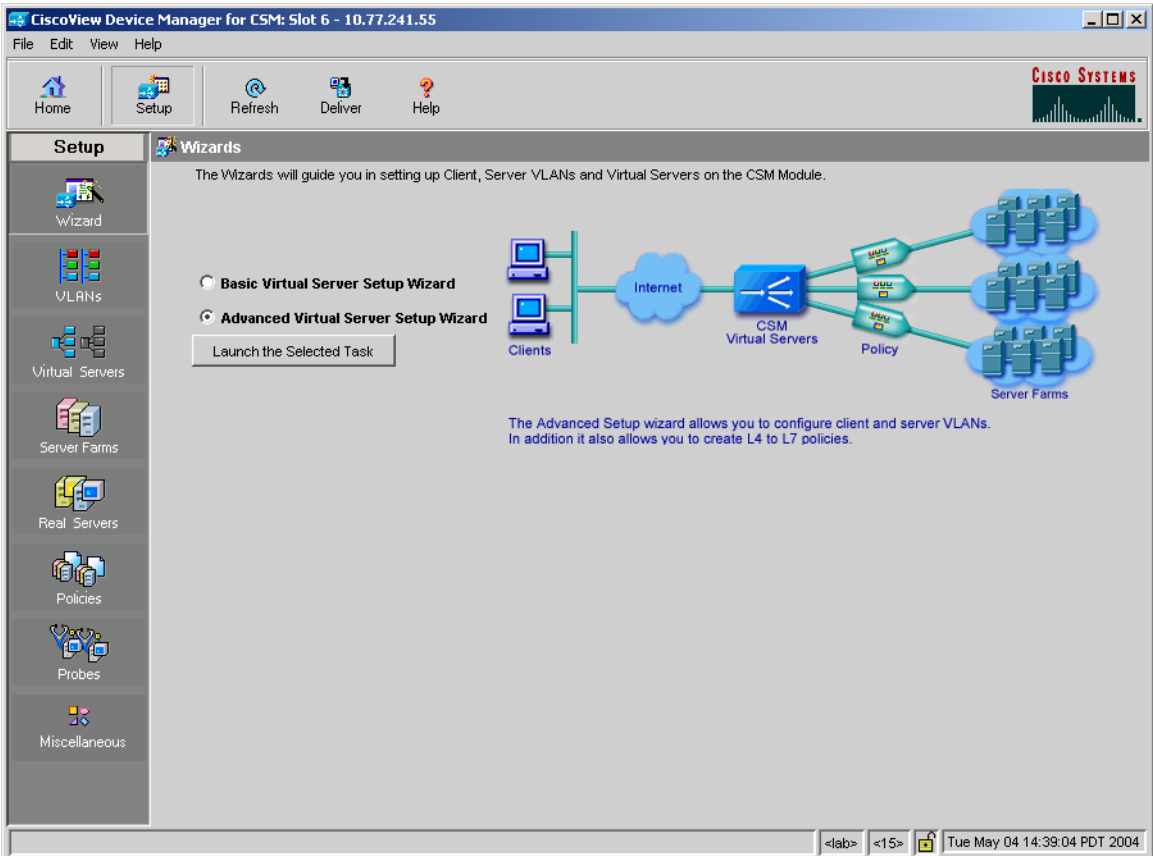
You can see a list of all the generated CLI commands that are delivered to the device after you click the **Finish** button.

- 
- Step 1** Click **Setup** from the task bar, click **Wizards** in the Setup pane. The Setup Wizards information appears in the content area.
- Step 2** You can select any of the following two wizards:
- **Basic Setup Wizard**
  - **Advanced Setup Wizard**
- Step 3** Click **Launch Selected Task** to launch the corresponding wizard dialog. The Welcome page appears.
- Step 4** Click **Next**. The Configure Client and Server Side VLAN dialog box appears.
- Step 5** Click **Next**. The Configure Virtual Server dialog box appears.  
If you selected Advanced Setup Wizard you will have to **Configure Layer 7 Policies**, then click **Next**.
- Step 6** Click **Next**. The Configure Default Policy dialog box appears.
- Step 7** Click **Next**. The Summary dialog box appears.
-

# Advanced Setup Wizard

The Advanced Setup Wizard allows you to configure client and server VLANs and also create layer 4 to layer 7 policies. [Figure 2-2](#) shows the Advanced Wizards page.

**Figure 2-2**      *Advanced Wizards Page*



115307

## Welcome Page of the Advanced Setup Wizard

This wizard guides you to setup a virtual server with a default server farm, set of real servers and create layer 4 to layer 7 policies. It also guides you to setup client-side or server side VLANs and associate a VLAN to virtual server.

The Welcome page lists the four configuration steps:

- Step 1: Configure Client and Server side VLANs in Route (different subnet) or Bridge (single subnet) Mode. For more information, see [Configuring Client and Server Side VLANs, page 2-4](#).
- Step 2: Configure a Virtual Server. For more information, see [Configuring a Virtual Server, page 2-9](#).
- Step 3: Configure Layer 7 Policies. For more information, see [Configuring Layer 7 Policies, page 2-14](#).
- Step 4: Configure a Default Policy. For more information, see, [Configuring the Default Policy, page 2-11](#).

## Configuring Layer 7 Policies

You can create and associate layer 7 policies to the virtual server. You can view the current policies, add new ones, delete existing ones, and also change the order of the policies.

You can configure the policy, and also configure and associate the following to the policy:

- One map of each type (URL, Header, Cookie and Return Code).
- One sticky group of any type (Cookie, SSL, Header or NetMask).
- One client group.

The Configure and Associate Layer 7 Policies dialog box appears. From this dialog box, you can do the following:

- Click **Add** and select one of the following:
  - **Select Policy**—Allows you to select from a list of configured policies.
  - **Create Policy**—Allows you to add a new policy. For more information on creating policies, see [Adding Policies, page 7-5](#).
- Select a policy and click **Delete** to remove it from the virtual server.

- Click the **Up** button to move the policies up in the list.
- Click the **Down** button to move the policies down in the list.

**Note**

---

Be sure to put the policies in the right order. Traffic is routed based on the order of the policies.

---

## FAQ

This section describes some common FAQs:

- [How Do I Set Up a Virtual Server with Default Policy using Wizards?](#)
- [How Do I Set Up a Virtual Server with Layer 7 Policy using Wizards?](#)
- [How Do I Set Up a Virtual Server with Default Policy and Layer 7 Policies?](#)

## How Do I Set Up a Virtual Server with Default Policy using Wizards?

The Basic Setup Wizard allows you to configure and associate multiple real servers to the server farm and delete the association of the existing real server.

To setup a virtual server with the default policy:

- 
- Step 1** Click **Setup** from the task bar, click **Wizards** in the Setup pane. The Setup Wizards information appears in the content area.
  - Step 2** Select **Basic Setup Wizard**, then click **Launch Selected Task**. The Welcome page appears.
  - Step 3** Click **Next** to proceed to step 1. The Configure Client and Server Side VLAN dialog box appears. To configure Client and Server Side VLANs, see [Configuring Client and Server Side VLANs, page 2-4](#).
  - Step 4** Click **Next** to proceed to step 2. The Configure Virtual Server dialog box appears. To configure a virtual server, see [Configuring a Virtual Server, page 2-9](#).
  - Step 5** Click **Next** to proceed to step 3. The Configure Default Policy dialog box appears. To configure the default policy, see [Configuring the Default Policy, page 2-11](#).
-



## How Do I Set Up a Virtual Server with Layer 7 Policy using Wizards?

The Advanced Setup Wizard allows you to configure client and server VLANs and create layer 4 to layer 7 policies.

To setup a virtual server with Layer 7 policy:

- 
- Step 1** Click **Setup** from the task bar, click **Wizards** in the Setup pane. The Setup Wizards information appears in the content area.
  - Step 2** Select **Advanced Setup Wizard**, then click **Launch Selected Task**. The Welcome page appears.
  - Step 3** Click **Next** to proceed to step 1. The Configure Client and Server Side VLAN dialog box appears. To configure client and server-side VLANs, see [Configuring Client and Server Side VLANs, page 2-4](#).
  - Step 4** Click **Next** to proceed to step 2. The Configure Virtual Server dialog box appears. To configure virtual server, see [Configuring a Virtual Server, page 2-9](#).
  - Step 5** Click **Next** to proceed to step 3. The Configure and Associate Layer 7 Policies dialog box appears. To configure and associate layer 7 policies, see [Configuring Layer 7 Policies, page 2-14](#).
  - Step 6** Click **Next** to proceed to step 4. The Configure Default Policy dialog box appears. To configure the default policy, see [Configuring the Default Policy, page 2-11](#).
-

## How Do I Set Up a Virtual Server with Default Policy and Layer 7 Policies?

To set up a virtual server with default Policy and Layer 7 policies:

- 
- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Virtual Servers** under Services Dashboard.
- Or
- Click **Setup** from the task bar and click **Virtual Servers** in the Setup pane.
- Step 2** Click **Add**. The Add Virtual Server dialog box appears.
- Step 3** Click one of the following tabs, then proceed to the corresponding section in this guide for configuration information:
- [General, page 2-19](#)
  - [Policies, page 2-21](#)
  - [Default Policy, page 2-22](#)
  - [Client Restriction, page 2-24](#)
  - [Sticky Connections, page 2-25](#)
  - [Other, page 2-28](#)
-

## General

Click the **General** tab to configure the basic configuration details.

**Figure 2-3 Add Virtual Server > General Dialog Box**

The following columns appear:

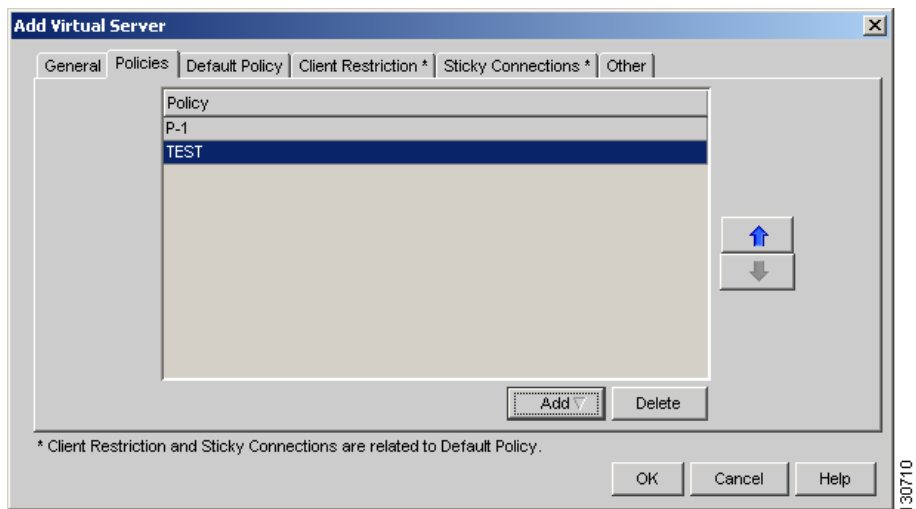
Columns	Action/Description
Name	Enter the name of the virtual server.
Status	From the list, select the status of the virtual server.
VLAN ID	From the list, specify a VLAN for incoming traffic. <ul style="list-style-type: none"> <li>• If you choose <b>All</b>, traffic from all VLANs is enabled.</li> <li>• If you choose <b>Local</b>, CSM-S directly forwards the packets to the real server.</li> </ul>
<b>Virtual IP Address</b>	

<b>Columns</b>	<b>Action/Description</b>
IP Address	Enter the IP Address of the virtual server.
Protocol	From the list, select the type of protocol to use. You can choose from Any, TCP, or UDP, or enter a number from 1 to 255.
Port	From the list, select the port number. This field is enabled only when you choose TCP or UDP.
Service Type	<p>From the list, select the service type. You can combine connections associated with the same service. This allows all related connections from a client to use a particular real server.</p> <p>The options depend on the protocol you choose. You can choose from the following:</p> <ul style="list-style-type: none"> <li>• FTP—Combines connections to FTP port 21.</li> <li>• RTSP—Combines connections to Real Time Streaming Protocol (RTSP) TCP port 554.</li> <li>• Termination—Enables TCP termination for DoS attack protection.</li> <li>• Per-packet—Load balances each packet independently. This option is for non-TCP only.</li> </ul>
Mask	Specify the virtual IP mask.
<b>Advertise</b>	
Advertise Virtual IP	Select this to advertise the IP address of the virtual server as the host route.
Advertise only if reals are active	Select this to advertise only if real servers are active.

## Policies

Click the **Policies** tab to add or delete policies.

**Figure 2-4** Add Virtual Server > Policies Dialog Box



You have the following options:

- Click **Add** and select one of the following to associate policies to the virtual server:
  - **Select Policy**—Allows you to select a policy from a list.
  - **Create Policy**—Allows you to create a policy. For more information, see [Adding Policies, page 7-5](#).
- Select a policy from the table and click **Delete** to remove policies from the virtual server.
- Click the Up button to move the policies up in the list.
- Click the Down button to move the policies down in the list.



### Note

Be sure to put the policies in the right order. Traffic is routed based on the order of the policies.

## Default Policy

Click the **Default Policy** tab to add the default and backup server farms. You can configure a backup server farm to operate when a server farm is out of service.

To enable partial server farm failover, you can now define the threshold number of real servers to be out of service for the backup server farm to take over. You can also define the number of real servers to be in service for the server farm to be considered active.

**Figure 2-5** Add Virtual Server > Default Policy Dialog Box

The screenshot shows a dialog box titled "Add Virtual Server" with a close button (X) in the top right corner. The dialog has several tabs: "General", "Policies", "Default Policy" (which is selected and highlighted with a dotted border), "Client Restriction \*", "Sticky Connections \*", and "Other".

Under the "Default Policy" tab, there are the following elements:

- "Default Server Farm:" followed by a text input field and a dropdown arrow button.
- "Backup Server Farm:" followed by a text input field and a dropdown arrow button.
- "Server Farm:" followed by a text input field, a dropdown arrow button, and a checkbox labeled "Sticky".
- A "Threshold" section containing two input fields: "Reals Inservice (1-16383):" and "Reals Out of Service (1-16383):".
- A note at the bottom: "\* Client Restriction and Sticky Connections are related to Default Policy."
- Three buttons at the bottom right: "OK", "Cancel", and "Help".

On the right side of the dialog box, there is a vertical text label "130707".

The following information appears:

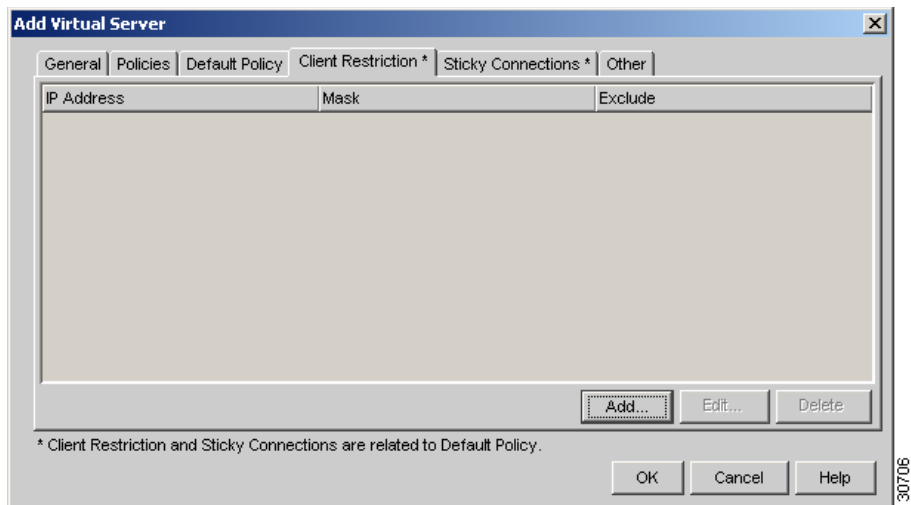
Column	Action/Description
Default Server Farm	<p>Click <input type="button" value="v..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Server Farm</b>—Allows you to select one from a list of server farms.</li> <li>• <b>Create Server Farm</b>—Allows you to create a server farm. For more information, see <a href="#">Adding Server Farms, page 5-5</a>.</li> <li>• <b>Clear Server Farm</b>—Allows you to clear the field.</li> </ul>
<b>Backup Server Farm</b>	
Server Farm	<p>Click <input type="button" value="v..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Server Farm</b>—Allows you to select a server farm from a list.</li> <li>• <b>Create Server Farm</b>—Allows you to create a server farm. For more information, see <a href="#">Adding Server Farms, page 5-5</a>.</li> <li>• <b>Clear Server Farm</b>—Allows you to clear the field.</li> </ul>
Sticky	<p>Select this check box to enable the sticky property.</p> <p>This ensures that multiple connections from the same client, that match the same SLB policy stick (or attach) to the same real server.</p>
<b>Threshold</b>	

Column	Action/Description
Reals Inservice	The number of real servers to be in service for the server farm to be active.
Reals Out of Service	The number of real servers to be out of service for the backup server farm to take over.

## Client Restriction

Click the **Client Restriction** tab to add details of the clients restricted to use the virtual server.

**Figure 2-6** Add Virtual Server > Client Restriction Dialog Box



You have the following options:

- Click **Add** to create client restrictions for multiple clients.
- Click **Edit** to edit the client restrictions for multiple clients.
- Select a row in the table and click **Delete** to delete the selected client restriction.



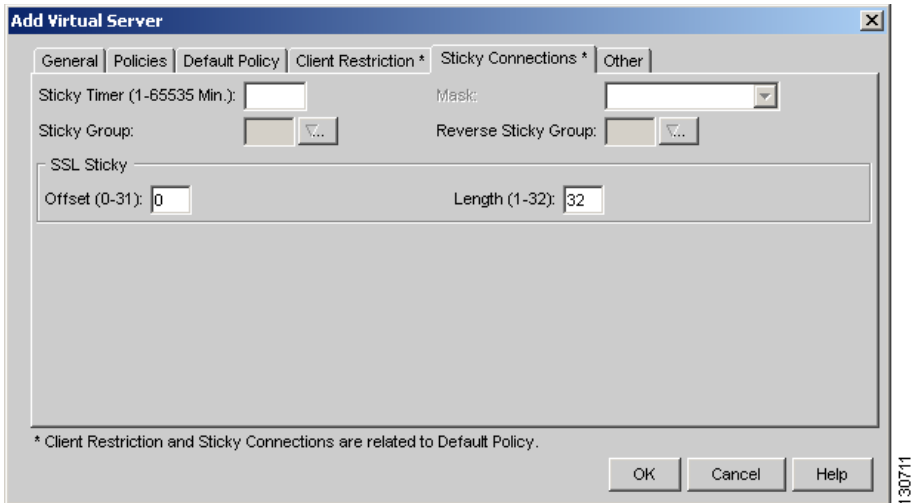
When you click **Add** or **Edit**, the following columns appear:

Column	Description
IP Address	IP Address of the client.
Mask	Specify the type of IP mask. It can be from Class A, Class B, Class C, or Class D masks.  If it is not specified, the default for network mask is 255.255.255.255.
<b>Exclude this Client</b>	Select this check box to exclude traffic from this client.

## Sticky Connections



Sticky connections are connections from a client that conform to an SLB policy. Sticky connections use the same real server for subsequent connections. To ensure that the CVDM-CSM changes its connections to the opposite direction and sends them back to the source, you can configure a reverse sticky group.

Click the **Sticky Connections** tab to add details.

**Figure 2-7 Add Virtual Server > Sticky Connections Dialog Box**

The following information appears:

Column	Description
Sticky Timer	Specifies the period of time (in minutes) that the sticky information is kept.
Mask	From the list, select, Class A, Class B, Class A, and Class D masks.  If it is not specified, the default for network mask is 255.255.255.255.

Column	Description
Sticky Group	<p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Sticky Group</b>—Allows you to select a sticky group from a list.</li> <li>• <b>Create Sticky Group</b>—Allows you to create a sticky group. For more information, see <a href="#">Adding a Sticky Group, page 9-6</a>.</li> <li>• <b>Clear Sticky Group</b>—Allows you to clear the field.</li> </ul>
Reverse Sticky Group	<p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Sticky Group</b>—Allows you to select from a list of sticky groups.</li> <li>• <b>Create Sticky Group</b>—Allows you to create a sticky group. For more information, see <a href="#">Adding a Sticky Group, page 9-6</a>.</li> <li>• <b>Clear Sticky Group</b>—Allows you to clear the field.</li> </ul>
<b>SSL Sticky</b>	You can stick an incoming SSL connection based only on the offset and length values of the SSL ID.
Offset	Enter the offset for the SSL ID.
Length	Enter the length of the SSL ID.

## Other

Click the **Other** tab to configure performance, load, and traffic parameters. You can configure each virtual server with a pending connection timeout to terminate connections quickly if the switch becomes flooded with traffic.

**Figure 2-8** Add Virtual Server > Other Dialog Box

The screenshot shows the 'Add Virtual Server' dialog box with the 'Other' tab selected. The 'Performance/Load Parameters' section contains the following fields:

- Idle Timer (4-65535 Sec.): 3600
- Pending Timeout (1-65535 Sec.): 30
- Parse Length (1-4000 Bytes): 600
- Maximum Connections: (empty field)

The 'URL Hash' section has an unchecked checkbox and two empty text boxes for 'Begin Pattern' and 'End Pattern'. The 'Connection/Traffic Parameters' section has two unchecked checkboxes: 'Enable HTTP Persistence' and 'Enable Unidirectional Traffic'. A note at the bottom reads: '\* Client Restriction and Sticky Connections are related to Default Policy.' Buttons for 'OK', 'Cancel', and 'Help' are located at the bottom right.

The following information appears:

Column	Description
<b>Performance/Load Parameters</b>	
Idle Timer	Enter the idle connection timer duration in seconds.
Pending Timeout	Enter the time (in seconds) to wait before a connection is considered unreachable.
Parse Length	Enter the maximum number of bytes to parse for URLs and cookies.
Maximum Connections	Enter the maximum number of connections to the real server.

<b>Column</b>	<b>Description</b>
URL Hash	<p>Select this check box to enable URL hash load-balancing algorithm.</p> <p>You can enable the Begin Pattern and End Pattern fields only if you select this check box.</p> <p>For more information on URL Hashing, see <a href="#">Configuring URL Hashing, page 4-15</a>.</p>
Begin Pattern	Specify the beginning pattern of the URL to parse.
End Pattern	Specify the ending pattern of the URL to parse.
<b>Connection/Traffic Parameters</b>	
Enable HTTP Persistence	Select this to enable or disable HTTP persistence for connections on the virtual server.
Enable Unidirectional Traffic	Select this to enable unidirectional traffic.





## Managing VLANs

---

Client-side or a server-side VLAN terminology logically distinguishes the VLANs facing the client-side and the VLANs connecting to the servers or destination devices. However, CVDM-CSM client and server VLANs function very similarly.

CVDM-CSM allows you to configure the client-side and server-side VLANs. You can configure up to 7 gateways and 255 alias IP addresses per VLAN.

This section includes the following topics:

- [Viewing a VLAN, page 3-2](#)
- [Adding a VLAN, page 3-4](#)
- [Editing a VLAN, page 3-6](#)
- [Viewing VLAN Clients, page 3-7](#)
- [Viewing a VLAN Server, page 3-8](#)

# Viewing a VLAN

Figure 3-1 VLAN Page

The screenshot shows the CiscoView Device Manager interface for CSM: Slot 6 - 10.77.241.55. The 'Setup' menu is active, and the 'VLANs' section is selected. The 'VLANs' table lists various VLANs with their IDs, types, IP addresses, masks, aliases, gateways, and static routes. The 'Details' section for VLAN 2 shows its type as 'Client' and provides fields for IP address, mask, aliases, gateways, and static routes.

VLAN ID	Type	IP Address/Mask	Aliases/Mask	Gateways	Static Routes
2	Client				0
4	Client	4.3.2.1/8			1
7	Client	7.8.9.10/8	7.8.9.11/32	7.8.9.12	0
12	Client	12.13.14.15/24	12.13.14.150/32	12.13.14.200	0
22	Server	5.4.4.5/16			0
23	Client	6.2.12.1/8			0
24	Server				0
29	Server				0
45	Client	77.66.55.44/24			0
46	Server	77.66.55.44/24			0
54	Client	192.3.4.5/24			0
55	Server				0
64	Client	10.77.241.34/29		10.77.241.33	1
73	Server				0

Details for VLAN 2:

- VLAN ID: 2
- Type: Client
- IP Address: [Field]
- Mask: [Field]
- Aliases: [Field]
- Gateways: [Field]
- Static Routes: [Table with columns: Destination IP, Mask, Next Hop]

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **VLANs** in the Setup pane.



The VLAN table appears, displaying the following columns.

Column	Description
VLAN ID	ID of the client or server VLAN.
Type	Specifies if the VLAN is of client or server type.
IP Address/Mask	IP address or mask of the VLAN.
Aliases/Mask	Alias IP address or mask. You can assign multiple IP addresses to the VLAN.
Gateways	IP address of the gateway.
Static Routes	Static Route of the VLAN.

**Step 3** When you select any row, the configuration details of the corresponding VLAN appears, displaying the following columns:

Column	Description
VLAN ID	ID of the client or server VLAN.
IP Address	IP Address of the VLAN.
Type	Specifies if the VLAN is of client or server type.
Mask	Mask of the VLAN.
Aliases	Alias IP address.
Gateways	IP address of the gateway.
<b>Static Routes</b>	
Destination IP	The IP address of the destination.
Mask	The mask address of the VLAN.
Next Hop	The next hop address.

From this dialog box, you can do the following:

- Click **Add** to add a VLAN. For more information, see [Adding a VLAN, page 3-4](#).
- Click **Edit** to edit a VLAN. For more information, see [Editing a VLAN, page 3-6](#).
- Select a row and click **Delete** to delete a VLAN.

## Adding a VLAN

---

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **VLANs** from the Setup pane.
- Step 3** Select **VLANs** from the object selector.
- Step 4** Click **Add**. The Add VLAN dialog box appears, displaying the following columns.

GUI Element	Description
VLAN ID field	Enter the ID of the client or server VLAN.
Type list	Specify, from the list, if the VLAN is of client or server type.
IP Address field	Enter the IP Address of the VLAN.
Mask field	Enter the subnet mask of the VLAN.
<b>Aliases and Gateways tab</b>	
<b>Aliases pane</b>	
IP Address field	Alias IP addresses of the VLAN.
<b>Gateways pane</b>	
IP Address field	IP address of the gateway.
<b>Static Routes pane</b>	
Destination IP address field	Enter the IP address of the destination.
Mask field	Enter the mask address of the destination IP address.
Next Hop field	Enter the next hop IP address.

From this dialog box, you can do the following:

- Click **Add** under aliases to add an alias IP address.
- Select an alias IP address and click **Delete** to delete it.
- Click **Add** under gateways to add a gateway.
- Select an alias IP address and click **Delete** to delete it.

## Editing a VLAN

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **VLANs** from the Setup pane.
- Step 3** Select **VLANs** from the object selector.
- Step 4** From the table, select the VLAN that you want to modify and click **Edit**.  
The Edit VLAN dialog box appears, displaying the following columns.

GUI Element	Description
VLAN ID field	ID of the client or server VLAN.
Type list	Specifies if the VLAN is of client or server type.
IP Address field	Enter the IP Address of the VLAN.
Mask field	Enter the subnet mask of the VLAN.
<b>Aliases and Gateways tab</b>	
<b>Aliases pane</b>	
IP Address field	Alias IP addresses of the VLAN.
<b>Gateways pane</b>	
IP Address field	IP address of the gateway.
<b>Static Routes pane</b>	
Destination IP address field	Enter the IP address of the destination.
Mask field	Enter the mask address of the destination IP address.
Next Hop field	Enter the next hop IP address.

From this dialog box, you can do the following:

- Click **Add** under aliases to add an alias IP address.
- Select an alias IP address and click **Delete** to delete it.

- Click **Add** under gateways to add a gateway.
- Select an alias IP address and click **Delete** to delete it.

## Viewing VLAN Clients

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **VLANs** in the Setup pane.
- Step 3** Select **Client** from the object selector. The Client table appears, displaying the following columns:

Field	Description
VLAN ID	The ID of the client VLAN.
IP Address/Mask	IP address and mask of VLAN.
Alias IP Address/Mask	Alias IP address or mask. You can assign multiple IP addresses to the VLAN.
Gateways	IP address of the gateway.
Static Routes	Static route of the VLAN.

From this dialog box, you can do the following:

- Click **Add** to add a client VLAN. For more information, see [Adding a VLAN, page 3-4](#).
- Click **Edit** to edit a client VLAN. For more information, see [Editing a VLAN, page 3-6](#).
- Select a row and click **Delete** to delete a client VLAN.

## Viewing a VLAN Server

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **VLAN** in the Setup pane.
- Step 3** Select **Server** from the object selector.

The following fields appear:

Field	Description
VLAN ID	The ID of the server VLAN.
IP Address/Mask	IP address and mask of VLAN.
Alias IP Address/Mask	Alias IP address or mask. You can assign multiple IP addresses to the VLAN.
Gateways	IP address of the <b>gateway</b> .
Static Routes	Static route of the <b>VLAN</b> .

From this dialog box, you can access functions to do the following:

- Click **Add** to add a server VLAN. For more **information**, see [Adding a VLAN, page 3-4](#).
- Click **Edit** to edit a server VLAN. For more information, see [Editing a VLAN, page 3-6](#).
- Select a row and click **Delete** to delete a server VLAN.



## Managing Virtual Servers

---

Virtual servers represent groups of real servers and are associated with real server farms through policies. CVDM-CSM displays the details of the configured virtual servers and allows you to create or delete virtual servers, associate them with server farms and policies, enable specific client IP addresses to connect to the virtual servers, and turn the virtual services on or off.

To configure a virtual server, you set its attributes by specifying the default server farm (default policy) and associate other server farms through a list of policies. The default policy is used if a request does not match any SLB policies or if there are no policies associated with the virtual server. Before you associate a server farm with the virtual server, you must configure the server farm.

Server farms that function as virtual servers can improve scalability and availability of services for your network. You can add new servers or remove failed servers at any time without affecting the virtual server's availability. A server farm must be configured before associating it to the virtual server.

Instead of using a virtual server on the CVDM-CSM for the server-side connection, you can now configure it to forward packets directly to a real server. To do this, the CVDM-CSM must have the virtual server configured for predictor-forward. Additionally, for all real servers for which direct forwarding of connections is to be done, each real server must be assigned to a server farm that is not associated with any virtual server.

To enable partial server farm failover, you can now define the threshold number of real servers to be out of service for the backup server farm to take over. You can also define the number of real servers to be in service for the server farm to be considered active.

From the Virtual Server window, you can do the following:

- Create and delete virtual servers.
- Enable and disable virtual service.
- Associate virtual servers with a server farm or policy.
- Restrict client access to virtual servers.
- Configure performance, load, connection, and traffic parameters.
- Configure sticky connections.
- Enable partial server farm failover.

This section includes the following topics:

- [Viewing Virtual Servers, page 4-3](#)
- [Viewing an Individual Virtual Server, page 4-26](#)
- [Viewing a Policy, page 4-34](#)
- [Viewing a Default Policy, page 4-36](#)
- [Adding a Virtual Server, page 4-5](#)
- [Editing a Virtual Server, page 4-17](#)



# Viewing Virtual Servers

Figure 4-1 Virtual Servers Page

The screenshot shows the CiscoView Device Manager interface for a Cisco Content Switching Module (CSM) Slot 6. The main window displays the 'Virtual Servers' page, which includes a tree view on the left and a table of virtual server details on the right.

Name	Virtual IP	VLAN ID	Protocol	Port	Server Farm	Backup Farm	Admin Status	Oper Status
012345678912345							Out of Service	Out of Service
1233444	1.1.1.11/32	54	ANY		CV		Inservice	Operational
152-6-VS	1.1.1.11/32	23	ANY				Out of Service	Out of Service
152-BATS-005	3.3.3.13/32	23	ANY				Out of Service	Out of Service
152-BATS006							Out of Service	Out of Service
152-V-153	3.3.3.13/32	123	ANY		152-V-153		Inservice	Out of Service
152-V-CHECK	3.3.3.13/32		ANY				Out of Service	Out of Service
ACCEPT-NAMED	1.1.1.11/32	23	ANY		CV		Out of Service	Out of Service
ADDCHECK	10.10.10.2/32		ANY				Out of Service	Out of Service
ASDASD							Out of Service	Out of Service
ASDASDASD							Out of Service	Out of Service
AUTO-VSERVER1	1.1.1.11/32		ANY				Out of Service	Out of Service
CNTT	3.3.3.13/32		ANY				Out of Service	Out of Service
DFDSF	6.2.96.1/32	111	ANY				Out of Service	Out of Service
GWVLAN	3.3.3.13/32	113	ANY		CV		Out of Service	Out of Service
NAME	3.3.3.13/32	22	TCP	21	SF-NEW1		Inservice	Out of Service
NH	3.3.3.13/32		ANY				Out of Service	Out of Service
NRALLOW	1.1.1.11/32		ANY				Out of Service	Out of Service
NREI	11.211.34.2/32		ANY				Out of Service	Out of Service
QWERTY21	1.1.1.11/32	23	ANY				Inservice	Out of Service
S	4.2.2.0/24		ANY				Inservice	Out of Service
SDFSF							Out of Service	Out of Service
SECURE-WEB	10.77.241.31/32	4094	TCP	0	SECURE-SF		Inservice	Operational
TEST							Out of Service	Out of Service
TEST-IP	8.4.3.2/32		TCP	21			Inservice	Out of Service
TEST-SSL	4.2.1.1/32		ANY				Inservice	Out of Service
TEST-URL	22.2.2.2/32		ANY				Inservice	Out of Service

You can view all virtual servers that exist on a device.

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Virtual Servers** under **Services Dashboard**.

Or

- Click **Setup** from the task bar and click **Virtual Servers** in the Setup pane.

The following virtual server details appear in a table:

Columns	Description
Name	Name of the virtual server.
Virtual IP Address	IP address of the virtual server.
VLAN ID	Specify a VLAN for incoming traffic from the list. <ul style="list-style-type: none"> <li>If it is <b>All</b>, traffic from all VLANs is enabled.</li> <li>If it is <b>Local</b>, CSM-S directly forwards the packets to the real server.</li> </ul>
Protocol	Specifies the load-balancing protocol used for virtual server traffic. You can choose from the following, or enter a number from 1 to 255. <ul style="list-style-type: none"> <li>TCP</li> <li>UDP</li> <li>ANY</li> </ul>
Port	TCP/UDP port number used by the protocol.
Server Farm	Name of the default server farm associated to the real server.
Backup Farm	Name of the backup server farm associated to the real server.
Admin Status	Lets you know the administrative status of the virtual server.
Operational Status	Lets you know the operational status of the virtual server.

You can group the virtual servers based on various common parameters.

To group the virtual servers, click  on top of the object selector; then select one of the following options from the list:

- All
- Group by Protocol
- Group by Admin Status

- Group by Policies

From the Virtual Servers dialog box, you can do the following:

- Click **Add** to add a virtual server. For more information, see [Adding a Virtual Server, page 4-5](#).
- Click **Edit** to edit a virtual server. For more information, see [Editing a Virtual Server, page 4-17](#).
- Select a row and click **Delete** to delete a virtual server.
- Click **Set Admin Status** to instantly set the status of the virtual server.

## Adding a Virtual Server

You can add a virtual server by giving the required configuration details.

- 
- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Virtual Servers** under Services Dashboard.
- Or
- Click **Setup** from the task bar and click **Virtual Servers** in the Setup pane.
- Step 2** Click **Add**. The Add Virtual Server dialog box appears.
- Step 3** Click one of the following tabs, then proceed to the corresponding section in this guide for configuration information:
- [General, page 4-6](#)
  - [Policies, page 4-8](#)
  - [Default Policy, page 4-9](#)
  - [Client Restriction, page 4-11](#)
  - [Sticky Connections, page 4-12](#)
  - [Other, page 4-14](#)
-

## General

Click the **General** tab to configure the basic configuration details.

**Figure 4-2** Add Virtual Server > General Dialog Box

**Add Virtual Server**

General | Policies | Default Policy | Client Restriction \* | Sticky Connections \* | Other

Name:  VLAN ID: All

Status: Out of Service

Virtual IP Address

IP Address:  Protocol (1-255): ANY

Mask: 255.255.255.255 Port (0-65535): ANY

Service Type:

Advertise

Advertise Virtual IP  Advertise only if reals are active

\* Client Restriction and Sticky Connections are related to Default Policy.

OK Cancel Help

The following columns appear:

Columns	Action/Description
Name	Enter the name of the virtual server.
Status	From the list, select the status of the virtual server.
VLAN ID	From the list, specify a VLAN for incoming traffic. <ul style="list-style-type: none"> <li>If you choose <b>All</b>, traffic from all VLANs is enabled.</li> <li>If you choose <b>Local</b>, CSM-S directly forwards the packets to the real server.</li> </ul>
<b>Virtual IP Address</b>	
IP Address	Enter the IP Address of the virtual server.

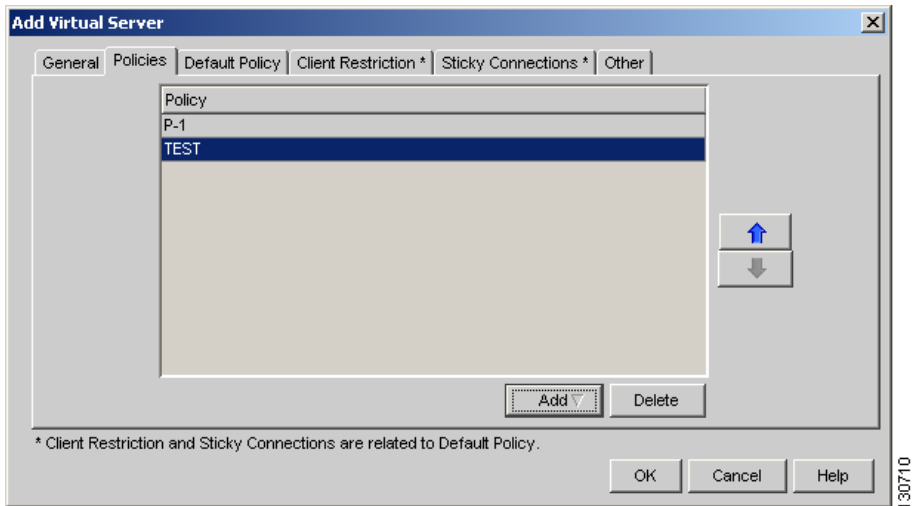
130708

<b>Columns</b>	<b>Action/Description</b>
Protocol	<p>From the list, select the load-balancing protocol for virtual server traffic.</p> <p>You can choose from Any, TCP, or UDP, or enter a number from 1 to 255. This field is enabled only when you enter the IP address.</p>
Port	<p>From the list, select the port number. This field is enabled only when you choose TCP or UDP.</p>
Service Type	<p>From the list, select the service type. You can combine connections associated with the same service. This allows all related connections from a client to use a particular real server.</p> <p>The options depend on the protocol you choose. You can choose from the following:</p> <ul style="list-style-type: none"> <li>• FTP—Combines connections to FTP port 21.</li> <li>• RTSP—Combines connections to Real Time Streaming Protocol (RTSP) TCP port 554.</li> <li>• Termination—Enables TCP termination for DoS attack protection.</li> <li>• Per-packet—Load balances each packet independently. This option is for non-TCP only.</li> </ul>
Mask	<p>Specify the virtual IP mask.</p>
<b>Advertise</b>	
Advertise Virtual IP	<p>Select this to advertise the IP address of the virtual server as the host route.</p>
Advertise only if reals are active	<p>Select this to advertise only if real servers are active.</p>

## Policies

Click the **Policies** tab to add or delete policies

**Figure 4-3** Add Virtual Server > Policies Dialog Box



You have the following options:

- Click **Add** and select one of the following to associate policies to the virtual server:
  - **Select Policy**—Allows you to select a policy from a list.
  - **Create Policy**—Allows you to create a policy. For more information, see [Adding Policies, page 7-5](#).
- Select a policy from the table and click **Delete** to remove policies from the virtual server.
- Click the Up button to move the policies up in the list.
- Click the Down button to move the policies down in the list.

**Note**

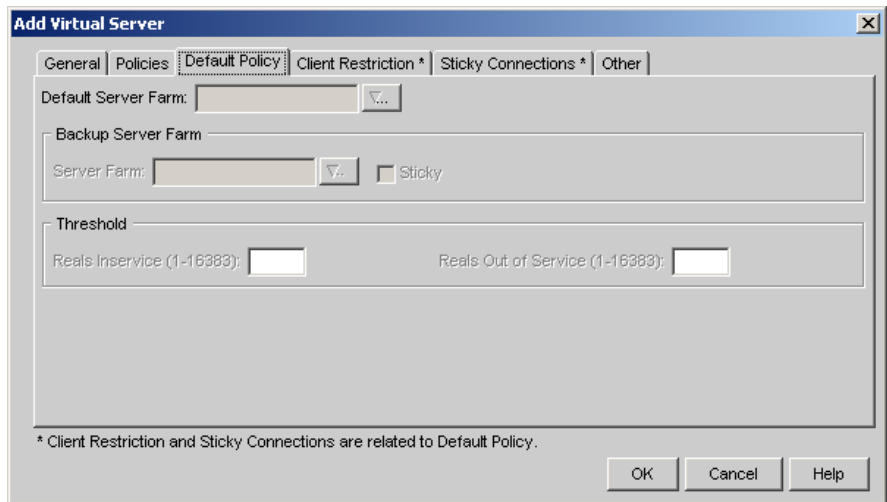
Be sure to put the policies in the right order. Traffic is routed based on the order of the policies.

## Default Policy

Click the **Default Policy** tab to configure a virtual server to operate at Level 4. You can specify the server farm (default policy) and backup server farms. You can configure a backup server farm to operate when a server farm is out of service.

To enable partial server farm failover, you can now define the threshold number of real servers to be out of service for the backup server farm to take over. You can also define the number of real servers to be in service for the server farm to be considered active.

**Figure 4-4** Add Virtual Server > Default Policy Dialog Box



The following details appear when you click this tab:

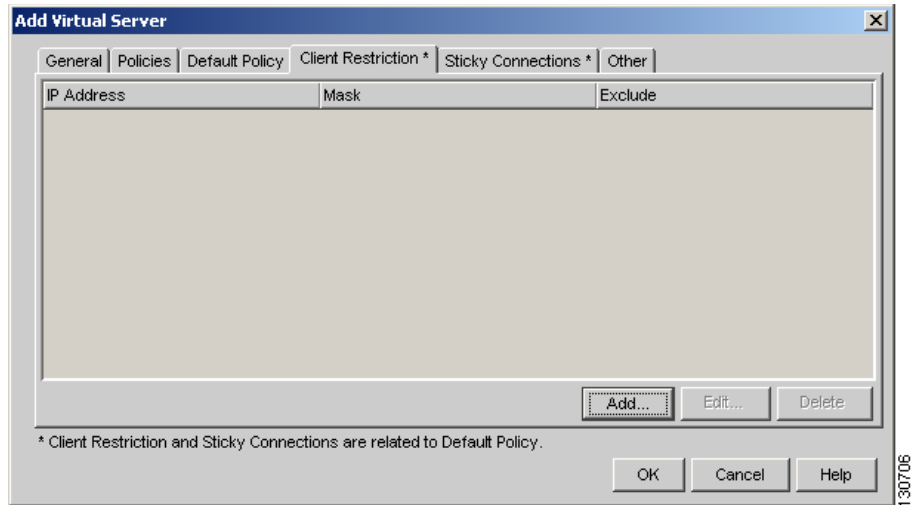
Column	Action/Description
Default Server Farm	<p>Click <input type="button" value="v..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Server Farm</b>—Allows you to select one from a list of server farms.</li> <li>• <b>Create Server Farm</b>—Allows you to create a server farm. For more information, see <a href="#">Adding Server Farms, page 5-5</a>.</li> <li>• <b>Clear Server Farm</b>—Allows you to clear the field.</li> </ul>
<b>Backup Server Farm</b>	
Server Farm	<p>Click <input type="button" value="v..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Server Farm</b>—Allows you to select a server farm from a list.</li> <li>• <b>Create Server Farm</b>—Allows you to create a server farm. For more information, see <a href="#">Adding Server Farms, page 5-5</a>.</li> <li>• <b>Clear Server Farm</b>—Allows you to clear the field.</li> </ul>
Sticky	<p>Select this check box to enable the sticky property.</p> <p>This ensures that multiple connections from the same client, that match the same SLB policy stick (or attach) to the same real server.</p>
<b>Threshold</b>	
Reals Inservice	The number of real servers to be in service for the server farm to be active.
Reals Out of Service	The number of real servers to be out of service for the backup server farm to take over.



## Client Restriction

Click the **Client Restriction** tab to add details of the clients restricted to use the virtual server.

**Figure 4-5** Add Virtual Server > Client Restriction Dialog Box



You have the following options:

- Click **Add** to create client restrictions for multiple clients.
- Click **Edit** to edit the client restrictions for multiple clients.
- Select a row in the table and click **Delete** to delete the selected client.

When you click **Add** or **Edit**, the following columns appear:

Column	Description
IP Address	IP address of the client.

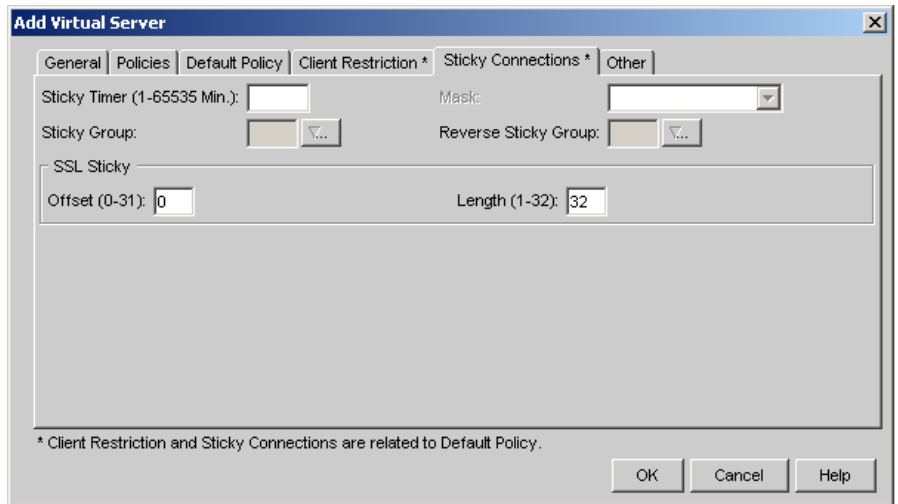
Mask	Specify the type of IP mask. It can be from Class A, Class B, Class C, or Class D masks.  If it is not specified, the default for network mask is 255.255.255.255.
Exclude this Client	Select this check box to exclude traffic from this client.

## Sticky Connections

Sticky connections are connections from a client that conform to an SLB policy. Sticky connections use the same real server for subsequent connections. To ensure that the CVDM-CSM changes its connections to the opposite direction and sends them back to the source, you can configure a reverse sticky group.

Click the **Sticky Connections** tab to add details.

**Figure 4-6** Add Virtual Server > Sticky Connections Dialog Box



The following details appear:

Column	Description
Sticky Timer	Specifies the period of time (in minutes) that the sticky information is kept.
Mask	From the list, select, Class A, Class B, Class A, and Class D masks.  If it is not specified, the default for network mask is 255.255.255.255.
Sticky Group	Click <input type="button" value="v..."/> and select one of the following: <ul style="list-style-type: none"> <li>• <b>Select Sticky Group</b>—Allows you to select a sticky group from a list.</li> <li>• <b>Create Sticky Group</b>—Allows you to create a sticky group. For more information, see <a href="#">Adding a Sticky Group, page 9-6</a>.</li> <li>• <b>Clear Sticky Group</b>—Allows you to clear the field.</li> </ul>
Reverse Sticky Group	Click <input type="button" value="v..."/> and select one of the following: <ul style="list-style-type: none"> <li>• <b>Select Sticky Group</b>—Allows you to select from a list of sticky groups.</li> <li>• <b>Create Sticky Group</b>—Allows you to create a sticky group. For more information, see <a href="#">Adding a Sticky Group, page 9-6</a>.</li> <li>• <b>Clear Sticky Group</b>—Allows you to clear the field.</li> </ul>
<b>SSL Sticky</b>	You can stick an incoming SSL connection based only on the offset and length values of the SSL ID.
Offset	Enter the offset for the SSL ID.
Length	Enter the length of the SSL ID.

## Other

Click the **Other** tab to configure performance, load, and traffic parameters. You can configure each virtual server with a pending connection timeout to terminate connections quickly if the switch becomes flooded with traffic.

**Figure 4-7** Add Virtual Server > Other Dialog Box

The screenshot shows the 'Add Virtual Server' dialog box with the 'Other' tab selected. The 'Performance/Load Parameters' section includes:
 

- Idle Timer (4-65535 Sec.): 3600
- Pending Timeout (1-65535 Sec.): 30
- Parse Length (1-4000 Bytes): 600
- Maximum Connections: (empty field)

 The 'URL Hash' section has an unchecked checkbox and two empty text boxes for 'Begin Pattern' and 'End Pattern'. The 'Connection/Traffic Parameters' section has two unchecked checkboxes: 'Enable HTTP Persistence' and 'Enable Unidirectional Traffic'. A note at the bottom reads: '\* Client Restriction and Sticky Connections are related to Default Policy.' Buttons for 'OK', 'Cancel', and 'Help' are located at the bottom right.

The following details appear:

Column	Description
<b>Performance/Load Parameters</b>	
Idle Timer	Enter the idle connection timer duration (in seconds). This is the time (in seconds) that connection information is maintained, in the absence of packet activity, for a connection
Pending Timeout	Enter the time (in seconds) to wait before a connection is considered unreachable.
Parse Length	Enter the maximum number of bytes to parse for URLs and cookies.

Column	Description
Maximum Connections	Enter the maximum number of active connections on the real server.
URL Hash	Select this check box to enable URL hash load-balancing algorithm.  You can enable the Begin Pattern and End Pattern fields only if you select this check box.  For more information on URL Hashing, see <a href="#">Configuring URL Hashing, page 4-15</a> .
Begin Pattern	Specify the beginning pattern of the URL to parse.
End Pattern	Specify the ending pattern of the URL to parse.
<b>Connection/Traffic Parameters</b>	
Enable HTTP Persistence	Select this to enable or disable HTTP persistence for connections on the virtual server.
Enable Unidirectional Traffic	Select this to enable unidirectional traffic.

## Configuring URL Hashing

When you choose a server farm for a connection, you can select a specific real server in that server farm. You can choose least connections, round robin, or URL hashing to select a real server.

URL hashing is a load-balancing predictor for Layer 7 connections. You can configure URL hashing on CVDM-CSM on a server farm-by-server farm basis. CVDM-CSM chooses the real server by using a hash value based on a URL. This hash value may be computed on the entire URL or on a portion of it.

You can specify the beginning and ending patterns in the URL to select only a portion of the URL for hashing. Hashing occurs from the start of the specified beginning pattern through the specified ending pattern.

For example, in the following URL, if the beginning pattern is `c&k=`, and the ending pattern is `&`, only the substring `c&k=c` is hashed:

`http://quote.mypage.com/q?s=cscoc&d=c&k=c1&t=2y&a=v&p=s&l=on\`



---

**Note** Beginning and ending patterns are restricted to fixed constant strings. You cannot specify general regular expressions as patterns. If you do not specify the beginning pattern, hashing begins at the beginning of the URL. If you do not specify the ending pattern, hashing ends at the end of the URL.

---

# Editing a Virtual Server

You can edit virtual server connection details and the list of policies for the selected virtual servers.

- 
- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Virtual Servers** under Services Dashboard.
- Or
- Click **Setup** from the task bar and click **Virtual Servers** in the Setup pane.
- Step 2** Select a row from the table. Click **Edit**. The Edit Virtual Server dialog box appears.
- Step 3** Click one of the following tabs, then proceed to the corresponding section for configuration information:
- [General, page 4-18](#)
  - [Policies, page 4-20](#)
  - [Default Policy, page 4-20](#)
  - [Client Restriction, page 4-22](#)
  - [Sticky Connections, page 4-23](#)
  - [Other, page 4-24](#)
-

## General

Click the **General** tab to edit basic configuration details.

The following details appear:

Column	Action/Description
Name	The name of the virtual server.
Status	From the list, select the status of the virtual server.
VLAN ID	From the list, specify a VLAN for incoming traffic. <ul style="list-style-type: none"> <li>If you choose <b>All</b>, traffic from all VLANs is enabled.</li> <li>If you choose <b>Local</b>, CSM-S directly forwards the packets to the real server.</li> </ul>
<b>Virtual IP Address</b>	
IP Address	Enter the IP address of the virtual server.
Protocol	From the list, select the load-balancing protocol for virtual server traffic. You can choose from Any, TCP, or UDP, or enter a number from 1 to 255.
Port	From the list, select the port number. This field is enabled only when you choose TCP or UDP.



Column	Action/Description
Service Type	<p>From the list, select the service type. You can combine connections associated with the same service. This allows all related connections from a client to use a particular real server.</p> <p>The options depend on the protocol you choose. You can choose from the following:</p> <ul style="list-style-type: none"> <li>• FTP—Combines connections to FTP port 21.</li> <li>• RTSP—Combines connections to the Real Time Streaming Protocol (RTSP) TCP port 554.</li> <li>• Termination—Enables TCP termination for DoS attack protection.</li> <li>• Per-packet—Load balances each packet independently. This option is for non-TCP only.</li> </ul>
<b>Advertise</b>	
Advertise Virtual IP	Select this to advertise the IP address of the virtual server as the host route.
Advertise only if reals are active	Select this to advertise only if real servers are active.

## Policies

Click the **Policies** tab to edit policies. You have the following options:

- Click **Add** to associate policies to the virtual server. For more information, see [Adding Policies, page 7-5](#).
- Click **Delete** to remove policies from the virtual server.
- Click the Up button to move the policies up in the list.
- Click the Down button to move the policies down in the list.



---

**Note**

Be sure to put the policies in the right order. Traffic is routed based on the order of the policies.



---

## Default Policy

Click the **Default Policy** tab to configure a virtual server to operate at Level 4. You can specify the server farm (default policy) and backup server farms. You can configure a backup server farm to operate when a server farm is out of service.

To enable partial server farm failover, you can now define the threshold number of real servers to be out of service for the backup server farm to take over. You can also define the number of real servers to be in service for the server farm to be considered active.

The following details appear when you click this tab:

Column	Action/Description
Default Server Farm	Click  and select one of the following: <ul style="list-style-type: none"> <li>• <b>Select Server Farm</b>—Allows you to select a server farms from a list.</li> <li>• <b>Create Server Farm</b>—Allows you to create a server farm. For more information, see <a href="#">Adding Server Farms, page 5-5</a>.</li> <li>• <b>Clear Server Farm</b>—Allows you to clear the field.</li> </ul>
<b>Backup Server Farm</b>	
Server Farm	Click  and select one of the following: <ul style="list-style-type: none"> <li>• <b>Select Server Farm</b>—Allows you to select a server farms from a list.</li> <li>• <b>Create Server Farm</b>—Allows you to create a server farm. For more information, see <a href="#">Adding Server Farms, page 5-5</a>.</li> <li>• <b>Clear Server Farm</b>—Allows you to clear the field.</li> </ul>
Sticky	Select this check box to enable the sticky property.  This ensures that multiple connections from the same client that match the same SLB policy stick (or attach) to the same real server.
<b>Threshold</b>	
Reals Inservice	The number of real servers to be in service for the server farm to be active.
Reals out of service	The number of real servers to be out of service for the backup server farm to take over.

## Client Restriction

Click the **Client Restriction** tab to add details of the clients restricted to use the virtual server. You have the following options:

- Click **Add** to create client restrictions for multiple clients.
- Click **Edit** to edit the client restrictions for multiple clients.
- Select a row in the table and click **Delete** to delete the selected client restriction.

When you click **Add** or **Edit**, the following details appear:

Field	Description
IP Address	IP Address of the client.
Mask	Specify the type of IP mask. It can be from Class A, Class B, Class C, or Class D masks.  If it is not specified, the default for network mask is 255.255.255.255.
<b>Exclude this Client</b>	Select this check box to exclude traffic from this client.

## Sticky Connections

Sticky connections are connections from a client that conform to an SLB policy. Sticky connections use the same real server for subsequent connections. To ensure that the CVDM-CSM changes its connections to the opposite direction and sends them back to the source, you can configure a reverse sticky group.

Click the **Sticky Connections** tab to add details of the sticky connections.

The following details appear:

Column	Description
Sticky Timer	Specifies the period of time (in minutes) that the sticky information is kept.
Mask	From the list, select, Class A, Class B, Class A and Class D masks.  If it is not specified, the default for network mask is 255.255.255.255.
Sticky Group	Click <input type="text" value="v..."/> and select one of the following: <ul style="list-style-type: none"> <li>• <b>Select Sticky Group</b>—Allows you to select a sticky group from a list.</li> <li>• <b>Create Sticky Group</b>—Allows you to create a sticky group. For more information, see <a href="#">Adding a Sticky Group, page 9-6</a>.</li> <li>• <b>Clear Sticky Group</b>—Allows you to clear the field.</li> </ul>
Reverse Sticky Group	Click <input type="text" value="v..."/> and select one of the following: <ul style="list-style-type: none"> <li>• <b>Select Sticky Group</b>—Allows you to select a sticky group from a list.</li> <li>• <b>Create Sticky Group</b>—Allows you to create a sticky group. For more information, see <a href="#">Adding a Sticky Group, page 9-6</a>.</li> <li>• <b>Clear Sticky Group</b>—Allows you to clear the field.</li> </ul>

Column	Description
SSL Sticky	You can stick an incoming SSL connection based only on the offset and length values of the SSL ID.
Offset	Enter the offset for the SSL ID.
Length	Enter the length of the SSL ID.

## Other

Click the **Other** tab to edit details of performance, load, and traffic parameters. You can configure each virtual server with a pending connection timeout to terminate connections quickly if the switch becomes flooded with traffic.

The following details appear:

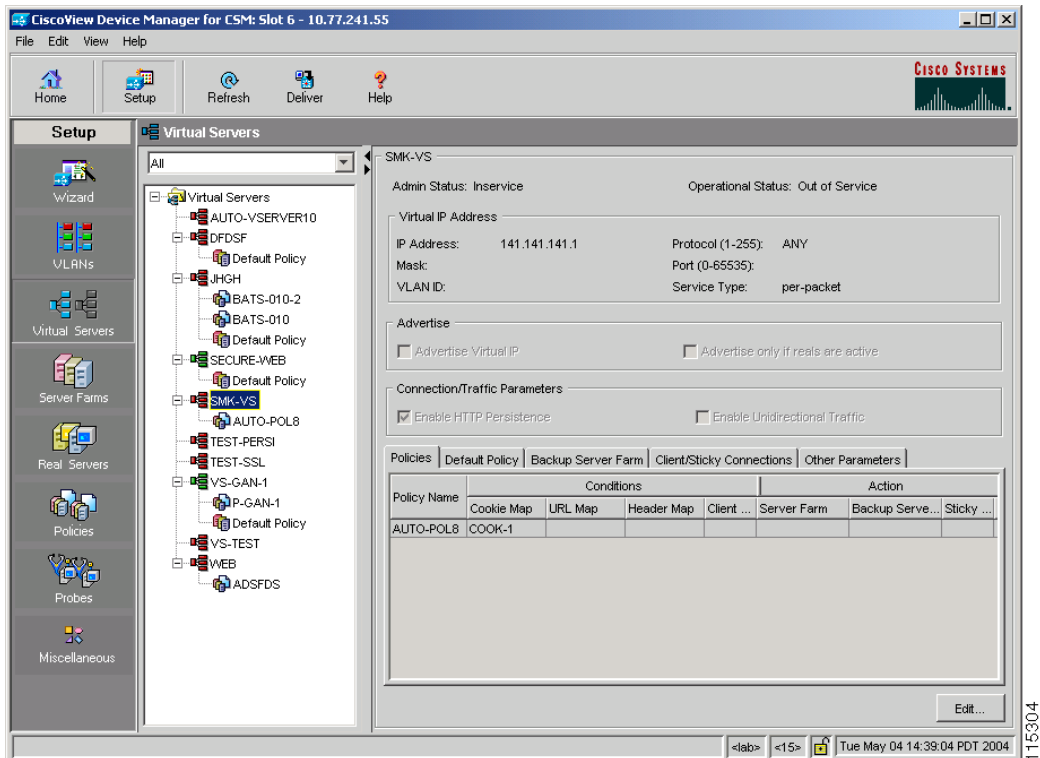
Column	Description
<b>Performance/Load Parameters</b>	
Idle Timer	Enter the idle connection timer duration (in seconds). This is the time that connection information is maintained, in the absence of packet activity, for a connection
Pending Timeout	Enter the time (in seconds) to wait before a connection is considered unreachable.
Parse Length	Enter the maximum number of bytes to parse for URLs and cookies.
Maximum Connections	Enter the maximum number of active connections on the real server.
URL Hash	Select this check box to enable URL hash load-balancing algorithm.  You can enable the Begin Pattern and End Pattern fields only if you select this check box.  For more information on URL Hashing, see <a href="#">Configuring URL Hashing, page 4-15</a> .
Begin Pattern	Specify the beginning pattern of the URL to parse.

<b>Column</b>	<b>Description</b>
End Pattern	Specify the ending pattern of the URL to parse.
<b>Connection/Traffic Parameters</b>	
Enable HTTP Persistence	Select this to enable or disable HTTP persistence for connections on the virtual server.
Enable Unidirectional Traffic	Select this to enable unidirectional traffic.

# Viewing an Individual Virtual Server

You can view the configuration details of each virtual server when you click any of them. When a virtual server is out of service it turns red, and when it is in service it turns green.

Figure 4-8 Virtual Servers - Individual Virtual Server Page



**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Virtual Servers** under Services Dashboard.

Or



- Click **Setup** from the task bar and click **Virtual Servers** in the Setup pane.
- Step 2** Click a virtual server to view its configuration details. The virtual server table appears, displaying the following columns.

Column	Description
Admin Status	Lets you know the administrative status of the real server.
Operational Status	Lets you know the operational status of the virtual server.
Virtual IP Address	IP address of the virtual server.
Protocol	From the list, select the load-balancing protocol for virtual server traffic. You can choose from Any, TCP, or UDP, or enter a number from 1 to 255.
Mask	Type of IP mask. It can be a Class A, Class B, Class C, or Class D mask.  If it is not specified, the default for network mask is 255.255.255.255.
Port	Port allotted for the traffic. This field is enabled only when you choose TCP or UDP.
VLAN ID	Specifies the VLAN for incoming traffic. <ul style="list-style-type: none"> <li>• If it is <b>All</b>, traffic from all VLANs is enabled.</li> <li>• If it is <b>Local</b>, CSM-S directly forwards the packets to the real server.</li> </ul>

Column	Description
Service Type	<p>Specifies the service type. You can combine connections associated with the same service. This allows all related connections from a client to use a particular real server.</p> <p>The options depend on the protocol you choose. You can choose from the following:</p> <ul style="list-style-type: none"> <li>• FTP—Combines connections to FTP port 21.</li> <li>• RTSP—Combines connections to the Real Time Streaming Protocol (RTSP) TCP port 554.</li> <li>• Termination—Enables TCP termination for DoS attack protection.</li> <li>• Per-packet—Load balances each packet independently. This option is for non-TCP only.</li> </ul>
<b>Advertise</b>	
Advertise Virtual IP	Select this to advertise the IP address of the virtual server as the host route.
Advertise only if reals are active	Select this to advertise only if real servers are active.
Enable HTTP Persistence	Select this to enable or disable HTTP persistence for connections in the virtual server.
Enable Unidirectional Traffic	Select this to enable unidirectional traffic.

**Step 3** Click one of the following tabs, then proceed to the corresponding section for configuration information:

- [Policies, page 4-29](#)
- [Default Policy, page 4-30](#)
- [Backup Server Farm, page 4-31](#)
- [Client and Sticky Connections, page 4-32](#)
- [Other Parameters, page 4-33](#)

## Policies

Click the **Policies** tab to view the details of various policies.

The following details appear:

Field	Description
Policy Name	Policy associated with a virtual server.
<b>Conditions</b>	
Cookie Map	Name of the cookie map associated with a policy. Only one cookie map can be associated with a policy.
URL Map	Name of the URL map associated with a policy. Only one URL map can be associated with a policy.
Header Map	Name of the Header map associated with a policy. Only one Header map can be associated with a policy.
Client Group	Client group can be either standard access lists names or an ID from 1 to 99. Only one client group can be associated with a given SLB policy.
<b>Action</b>	
<ul style="list-style-type: none"> <li>• Server Farm</li> <li>• Backup Server Farm</li> </ul>	Name of the server farm associated to the real server. You can choose one server farm and/or backup server farm to associate to the policy.
Sticky Group	Number identifying the sticky group to which the virtual server belongs.
Reverse Sticky Group	Number identifying the reverse sticky group to which the virtual server belongs.

## Default Policy

Click the **Default Policy** tab to configure a virtual server to operate at Level 4. You can specify the server farm (default policy) and backup server farms. You can configure a backup server farm to operate when a server farm is out of service.

To enable partial server farm failover, you can now define the threshold number of real servers to be out of service for the backup server farm to take over. You can also define the number of real servers to be in service for the server farm to be considered active.

The following information appears:

Column	Action/Description
<b>Server Farm</b>	
<b>Associated Real Servers</b>	
Real	Real server associated to the Server farms through policies.
Local SSL	Indicates if the real server is the SSL card.
Minimum Connections	Minimum number of connections to the real server.
Maximum Connections	Maximum number of connections to the real server.
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Lets you know the status of the real server.

## Backup Server Farm

Click the **Backup Server Farm** tab to view the details of the backup server farm.

The following information appears:

Column	Action/Description
<b>Backup Server Farm</b>	
Sticky	Select this check box to enable the sticky property.  This ensures that multiple connections from the same client that conform to an SLB policy stick (or attach) to the same real server.
<b>Associated Real Servers</b>	
Real	Real server associated to the Server farms through policies.
Local SSL	Indicates if the real server is the SSL card.
Minimum Connections	Minimum number of active connections on the real server.
Maximum Connections	Maximum number of active connections on the real server.
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Lets you know the status of the real server.

## Client and Sticky Connections

Sticky connections are connections from a client that conform to an SLB policy. Sticky connections use the same real server for subsequent connections. To ensure that the CVDM-CSM changes its connections to the opposite direction and sends them back to the source, you can configure a reverse sticky group.

Click the **Client/Sticky Connections** tab to view details of the restricted clients and sticky connections. The following information appears:

Column	Description
<b>Client Restriction</b>	
IP Address	IP address of the client to be restricted.
Mask	Specify the type of IP mask. It can be from Class A, Class B, Class C or Class D masks.  If it is not specified, the default for network mask is 255.255.255.255.
Exclude	If this check box is selected, traffic from this client will be excluded.
<b>Sticky Connections</b>	
Sticky Timer	Specifies the period of time (in minutes) that the sticky information is kept.
Mask	Specifies if it is a Class A, Class B, Class A and Class D mask.  If it is not specified, the default for network mask is 255.255.255.255.
Sticky Group	Sticky group associated with the virtual server.
Reverse Sticky	Number identifying the reverse sticky group to which the virtual server belongs.
<b>SSL Sticky</b>	
Offset	You can stick an incoming SSL connection based only on the offset and length values of the SSL ID.  The offset for the SSL ID.
Length	The length of the SSL ID.

## Other Parameters

Click the **Other Parameters** tab to view details of performance, load and traffic related parameters. You can configure each virtual server with a pending connection timeout to terminate connections quickly if the switch becomes flooded with traffic.

You can limit the number of connections going through the CVDM-CSM to a particular virtual server by specifying the maximum and minimum number of connections.

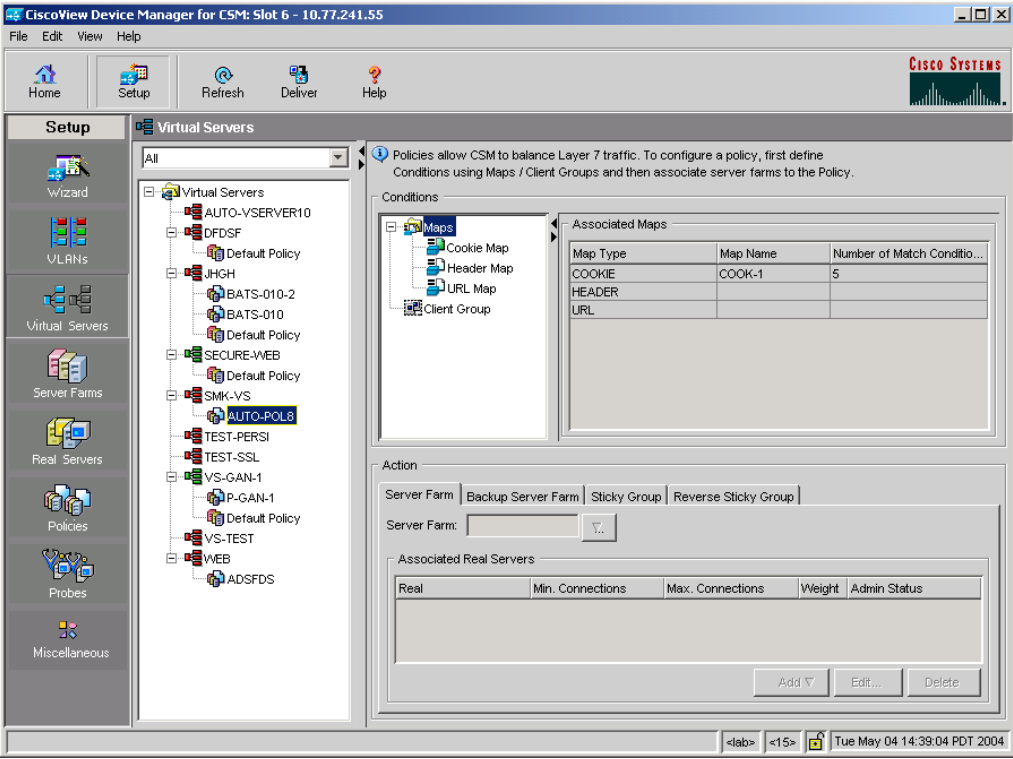
Field	Description
<b>Performance/Load Parameters</b>	
Idle Timer	Enter the idle connection timer duration (in seconds). This is the time that connection information is maintained, in the absence of packet activity, for a connection
Pending Timeout	Enter the time (in seconds) to wait before a connection is considered unreachable.
Parse Length	Enter the maximum number of bytes to parse for URLs and cookies.
Maximum Connections	Enter the maximum number of connections to the real server.
URL Hash	Select this check box to enable URL hash load-balancing algorithm. You can enable the Begin Pattern and End Pattern fields only if you select this check box. For more information on URL Hashing, see <a href="#">Configuring URL Hashing, page 4-15</a> .
Begin Pattern	Specify the beginning pattern of the URL to parse.
End Pattern	Specify the ending pattern of the URL to parse.
<b>Connection/Traffic Parameters</b>	

Field	Description
Enable HTTP Persistence	Select this check box to enable or disable HTTP persistence for connections in the virtual server.
Enable Unidirectional Traffic	Select this check box to enable unidirectional traffic.

# Viewing a Policy

You can view the details of the conditions and actions of the policy associated with each virtual server.

Figure 4-9 Virtual Servers - Policy Page



116305



---

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Virtual Servers** under **Services Dashboard**.

Or

- Click **Setup** from the task bar and click **Virtual Servers** in the Setup pane.

**Step 2** Select the required virtual server and click the policy associated with it.

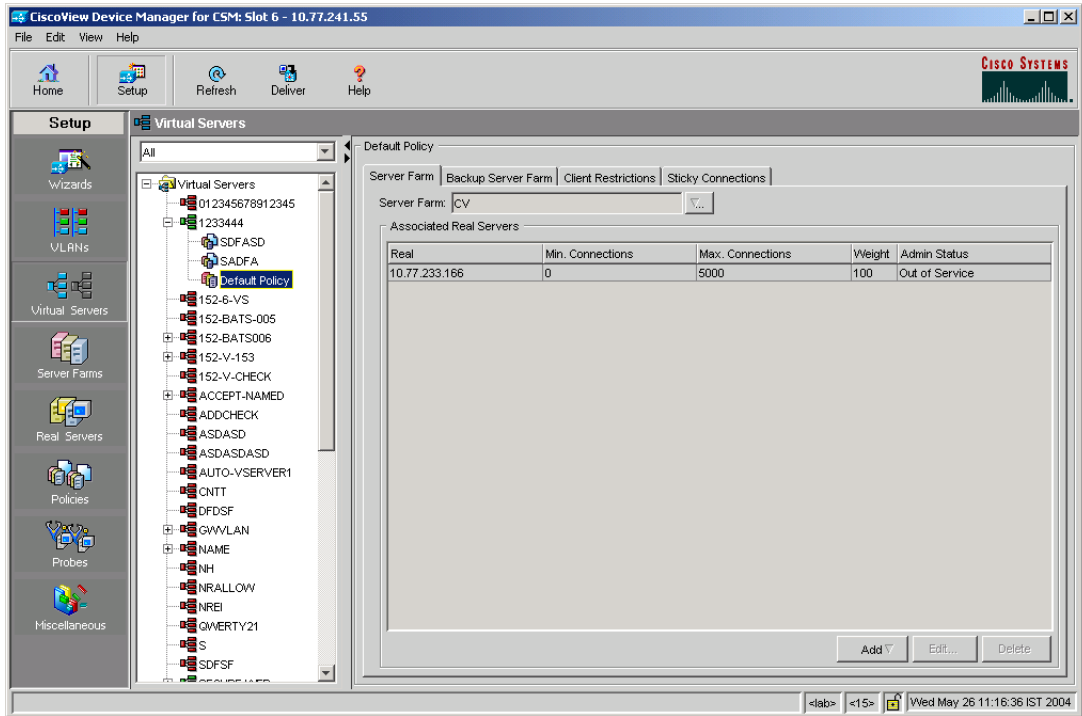
For more information on policies associated with the individual virtual servers see [Viewing Policy Nodes, page 7-16](#).

---

# Viewing a Default Policy

You can view the details of the default policy associated with each virtual server.

**Figure 4-10** Virtual Servers - Default Policy Page



**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Virtual Servers** under **Services Dashboard**.

Or

- Click **Setup** from the task bar and click **Virtual Servers** in the Setup pane.

**Step 2** Select a virtual server and click the default policy associated with it.


**Step 3** Click one of the following tabs, then proceed to the corresponding section for configuration information:

- [Server Farms, page 4-37](#)
- [Backup Server Farms, page 4-39](#)
- [Client Restrictions, page 4-40](#)
- [Sticky Connections, page 4-41](#)

## Server Farms

Click the **Server Farms** tab to view details of all the server farms that are associated to a policy.

The following details appear:

Field	Description
Server Farm	<p>You can create or choose one server farm to associate it to the policy.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Server Farm</b>—Allows you to select a server farm from the list.</li> <li>• <b>Create Server Farm</b>—Allows you to create a server farm. For more information, see <a href="#">Adding Server Farms, page 5-5</a>.</li> </ul>
<b>Associated Real Servers</b>	
Real	Real server associated to the Server farms through the policy.
Local SSL	Indicates if the real server is the SSL card.
Minimum Connections	Minimum number of connections to the real server.
Maximum Connections	Maximum number of connections to the real server.

Field	Description
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Lets you know the status of the real server.

From this dialog box, you can do the following:

- Click **Add** and do one of the following:
  - Click **Select Named Real Server** to create a named real server. For more information, see [Adding a Named Real Server, page 5-23](#).
  - Click **Select Unnamed Real Server** to create an unnamed real server. For more information, see [Adding an Unnamed Real Server, page 5-27](#).
- Select a real server and click **Edit** to edit its configuration values.
- Select a real server and click **Delete** it.

For more information on server farms, see [Viewing Server Farms, page 5-3](#).

## Backup Server Farms

Click the **Backup Server Farms** tab to view details of all the backup server farms that are associated to this policy.

The following information appears:

Column	Description
Backup Server Farm	<p>You can create or choose one backup server farm to associate it to the policy.</p> <p>Click <input type="button" value="v..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Server Farm</b>—Allows you to select a backup server farm from the list.</li> <li>• <b>Create Server Farm</b>—Allows you to create a backup server farm. For more information, see <a href="#">Adding Server Farms, page 5-5</a>.</li> </ul>
Sticky	<p>Select this check box to enable the sticky property.</p> <p>This ensures that multiple connections from the same client that match the same SLB policy stick (or attach) to the same real server.</p>
<b>Associated Real Servers</b>	
Real	Real server associated to the Server farms through the policy.
Local SSL	Indicates if the real server is the SSL card.
Minimum Connections	Minimum number of connections to the real server.
Maximum Connections	Maximum number of connections to the real server.
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Lets you know the status of the real server.

From this dialog box, you can do the following:

- Click **Add** and do one of the following:

- Select **Create Named Real Server** to create a named real server. For more information, see [Adding a Named Real Server, page 5-23](#).
- Select **Create Unnamed Real Server** to create an unnamed real server. For more information, see [Adding an Unnamed Real Server, page 5-27](#).
- Select a real server and click **Edit** to edit the configuration values.
- Select a real server and click **Delete** it.

For more information on server farms, see [Viewing Server Farms, page 5-3](#).

## Client Restrictions

Click the **Client Restrictions** tab to add details of the restricted clients.

The following details appear:

Field	Description
IP Address	IP Address of the client.
Mask	Specify the type of IP mask. It can be from Class A, Class B, Class C, or Class D masks.  If it is not specified, the default for network mask is 255.255.255.255.
Exclude	Select this check box to exclude traffic from this client.

## Sticky Connections

Sticky connections are connections from a client that conform to an SLB policy. Sticky connections use the same real server for subsequent connections. To ensure that the CVDM-CSM changes its connections to the opposite direction and sends them back to the source, you can configure a reverse sticky group.

Click the **Sticky Connections** tab to add details of the sticky connections.

The following details appear:

Field	Description
Sticky Timer	Specifies the duration of time (in minutes) that the sticky information is kept.
Mask	From the list, select Class A, Class B, Class A, and Class D masks. If it is not specified, the default for network mask is 255.255.255.255.
Sticky Group	Specify the sticky group associated with the virtual server.
Reverse Sticky Group	Enter the number identifying the reverse sticky group to which the virtual server belongs.
<b>SSL Sticky</b>	You can stick an incoming SSL connection based only on the offset and length values of the SSL ID.
Offset	Enter the offset for the SSL ID.
Length	Enter the length of the SSL ID.







# Managing Server Farms

---

From the Server Farms page, you can do the following:

- Configure server farms.
- Specify load balancing algorithm, and monitor in-band health for each server farm.
- Configure a set of real servers and their attributes.
- Configure client NAT pools.
- Configure redirect virtual servers and their attributes.
- Configure health monitoring probes, and enable inband health checkup.
- Direct the traffic to the SSL daughter card.

This section includes the following topics:

- [Server Farms, page 5-2](#)
- [NAT Pools, page 5-39](#)

# Server Farms

A server farm (or server pool) is a collection of servers that contain the same content. You can specify the server farm name when you configure the server farm and add real servers to it, and when you bind the server farm to a virtual server.

When you configure server farms, do the following:

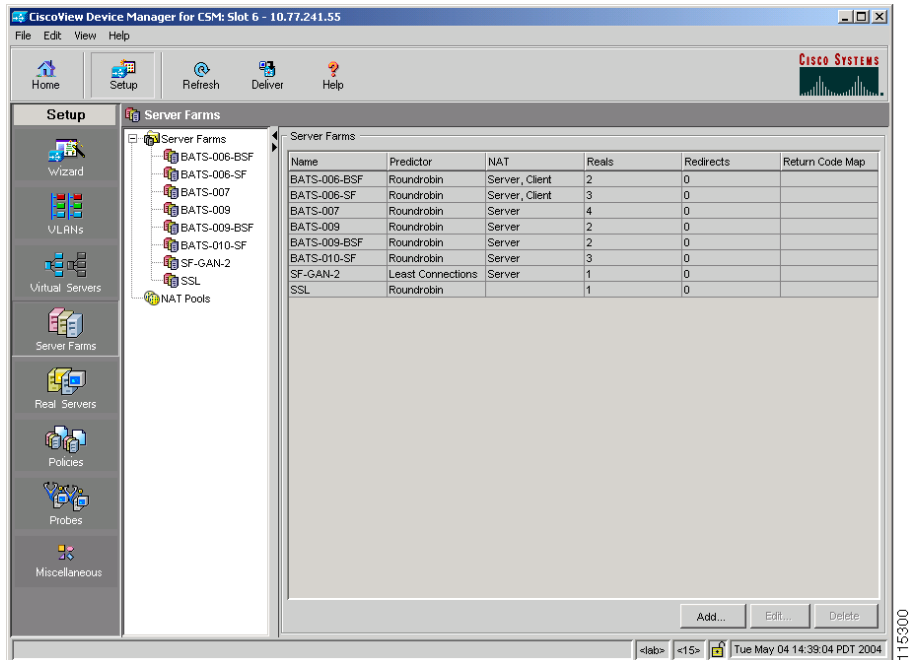
- Name the server farm.
- Configure a load-balancing algorithm (predictor) and other attributes of the farm.
- Configure client NAT pools.
- Configure a set of real servers and their attributes.
- Configure in-band health monitoring for each server farm.

## Related Topics:

- [Viewing Server Farms, page 5-3](#)
- [Adding Server Farms, page 5-5](#)
- [Editing Server Farms, page 5-12](#)
- [Viewing a Server Farm Node, page 5-19](#)
- [Adding a Named Real Server, page 5-23](#)
- [Adding an Unnamed Real Server, page 5-27](#)
- [Editing a Real Server, page 5-30](#)
- [Redirect Virtual Servers, page 5-34](#)

# Viewing Server Farms

Figure 5-1 Server Farms Page



**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Server Farms** in the Setup pane.

The Server Farm dialog box appears with the following columns.

Column	Description
Name	Name of the server farm.
Predictor	<p>Type of load-balancing algorithm used by the server farm. If not specified, the default is Round Robin.</p> <p>It can be one of the following:</p> <ul style="list-style-type: none"> <li>• Round Robin—Selects the next server in the list of real servers.</li> <li>• Least Connections—Selects the server with the least number of connections.</li> <li>• Forward—Allows the CVDM-CSM to forward traffic according with its internal routing tables.</li> <li>• Hash URL—Selects the server using a hash value, based on the URL.</li> <li>• Hash Address—Selects the server using a hash value, based on the source and destination IP addresses.</li> </ul>
NAT	Shows whether server and client Network Address Translation (NAT) is enabled.
Reals	Number of real servers configured in the server farm.
Redirects	Shows the number of redirect virtual servers configured in the server farm.
Return Code Map	Specifies the return code map associated with the server farm.

From this dialog box, you can do the following:

- Click **Add** to add server farms. For more information, see [Adding Server Farms, page 5-5](#).
- Select a server farm and click **Edit** to edit its configurations. For more information, see [Editing Server Farms, page 5-12](#).
- Select a server farm and click **Delete** to delete it.

## Adding Server Farms

- 
- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Server Farms** in the Setup pane.
- Step 2** Click **Add** to create a new server farm. The Add Server Farm dialog box appears.
- Step 3** Click one of the following tabs, then proceed to the corresponding section for configuration information:
- [General, page 5-6](#)
  - [Real Servers, page 5-8](#)
  - [Health Checkup, page 5-9](#)
  - [Redirect Virtual Server, page 5-10](#)
-

## General

When you click on the **General** tab, the following information appears:

Column	Descriptions
Name	Enter the name of the server farm.
<b>Predictor</b>	
Load-Balancing Algorithm	<p>Specify the load-balancing algorithm for the server farm from the list. Based on the load balancing algorithm the traffic will be diverted to the respective real server. If not specified, the default is Round Robin.</p> <p>It can be one of the following:</p> <ul style="list-style-type: none"> <li>• Round Robin—Selects the next server in the list of real servers.</li> <li>• Least Connections—Selects the server with the least number of connections.</li> <li>• Forward—Allows the CVDM-CSM to forward traffic according with its internal routing tables.</li> <li>• Hash URL—Selects the server using a hash value, based on the URL.</li> <li>• Hash Address—Selects the server using a hash value, based on the source and destination IP addresses.</li> </ul>
Mask Type	<p>It can be source, destination, or both.</p> <p>This field is enabled only for Hash Address algorithm type.</p>

Column	Descriptions
Mask	The mask of the real server in the server farm. This field is enabled only for Hash Address algorithm type.
<b>NAT</b>	
Server NAT	Select the check box to enable Server NAT.
Client NAT	Select the check box to enable Client NAT.
Back-End SSL encryption	Select the check box to enable backend SSL encryption.  This field will be enabled only when you select the Server NAT check box.
Pool	Enter the name of the client pool. You can modify this field only if client NAT is enabled in this server farm.  Click <input type="text" value="▽..."/> and select one of the following: <ul style="list-style-type: none"> <li>• <b>Select Pool</b>—Opens the Client NAT Pool Selector dialog box and allows you to select a client pool from the list.</li> <li>• <b>Create Pool</b>—Opens the Add NAT Pool dialog box and allows you to create a client pool. For more information, see <a href="#">Adding NAT Pools, page 5-42</a>.</li> <li>• <b>Clear Pool</b>—Allows you to clear the field.</li> </ul>

## Real Servers

When you select the **Real Servers** tab, the following information appears:

Column	Description
Real	Name of real servers configured in the server farm.
Local	Indicates if this real server is the SSL daughter card.
Min. Connections	The minimum number of connections for the real server.
Max. Connections	The maximum number of connections for the real server.
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Lets you know if the status of the real server.


From this dialog box, you can do the following:

- Click **Add** and select one of the following:
  - **Select Named Real Server**—Opens the Add Named Real Server dialog box. For more information, see [“Adding a Named Real Server” section on page 5-23](#).
  - **Create Unnamed Real Server**—Opens the Add Unnamed Real Server dialog box. For more information, see [“Adding an Unnamed Real Server” section on page 5-27](#).
  - **Add Multiple Real Servers**—Opens the Real Server Selector and allows you to add multiple real servers. For more information, see [Adding Multiple Real Servers, page 5-11](#).
- Select a real server and click **Edit** to edit its configurations. For more information, see [“Editing a Real Server” section on page 5-30](#).
- Select a real server and click **Delete** to delete it.



## Health Checkup

When you select the **Health Checkup** tab, the following information appears:

Column	Description
Fail Action	<p>From the list, specify the behavior of the connection when the real server fails. It can be one of the following:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Purge</li> <li>• Reassign</li> </ul>
Return Code Map	<p>Specify the return code map.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Return Code Map</b>—Opens the Return Code Map Selector dialog box. Allows you to select a return code map from the list.</li> <li>• <b>Create Return Code Map</b>—Opens the Add Return Code Map dialog box to create a return code map. For more information, see <a href="#">Adding a Return Code Map, page 8-13</a>.</li> <li>• <b>Clear Return Code Map</b> to clear the field.</li> </ul>
Inband Health Checkup	<p>Select the check box to enable inband health monitoring for all the servers in the server farm. You can set the retry attempts and the number of retries.</p>
Number of Retries	<p>Enter the number of consecutive connection attempts before considering the real server failed.</p>
Retry Interval	<p>Enter the retry interval in seconds.</p>

Column	Description
<b>Associated Probes</b>	
Name	You can see the probes associated to the server farm.

From this dialog box, you can do the following:

- Click **Add** under the Associated Probes pane, to choose a probe from the list and associate it to the real server.
- Click **Delete** under the Associated Probes pane, to delete a probe.

## Redirect Virtual Server

When you select the **Redirect Virtual Server** tab specify a virtual server to receive traffic redirected by a server farm. When you map real servers to redirect virtual servers, it provides persistence for clients to real servers across TCP sessions.

The following information appears:

Column	Description
Name	The name of the redirect virtual server.
SSL Port	The SSL port number.
Status	Status of the redirect virtual server.

From this dialog, you can do the following:

- Click **Add** to add a new redirect virtual server. For more information, see [“Adding a Redirect Virtual Server” section on page 5-35](#).
- Click **Edit** to edit the properties of the redirect virtual server. For more information, see [“Editing Redirect Virtual Servers” section on page 5-37](#).
- Select a row and click **Delete** to delete a redirect virtual server.

## Adding Multiple Real Servers

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.
  - Or:
  - Click **Setup** from the task bar and click **Server Farms** in the Setup pane.
- Step 2** Click **Add** to create a new server farm. The Add Server Farm dialog box appears.
- Step 3** Click the **Real Servers** tab.
- Step 4** Click **Add** and from the list select **Add Multiple Real Servers**. The Real Server Selector appears, displaying the following columns.

GUI Element	Action/Description
<b>Available Named Real Server pane</b>	
Name field	Select the real server.
<b>Selected Named Real Server pane</b>	
Name field	Name of the selected real server.
Port field	Port number of the real server.
Local SSL field	Indicates if this real server is the SSL daughter card.  This column is visible only if you launch the CVDM-CSM for a CSM-S service module. It will not be visible if you launch CVDM-CSM.
Weight field	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.

From this dialog box, you can do the following:

- Select a real server from the Available Named Real Server pane and click **Add** to include it in the Selected named Real Server pane.
- Select a real server from the Selected named Real Server pane and click **Remove**, to remove the real server from the selected list.
- Click **Clear All** to remove all the real servers from the Selected named Real Server pane.
- Click **Add New** to add a new real server in the Selected named Real Server pane. For more information, see [Adding a Real Server, page 6-9](#).

## Editing Server Farms

- 
- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Server Farms** in the Setup pane.
- Step 2** Select a sever farm and click **Edit**. The Edit Server Farm dialog box appears.
- Step 3** Click one of the following tabs, then proceed to the corresponding section for configuration information:
- [General, page 5-13](#)
  - [Real Server, page 5-15](#)
  - [Health Checkup, page 5-16](#)
  - [Redirect Virtual Server, page 5-18](#)
-

## General

When you select the **General** tab the following information appears:

Column	Descriptions
Name	Enter the name of the server farm.
<b>Predictor</b>	
Load-Balancing Algorithm	<p>Specify the load-balancing algorithm for the server farm from the list. Based on the load balancing algorithm the traffic will be diverted to the respective real server. If not specified, the default is Round Robin.</p> <p>It can be one of the following:</p> <ul style="list-style-type: none"> <li>• Round Robin—Selects the next server in the list of real servers.</li> <li>• Least Connections—Selects the server with the least number of connections.</li> <li>• Forward—Allows the CVDM-CSM to forward traffic according with its internal routing tables.</li> <li>• Hash URL—Selects the server using a hash value, based on the URL.</li> <li>• Hash Address—Selects the server using a hash value, based on the source and destination IP addresses.</li> </ul>
Mask Type	<p>It can be source, destination or both.</p> <p>This field is enabled only for Hash Address algorithm type.</p>

Column	Descriptions
Mask	The mask of the real server in the server farm. This field is enabled only for Hash Address algorithm type.
<b>NAT</b>	
Server NAT	Select the check box to enable Server NAT.
Client NAT	Select the check box to enable Client NAT.
Back-end SSL encryption	<p>Select the check box to enable back-end SSL encryption.</p> <p>This field will be enabled only when you select the Server NAT check box.</p>
Pool	<p>Enter the name of the client pool. You can modify this field only if client NAT is enabled in this server farm.</p> <p>Click <input type="text" value="▽..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Pool</b>—Opens the Client NAT Pool Selector dialog box and allows you to select a client pool from the list.</li> <li>• <b>Create Pool</b>—Opens the Add NAT Pool dialog box and allows you to create a client pool. For more information, see <a href="#">Adding NAT Pools, page 5-42</a>.</li> <li>• <b>Clear Pool</b>—Allows you to clear the field.</li> </ul>

## Real Server

When you select the **Real Servers** tab the following information appears:

Fields	Description
Real	Name of real servers configured in the server farm.
Local	Indicates if this real server is the SSL daughter card.
Min. Connections	The minimum number of connections for the real server.
Max. Connections	The maximum number of connections for the real server.
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Lets you know if the status of the real server.

From this dialog box, you can do the following:

- Click **Add** and select one of the following:
  - **Select Named Real Server**—Opens the Add Named Real Server dialog box. For more information, see [“Adding a Named Real Server” section on page 5-23](#).
  - **Create Unnamed Real Server**—Opens the Add Unnamed Real Server dialog box. For more information, see [“Adding an Unnamed Real Server” section on page 5-27](#).
  - **Add Multiple Real Servers**—Opens the Real Server Selector and allows you to add multiple real servers. For more information, see
- Select a real server and click **Edit** to edit its configurations. For more information, see [“Editing a Real Server” section on page 5-30](#).
- Select a real server and click **Delete** to delete it.

## Health Checkup

You can configure probes by specifying the probe name and type. After configuring a probe, you must associate it with a server farm for the probe to take effect. All servers in the server farm receive probes of the probe types that are associated with that server farm. You can associate one or more probe types with a server farm.

When you select the **Health Checkup** tab, the following information appears:

Field	Description
Fail Action	<p>From the list, specify the behavior of the connection when the real server fails. It can be one of the following:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Purge</li> <li>• Reassign</li> </ul>
Return Code Map	<p>Specify the return code map.</p> <p>Click <input type="button" value="▽..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Return Code Map</b>—Opens the Return Code Map Selector dialog box. Allows you to select a return code map from the list.</li> <li>• <b>Create Return Code Map</b>—Opens the Add Return Code Map dialog box to create a return code map. For more information, see <a href="#">Adding a Return Code Map, page 8-13</a>.</li> <li>• <b>Clear Field</b>—Allows you to clear the field.</li> </ul>



<b>Field</b>	<b>Description</b>
Inband Health Checkup	Select the check box to enable inband health monitoring for all the servers in the server farm. You can set the retry attempts and the number of retries.
Number of Retries	Enter the number of consecutive connection attempts before considering the real server failed.
Retry Interval	Enter the retry interval (in seconds).
<b>Associated Probes</b>	
Name	You can see the probes associated to the server farm.

From this dialog box, you can do the following:

- Click **Add** under the Associated Probes pane, to choose a probe from the list and associate it to the real server.
- Click **Delete** under the Associated Probes pane, to delete a probe.

## Redirect Virtual Server

When you select the **Redirect Virtual Server** tab to specify a virtual server to receive traffic redirected by a server farm. A table appears with the following informations:

Field	Description
Name	The name of the redirect virtual server.
SSL Port	The SSL port number.
Status	Status of the redirect virtual server.

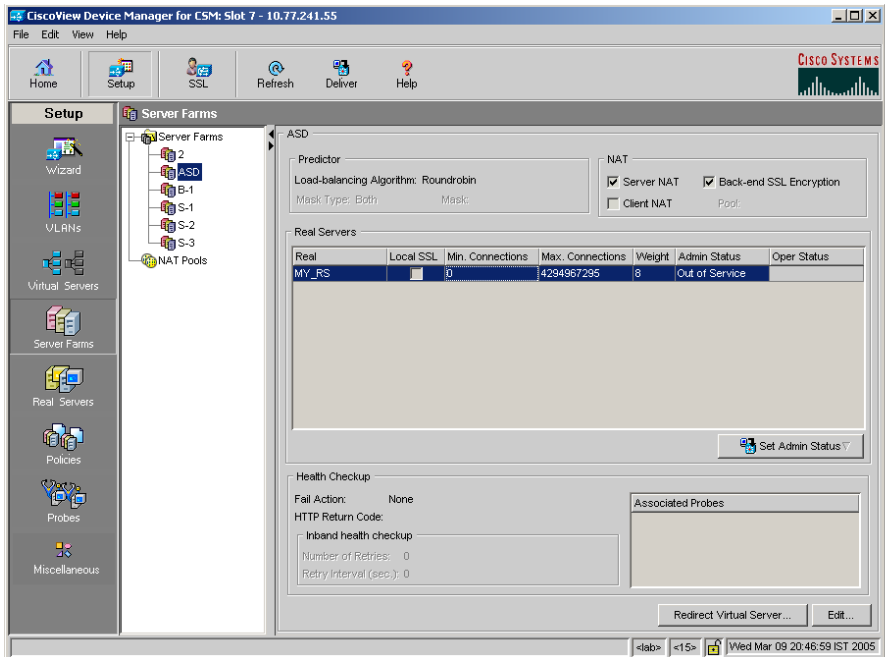
From this dialog box, you can do the following:

- Click **Add** to add a new redirect virtual server. For more information, see [“Adding a Redirect Virtual Server” section on page 5-35](#).
- Click **Edit** to edit the properties of the redirect virtual server. For more information, see [“Editing Redirect Virtual Servers” section on page 5-37](#).
- Select a row and click **Delete** to delete a redirect virtual server.

## Viewing a Server Farm Node

You can see details of individual server farms. You can add redirect virtual servers and also set the administrative status of real servers in the server farm.

**Figure 5-2** Server Farm Node Page



**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Server Farms** under Services Dashboard.

Or:

- Click **Setup** from the task bar and click **Server Farms** in the Setup pane.

**Step 2** Select a server farm from the object selector to view its details. The server farm table appears, displaying the following columns.

Field	Description
<b>Predictor</b>	
Load-Balancing Algorithm	<p>The load-balancing algorithm for the server farm. Based on the load balancing algorithm the traffic will be diverted to the respective real server. If not specified, the default is Round Robin.</p> <p>It can be one of the following:</p> <ul style="list-style-type: none"> <li>• Round Robin—Selects the next server in the list of real servers.</li> <li>• Least Connections—Selects the server with the least number of connections.</li> <li>• Forward—Allows the CVDM-CSM to forward traffic according with its internal routing tables.</li> <li>• Hash URL—Selects the server using a hash value, based on the URL.</li> <li>• Hash Address—Selects the server using a hash value, based on the source and destination IP addresses.</li> </ul>
Mask Type	<p>It can be source, destination or both.</p> <p>This field is enabled only for Hash Address algorithm type.</p>
Mask	<p>Enter the mask of the real server in the server farm. This field appears only for Hash Address algorithm type.</p>
<b>NAT</b>	
Server NAT	<p>Lets you know if server NAT is enabled in this server farm.</p>

<b>Field</b>	<b>Description</b>
Client NAT	Lets you know if client NAT is enabled in this server farm.
Back-end SSL encryption	Lets you know that back-end SSL encryption is enabled.
Pool	The name of the client pool. This field will appear only when client NAT is enabled in this server farm.
<b>Real Servers</b>	
Real	The name of the real server.
Local	Indicates if this real server is the SSL daughter card.
Min. Connections	The minimum number of connections for the real server.
Max. Connections	The maximum connections for the real server.
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	The admin status of the real server with respect to this server farm.
Operational Status	The operational status of the real server with respect to this server farm.
<b>Health Checkup</b>	
Fail Action	The course of action determined for the server farm in case of failure.
HTTP Return Code	The HTTP return code map for the server farm.
<b>Inband Health Checkup</b>	
Number of Retries	The number of consecutive connection attempts before considering the real server failed.

Field	Description
Retry Interval	The retry interval (in seconds).
Associated Probes	The list of probes associated with the server farm.


From this dialog box, you can do the following:

- Select a real server and click **Set Admin Status** to instantly set its state.
- Click the **Redirect Virtual Server** button to view the redirect virtual servers associated with this real server. You can also add, edit, or delete a redirect virtual server. For more information, see:
  - [Adding a Redirect Virtual Server, page 5-35](#)
  - [Editing Redirect Virtual Servers, page 5-37](#)
- Click **Edit** to edit the server farm. For more information, see “[Editing Server Farms](#)” section on page 5-12.


# Adding a Named Real Server

---

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under Services Dashboard.
- Or:
- Click **Setup** from the task bar and click **Server Farms** in the Setup pane.
- Step 2** Click **Add**. The Add Server Farm dialog box appears.
- Step 3** Select the **Real Server** tab in this dialog box.
- Step 4** Click **Add**, and choose **Select Named Real Server** from the options.
- The Add Named Real Server dialog box appears, displaying the following columns.

Column	Description
Name	From the list, select the name of the named real server.
Real Server	<p>Enter the name of the real server.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Real Server</b>—Opens the Named Real Server Selector dialog box and allows you to select a real server from the list.</li> <li>• <b>Create Real Server</b>—Opens the Add Real Server dialog box and allows you to create a real server. For more information, see <a href="#">Adding a Real Server, page 6-9</a>.</li> <li>• <b>Clear Real Server</b>—Allows you to clear the field.</li> </ul>
Port	Enter the port number.
Min. Connections	Enter the minimum number of connections for the real server.
Max. Connections	Enter the maximum number of connections for the real server.
Weight	<p>Enter the weight assigned to the real server.</p> <p>The weight identifies the capacity of the real server compared to other real servers in the server farm.</p>




Column	Description
Redirect Virtual Server	<p>Click  and do one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Redirect Virtual Server</b>—Opens the Redirect Virtual Server Selector dialog box. It allows you to select a redirect virtual server from the list.</li> <li>• <b>Create Redirect Virtual Server</b>—Opens the Add Redirect Virtual Server dialog box and allows you to add a redirect virtual server. For more information, see <a href="#">Adding a Redirect Virtual Server, page 5-35</a>.</li> <li>• <b>Clear Redirect Virtual Server</b>—Allows you to clear the field.</li> </ul>
Local SSL	Select the check box to indicate that the real server is the SSL daughter card.
Status	Specify the status of the real server.
<b>Back Up Real Server</b>	

Column	Description
Name	<p>Click <input type="text" value="▽..."/> and do one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Named Backup Real Server</b>—Opens the Backup Real Server Selector dialog box and allows you to select a named backup real server from the list.</li> <li>• <b>Select Unnamed Backup Real Server</b>—Opens the Backup Real Server Selector dialog box and allows you to select an unnamed backup real server from the list.</li> <li>• <b>Clear Backup Real Server</b>—Allows you to clear the field.</li> </ul>
Port	Displays the port number of the backup real server.
<b>Probe</b>	
Probe Name	<p>Click <input type="text" value="▽..."/> and do one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Probe</b>—Opens the Probe Selector dialog box and allows you to select a probe from the list.</li> <li>• <b>Create Probe</b>—Opens the Add Probe dialog box and allows you to create new probes. For more information, see <a href="#">“Adding Probes” section on page 10-5</a>.</li> <li>• <b>Clear Probe</b>—Allows you to clear the field.</li> </ul>
Tag	Enter the tag for the probe.

# Adding an Unnamed Real Server

---

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under Services Dashboard.
- Or:
- Click **Setup** from the task bar and click **Server Farms** in the Setup pane.
- Step 2** Click **Add**. The Add Server Farm dialog box appears.
- Step 3** Select the **Real Server** tab in this dialog box.
- Step 4** Click **Add**, and choose **Create Unnamed Real Server** from the options. The Add Unnamed Real Server dialog box appears, displaying the following columns.


Column	Description
IP Address	Enter the IP address of the destination.
Port	Enter the port number.
Min. Connections	Enter the minimum number of connections for the real server.
Max. Connections	Enter the maximum number of connections for the real server.
Weight	<p>Enter the weight assigned to the real server.</p> <p>The weight identifies the capacity of the real server compared to other real servers in the server farm.</p>
Redirect Virtual Server	<p>Click  and do one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Redirect Virtual Server</b>—Opens the Redirect Virtual Server Selector dialog box. It allows you to select a redirect virtual server from the list.</li> <li>• <b>Create Redirect Virtual Server</b>—Opens the Add Redirect Virtual Server dialog box and allows you to add a redirect virtual server. For more information, see <a href="#">Adding a Redirect Virtual Server, page 5-35</a>.</li> <li>• <b>Clear Redirect Virtual Server</b>—Allows you to clear the field.</li> </ul>
Local SSL	Select the check box to indicate that the real server is the SSL daughter card.
Status	Specify the status of the real server.
<b>Backup Real Server</b>	

Column	Description
Name	<p>Click <input type="button" value="▽..."/> and do one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Named Backup Real Server</b>—Opens the Backup Real Server Selector dialog box and allows you to select a named backup real server from the list.</li> <li>• <b>Select Unnamed Backup Real Server</b>—Opens the Backup Real Server Selector dialog box and allows you to select an unnamed backup real server from the list.</li> <li>• <b>Clear Backup Real Server</b>—Allows you to clear the field.</li> </ul>
Port	Displays the port number of the backup real server.
<b>Probe</b>	
Probe Name	<p>Click <input type="button" value="▽..."/> and do one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Probe</b>—Opens the Probe Selector dialog box and allows you to select a probe from the list.</li> <li>• <b>Create Probe</b>—Opens the Add Probe dialog box and allows you to create new probes. For more information, see <a href="#">Adding Probes, page 10-5</a>.</li> <li>• <b>Clear Probe</b>—Allows you to clear the field.</li> </ul>
Tag	Enter the tag for the probe.

# Editing a Real Server


---

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under Services Dashboard.
- Or:
- Click **Setup** from the task bar and click **Server Farms** in the Setup pane.
- Step 2** Click the **Add** button provided at the end of the table.  
The Add Server Farm dialog box appears.
- Step 3** Select the **Real Server** tab in this dialog box.
- Step 4** Select a real server and click **Edit**.  
The Edit Real Server dialog box appears, displaying the following columns.

Field	Description
IP Address	(For unnamed real servers) Enter the IP address of the real server.
Port	Enter the port number.
Real Server	(For the named real server) IP address of the named real server.
Min. Connections	Enter the minimum number of connections for the real server.
Max. Connections	Enter the maximum number of connections for the real server.
Weight	<p>Enter the weight assigned to the real server.</p> <p>The weight identifies the capacity of the real server compared to other real servers in the server farm.</p>
Redirect Virtual Server	<p>Click  and do one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Redirect Virtual Server</b>—Opens the Redirect Virtual Server Selector dialog box. It allows you to select a redirect virtual server from the list.</li> <li>• <b>Create Redirect Virtual Server</b>—Opens the Add Redirect Virtual Server dialog box and allows you to add a redirect virtual server. For more information, see <a href="#">Adding a Redirect Virtual Server, page 5-35</a>.</li> <li>• <b>Clear Redirect Virtual Server</b>—Allows you to clear the field.</li> </ul>

Field	Description
Local SSL	Select the check box to indicate that the real server is the SSL daughter card.
Status	Specify the status of the real server.
<b>Back Up Real Server</b>	
Name	<p>Click <input type="button" value="v..."/> and do one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Named Backup Real Server</b>—Opens the Backup Real Server Selector dialog box and allows you to select a named backup real server from the list.</li> <li>• <b>Select Unnamed Backup Real Server</b>—Opens the Backup Real Server Selector dialog box and allows you to select an unnamed backup real server from the list.</li> <li>• <b>Clear Backup Real Server</b>—Allows you to clear the field.</li> </ul>
Port	Displays the port number of the backup real server.
<b>Probe</b>	



Field	Description
Probe Name	<p>Click  and do one of the following:</p> <ul style="list-style-type: none"><li>• <b>Select Probe</b>—Opens the Probe Selector dialog box and allows you to select a probe from the list.</li><li>• <b>Create Probe</b>—Opens the Add Probe dialog box and allows you to create new probes. For more information, see <a href="#">Adding Probes, page 10-5</a>.</li><li>• <b>Clear Probe</b>—Allows you to clear the field.</li></ul>
Tag	Enter the tag for the probe.

# Redirect Virtual Servers

You can specify a virtual server to receive traffic redirected by a server farm. When you map real servers to redirect virtual servers, it provides persistence for clients to real servers across TCP sessions.

If the redirect virtual server does not have any real servers available, you need to specify a backup or relocation string sent in response to HTTP requests.

To see the details of the redirect virtual servers that you have configured for a server farm:

- 
- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Server Farms** in the Setup pane.
- Step 2** Select a server farm from the object selector.
- Step 3** Click the **Redirect Virtual Server** button. The Redirect Virtual Server dialog box appears, displaying the following columns:

Column	Description
Name	Name of the redirect virtual server.
SSL Port	SSL port number. The range is from 1 to 65535 or one of the following: <ul style="list-style-type: none"> <li>• HTTP</li> <li>• WWW</li> <li>• FTP</li> </ul>
Status	Specify the status of the redirect virtual server.

---

From this dialog box, you can do the following:

- Click **Add** to add a redirect virtual server. For more information, see [Adding a Redirect Virtual Server, page 5-35](#).
- Select a redirect virtual server and click **Edit** to edit the configurations of the redirect virtual server. For more information, see [Editing Redirect Virtual Servers, page 5-37](#).

## Adding a Redirect Virtual Server

You can specify a virtual server to receive traffic redirected by a server farm. When you map real servers to redirect virtual servers, it provides persistence for clients to real servers across TCP sessions.

If the redirect virtual server does not have any real servers available, you need to specify a backup or relocation string sent in response to HTTP requests.

- 
- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Server Farms** in the Setup pane.
- Step 2** Select the required server farm from the object selector.
- Step 3** Click the **Redirect Virtual Server** button.
- The Redirect Virtual Server dialog box appears.
- Step 4** Click **Add** to add a new redirect virtual server.
- The Add Redirect Virtual Server dialog box appears, displaying the following columns.

<b>Column</b>	<b>Description</b>
Name	Specify the name of the redirect virtual server.
SSL Port	SSL port number. The range is from 1 to 65535 or you can select one of the following from the list: <ul style="list-style-type: none"> <li>• HTTP</li> <li>• WWW</li> <li>• FTP</li> </ul>
Status	Specify the status of the redirect virtual server.
<b>Backup</b>	
Response	Specify the backup response. This is sent in response to redirected HTTP requests.
HTTP Status Code	Select the HTTP status code. It can be one of the following: <ul style="list-style-type: none"> <li>• 301—Requested resource has been assigned a new permanent URL.</li> <li>• 302—Requested resource resides temporarily under a different URL.</li> </ul> <p>The default status code is 302.</p>
<b>Relocation</b>	
Response	Specify the relocation response. This is sent in response to redirected HTTP requests.
HTTP Status Code	Select the HTTP status code.

# Editing Redirect Virtual Servers

---

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Server Farms** in the Setup pane.
- Step 2** Select the required server farm from the object selector.
- Step 3** Click the **Redirect Virtual Server** button.
- The Redirect Virtual Server dialog box appears.
- Step 4** Select a redirect virtual server and click **Edit** to add a new redirect virtual server.
- The Edit Redirect Virtual Server dialog box appears, displaying the following columns.

<b>Column</b>	<b>Description</b>
Name	Specify the name of the redirect virtual server.
SSL Port	SSL port number. The range is from 1 to 65535 or you can select one of the following from the list: <ul style="list-style-type: none"> <li>• HTTP</li> <li>• WWW</li> <li>• FTP</li> </ul>
Status	Specify the status of the redirect virtual server.
<b>Backup</b>	
Response	Specify the backup response. This is sent in response to redirected HTTP requests.
HTTP Status Code	Select the HTTP status code. It can be one of the following: <ul style="list-style-type: none"> <li>• 301—Requested resource has been assigned a new permanent URL.</li> <li>• 302—Requested resource resides temporarily under a different URL.</li> </ul> <p>The default status code is 302.</p>
<b>Relocation</b>	
Response	Specify the relocation response. This is sent in response to redirected HTTP requests.
HTTP Status Code	Select the HTTP status code.

# NAT Pools

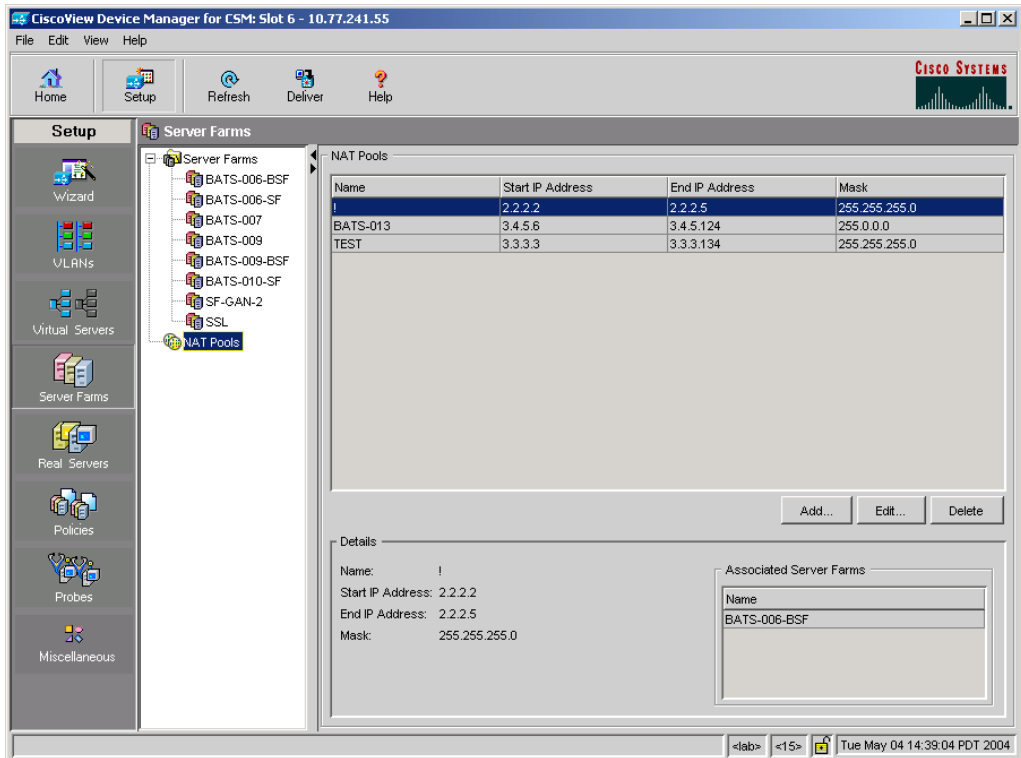
When you configure client Network Address Translation (NAT) pools, NAT converts the source IP address of the client requests into an IP address on the server-side VLAN. You can configure a NAT pool with a range of IP addresses. To configure an NAT pool with a single IP address, you can specify the same IP address for starting and ending IP address.

**Related Topics:**

- [Viewing NAT Pools, page 5-40](#)
- [Adding NAT Pools, page 5-42](#)
- [Editing NAT Pools, page 5-43](#)

# Viewing NAT Pools

Figure 5-3 NAT Pools Window



- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.
  - Or:
  - Click **Setup** from the task bar and click **Server Farm** in the Setup pane.
- Step 2** Select **NAT Pools** from the object selector.
- The NAT Pools dialog box appears, displaying the following columns.



Column	Description
Name	Name of the NAT pool.
Start IP Address	The starting IP address of the range of addresses in the NAT pool. An NAT pool with a single IP address will have the same the IP address for the starting and the ending IP address.
End IP Address	The ending IP address of the range of addresses in the NAT Pool.
Mask	The mask IP of the for the associated IP subnet.

When you select a NAT pool from the table, you can see the corresponding details:

Column	Description
<b>Details</b>	
Name	Name of the NAT pool.
Start IP Address	The starting IP address of the range of addresses in the NAT pool. An NAT pool with a single IP address will have the same the IP address for the starting and the ending IP address.
End IP Address	The ending IP address of the range of addresses in the NAT Pool.
Mask	The mask IP of the for the associated IP subnet.
<b>Associated Server Farms</b>	
Name	Displays the name of the server farm that has this NAT pool is associated with.

From this section, you can do the following:

- Click **Add** to add NAT Pools. For more information, see [Adding NAT Pools, page 5-42](#).
- Select a NAT pool and click **Edit** to edit it. For more information, see [Editing NAT Pools, page 5-43](#).
- Select a node and click **Delete** to delete the NAT Pool.

## Adding NAT Pools

**Note**

---

To create a NAT pool with a single IP address, provide the same IP address in the Start IP Address and End IP Address fields.

---

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Server Farm** in the Setup pane.
- Step 2** Select **NAT Pools** from the object selector.
- Step 3** Click **Add**. The Add NAT Pool dialog box appears, displaying the following columns.

Column	Description
Name	Name of the NAT pool.
Start IP Address	The starting IP address of the range of addresses in the NAT pool. An NAT pool with a single IP address will have the same the IP address for the starting and the ending IP address.
End IP Address	The ending IP address of the range of addresses in the NAT Pool.
Mask	The mask IP of the for the associated IP subnet.

## Editing NAT Pools

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Server Farm** in the Setup pane.
- Step 2** Select **NAT Pools** from the object selector.
- Step 3** Click **Edit**. The Edit NAT Pool dialog box appears, displaying the following columns.

<b>Column</b>	<b>Description</b>
Name	Name of the NAT pool.
Start IP Address	The starting IP address of the range of addresses in the NAT pool. An NAT pool with a single IP address will have the same the IP address for the starting and the ending IP address.
End IP Address	The ending IP address of the range of addresses in the NAT Pool.
Mask	The mask IP of the for the associated IP subnet.

---



## Managing Real Servers

---

Real servers are physical devices that are assigned to a server farm and provide services that are load balanced. When a server receives a client request, it sends the reply to the CVDM-CSM to forward it to the client.

From the Real Server page, you can configure the named real servers by their IP address and location.

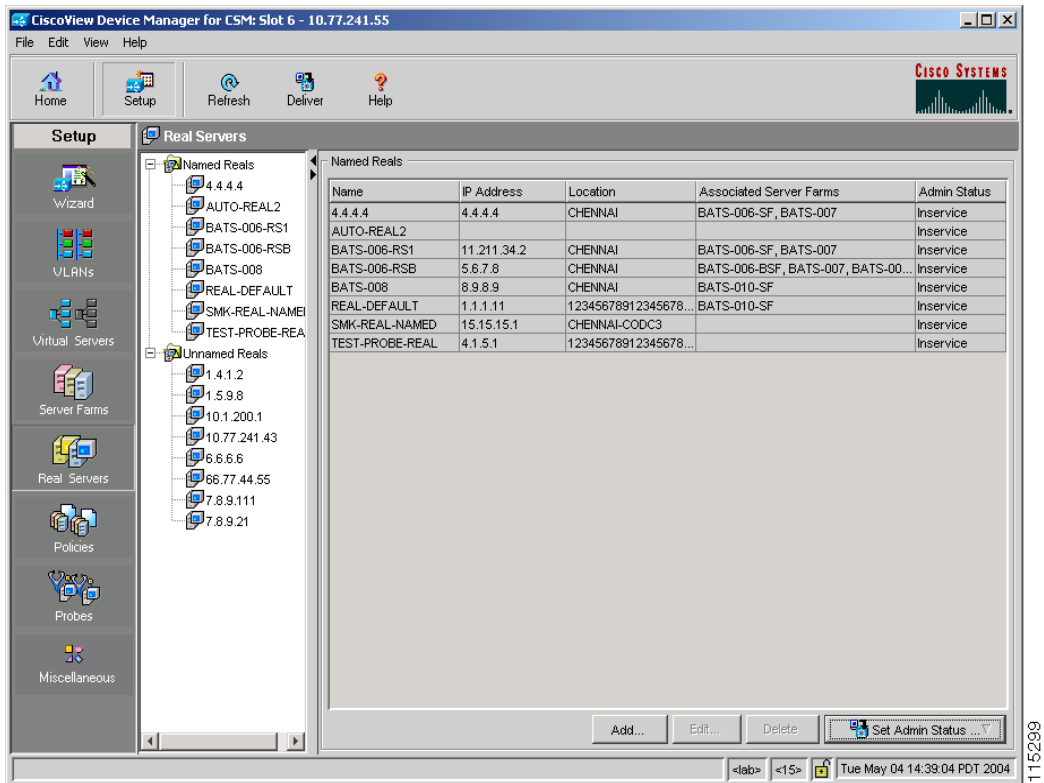
In the Content Switching Module with SSL (CSM-S) daughter card, the CSM treats the SSL daughter card as a special real server. You can configure the real server inside a Server farm with the local SSL option to direct the traffic to the SSL daughter card.

This section includes the following topics:

- [Viewing Named Real Servers, page 6-2](#)
- [Viewing an Individual Named Real Server, page 6-4](#)
- [Viewing Unnamed Real Servers, page 6-6](#)
- [Viewing an Individual Unnamed Real Server, page 6-7](#)
- [Adding a Real Server, page 6-9](#)
- [Editing a Real Server, page 6-10](#)

# Viewing Named Real Servers

Figure 6-1 Named Real Servers Page



You can view information about all the existing real servers details on the device. To view the configuration details of the named real servers:

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.
  - Or:
  - Click **Setup** from the task bar and click **Real Server** in the Setup pane.

**Step 2** Select **Named Reals** from the object selector.

The Named Reals dialog box appears, displaying the following details:

Field	Description
Name	Name of the real server.
IP Address	IP address of the real server.
Location	Location of the real server.
Associated Server Farms	Real server associated with the server farms.
Admin Status	Status of the real server.

From the real server dialog box, you can do the following:

- Click **Add** to add a new named real server. For more information, see [“Adding a Real Server” section on page 6-9](#).
- Select a named real server and click **Edit** to edit its configuration details. For more information, see [“Editing a Real Server” section on page 6-10](#).
- Click **Delete** to delete a named real server.
- Click **Set Admin Status** to instantly set the admin status of the named real server.

# Viewing an Individual Named Real Server

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Real Server** in the Setup pane.

**Step 2** Select **Named Reals** from the object selector and then select a named real server. A table appears, displaying the following columns:

Column	Description
Real Server Name	Name of the real server.
Location	Location of the real server.
Real Server IP Address	IP address of the real server.
Admin Status	Status of the real server.
Server Farm	Server Farm to which the real server is associated.
Port	TCP/UDP port number or name.
Min. Connections	Minimum number of active connections on the real server.
Max. Connections	Maximum number of active connections on the real server.
Weight	Weight of the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Admin status of the real server with respect to the server farm.
Operational Status	Operational status of the real server with respect to the server farm.



- Step 3** More specific details of the named real server appear in the lower half of the window.

Field	Description
<b>Details</b>	
Real Server Name/IP Address	Name or the IP address of the real server.
Port	Port number of the real server.
Local	Indicates if this real server is the SSL card.
Status	Indicates the status of the real server.
Min. Connections	Minimum number of active connections on the real server.
Max. Connections	Maximum number of active connections on the real server.
Weight	Weight of the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Redirect Virtual Server	Redirect virtual server that redirects traffic to this real server.
<b>Backup Real Server</b>	
Real Server Name/IP Address	Name or the IP address of the backup real server.
Port	Port number of the backup real server.
<b>Probe</b>	
Name	Name of the probe configured for the real server.
Tag	Specifies the tag for the probe.

From this dialog box, click **Set Admin Status** to instantly set the status of the real server.

# Viewing Unnamed Real Servers



**Note** You can create unnamed real servers only from a server farm.

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.
  - Or:
  - Click **Setup** from the task bar and click **Real Server** in the Setup pane.
- Step 2** Select **Unnamed Reals** from the object selector. The Unnamed Reals dialog box appears, displaying the following details:

Field	Description
Real	Name or IP address of the real server.
Associated Server Farms	Server Farm to which the real server is associated.

# Viewing an Individual Unnamed Real Server


**Note**

You can create unnamed real servers only from a server farm.

**Step 1**

Do one of the following:

- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Real Server** in the Setup pane.

**Step 2**

Select **Unnamed Reals** from the object selector. The Unnamed Reals dialog box appears.

**Step 3**

Select an unnamed real server to see its configuration details. A table appears, displaying the following columns:

Column	Description
Real Server IP Address	IP address of the unnamed real server.
Server Farm	Server Farm to which the real server is associated.
Port	Port number of the real server.
Min. Connections	Minimum number of active connections on the real server.
Max. Connections	Maximum number of active connections on the real server.
Weight	Weight of the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Admin status of the real server with respect to the server farm.
Operational Status	Operational status of the real server with respect to the server farm.

- Step 4** More specific details of the named real server appear in the lower half of the dialog box.

Column	Description
<b>Details</b>	
Real Server Name/IP Address	Name or IP address of the real server.
Port	Port number of the real server.
Local	Indicates if this real server is the SSL card.
Status	Indicates the status of the real server.
Min. Connections	Minimum number of active connections on the real server.
Max. Connections	Maximum number of active connections on the real server.
Weight	Weight of the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Redirect Virtual Server	The redirect virtual server that redirects traffic to this real server.
<b>Backup Real Server</b>	
Real Server Name/IP	Name or the IP of the backup real server.
Port	Port number of the backup real server.
<b>Probe</b>	
Name	Name of the probe configured for the real server.
Tag	Specifies the tag for the probe.

From this dialog box, click **Set Admin Status** to instantly set the status of the real server.

# Adding a Real Server


**Note**

You can associate a real server to a server farm only from the corresponding server farm.

**Step 1**

Do one of the following:

- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Real Server** in the Setup pane.

**Step 2**

Click **Add** to create a new real server.

The Add Real Server dialog box appears, displaying the following columns.

Field	Description
Name	Enter the name of the real server.
IP Address	Enter the IP address of the real server.
Local	Indicates if this real server is the SSL card.
Location	Enter the location of the real server.
Status	Specify the status.

# Editing a Real Server

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Server Farms** under **Services Dashboard**.
  - Or:
  - Click **Setup** from the task bar and click **Real Server** in the Setup pane.

- Step 2** Click **Edit** to create a new real server.

The Edit Real Server dialog box appears, displaying the following columns.

Field	Description
Name	Enter the name of the real server.
IP Address	Enter the IP address of the real server.
Location	Enter the location of the real server.
Service	Specify the status.



## Managing Policies

---

Policies are access rules that traffic must match when load balancing to a server farm. Policies allow the CVDM-CSM to balance Layer 7 traffic. Multiple policies can be assigned to one virtual server, creating multiple access rules for that virtual server. The server farm associated with a policy receives all the requests that match that policy.

When configuring policies, you must first configure the access rules (maps and/or client groups) and then you combine these access rules under a particular policy.



### Note

---

You must associate a server farm with a policy. A policy that does not have an associated server farm cannot forward traffic.

---

When the CVDM-CSM is able to match policies, it selects the policy that appears first in the policy list. Policies appear in the policy list in the sequence in which they are bound to the virtual server.

A policy will match even if all the servers in the associated server farm are down. The default behavior of the policy in that case is to not accept those connections and to send back a reset (RST) to the clients. To change this behavior, you can add a backup server farm for that policy.

If you configure a sticky group for a policy, the primary server farm in this policy becomes sticky. The client will stick to the configured real server in the primary server farm. When all of the real servers in the primary server farm fail, new requests from this client are sent to the backup server farm. When the real server in the primary server farm returns to the operational state, the following will occur:

- If you enable sticky option for the backup server farm, the new requests from the client will be sent to the backup real server.
- If you do not use sticky option on the backup server farm, the new requests will go back to the primary real server.
- The backup real server will continue to service existing connections.

From the Policy page, you can do the following:

- Configure access rules such as maps (cookie map, header map, URL map), client groups (access control lists), sticky group (cookie, header, netmask, and SSL).
- Associate server farm and backup server farm with a particular policy.

### Related Topics

- [Viewing Policies, page 7-3](#)
- [Adding Policies, page 7-5](#)
- [Editing Policies, page 7-11](#)
- [Viewing Policy Nodes, page 7-16](#)



# Viewing Policies

Figure 7-1 Policies Page

The screenshot shows the CiscoView Device Manager interface for CSM: Slot 6 - 10.77.241.55. The main window displays the 'Policies' page, which includes a tree view on the left and a table of policies on the right.

Policy Name	Conditions						Action	
	Cookie Map	URL Map	Header Map	Client ...	Server Farm	Backup Serve...	Sticky ...	Reverse Sticky Group
152-BATS-...	152-6-CM	152-6-UM	152-6-HM	152	152-6-SF	152-6-BSF	152	153
152-V-153	152-V-153-...	152-V-153-...	152-V-153-...	152-v-...	152-V-153	BATS-010-SF	24	66
ABCD			TUITY					
ADFADSFAD				0				
ADSFADS								
ADSFADSF								
ADVVMZP...	ADFASD	ALLURL	TEST	1222	SF-NEW1	SF-SOL	74	55
ASDF								
DDD								
DSFADS								
EDT*EFT								
POL-FULL	100C	DD	TEST-COOK	1	SF-SOL	SMK-SF-2	77	55
SADFA	152-6-CM	22	222111	12	SF	SF-FINAL	23	23
SDFADS				test				
SDFASD								
SMK-PL-1				1123	SMK-SF-2		233	
SSS			TITYI					
START								
TR-POL	TR-CMAP	TR-UMAP	TR-HMAP				1	
XYZ*ABC								

You can view all policies configured in the device.

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Policies** from the object selector. A table appears, displaying the following columns:

Column	Action/Description
Policy Name	Policy associated with a virtual server.
<b>Conditions</b>	
Cookie Map	Name of the cookie map associated with a policy. Only one cookie map can be associated with a policy.
URL Map	Name of the URL map associated with a policy. Only one URL map can be associated with a policy.
Header Map	Name of the header map associated with a policy. Only one header map can be associated with a policy.
Client Group	Client group can be either standard access lists names or an ID from 1 to 99. Only one client group can be associated with a given SLB policy.
<b>Action</b>	
<ul style="list-style-type: none"> <li>Server Farm</li> <li>Backup Server Farm</li> </ul>	Name of the server farm associated to the real server. You can choose one server farm and/or backup server farm to associate to the policy.
Sticky Group	Number identifying the sticky group to which the virtual server belongs.
Reverse Sticky Group	Number identifying the sticky group to which the virtual server belongs.  Ensures that CVDM-CSM changes its connections to the opposite direction and sends them back to the source.

From this dialog box, you can do the following:

- Click **Add** to add new policies. For more information, see [Adding Policies, page 7-5](#).
- Click **Edit** to edit policies. For more information, see [Editing Policies, page 7-11](#).
- Select a row and click **Delete** to delete policies.

# Adding Policies

You can add a policy, and you can associate one map of each type and one sticky group to the policy.

**Figure 7-2** Add Policy Dialog Box

**Add Policy**

Policy Name:

Maps

Cookie Map:  ▾

URL Map:  ▾

Header Map:  ▾

Client Group

*i* Client Group can be either Standard Access List Name or ID (1-99).

Client Group:  ▾

Server Farm

Server Farm:  ▾

Backup Server Farm:  ▾  Sticky



Sticky Group

Sticky Group:  ▾


Reverse Sticky Group:  ▾



130705

- 
- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Policies** in the Setup pane.
- Step 2** Select **Policies** from the object selector.
- Step 3** Click **Add** to add policies. The Add Policy table appears, displaying the following columns.

Column	Description
Policy Name	Enter the policy associated with a virtual server. The string is limited to 15 characters.
<b>Maps</b>	
Cookie Map	<p>From the list, select the name of the cookie map to be associated with the policy. Only one cookie map can be associated with a policy.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Cookie Map</b>—Opens the Select Cookie Map dialog box and allows you to select from a list of configured cookie maps.</li> <li>• <b>Create Cookie Map</b>—Opens the Add Cookie Map dialog box and allows you to create a cookie map. For more information, see <a href="#">Adding a Cookie Map, page 8-9</a>.</li> <li>• <b>Clear Cookie Map</b>—Allows you to clear the field.</li> </ul>
URL Map	<p>From the list, select the name of the URL map to be associated with the policy. Only one URL map can be associated with a policy</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select URL Map</b>—Opens the Select URL Map dialog box and allows you to select from a list of configured URL maps.</li> <li>• <b>Create URL Map</b>—Opens the Add URL Map dialog box and allows you to create a URL map. For more information, see <a href="#">Adding a URL Map, page 8-19</a>.</li> <li>• <b>Clear URL Map</b>—Allows you to clear the field.</li> </ul>

Column	Description
Header Map	<p>From the list, select the name of the header map to be associated with the policy. Only one header map can be associated with a policy.</p> <p>Click <input type="text" value="v..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Header Map</b>—Opens the Select Header Map dialog box and allows you to select from a list of configured header maps.</li> <li>• <b>Create Header Map</b>—Opens the Add Header Map dialog box and allows you to create one. For more information, see <a href="#">Adding a Header Map, page 8-23</a>.</li> <li>• <b>Clear Header Map</b>—Allows you to clear the field.</li> </ul>
Client Group	<p>From the list, select the client group number or name. Only one client group can be associated with a given server-load balancing (SLB) policy.</p> <p>Click <input type="text" value="v..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Create Client Group</b>—Allows you to create a Client group. Enter the Client group ID or Name.</li> <li>• <b>Clear Client Group</b>—Allows you to clear the field.</li> </ul>
<b>Server Farm</b>	
Server Farm	<p>From the list, select the name of the server farm associated to the real server. You can choose one server farm to associate to the policy.</p> <p>Click <input type="text" value="v..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Server Farms</b>—Opens the Server Farm dialog box and allows you to select from a list of configured server farms.</li> <li>• <b>Create Server Farms</b>—Opens the Add Server Farm dialog box and allows you to create the server farms. For more information, see <a href="#">Adding Server Farms, page 5-5</a>.</li> <li>• <b>Clear Server Farms</b>—Allows you to clear the field.</li> </ul>

Column	Description
Backup Server Farm	<p>From the list, select the name of the backup server farm associated to the real server. You can choose one backup server farm to associate to the policy.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"><li>• <b>Select Server Farms</b>—Opens the Server Farm dialog box and allows you to select from a list of configured server farms.</li><li>• <b>Create Server Farms</b>—Opens the Add Server Farm dialog box and allows you to create the server farms. For more information, see <a href="#">Adding Server Farms, page 5-5</a>.</li><li>• <b>Clear Server Farms</b>—Allows you to clear the field.</li></ul>
Sticky	<p>Select this check box to enable the sticky property.</p> <p>This ensures that multiple connections from the same client that match the same SLB policy stick (or attach) to the same real server.</p>
<b>Sticky Group</b>	



Column	Description
Sticky Group	<p>From the list, select the number identifying the sticky group to which the virtual server belongs.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Sticky Groups</b>—Opens the Select Sticky Group dialog box and allows you to select from a list of configured Sticky Groups.</li> <li>• <b>Create Sticky Groups</b>—Opens the Add Sticky Groups dialog box and allows you to create Sticky Groups. For more information, see <a href="#">Adding a Sticky Group, page 9-6</a>.</li> <li>• <b>Clear Sticky Groups</b>—Allows you to clear the field.</li> </ul>
Reverse Sticky Group	<p>From the list, select the number identifying the reverse sticky group to which the virtual server belongs.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Sticky Groups</b>—Opens the Select Sticky Group dialog box and allows you to select from a list of configured Sticky Groups.</li> <li>• <b>Create Sticky Groups</b>—Opens the Add Sticky Groups dialog box and allows you to create Sticky Groups. For more information, see <a href="#">Adding a Sticky Group, page 9-6</a>.</li> <li>• <b>Clear Sticky Groups</b>—Allows you to clear the field.</li> </ul>






# Editing Policies



---

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Policies** in the Setup pane.
- Step 2** Select **Policies** from the object selector.
- Step 3** Select a row in the table and click **Edit** to launch Edit Policy dialog box for the selected policy. A table appears, displaying the following columns.

Column	Description
Policy Name	Enter the policy associated with a virtual server. The string is limited to 15 characters.
Cookie Map	<p>From the list, select the name of the cookie map to be associated with the policy. Only one cookie map can be associated with a policy.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Cookie Map</b>—Opens the Select Cookie Map dialog box and allows you to select from a list of configured cookie maps.</li> <li>• <b>Create Cookie Map</b>—Opens the Add Cookie Map dialog box and allows you to create a cookie map. For more information, see <a href="#">Adding a Cookie Map, page 8-9</a>.</li> <li>• <b>Clear Cookie Map</b>—Allows you to clear the field.</li> </ul>
URL Map	<p>From the list, select the name of the URL map to be associated with the policy. Only one URL map can be associated with a policy</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select URL Map</b>—Opens the Select URL Map dialog box and allows you to select from a list of configured URL maps.</li> <li>• <b>Create URL Map</b>—Opens the Add URL Map dialog box and allows you to create a URL map. For more information, see <a href="#">Adding a URL Map, page 8-19</a>.</li> <li>• <b>Clear URL Map</b>—Allows you to clear the field.</li> </ul>

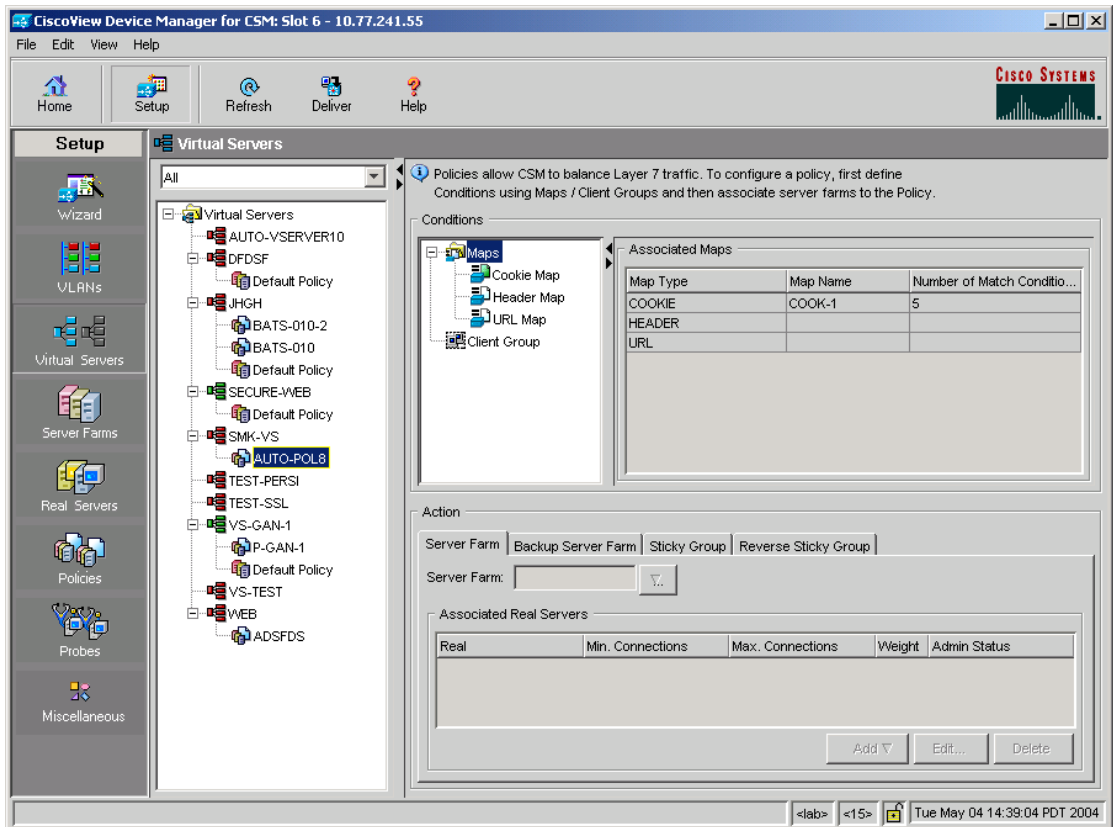
Column	Description
Header Map	<p>From the list, select the name of the header map to be associated with the policy. Only one header map can be associated with a policy.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Header Map</b>—Opens the Select Header Map dialog box and allows you to select from a list of configured header maps.</li> <li>• <b>Create Header Map</b>—Opens the Add Header Map dialog box and allows you to create one. For more information, see <a href="#">Adding a Header Map, page 8-23</a>.</li> <li>• <b>Clear Header Map</b>—Allows you to clear the field.</li> </ul>
Client Group	<p>From the list, select the client group number or name. Only one client group can be associated with a given server load-balancing (SLB) policy.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Create Client Group</b>—Allows you to create a Client group. Enter the Client group ID or Name.</li> <li>• <b>Clear Client Group</b>—Allows you to clear the field.</li> </ul>
<b>Server Farm</b>	
Server Farm	<p>From the list, select the name of the server farm associated to the real server. You can choose one server farm to associate to the policy.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Server Farms</b>—Opens the Server Farm dialog box and allows you to select from a list of configured server farms.</li> <li>• <b>Create Server Farms</b>—Opens the Add Server Farm dialog box and allows you to create the server farms. For more information, see <a href="#">Adding Server Farms, page 5-5</a>.</li> <li>• <b>Clear Server Farms</b>—Allows you to clear the field.</li> </ul>

Column	Description
Backup Server Farm	<p>From the list, select the name of the backup server farm associated to the real server. You can choose one backup server farm to associate to the policy.</p> <p>Click <input type="button" value="v..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Server Farms</b>—Opens the Server Farm dialog box and allows you to select from a list of configured server farms.</li> <li>• <b>Create Server Farms</b>—Opens the Add Server Farm dialog box and allows you to create the server farms. For more information, see <a href="#">Adding Server Farms, page 5-5</a>.</li> <li>• <b>Clear Server Farms</b>—Allows you to clear the field.</li> </ul>
Sticky	<p>Select this check box to enable the sticky property.</p> <p>This ensures that multiple connections from the same client that match the same SLB policy stick (or attach) to the same real server.</p>
<b>Sticky Group</b>	

Column	Description
Sticky Group	<p>From the list, select the number identifying the sticky group to which the virtual server belongs.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"><li>• <b>Select Sticky Groups</b>—Opens the Select Sticky Group dialog box and allows you to select from a list of configured Sticky Groups.</li><li>• <b>Create Sticky Groups</b>—Opens the Add Sticky Groups dialog box and allows you to create Sticky Groups. For more information, see <a href="#">Adding a Sticky Group, page 9-6</a>.</li><li>• <b>Clear Sticky Groups</b>—Allows you to clear the field.</li></ul>
Reverse Sticky Group	<p>From the list, select the number identifying the reverse sticky group to which the virtual server belongs.</p> <p>Click  and select one of the following:</p> <ul style="list-style-type: none"><li>• <b>Select Sticky Groups</b>—Opens the Select Sticky Group dialog box and allows you to select from a list of configured Sticky Groups.</li><li>• <b>Create Sticky Groups</b>—Opens the Add Sticky Groups dialog box and allows you to create Sticky Groups. For more information, see <a href="#">Adding a Sticky Group, page 9-6</a>.</li><li>• <b>Clear Sticky Groups</b>—Allows you to clear the field.</li></ul>

# Viewing Policy Nodes

Figure 7-3 Policy Node Window



**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Policies** in the Setup pane.

- Step 2** Select **Policies** from the object selector and click any of the policy nodes.
- Step 3** Click one of the following tabs, then proceed to the corresponding section for configuration information:
- [Conditions and Action, page 7-17](#)
  - [Virtual Servers, page 7-24](#)
- 

## Conditions and Action

Click on the **Conditions and Action** tab to see the various conditions and their actions. The Conditions tree displays the various conditions such as maps or client groups. The columns under the Conditions tree will change according to the map and client groups that you select.

When you click **Maps**, you can see a table with a summary of details of all the associated maps. You can associate the different types of maps when you click **Cookie Maps**, **Header Maps**, or **URL Maps** under **Maps**.

The following fields appear when you click **Maps**:

Column	Description
Map Type	Specifies if it is a cookie, header or a URL type map.
Map Name	Name of the map.
Number of Match Conditions	Specifies the total number of match conditions.



### Note

When you click the **Maps** tree, a list of maps and icons appears. The icons have a color status display; for example, the icons are white by default. When you associate a map, it turns green. This icon appears for all the three types of maps: Cookie, Header, and URL maps.

---

The following types of conditions are available:

- [Cookie Maps](#)
- [Header Maps](#)
- [URL Maps](#)
- [Client Group](#)

## Cookie Maps

From the **Conditions** tab, when you select **Cookie Maps** the following columns appear:

Column	Description
Cookie Map	<p>Name of the cookie map associated with the policy selected in the object selector.</p> <p>Click <input type="text" value="▽..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Cookie Map</b>—Opens the Select Cookie Map dialog box and allows you to select from a list of configured cookie maps.</li> <li>• <b>Create Cookie Map</b>—Opens the Create Cookie Map dialog box and allows you to create cookie maps. For more information on creating cookie maps, see <a href="#">Adding a Cookie Map, page 8-9</a>.</li> <li>• <b>Clear Cookie Map</b>—Allows you to clear the field.</li> </ul>
Cookie Name	Name of the cookie.
Cookie Value	Value of the cookie.


From this dialog box, you can do the following:

- Click **Add** to add new match conditions by entering the name and value.
- Click **Edit** to edit match conditions.
- Select a match condition and click **Delete** to delete it.



## Header Maps

From the **Conditions** tab, when you select **Header Maps** the following columns appear:

Column	Description
Header Map	Click  and select one of the following: <ul style="list-style-type: none"><li>• <b>Select Header Map</b>—Opens the Select Header Map dialog box and allows you to select from a list of configured header maps.</li><li>• <b>Create Header Map</b>—Opens the Create Header Map dialog box and allows you to create header maps. For more information, see <a href="#">Adding a Header Map, page 8-23</a>.</li><li>• <b>Clear Header Map</b>—Allows you to clear the field.</li></ul>
Header Name	Name of the header.
Header Value	Value of the header.

From this dialog box, you can do the following:

- Click **Add** to add new header maps and values by entering the name and value.
- Click **Edit** to edit the header maps and values.
- Select a row and click **Delete** to delete a header map.

## URL Maps

From the **Conditions** tab, when you select **URL Maps** the following columns appear:

Column	Description
URL Map	<p>Click <input type="button" value="v..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select URL Map</b>—Opens the Select URL Map dialog box and allows you to select from a list of configured URL maps.</li> <li>• <b>Create URL Map</b>—Opens the Create URL Map dialog box and allows you to create URL maps. For more information on creating URL maps, see <a href="#">Adding a URL Map, page 8-19</a>.</li> <li>• <b>Clear URL Map</b>—Allows you to clear the field.</li> </ul>
URL Method	Specifies the method in incoming HTTP requests.
URL	Specifies the URL in incoming HTTP requests.

From this dialog box, you can do the following:

- Click **Add** to add new URL expressions by entering the name and value.
- Click **Edit** to edit the URL expressions.
- Select a row and click **Delete** to delete a URL map.

## Client Group

From the **Conditions** tab, when you choose the **Client Group** the following columns appear:

Column	Description
Client Group	<p>Client group can be either standard access lists names or an ID from 1 to 99. Only one client group can be associated with a given SLB policy.</p> <p>Click <input type="text" value="▽..."/> and select one of the following:</p> <ul style="list-style-type: none"><li>• <b>Create Client Group</b>—Opens a dialog box and allows you to create Client Group by entering the Client Group ID.</li><li>• <b>Clear Client Group</b>—Allows you to clear the field.</li></ul>

## Action

The following tabs appear under the actions section when you select a policy:

- [Server Farms and Backup Server Farms](#)
- [Sticky Group](#)
- [Reverse Sticky Group](#)

## Server Farms and Backup Server Farms



### Note

You can configure a backup server farm only after you configure a server farm.

Click **Server Farms** and/or **Backup Server Farms** to view all the server farms and backup server farms that are associated to this policy.

The following columns appear:

Column	Description
Server Farm/Backup Server Farm	<p>You can choose one server farms and/or backup server farm to associate to the policy.</p> <p>Click <input type="button" value="v..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Server Farm</b>—Opens a dialog box and allows you to select from a list of configured server farms.</li> <li>• <b>Create Server Farm</b>—Opens the Add Server Farm dialog box and allows you to create server farms or backup server farms. For more information, see <a href="#">Adding Server Farms, page 5-5</a>.</li> <li>• <b>Clear Server Farm</b>—Allows you to clear the field.</li> </ul>
Real	Number of real servers configured in the server farm.
Local	Indicates if this real server is the SSL card.
Min. Connections	The minimum number of connections for the real server.
Max. Connections	The maximum number of connections for the real server.
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Lets you know if the status of the real server.

From this dialog box, you can do the following:

- Click **Add** and do one of the following:

- **Select Named Real Server**—Opens the Add Named Real Server dialog box and allows you to create a named real server. For more information, see [Adding a Named Real Server, page 5-23](#).
- **Create Unnamed Real Server**—Opens the Add Unnamed Real Server dialog box and allows you to create an unnamed real server. For more information, see [Adding an Unnamed Real Server, page 5-27](#).
- Select a real server and click **Edit** to edit the configuration values.
- Select a real server and click **Delete** to delete it.

For more information on server farms, see [Viewing Server Farms, page 5-3](#).

## Sticky Group

Click the **Sticky Groups** tab to view all the sticky groups that are associated to this policy.

The following columns appear:

Column	Description
Sticky Groups	<p>Number identifying the sticky group to which the virtual server belongs. The range is from 0 to 255.</p> <p>Click <input type="text" value="▽..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Sticky Groups</b>—Opens the Select Sticky Group dialog box and allows you to select from a list of configured Sticky Groups.</li> <li>• <b>Create Sticky Groups</b>—Opens the Add Sticky Group dialog box and allows you to create Sticky Groups. For more information on creating Sticky Groups, see <a href="#">Adding a Sticky Group, page 9-6</a>.</li> <li>• <b>Clear Sticky Groups</b>—Allows you to clear the field.</li> </ul>
Type	Type of Sticky Group.
Timeout	Time in seconds to wait before a connection is considered unreachable.

## Reverse Sticky Group

Click the **Reverse Sticky Groups** tab to view all the reverse Sticky Groups that are associated to this policy. To ensure that the CVDM-CSM changes its connections to the opposite direction and sends them back to the source, you can configure a reverse sticky group.

The following columns appear:

Column	Description
Reverse Sticky Groups	<p>Number identifying the sticky group to which the virtual server belongs. The range is from 0 to 255.</p> <p>Click <input type="text" value="▽..."/> and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Sticky Groups</b>—Opens the Select Sticky Group dialog box and allows you to select from a list of configured Sticky Groups.</li> <li>• <b>Create Sticky Groups</b>—Opens the Add Sticky Group dialog box and allows you to create Sticky Groups. For more information, see <a href="#">Adding a Sticky Group, page 9-6</a>.</li> <li>• <b>Clear Sticky Groups</b>—Allows you to clear the field.</li> </ul>
Type	Type of reverse sticky group.
Timeout	Time in seconds to wait before a connection is considered unreachable.

## Virtual Servers

Click the **Virtual Servers** tab to view the details of all the virtual servers to which the policy selected in the object selector is associated.

For more information on Virtual Servers, see [Viewing Virtual Servers, page 4-3](#).



## Managing Maps

---

You can configure maps to define multiple URLs, cookies, HTTP headers, and return codes as groups that can be associated when you configure a policy.

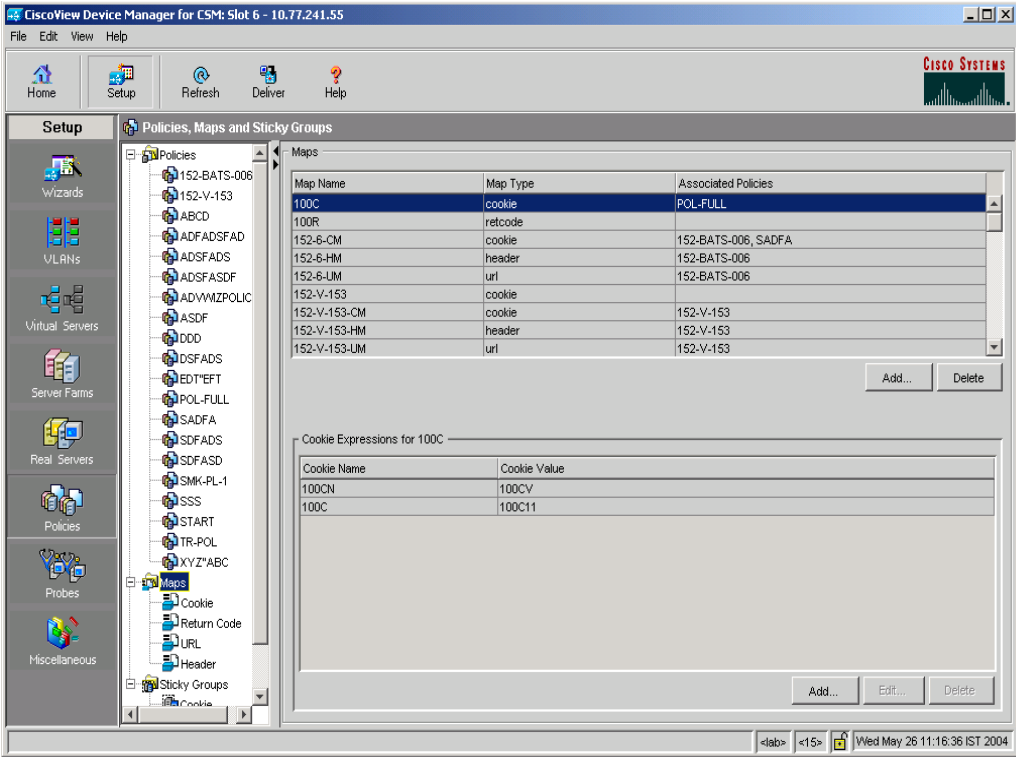
HTTP header insert allows CVDM-CSM to insert information such as the client's IP address into the HTTP header. This feature is useful when CVDM-CSM performs source NAT and the application on the server side requires client information.

This section contains the following topics:

- [Viewing Maps, page 8-2](#)
- [Adding a Map, page 8-7](#)
- [Viewing Cookie Maps, page 8-8](#)
- [Adding a Cookie Map, page 8-9](#)
- [Viewing Return Code Maps, page 8-11](#)
- [Adding a Return Code Map, page 8-13](#)
- [Adding and Editing Match Conditions for a Return Code Map, page 8-16](#)
- [Viewing URL Maps, page 8-18](#)
- [Adding a URL Map, page 8-19](#)
- [Viewing Header Maps, page 8-20](#)
- [Adding a Header Map, page 8-23](#)

# Viewing Maps

Figure 8-1 Maps Page



113851



You can view information about all maps on the device.

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Maps** from the object selector. A table appears, displaying the following columns.

Column	Description
Map Name	Displays the map name.
Map Type	Displays the type for the corresponding map name.
Associated Policies	Displays the associated policies for the map type.

From this main dialog box, you can do the following:

- Click **Add** under the Maps table to add a new map. For more information, see the [Adding a Map, page 8-7](#).
- Select a map and click **Delete** to delete an existing map.
- View a cookie map. For more information, see [Viewing Cookie Maps, page 8-8](#).
- View a return code map. For more information, see [Viewing Return Code Maps, page 8-11](#).
- View a URL map. For more information, see [Viewing URL Maps, page 8-18](#).
- View a header map. For more information, see [Viewing Header Maps, page 8-20](#).

The lower pane of the Map window displays the various match conditions of the selected map. The match conditions will differ according to the type of map that you select in the table.

- If you choose cookie map, the following columns appear:

Column	Description
Cookie Name	Name of the cookie.
Cookie Value	Value of the cookie.

From this dialog box, you can do the following:

- Click **Add** to add a cookie match conditions by entering the cookie name and value.
- Select a match condition and click **Edit** to edit cookie match conditions.
- Select a match condition and click **Delete** to delete the cookie match conditions.
- If you choose return code map, the following columns appear:

Column	Description
<b>Match Conditions</b>	
Lowest Return Code	The lowest return code.
Highest Return Code	The highest return code.

Column	Description
Action for Return Codes	Action for the return code. It can one of the following: <ul style="list-style-type: none"> <li>Count—Specifies the number of occurrences of return codes received.</li> <li>Log—Specifies where syslog messages are sent when a threshold is reached.</li> <li>Remove—Specifies where the syslog messages are sent when a threshold is reached and the server is removed from service.</li> </ul>
Return Code Instances	Instances of the return code.
Reset Time after Threshold	Number of seconds to wait before the processing can resume.

From this dialog box, you can do the following:

- Click **Add** to add match conditions. For more information, see [Adding and Editing Match Conditions for a Return Code Map, page 8-16](#).
- Select a match condition and click **Edit** to edit match conditions for return code maps.
- Select a match condition and click **Delete** to delete the match conditions for return code maps.
- If you choose URL Map, the following columns appear:

Column	Description
URL Method	Specifies the method in incoming HTTP requests.
URL	Specifies the URL in incoming HTTP requests.

From this dialog, you can do the following:

- Click **Add** to add URL expressions and enter the URL method and URL.
- Select a URL expression and click **Edit** to edit URL expressions.
- Select a URL expression and click **Delete** to delete it.
- If you choose header map, the following columns appear:

Column	Description
<b>Header Name</b>	Name of the generic field in the HTTP header.
<b>Header Value</b>	Header value string to insert in the request.

From this dialog box, you can access functions to do the following:

- Click **Add** to add header match conditions by entering the cookie name and value.
- Select a header match condition and click **Edit** to edit header match conditions.
- Select a header match condition and click **Delete** to delete the header match condition.

# Adding a Map

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Maps** from the object selector.

**Step 3** Click **Add**. The Add map dialog box appears, displaying the following columns.

Column	Description
Map Type	Specify the map type. The map types are cookie, header, URL, and return code.
Map Name	Enter the map name.

The fields will differ according to the type of map that you select in the table.

## Related Topics

- [Adding a Cookie Map, page 8-9](#)
- [Adding a Return Code Map, page 8-13](#)
- [Adding a URL Map, page 8-19](#)
- [Adding a Header Map, page 8-23](#)

# Viewing Cookie Maps

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Maps > Cookie Maps** from the object selector. The Cookie Map table appears, displaying the following columns.

Column	Description
Map Name	Enter the map name.
Associated Policies	The policy associated to the cookie map.

**Step 3** When you select a map, the following columns appear in the Cookie Expressions pane:

Column	Description
Cookie Name	Name of the cookie map.
Cookie Value	Value of the cookie map.

From the Cookie Map dialog box, you can do the following:

- Click **Add** to add a new cookie map. For more information, see [Adding a Cookie Map, page 8-9](#).
- Select a row and click **Delete** to delete a cookie map.
- Click **Edit** to edit the cookie value.

From the Cookie Expressions dialog box, you can do the following:

- Click **Add** to add a cookie match conditions by entering the cookie name and value.
- Select a match condition and click **Edit** to edit cookie match conditions.
- Select a match condition and click **Delete** to delete the cookie match conditions.

## Adding a Cookie Map

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Maps > Cookie Maps** from the object selector.

**Step 3** Click **Add**. The Add Cookie Map dialog box appears, displaying the following columns.

Column	Description
Cookie Map Name	Enter the cookie map name.

- Step 4** To add the match conditions for the cookie map, click **Add**. The Match Conditions page appears, displaying the following columns.

Column	Description
Cookie Name	Enter a name for the cookie.
Cookie Value	Enter a value for the cookie.

**Note**

The cookie map can have a maximum of five match conditions.

From this dialog box, you can select a cookie map and click **Delete** to delete it.



# Viewing Return Code Maps

Return code maps are used for return code error checking.

- 
- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Policies** in the Setup pane.
- Step 2** Select **Maps > Return Code Map** from the object selector. A table appears, displaying the following columns.

Column	Description
Map Name	Name of the map.
Associated Server Farms	Server Farms associated with the map.

- Step 3** When you select a return code map, the following details appear in the Match Condition pane:

Column	Description
Lowest Return Code	<p>The lowest return code.</p> <p><b>Note</b> You cannot configure overlapping return codes.</p>
Highest Return Code	<p>The highest return code. Maximum number of return codes that can be configured is 100.</p> <p><b>Note</b> You cannot configure overlapping return codes.</p> <p>For example, if you are already using 100-116,200-216, you cannot configure more than <math>(100 - (116-100+1)) - (216-200_1) = 66</math>. You are limited to 300 - 365. If you add 300 - 366, an error message will appear.</p>
Action for Return Codes	<p>Action for the return code. It can one of the following:</p> <ul style="list-style-type: none"> <li>• Count—Specifies the number of occurrences of return codes received.</li> <li>• Log—Specifies where syslog messages are sent when a threshold is reached.</li> <li>• Remove—Specifies where the syslog messages are sent when a threshold is reached and the server is removed from service.</li> </ul>
Return Code Instances	Instances of the return code.
Reset Time after Threshold	Number of seconds to wait before the processing can resume.

From the return code map dialog box, you can do the following:

- Click **Add** to add a new return code map. For more information, see [Adding a Return Code Map, page 8-13](#).
- Select a row and click **Delete** to delete a return code map.

From the Match Condition pane, you can do the following:

- Click **Add** to add match conditions. For more information, see [Adding and Editing Match Conditions for a Return Code Map, page 8-16](#).
- Select a match condition and click **Delete** to delete the match condition.

## Adding a Return Code Map

- 
- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Policies** in the Setup pane.
- Step 2** Select **Maps > Return Code Map** from the object selector.
- Step 3** Click **Add**. The Add Return Code Map dialog box appears, displaying the following columns.

Column	Description
Map Name	<p>Enter a map name.</p> <p>Click <b>Add</b> to add match conditions.</p> <p>For more information, see <a href="#">Adding and Editing Match Conditions for a Return Code Map, page 8-16</a>.</p>
Lowest Return Code	<p>Enter the lowest return code.</p> <p><b>Note</b> You cannot configure overlapping return codes.</p>
Highest Return Code	<p>Enter the highest return code.</p> <p>Maximum number of return codes that can be configured is 100.</p> <p><b>Note</b> You cannot configure overlapping return codes.</p> <p>For example, if you are already using 100-116,200-216, you cannot configure more than <math>(100 - (116-100+1)) - (216-200_1) = 66</math>. You are limited to 300 - 365. If you add 300 - 366, an error message will appear.</p>
Action for Return Codes	<p>The action for the return code. It can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Count</b>—Specifies the number of occurrences of return codes received.</li> <li>• <b>Log</b>—Specifies where syslog messages are sent when a threshold is reached.</li> <li>• <b>Remove</b>—Specifies where the syslog messages are sent when a threshold is reached and the server is removed from service.</li> </ul>

Column	Description
Return Code Instances	Enter the instances of the return code. This feature is enabled if you select <b>log</b> or <b>remove</b> .
Return Code Reset	Select this checkbox to enable reset.
Reset Time after Threshold	Number of seconds to wait before the processing can resume.

From this dialog box, you can do the following:

- Click **Add** to add match conditions. For more information, see [“Adding and Editing Match Conditions for a Return Code Map”](#) section on page 8-16.
- Select a row and click **Delete** to delete a match condition.

# Adding and Editing Match Conditions for a Return Code Map

---

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Policies** in the Setup pane.
- Step 2** Select **Maps > Return Code Map** from the object selector.
- Step 3** Click **Add**. The Add Return Code Map dialog box appears.
- Step 4** Click **Add** in the dialog box to add match conditions for the selected type of return code map. The Match Conditions for Return Code Maps dialog box appears, displaying the following columns.

Column	Description
Lowest Return Code	Enter the lowest return code.  <b>Note</b> You cannot configure overlapping return codes.
Highest Return Code	Enter the highest return code. Maximum number of return codes that can be configured is 100.  <b>Note</b> You cannot configure overlapping return codes.  For example, if you are already using 100-116,200-216, you cannot configure more than $(100 - (116-100+1)) - (216-200_1) = 66$ . You are limited to 300 - 365. If you add 300 - 366, an error message will appear.
Action for Return Code	The action for the return code. It can be one of the following: <ul style="list-style-type: none"> <li>• Count—Specifies the number of occurrences of return codes received.</li> <li>• Log—Specifies where syslog messages are sent when a threshold is reached.</li> <li>• Remove—Specifies where the syslog messages are sent when a threshold is reached and the server is removed from service.</li> </ul>
Return Code Instances	Enter the instances of the return code.
Return Code Reset	Select this check box to enable reset time after threshold.
Reset Time after Threshold	Enter the number of seconds to wait before the processing can resume.

## Viewing URL Maps

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Maps > URL Maps** from the object selector. The following fields appear:

Column	Description
Map Name	The name of the map
Associated Policies	Policies associated with the map.

**Step 3** When you select a map, the match conditions for the map appears:

Column	Description
URL Method	Specifies the URL Method to match.
URL	Specifies the URL associated with the map.

From the URL Map dialog box, you can do the following:

- Click **Add to** add a new URL Map. For more information, see [Adding a URL Map, page 8-19](#).
- Select a row and click **Delete** to delete a URL Map.

From the Match Conditions pane, you can do the following:

- Click **Add** to add match conditions by specifying the URL method and URL. For more information, see [Adding a URL Map, page 8-19](#).



- Select a URL expression and click **Edit** to edit the match conditions to edit the URL.
- Select a URL expression and click **Delete** to delete a match condition.

## Adding a URL Map

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Maps > URL Maps** from the object selector.

**Step 3** Click **Add**. The Add URL Map dialog box appears, displaying the following columns:

Column	Description
URL Map Name	Enter the URL map name.

**Step 4** To add the match conditions for the URL map, click **Add**. The Add URL Conditions dialog box appears, displaying the following columns.

Column	Description
URL Method	Click <input type="text" value="▽..."/> and from the list, select or enter a URL method to match.
URL	Enter the URL associated with the map.

# Viewing Header Maps

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Maps > Header Maps** from the object selector. The Header Maps table appears, displaying the following columns:

Column	Description
Map Name	The name of the header map.
Associated Policies	The policies associated with the header map.

**Step 3** When you select a header map, the following columns appear in the Match Conditions/Insert Conditions pane:

Column	Description
Header Name	Name of the generic field in the HTTP header.
Header Value	Header value string to insert in the request.

When receiving an HTTP request, you can specify the name of the field and the corresponding value for the CVDM-CSM to match.

**Note**

---

CVDM-CSM allows you to specify one or more fields in the HTTP header for policy matching. When you configure multiple fields in a single HTTP header group, all of the expressions in this group must match in order to satisfy this criteria.

---

For more information on HTTP Header Insert, see [HTTP Header Insert, page 8-22](#).

From this dialog box, you can do the following:

- Click **Add** to add a new header map. For more information, see [Adding a Header Map, page 8-23](#).
- Select a map and click **Delete** to delete a header map.
- Click **Add** under the Match Conditions/Insert Conditions pane, to add match condition by entering the header name and value. For more information, see [Adding a Header Map, page 8-23](#).
- Click **Edit** under the Match Conditions/Insert Conditions pane to edit the match conditions.
- Select a match condition, and click **Delete** under the Match Conditions/Insert Conditions pane, to delete a match condition.

## HTTP Header Insert

The HTTP header insert feature provides CVDM-CSM with the ability to insert information, such as the client's IP address, into the HTTP header. This is useful when CVDM-CSM performs source NAT and the application on the server side requires client information.

Specify the header name and value to insert information into the HTTP header. You can also use the `%is` and `%id` special parameters for header values. The `%is` value inserts the source IP into the HTTP header and the `%id` value inserts the destination IP into the header. You can specify each special parameter once per header map.



---

**Note** A header map may contain multiple insert headers. If you insert header values that are made of multiple keywords that includes spaces, you must use double quotes around the entire expression.

---

# Adding a Header Map

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
  - Or:
  - Click **Setup** from the task bar and click **Policies** in the Setup pane.
- Step 2** Select **Maps > Header Maps** from the object selector.
- Step 3** Click **Add**. The Add header map dialog box appears.

Column	Description
Header Map Name	Enter a header name.

- Step 4** Do one of the following:
- Click the **Match Conditions** tab. A table appears, displaying the following. When receiving an HTTP request, you can specify the name of the field and the corresponding value for the CVDM-CSM to match.



**Note** CVDM-CSM allows you to specify one or more fields in the HTTP header for policy matching. When you configure multiple fields in a single HTTP header group, all of the expressions in this group must match in order to satisfy this criteria.

Column	Description
Header Name	Name of the generic field in the HTTP header.
Header Value	Header value string to insert in the request.

From this dialog box, you can do the following:

- Click **Add** to add match conditions. The Add Header Insert Conditions dialog box appears and allows you to enter the header name and value
- Select a match condition and click **Delete** to delete it.
- Click the **Insert Conditions** tab. A table appears, displaying the following.

Column	Description
Header Name	Name of the generic field in the HTTP header.
Header Value	Header value string to insert in the request.

For more information on HTTP Header Insert, see [HTTP Header Insert, page 8-22](#).

From this dialog box, you can do the following:

- Click **Add** to add match conditions. The Add Header Match Conditions dialog box appears and allows you to enter the header name and value.
- Select a match condition and click **Delete** to delete it.



## Managing Sticky Groups

---

Sticky connections limit traffic to individual servers by allowing multiple connections from the same client to stick to the same real server using source IP addresses, source IP subnets, cookies, and the secure socket layer (SSL) or by redirecting these connections using HTTP redirect messages.

Configuring a sticky group involves configuring the attributes of that group and associating it with a policy. This ensures that connections from the same client matching the same policy use the same real server. The default sticky time value is 1440 minutes (24 hours).

Session persistence (or stickiness) refers to the functionality of sending multiple (simultaneous or subsequent) connections from the same client consistently to the same server. This is a typical requirement in certain load balancing environments.

The CVDM-CSM can uniquely identify clients and perform stickiness with the following methods:

- **Cookie sticky, offset and length**—Allows you to configure a specific cookie name and automatically learn its value either from the client request HTTP header or from the server Set Cookie message.  
By default CVDM-CSM learns the entire cookie value, this feature enables CVDM-CSM to learn only a portion of the cookie value.
- **Cookie insert**—Allows the CVDM-CSM to insert a cookie in the Set-Cookie header of the HTTP response. This enables cookie sticky even when the servers are not configured to set cookies. The cookie contains information that the CVDM-CSM uses to ensure persistence to a specific real server.

This section contains the following topics:

- [Viewing Sticky Groups, page 9-3](#)
- [Viewing Cookie Sticky Groups, page 9-8](#)
- [Viewing Header Sticky Groups, page 9-13](#)
- [Viewing SSL Sticky Groups, page 9-22](#)
- [Viewing Netmask Sticky Groups, page 9-18](#)

**Note**

---

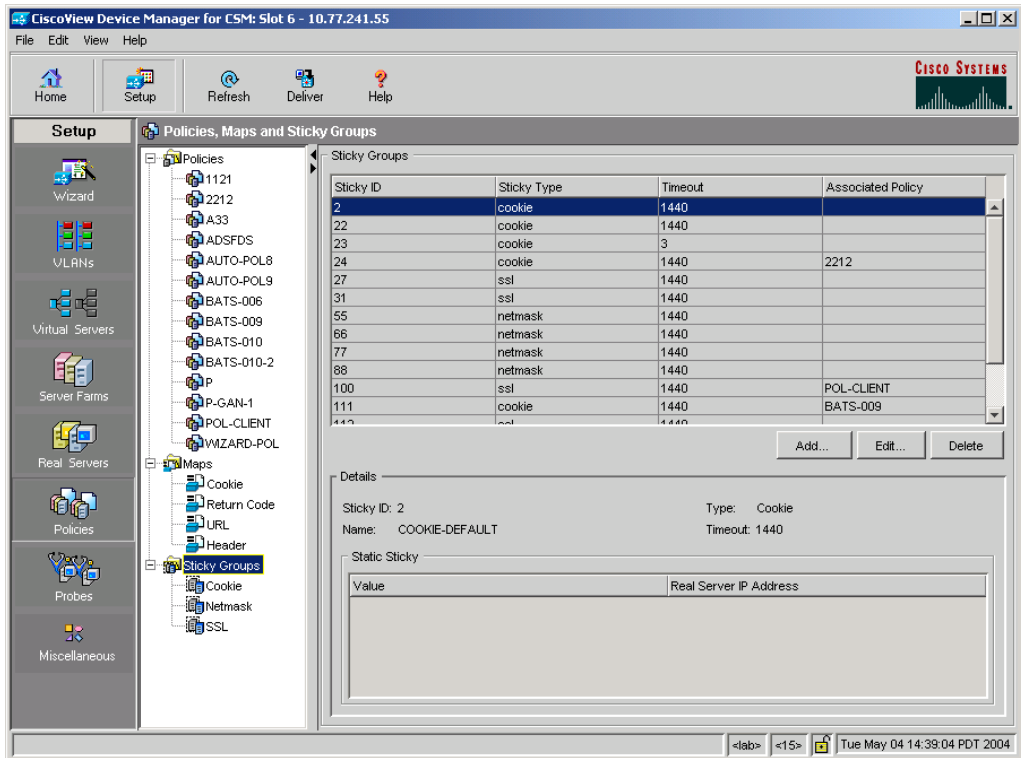
You can view Header Sticky Groups only in 12.2(18)SXD1 and later IOS versions.

---



# Viewing Sticky Groups

Figure 9-1 Sticky Groups Page



You can view the existing configuration details in the configuration dialog box and edit the specified fields.

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Sticky Groups** from the object selector. The Sticky Group table appears, displaying the following columns:

Column	Action/Description
Sticky ID	ID of the sticky group to which the virtual server belongs.
Sticky Type	Type of sticky group. The different types are: <ul style="list-style-type: none"> <li>• Cookie</li> <li>• Header</li> <li>• SSL</li> <li>• Netmask</li> </ul>
Timeout	Specifies the sticky timer duration (in minutes).
Associated Policy	The list of policies to which this sticky group is associated.

**Step 3** When you select any row, the configuration details of the corresponding sticky group appears, displaying the following columns:

Column	Action/Description
Sticky ID	A unique ID for the sticky group.
Name	Name of the sticky group attached to the Sticky ID value.
Type	Type of sticky group. The different types are: <ul style="list-style-type: none"> <li>• Cookie</li> <li>• Header</li> <li>• SSL</li> <li>• Netmask</li> </ul>
Timeout	Specifies the sticky timer duration (in minutes).
Offset	Specifies the byte offset count.
Length	Specifies the length of the portion of the cookie.
<b>Static Sticky</b>	

Column	Action/Description
Value	Value of the static sticky.
Real Server IP Address	IP address of the real server.

- Step 4** Select **Cookie**, **SSL**, **Header** or **Netmask** from the object selector under **Sticky Groups**, to view the configuration details of the corresponding sticky group.

From the Sticky Group dialog box, you can do the following:

- Click **Add** to add a new sticky group. For more information, see [“Adding a Sticky Group” section on page 9-6](#).
- Click **Edit** to edit a sticky group. For more information, see [“Editing a Sticky Group” section on page 9-7](#).

#### Related Topics

- [Viewing Cookie Sticky Groups, page 9-8](#)
- [Viewing Header Sticky Groups, page 9-13](#)
- [Viewing SSL Sticky Groups, page 9-22](#)
- [Viewing Netmask Sticky Groups, page 9-18](#)

## Adding a Sticky Group

---

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Sticky Groups** from the object selector.

**Step 3** Click **Add**. The Add Sticky Group dialog box appears.

The columns that appear in the dialog box will vary according to the type of sticky group that you choose.

---

### Related Topics

- [Adding a Cookie Sticky Group, page 9-10](#)
- [Adding a Header Sticky Group, page 9-15](#)
- [Adding a Netmask Sticky Group, page 9-20](#)
- [Adding an SSL Sticky Group, page 9-23](#)

## Editing a Sticky Group

---

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Sticky Groups** from the object selector.

**Step 3** Click **Edit** or double click the selected sticky group to edit its configuration details. The Edit Sticky Group dialog box appears.

The columns that appear in the dialog box will vary according to the type of sticky group that you choose.

---

### Related Topics

- [Editing a Cookie Sticky Group, page 9-11](#)
- [Editing a Header Sticky Group, page 9-16](#)
- [Editing a Netmask Sticky Group, page 9-21](#)
- [Editing an SSL Sticky Group, page 9-24](#)

# Viewing Cookie Sticky Groups

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Sticky Groups > Cookies** from the object selector. The Cookie Sticky Group table appears, displaying the following columns.

Column	Action/Description
Sticky ID	ID of the sticky group to which the virtual server belongs.
Timeout	Specifies the sticky timer duration (in minutes).
Associated Policy	The list of policies to which this sticky group is associated.

**Step 3** When you select any row, the configuration details of the corresponding cookie sticky group appears in the Details pane, displaying the following columns:

Column	Action/Description
Sticky ID	The unique ID of the sticky group.
Type	Type of sticky group. Here it would be Cookie.
Name	Name of the cookie sticky group.
Timeout	Specifies the sticky timer duration (in minutes).
Secondary Cookie Name	The secondary name of the sticky group attached to the sticky ID value.
Insert Cookie	The cookie insert feature allows the CVDM-CSM to insert a cookie in the Set-Cookie header of the header response.
Offset	Specifies the byte offset count.
Length	Specifies the length of the portion of the cookie.
<b>Static Sticky</b>	
Value	Value of the static sticky.
Real Server IP Address	IP address of the real server.

From the Cookie Sticky Group dialog box, you can do the following:

- Click **Add** to add a new cookie sticky group. For more information, see [Adding a Cookie Sticky Group, page 9-10](#).
- Select a cookie sticky group and click **Edit** to edit its configuration details. For more information, see [Editing a Cookie Sticky Group, page 9-11](#).
- Select a cookie sticky group and click **Delete** to delete it.

## Adding a Cookie Sticky Group

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
  - Or:
  - Click **Setup** from the task bar and click **Policies** in the Setup pane.
- Step 2** Select **Sticky Groups > Cookies** from the object selector.
- Step 3** Click **Add** to add a new cookie sticky group. The Add Sticky Group dialog box appears, displaying the following columns.

Column	Action/Description
Sticky ID	Enter the ID of the sticky group to which the virtual server belongs.
Name	Enter the name of the cookie sticky group.
Timeout	Enter the sticky timer duration (in minutes).
Secondary Cookie Name	Enter the secondary name of the sticky group attached to the Sticky ID value.
Insert Cookie	Select the check box to allow the CVDM-CSM to insert a cookie in the Set-Cookie header of the header response.
Offset/Length	Select the check box to enable the Offset and Length fields.
Offset	Specify the byte offset count.
Length	Specify the length of the portion of the cookie.
<b>Static Sticky</b>	
Value	Enter the value of the static sticky.
Real Server IP Address	IP address of the real server.



From this dialog box, you can do the following:

- Click **Add** to add a static sticky by entering the value and real server IP address.
- Select a row and click **Delete** to delete a static route.

## Editing a Cookie Sticky Group

- 
- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Policies** in the Setup pane.
- Step 2** Select **Sticky Groups > Cookies** from the object selector.
- Step 3** Click **Edit** to edit a cookie Sticky Group. The Edit Sticky Group dialog box appears, displaying the following columns.

Column	Action/Description
Sticky ID	Unique ID of the sticky group to which the virtual server belongs.
Name	Enter the name of the cookie sticky group.
Type	Type of sticky group. Here it will be Cookie.
Timeout	Enter the sticky timer duration (in minutes).
Secondary Cookie Name	Enter the secondary name of the sticky group attached to the Sticky ID value.
Insert Cookie	Select the check box to allow the CVDM-CSM to insert a cookie in the Set-Cookie header of the header response.
Offset/Length	Select the check box to enable the Offset and Length fields.
Offset	Specify the byte offset count.
Length	Specify the length of the portion of the cookie.
<b>Static Sticky</b>	
Value	Specify the value of the static sticky.
Real Server IP Address	IP address of the real server.

From this dialog box, you can do the following:

- Click **Add** to add a static sticky by entering the value and real server IP address.
- Select a row and click **Delete** to delete a static route.

# Viewing Header Sticky Groups

**Note**

You can view Header Sticky Groups only in 12.2(18)SXD1 and later IOS versions.

**Step 1**

Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or:

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2**

Select **Sticky Groups > Header** from the object selector. The Header Sticky Group table appears, displaying the following columns:

Column	Description
Sticky ID	Unique ID of the header Sticky Group.
Timeout	Specifies the sticky timer duration (in minutes).
Associated Policy	The list of policies to which this sticky group is associated.

**Step 3**

When you select any row, the configuration details of the corresponding header sticky group appears, displaying the following columns.

Field	Description
Sticky ID	Unique ID of the header Sticky Group.
Type	Type of sticky group. Here it will be header.
Name	Enter the name of the header sticky group.
Timeout	Specifies the sticky timer duration (in minutes).
Offset	Specify the byte offset count.
Length	Specify the length of the HTTP header.
<b>Static Sticky</b>	
Value	Value of the static sticky.
Real Server IP Address	IP address of the real server.

From the Header Sticky Group dialog box, you can do the following:

- Click **Add** to add a new header Sticky Group. For more information, see the [Adding a Header Sticky Group](#).
- Click **Edit** to edit a header Sticky Group. For more information, see the [Editing a Header Sticky Group](#).
- Select a header Sticky Group and click **Delete** to delete it.

## Adding a Header Sticky Group


**Note**

You can view Header Sticky Groups only in 12.2(18)SXD1 and later IOS versions.

**Step 1**

Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2**

Select **Policies > Sticky Groups > Header** from the object selector.

**Step 3**

Click **Add** to create a new header Sticky Group. The Add Sticky Group dialog box appears, displaying the following columns.

Column	Description
Sticky ID	Enter the ID of the header Sticky Group.
Name	Enter the name of the header sticky group.
Timeout	Enter the sticky timer duration (in minutes).
Offset/Length	Select the check box to enable the Offset and Length fields.
Offset	Specify the byte offset count.
Length	Specify the length of the HTTP header.
<b>Static Sticky</b>	
Value	Value of the static sticky.
Real Server IP Address	IP address of the real server.

From this dialog box, you can do the following:

- Click **Add** to add a static sticky by entering the value and real server IP address.
- Select a row and click **Delete** to delete a static sticky.

## Editing a Header Sticky Group

**Note**

---

You can view Header Sticky Groups only in 12.2(18)SXD1 and later IOS versions.

---

- 
- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Policies** in the Setup pane.
- Step 2** Select **Sticky Groups > Header** from the object selector.
- Step 3** Click **Edit** to edit a header sticky group. The Edit Sticky Group dialog box appears, displaying the following columns:

Field	Description
Sticky ID	ID of the header sticky group.
Name	Enter the name of the header sticky group.
Timeout	Enter the sticky timer duration (in minutes).
Offset/Length	Select the check box to enable the Offset and Length fields.
Offset	Specify the byte offset count.
Length	Specify the length of the HTTP header.
<b>Static Sticky</b>	
Value	Value of the static sticky.
Real Server IP Address	IP address of the real server.

From this dialog box, you can do the following:

- Click **Add** to add a static sticky by entering the value and real server IP address.
- Select a row and click **Delete** to delete a static sticky.

# Viewing Netmask Sticky Groups

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Sticky Groups > Netmask** from the object selector. The Netmask Sticky Group dialog box appears, displaying the following columns:

Column	Action/Description
Sticky ID	ID of the netmask sticky group.
Timeout	Specifies the sticky timer duration (in minutes).
Associated Policy	The list of policies to which this sticky group is associated.

**Step 3** When you select a netmask sticky group, its the configuration details appears, displaying the following columns:



Column	Action/Description
Sticky ID	ID of the netmask sticky group.
Type	Type of sticky group. Here it will be Netmask.
Timeout	Specifies the sticky timer duration (in minutes).
Mask Type	It can be one of the following: <ul style="list-style-type: none"> <li>• Source</li> <li>• Destination</li> <li>• Both</li> </ul>
Mask	Specifies the type of IP mask to be applied. It can be Class A, Class B, Class C, or Class D mask.  If it is not specified, the default for network mask is 255.255.255.255.
Timeout	Specifies the sticky timer duration (in minutes).
<b>Static Sticky</b>	
Source IP	IP address of the source.
Destination IP	IP address of the destination.
Real Server IP	IP address of the real server.

From this dialog box, you can do the following:

- Click **Add** to add a netmask sticky group. For more information, see [Adding a Netmask Sticky Group, page 9-20](#).
- Click **Edit** to edit a netmask sticky group. For more information, see [Editing a Netmask Sticky Group, page 9-21](#).
- Select a netmask sticky group and click **Delete** to it.

## Adding a Netmask Sticky Group

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
  - Or:
  - Click **Setup** from the task bar and click **Policies** in the Setup pane.
- Step 2** Select **Sticky Groups > Netmask** from the object selector.
- Step 3** Click **Add** to add a new netmask sticky group. The Add Sticky Group dialog box appears, displaying the following columns:

Column	Action/Description
Sticky ID	Enter the ID of the netmask sticky group.
Mask Type	From the list, select source, destination or both.
Mask	Specify the type of IP mask to be applied. It can be Class A, Class B, Class C, or Class D mask.  If it is not specified, the default for network mask is 255.255.255.255.
Timeout	Specifies the sticky timer duration (in minutes).
<b>Static Sticky</b>	
Source IP	IP address of the source.
Destination IP	IP address of the destination.
Real Server IP	IP address of the real server.

From this dialog box, you can do the following:

- Click **Add** to add a static sticky by entering the source IP address, destination IP address and the real server IP address.
- Select a row and click **Delete** to delete a static sticky.

## Editing a Netmask Sticky Group

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
  - Or:
  - Click **Setup** from the task bar and click **Policies** in the Setup pane.
- Step 2** Select **Sticky Groups > Netmask** from the object selector.
- Step 3** Click **Edit** to edit a netmask sticky group. The Edit Sticky Group dialog box appears, displaying the following columns.

Column	Action/Description
Sticky ID	ID of the netmask sticky group.
Type	Type of sticky group. Here it will be netmask.
Mask Type	From the list, select source, destination or both.
Mask	Specify the type of IP mask to be applied. It can be Class A, Class B, Class C, or Class D masks. If it is not specified, the default for network mask is 255.255.255.255.
Timeout	Specifies the sticky timer duration (in minutes).
<b>Static Sticky</b>	
Source IP	IP address of the source.
Destination IP	IP address of the destination.
Real Server IP	IP address of the real server.

From this dialog box, you can do the following:

- Click **Add** to add a static sticky by entering the source IP address, destination IP address and the real server IP address.
- Select a row and click **Delete** to delete a static sticky.

# Viewing SSL Sticky Groups

**Step 1** Do one of the following:

- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.

Or

- Click **Setup** from the task bar and click **Policies** in the Setup pane.

**Step 2** Select **Sticky Groups > SSL** from the object selector. The SSL Sticky Group dialog box appears, displaying the following columns:

Column	Action/Description
Sticky ID	ID of the sticky group to which the virtual server belongs.
Timeout	Specifies the sticky timer duration (in minutes).
Associated Policy	The list of policies to which this sticky group is associated.

**Step 3** When you select any row, the configuration details of the corresponding SSL sticky group appears, displaying the following columns:

Column	Action/Description
Sticky ID	ID of the SSL sticky group.
Type	Type of sticky group. Here it will be SSL.
Timeout	Specifies the sticky timer duration (in minutes).
<b>Static Sticky</b>	
SSL ID	ID of the SSL map.
Real Server IP Address	IP address of the real server.

From the SSL sticky group dialog box, you can do the following:

- Click **Add** to add a new SSL sticky group. For more information, see [Adding an SSL Sticky Group, page 9-23](#).
- Click **Edit** to edit an SSL sticky group. For more information, see [Editing an SSL Sticky Group, page 9-24](#).
- Select a row and click **Delete** to delete SSL sticky group.

## Adding an SSL Sticky Group

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
- Or:
- Click **Setup** from the task bar and click **Policies** in the Setup pane.
- Step 2** Select **Sticky Groups > SSL** from the object selector.
- Step 3** Click **Add** to add a new SSL sticky group. The Add Sticky Group dialog box appears, displaying the following columns.

Column	Action/Description
Sticky ID	Enter the ID of the SSL sticky group.
Timeout	Specifies the sticky timer duration (in minutes).
<b>Static Sticky</b>	
SSL ID	ID of the SSL map.
Real Server IP Address	IP address of the real server.

From this dialog box, you can do the following:

- Click **Add** to add a static sticky by entering the SSL ID and real server IP address.
- Select a row and click **Delete** to delete the static route.

## Editing an SSL Sticky Group

- Step 1** Do one of the following:
- Click **Home** at the top of the window and click **Policies** under **Services Dashboard**.
  - Or
  - Click **Setup** from the task bar and click **Policies** in the Setup pane.
- Step 2** Select **Sticky Groups > SSL** from the object selector.
- Step 3** Click **Edit** to edit a SSL sticky group. The Edit Sticky Group dialog box appears, displaying the following columns.

Column	Action/Description
Sticky ID	ID associated with the SSL sticky group.
Type	Type of sticky group. Here it will be SSL.
Timeout	Specifies the sticky timer duration (in minutes).
<b>Static Sticky</b>	
SSL ID	ID of the SSL map.
Real Server IP Address	IP address of the real server.

From this dialog box, you can do the following:

- Click **Add** to add a static sticky by entering the SSL ID and real server IP address.
- Select a row and click **Delete** to delete a static sticky.



## Managing Probes

---

CVDM-CSM lets you monitor real servers and server farms using probes to determine if the real servers are operational. CVDM-CSM supports a variety of probe types that monitor real servers, such as HTTP, FTP, SMTP, TELNET, TCP, UDP, ICMP and Script probes.

You can configure probes by specifying the probe name and type. After configuring a probe, you must associate it with a server farm for the probe to take effect. You can associate single or multiple probes with a server farm. All servers in the server farm receive probes of the probe types that are associated with that server farm. You can associate one or more probe types with a server farm.

If a real server fails to reply after a specified number of consecutive retries, you will be notified and CVDM-CSM will adjust the incoming connections accordingly. Probes will continue to monitor failed servers until they become active again.

To support a more flexible health-probing functionality, you can upload and execute Toolkit Command Language (TCL) scripts on the CVDM-CSM. You can create a script probe that the CVDM-CSM periodically executes for each real server in any server farm associated with a probe. Depending upon the exit code of such a script, the real server is considered healthy, suspect, or failed. Probe scripts test the health of a real server by creating a network connection to the server, sending data to the server, and checking the response.

This section contains the following topics:

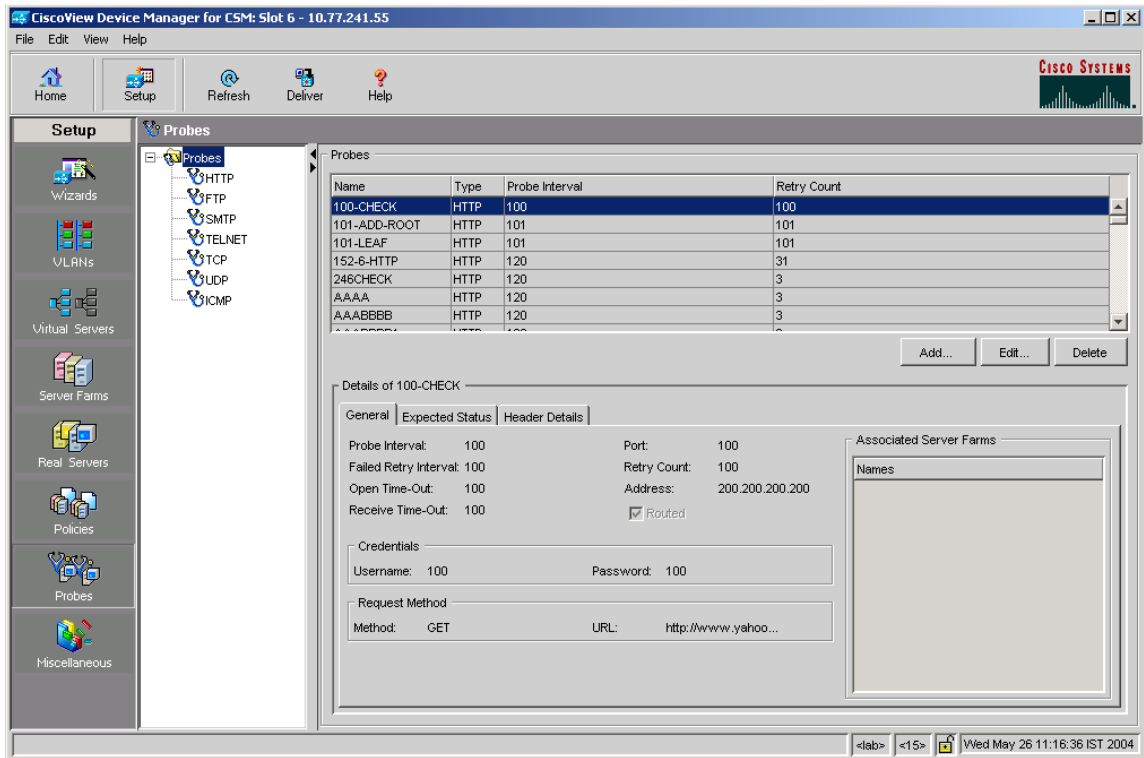
- [Viewing Probes, page 10-3](#)
- [Adding Probes, page 10-5](#)
- [Editing Probes, page 10-6](#)

- [Viewing HTTP Probes, page 10-7](#)
- [Viewing FTP Probes, page 10-18](#)
- [Viewing SMTP Probes, page 10-23](#)
- [Viewing TELNET Probes, page 10-29](#)
- [Viewing TCP Probes, page 10-36](#)
- [Viewing UDP Probes, page 10-40](#)
- [Viewing ICMP Probes, page 10-44](#)
- [Viewing Script Probes, page 10-48](#)



# Viewing Probes

Figure 10-1 Probes Page



You can view information about all probes on the device.

- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Probes** in the Setup pane. The Probes dialog box appears, displaying the following columns.

Column	Action/Description
Name	Name of the probe.
Type	Type of probe. The different types are HTTP, FTP, SMTP, TELNET, TCP, UDP, ICMP, and Script.
Probe Interval	Time (in seconds) between the probes.
Retry Count	Number of probe attempts to wait for before marking a server as failed.
Details	The details of the selected probe appear.

From this dialog box, you can do the following:

- Click **Add** to add probes. For more information, see [Adding Probes, page 10-5](#).
- Click **Edit** to add probes. For more information, see [Editing Probes, page 10-6](#).
- Select a probe, then click **Delete** to delete it.

#### Related Topics

- [Viewing HTTP Probes, page 10-7](#)
- [Viewing FTP Probes, page 10-18](#)
- [Viewing SMTP Probes, page 10-23](#)
- [Viewing TELNET Probes, page 10-29](#)
- [Viewing TCP Probes, page 10-36](#)
- [Viewing UDP Probes, page 10-40](#)
- [Viewing ICMP Probes, page 10-44](#)
- [Viewing Script Probes, page 10-48](#)

# Adding Probes

- 
- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Probes** in the Setup pane. A table with details of all configured probes appears.
- Step 3** Click **Add**. The Add Probes dialog box appears.

In the **Type** field, choose the type of probe which you want to add. The fields in the pane change according to the type of probe.

Possible probe types are:

- HTTP
- FTP
- SMTP
- TELNET
- TCP
- UDP
- ICMP
- Script

---

## Related Topics

- [Adding HTTP Probes, page 10-12](#)
- [Adding FTP Probes, page 10-20](#)
- [Adding SMTP Probes, page 10-26](#)
- [Adding TELNET Probes, page 10-32](#)
- [Adding TCP Probes, page 10-38](#)
- [Adding UDP Probes, page 10-42](#)
- [Adding ICMP Probes, page 10-46](#)
- [Adding Script Probes, page 10-50](#)

# Editing Probes

- 
- Step 1** Click **Setup** from the task bar.
- Step 2** Click **Probes** in the Setup pane. A table with details of all configured probes appears.
- Select the probe that you wish to modify and click **Edit**. The Edit Probes dialog box appears. The fields in the pane change according to the type of probe.
- Step 3** In the **Edit Probe** pane, the field **Type** shows the type of probe. The fields in the pane change according to the type of probe.

Possible probe types are:

- HTTP
- FTP
- SMTP
- TELNET
- TCP
- UDP
- ICMP
- Script

---

## Related Topics

- [Editing HTTP Probes, page 10-15](#)
- [Editing FTP Probes, page 10-22](#)
- [Editing SMTP Probes, page 10-28](#)
- [Editing TELNET Probes, page 10-34](#)
- [Editing TCP Probes, page 10-39](#)
- [Editing UDP Probes, page 10-43](#)
- [Editing ICMP Probes, page 10-47](#)
- [Editing Script Probes, page 10-52](#)

# Viewing HTTP Probes

An HTTP probe establishes an HTTP connection to a real server, sends an HTTP request, and then verifies the response.

- 
- Step 1** Click **Setup** from the task bar. Click Probes in the Setup pane.
- Step 2** Select **Probes > HTTP** in the object selector. The HTTP Probes dialog box appears, displaying the following columns:

Column	Action/Description
Name	Name of the probe.
Probe Interval	Time (in seconds) between the probes.
Retry Count	Number of probe attempts to wait for before marking a server as failed.

More information about the selected probe appears at the bottom of the table. The following sections describe the types of information available:

- [General Tab, page 10-8](#)
  - [Expected Status Tab, page 10-10](#)
  - [Header Details Tab, page 10-11](#)
-

## General Tab

When you click the **General** tab, the following information appears:

Column	Action/Description
<b>Details</b>	
Probe Interval	Number of seconds to wait between probes, from the end of the previous probe to the beginning of the next probe.
Port	Decimal TCP/UDP port number or port name.
Failed Retry Interval	Time (in seconds) before retrying a failed server.
Retry Count	Number of probes to wait before marking a server as failed.
Open Timeout	Maximum time in seconds to wait for a TCP connection.
Address	IP address of the real server.
Receive Timeout	Maximum time in seconds to wait for a reply from the real server.
Routed	Displays the check box status, selected or deselected.  Specifies that the probe is routed according to the CVDM-CSM routing table.
<b>Credentials</b>	
Username	Name that appears in the HTTP header.
Password	Password that appears in the HTTP header.
<b>Associated Server Farms</b>	

Column	Action/Description
Name	<p>Server Farm associated with the probe.</p> <p>All servers in the server farm receive probes of the types that are associated with that server farm.</p> <p>You can associate one or more probe types with a server farm.</p>
Request Method	
Method	<p>Specifies either of the following methods for the probe request:</p> <ul style="list-style-type: none"><li>• <i>get</i>—The probe directs the server to get this page.</li><li>• <i>head</i>—The probe directs the server to get only the header for this page.</li></ul>
URL	Specifies the URL.

## Expected Status Tab

When you click the **Expected Status** tab, you can configure status codes to expect from the HTTP probe. A table appears with the following information:

Column	Action/Description
Minimum Value	Minimum status code in a range. There will be only a single status code if a maximum number is not specified.  <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.
Maximum Value	Maximum status code in a range.  <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.

- Click **Add** to add the minimum and maximum expected status.
- Select a probe and click **Delete** to delete the probe.



## Header Details Tab

When you click the **Header Details** tab, the following information appears:

Column	Action/Description
Name	Name of the header being defined.
Value	Content for the header.

From this dialog box, you can do the following:

- Click **Add** to add HTTP probes. For more information, see [“Adding HTTP Probes” section on page 10-12](#).
- Click **Edit** to edit an HTTP probe. For more information, see [“Editing HTTP Probes” section on page 10-15](#).
- Select a HTTP probe, then click **Delete** to delete the probe.

# Adding HTTP Probes

---

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > HTTP** in the object selector.
- Step 3** Click **Add**. The Add Probe dialog box appears, displaying the following columns.

Column	Action/Description
Name	Enter the name of the probe.
Type	The type of probe. Here it will be HTTP.
Port	Enter the decimal TCP/UDP port number or port name.
Retry Count	Enter the number of probe attempts to wait for before marking a server as failed.
Probe Interval	Enter the time (in seconds) between the probes.
Failed Retry Interval	Enter the time (in seconds) before retrying a failed server.
Open Timeout	Enter the maximum time (in seconds) to wait for a TCP connection.
Receive Timeout	Enter the maximum time (in seconds) to wait for a reply from the real server.
Address	Enter the IP address of the real server.
Routed	If this check box is selected, it implies that CVDM-CSM routes this probe according to its routing table.
<b>User Credentials</b>	
Username	Enter the name that appears in the HTTP header.
Password	Enter the password that appears in the HTTP header.
<b>Request Method</b>	
Method	Specifies either of the following methods for the probe request: <ul style="list-style-type: none"> <li><i>get</i>—The probe directs the server to get this page.</li> <li><i>head</i>—The probe directs the server to get only the header for this page.</li> </ul>
URL	Specify the URL.
<b>Expected Status</b>	

Column	Action/Description
Minimum Value	Enter the minimum status code in a range. There will be only a single status code if a maximum number is not specified.  <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.
Maximum Value	Enter the maximum status code in a range.  <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.
Header Name and Value	
Name	Click <b>Add</b> , then enter the name for the header being defined.
Value	Enter the content for the header.

From this dialog box, you can do the following:

- Under Expected Status:
  - Click **Add** to add the minimum and maximum expected status.
  - Select a probe and click **Delete** to delete the probe.
- Under Header Name and Value:
  - Click **Add** to add the header name and values of the probe.
  - Select a range and click **Delete** to delete the values.

# Editing HTTP Probes

---

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > HTTP** in the object selector.
- Step 3** Click **Edit**. The Edit Probe dialog box appears, displaying the following columns.

Column	Action/Description
Name	Name of the probe.
Type	Type of probe. Here it will be HTTP.
Port	Enter the decimal TCP/UDP port number or port name.
Retry Count	Enter the number of probe attempts to wait for before marking a server as failed.
Probe Interval	Enter the time (in seconds) between the probes.
Failed Retry Interval	Enter the time (in seconds) before retrying a failed server.
Open Timeout	Enter the maximum time (in seconds) to wait for a TCP connection.
Receive Timeout	Enter the maximum time (in seconds) to wait for a reply from real server.
Address	Enter the IP address of the real server.
Routed	If this check box is selected, it implies that CVDM-CSM routes this probe according to its routing table.
<b>User Credentials</b>	
Username	Enter the name that appears in the HTTP header.
Password	Enter the password that appears in the HTTP header.
<b>Request Method</b>	
Method	Specifies either of the following methods for the probe request: <ul style="list-style-type: none"> <li><i>get</i>—The probe directs the server to get this page.</li> <li><i>head</i>—The probe directs the server to get only the header for this page.</li> </ul>
URL	Specify the URL.
<b>Expected Status</b>	

Column	Action/Description
Minimum Value	Enter the minimum status code in a range. There will be only a single status code if a maximum number is not specified.  <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.
Maximum Value	Enter the maximum status code in a range.  <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.
<b>Header Name and Value</b>	
Name	Click <b>Add</b> , then enter the name for the header being defined.
Value	Enter the content for the header.

From this dialog box, you can do the following:

- Under Expected Status:
  - Click **Add** to add the minimum and maximum expected status.
  - Select a probe and click **Delete** to delete the probe.
- Under Header Name and Value:
  - Click **Add** to add the header name and values of the probe.
  - Select a range and click **Delete** to delete the values.

# Viewing FTP Probes

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > FTP** in the object selector. The FTP probes dialog box appears, displaying the following columns:

Column	Action/Description
Name	Name of the probe.
Probe Interval	Time (in seconds) between the probes.
Retry Count	Number of probe attempts to wait for before marking a server as failed.

More details about the selected probe appear at the bottom of the table. These are of two types:

- [General Tab](#)
- [Expected Status Tab](#)

## General Tab

When you click the **General** tab, the following information appears:

Column	Action/Description
Port	Decimal TCP/UDP port number or port name.
Retry Count	Number of probe attempts to wait for before marking a server as failed.
Probe Interval	Time (in seconds) between the probes.
Failed Retry Interval	Time (in seconds) before retrying a failed server.
Open Timeout	Maximum time (in seconds) to wait for a TCP connection.



Column	Action/Description
Receive Timeout	Maximum time (in seconds) to wait for a reply from the real server.
<b>Associated Server Farms</b>	
Name	<p>Server Farm associated with the probe.</p> <p>All servers in the server farm receive probes of the probe types that are associated with that server farm.</p> <p>You can associate one or more probe types with a server farm.</p>

## Expected Status Tab

When you click the **Expected Status** tab, you can configure status codes to expect from the HTTP probe. A table appears with the following information:

Column	Action/Description
Minimum Value	<p>Minimum status code in a range. There will be only a single status code if max-number is not specified.</p> <p><b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.</p>
Maximum Value	<p>Maximum status code in a range.</p> <p><b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.</p>

- Click **Add** to add the minimum and maximum expected status.
- Select a probe and click Delete to delete the probe.

From this dialog box, you can do the following:

- Click **Add** to add FTP probes. For more information, see [“Adding FTP Probes” section on page 10-20](#)

- Click **Edit** to edit a FTP probes. For more information, see [“Editing FTP Probes” section on page 10-22](#).
- Select a FTP probe, then click **Delete** to delete the probe.

## Adding FTP Probes

---

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > FTP** in the object selector.
- Step 3** Click **Add**. The Add Probe dialog box appears, displaying the following columns.

Column	Action/Description
Name	Enter the name of the probe.
Type	Displays the type of probe. Here it will be FTP.
Probe Interval	Enter the time (in seconds) between the probes.
Failed Retry Interval	Enter the time in seconds before retrying a failed server.
Open Timeout	Enter the maximum time (in seconds) to wait for a TCP connection.
Receive Timeout	Enter the maximum time (in seconds) to wait for a reply from real server.
Port	Enter the decimal TCP/UDP port number or port name.
Retry Count	Enter the number of probe attempts to wait for before marking a server as failed.
<b>Expected Status</b>	
Minimum Value	<p>Click <b>Add</b>. Enter the minimum status code in a range. There will be only a single status code if a maximum number is not specified.</p> <p><b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.</p>
Maximum Value	<p>Enter the maximum status code in a range.</p> <p><b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.</p>

From this dialog box, you can do the following:

- Click **Add** to add expect status details by adding the minimum and maximum expect status..
- Select a probe and click **Delete** to delete the probe.

# Editing FTP Probes

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > FTP** in the object selector.
- Step 3** Click **Edit**. The Edit Probe dialog box appears, displaying the following columns:

Column	Action/Description
Name	The name of the probe.
Type	Type of probe. Here it will be FTP.
Probe Interval	Enter the time (in seconds) between the probes.
Failed Retry Interval	Enter the time (in seconds) before retrying a failed server.
Open Timeout	Enter the maximum time (in seconds) to wait for a TCP connection.
Receive Timeout	Enter the maximum time (in seconds) to wait for a reply from real server.
Port	Enter the decimal TCP/UDP port number or port name.
Retry Count	Enter the number of probe attempts to wait for before marking a server as failed.
<b>Expected Status</b>	
Minimum Value	Click <b>Add</b> . Modify the minimum status code in a range. There will be only a single status code if a maximum number is not specified.  <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.
Maximum Value	Modify the maximum status code in a range.  <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.

From this dialog box, you do the following:

- Click **Add** to add the minimum and maximum expected status.
  - Select a probe and click **Delete** to delete the probe.
- 

## Viewing SMTP Probes

---

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > SMTP** in the object selector. The SMTP Probe dialog box appears, displaying the following columns.

Column	Action/Description
Name	Name of the probe.
Probe Interval	Time (in seconds) between the probes.
Retry Count	Number of probe attempts to wait for before marking a server as failed.

More details about the selected probe appear at the bottom of the table when you select the two tabs. These are of two types:

- [General Tab](#)
  - [Expected Status Tab](#)
- 

From this dialog box, you can do the following:

- Click **Add** to add SMTP probes. For more information, see [“Adding SMTP Probes” section on page 10-26](#).
- Click **Edit** to edit a SMTP probe. For more information, see [“Editing SMTP Probes” section on page 10-28](#).
- Select a SMTP probe, then click **Delete** to delete the probe.

## General Tab

When you click the **General** tab, the following information appears:

Column	Action/Description
Probe Interval	Time (in seconds) between the probes.
Port	Decimal TCP/UDP port number or port name.
Failed Retry Interval	Time (in seconds) before retrying a failed server.
Retry Count	Number of probe attempts to wait for before marking a server as failed.
Open Timeout	Maximum time (in seconds) to wait for a TCP connection.
Receive Timeout	Maximum time (in seconds) to wait for a reply from the real server.
<b>Associated Server Farms</b>	
Name	<p>Server Farm associated with the probe.</p> <p>All servers in the server farm receive probes of the probe types that are associated with that server farm.</p> <p>You can associate one or more probe types with a server farm.</p>

## Expected Status Tab

When you click the **Expected Status** tab, you can configure status codes to expect from the HTTP probe. A table appears with the following information:

Field	Action/Description
Minimum Value	Minimum status code in a range. There will be only a single status code if a maximum number is not specified. <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.
Maximum Value	Maximum status code in a range. <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.

From this dialog box, you can do the following:

- Click **Add** to add the minimum and maximum expected status.
- Select a probe and click **Delete** to delete the probe.

# Adding SMTP Probes

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > SMTP** in the object selector.
- Step 3** Click **Add**. The Add Probe dialog box appears, displaying the following columns:

Column	Action/Description
Name	Enter the name of the probe.
Type	Specifies the type of probe. Here it will be SMTP.
Probe Interval	Enter the time (in seconds) between the probes.
Failed Retry Interval	Enter the time (in seconds) before retrying a failed server.
Open Timeout	Enter the maximum time (in seconds) to wait for a TCP connection.
Receive Timeout	Enter the maximum time (in seconds) to wait for a reply from real server.
Port	Enter the decimal TCP/UDP port number or port name.
Retry Count	Enter the number of probe attempts to wait for before marking a server as failed.
<b>Expected Status</b>	



Column	Action/Description
Minimum Value	Click <b>Add</b> . Enter the minimum status code in a range. There will be only a single status code if a maximum number is not specified.  <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.
Maximum Value	Enter the maximum status code in a range.  <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.

From this dialog box, you can do the following:

- Click **Add** to add expect status details by adding the minimum and maximum expect status.
- Select a probe and click **Delete** to delete the probe.

# Editing SMTP Probes

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > SMTP** in the object selector.
- Step 3** Click **Edit**. The Edit Probe dialog box appears, displaying the following columns:

Column	Action/Description
Name	Name of the probe.
Type	Type of probe. Here it will be SMTP.
Probe Interval	Enter the time (in seconds) between the probes.
Failed Retry Interval	Enter the time (in seconds) before retrying a failed server.
Open Timeout	Enter the maximum time (in seconds) to wait for a TCP connection.
Receive Timeout	Enter the maximum time (in seconds) to wait for a reply from the real server.
Port	Enter the decimal TCP/UDP port number or port name.
Retry Count	Enter the number of probe attempts to wait for before marking a server as failed.
<b>Expected Status</b>	
Minimum Value	Click <b>Add</b> . Enter the minimum status code in a range. There will be only a single status code if a maximum number is not specified.  <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.
Maximum Value	Enter the maximum status code in a range.  <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.

From this dialog box you can do the following:

- Click **Add** to add the minimum and maximum expected status.
- Select a probe and click **Delete** to delete the probe.

## Viewing TELNET Probes

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > TELNET** in the object selector. The TELNET Probe dialog box appears, displaying the following columns.

Column	Action/Description
Name	Name of the probe.
Probe Interval	Time interval (in seconds) between the probes.
Retry Count	Number of probe attempts to wait for before marking the server as failed.

More details about the selected probe appear at the bottom of the table when you select the to tabs. These are of two types:

- [General Tab](#)
- [Expected Status Tab](#)

From this dialog box, you can do the following:

- Click **Add** to add TELNET probes. For more information, see [“Adding TELNET Probes” section on page 10-32](#).
- Click **Edit** to edit a TELNET probe. For more information, see [“Editing TELNET Probes” section on page 10-34](#).
- Select a TELNET probe, then click **Delete** to delete the probe.

## General Tab

When you click the **General** tab, the following information appears:

<b>Field</b>	<b>Action/Description</b>
Probe Interval	Time (in seconds) between the probes.
Port	Decimal TCP/UDP port number or port name.
Failed Retry Interval	Time (in seconds) before retrying a failed server.
Retry Count	Number of probe attempts to wait for before marking a server as failed.
Open Timeout	Maximum time (in seconds) to wait for a TCP connection.
Receive Timeout	Maximum time (in seconds) to wait for a reply from the real server.
<b>Associated Server Farms</b>	
Name	<p>Server Farm associated with the probe.</p> <p>All servers in the server farm receive probes of the probe types that are associated with that server farm.</p> <p>You can associate one or more probe types with a server farm.</p>

## Expected Status Tab

When you click the **Expected Status** tab, you can configure status codes to expect from the HTTP probe. A table appears with the following information:

Column	Action/Description
Minimum Value	Minimum status code in a range. There will be only a single status code if a maximum number is not specified. <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.
Maximum Value	Maximum status code in a range. <b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.

From this dialog box, you can do the following:

- Click **Add** to add the minimum and maximum expected status.
- Select a probe and click **Delete** to delete the probe.

# Adding TELNET Probes

---

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > TELNET** in the object selector.
- Step 3** Click **Add**. The Add Probe dialog box appears, displaying the following columns:

Column	Action/Description
Name	Enter the name of the probe.
Type	Displays the type of probe. Here it will be TELNET.
Probe Interval	Enter the time (in seconds) between the probes.
Failed Retry Interval	Enter the time (in seconds) before retrying a failed server.
Open Timeout	Enter the maximum time (in seconds) to wait for a TCP connection.
Receive Timeout	Enter the maximum time (in seconds) to wait for a reply from real server.
Port	Enter the decimal TCP/UDP port number or port name.
Retry Count	Enter the number of probe attempts to wait for before marking a server as failed.
<b>Expected Status</b>	
Minimum Value	<p>Click <b>Add</b>. Enter the minimum status code in a range. There will be only a single status code if a maximum number is not specified.</p> <p><b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.</p>
Maximum Value	<p>Enter the maximum status code in a range.</p> <p><b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.</p>

From this dialog box, you can do the following:

- Click **Add** to add expect status details by adding the minimum and maximum expect status.
- Select a probe and click **Delete** to delete the probe.

# Editing TELNET Probes

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > TELNET** in the object selector.
- Step 3** Click **Edit**. The Edit Probe dialog box appears, displaying the following columns:

Column	Action/Description
Name	Name of the probe.
Type	Type of probe. Here it will be TELNET.
Probe Interval	Time (in seconds) between the probes.
Failed Retry Interval	Enter the time (in seconds) before retrying a failed server.
Open Timeout	Enter the maximum time (in seconds) to wait for a TCP connection.
Receive Timeout	Enter the maximum time (in seconds) to wait for a reply from real server.
Port	Enter the decimal TCP/UDP port number or port name.
Retry Count	Enter the number of probe attempts to wait for before marking a server as failed.
<b>Expected Status</b>	



Column	Action/Description
Minimum Value	<p>Click <b>Add</b>. Enter the minimum status code in a range. There will be only a single status code if a number is not specified.</p> <p><b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.</p>
Maximum Value	<p>Enter the maximum status code in a range.</p> <p><b>Note</b> You cannot add overlapping status codes. The range should be outside what you have already added.</p>

From this dialog box, you can do the following:

- Click **Add** to add the minimum and maximum expected status.
- Select a probe and click **Delete** to delete the probe.

# Viewing TCP Probes

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > TCP** in the object selector. The TCP Probes dialog box appears, displaying the following columns:

Column	Action/Description
Name	Name of the probe.
Interval	Time (in seconds) between the probes.
Retry Count	Number of probe attempts to wait for before marking a server as failed.

More details about the selected probe appear at the bottom of the table.

Column	Action/Description
Probe Interval	Time (in seconds) between the probes.
Port	Decimal TCP/UDP port number or port name.
Failed Retry Interval	Time (in seconds) before retrying a failed server.
Retry Count	Number of probe attempts to wait for before marking a server as failed.
Open Timeout	Maximum time (in seconds) to wait for a TCP connection.
Receive Timeout	Maximum time (in seconds) to wait for a reply from real server.
<b>Associated Server Farms</b>	
Name	<p>Server Farm associated with the probe.</p> <p>All servers in the server farm receive probes of the probe types that are associated with that server farm.</p> <p>You can associate one or more probe types with a server farm.</p>

From this dialog box, you can do the following:

- Click **Add** to add TCP probes. For more information, see [“Adding TCP Probes” section on page 10-38](#).
- Click **Edit** to edit a TCP probe. For more information, see [“Editing TCP Probes” section on page 10-39](#).
- Select a TCP probe, then click **Delete** to delete the probe.

# Adding TCP Probes

- 
- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > TCP** in the object selector.
- Step 3** Click **Add**. The Add Probe dialog box appears, displaying the following columns:

Column	Action/Description
Name	Enter the name of the probe.
Type	Type of probe. Here it will be TCP.
Probe Interval	Enter the time (in seconds) between the probes.
Failed Retry Interval	Enter the time (in seconds) before retrying a failed server.
Open Timeout	Enter the maximum time (in seconds) to wait for a TCP connection.
Port	Enter the decimal TCP/UDP port number or port name.
Retry Count	Number of probe attempts to wait for before marking a server as failed.

---

# Editing TCP Probes

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > FTP** in the object selector.
- Step 3** Click **Edit**. The Edit Probe dialog box appears, displaying the following columns:

Column	Action/Description
Name	Name of the probe.
Type	Type of probe. Here it will be TCP.
Probe Interval	Enter the time (in seconds) between the probes.
Failed Retry Interval	Modify the time (in seconds) before retrying a failed server.
Open Time- Out	Modify the maximum time (in seconds) to wait for a TCP connection.
Port	Modify the decimal TCP/UDP port number or port name.
Retry Count	Number of probe attempts to wait for before marking a server as failed.

# Viewing UDP Probes


**Note**

You cannot view UDP probes in the following IOS versions: 12.1(13)E, 12.2(14)SY and 12.2(14)SX1.

You must configure an ICMP probe in addition to a UDP probe for any given server. The UDP probe requires ICMP because the UDP probe will be unable to detect when a server has gone down or has been disconnected. The CSM uses the ICMP Unreachable message to determine if the UDP application is not reachable. If there is no ICMP Unreachable reply in the receive timeout, the CSM assumes that the probe is operating correctly.

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > UDP** in the object selector. The UDP probes window appears, displaying the following columns:

Column	Action/Description
Name	Name of the probe.
Probe Interval	Time (in seconds) between the probes.
Retry Count	Number of probe attempts to wait for before marking a server as failed.

More details about the selected probe appear at the bottom of the table with the following information:

Column	Action/Description
Probe Interval	Time (in seconds) between the probes.
Port	Decimal TCP/UDP port number or port name.
Failed Retry Interval	Time (in seconds) before retrying a failed server.
Retry Count	Number of probe attempts to wait for before marking a server as failed.
Receive Timeout	Maximum time (in seconds) to wait for a reply from real server.
<b>Associated Server Farms</b>	
Name	<p>Server Farm associated with the probe.</p> <p>All servers in the server farm receive probes of the probe types that are associated with that server farm.</p> <p>You can associate one or more probe types with a server farm.</p>

From this dialog box, you can do the following:

- Click **Add** to add UDP probe. For more information, see [“Adding UDP Probes” section on page 10-42](#).
- Click **Edit** to edit a UDP probe. For more information, see [“Editing UDP Probes” section on page 10-43](#).
- Select a UDP probe, then click **Delete** to delete the probe.

# Adding UDP Probes

- 
- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > UDP** in the object selector.
- Step 3** Click **Add**. The Add Probe dialog box appears, displaying the following columns:

Column	Action/Description
Name	Enter the name of the probe.
Type	Type of probe. Here it will be UDP.
Probe Interval	Enter the time (in seconds) between the probes.
Failed Retry Interval	Enter the time (in seconds) before retrying a failed server.
Receive Time-Out	Enter the maximum time (in seconds) to wait for a reply from real server.
Port	Enter the decimal TCP/UDP port number or port name.
Retry Count	Number of probe attempts to wait for before marking a server as failed.

---



# Editing UDP Probes

- 
- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > UDP** in the object selector.
- Step 3** Click **Edit**. The Edit Probe dialog box appears, displaying the following columns:

Column	Action/Description
Name	Name of the probe.
Type	Type of probe. Here it will be UDP.
Probe Interval	Enter the time (in seconds) between the probes.
Failed Retry Interval	Enter the time (in seconds) before retrying a failed server.
Receive Timeout	Enter the maximum time (in seconds) to wait for a reply from the real server.
Port	Enter the decimal TCP/UDP port number or port name.
Retry Count	Number of probe attempts to wait for before marking a server as failed.

---

# Viewing ICMP Probes

An ICMP probe sends an ICMP echo (for example, ping) to the real server, and then verifies the response.

- 
- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > ICMP** in the object selector. The ICMP probes window appears, displaying the following columns:

Column	Action/Description
Name	Name of the probe.
Probe Interval	Time (in seconds) between the probes.
Retry Count	Number of probe attempts to wait for before marking a server as failed.

More details about the selected probe appear at the bottom of the table with the following information.

Column	Action/Description
Probe Interval	Time (in seconds) between the probes.
Retry Count	Number of probe attempts to wait for before marking a server as failed.
Failed Retry Interval	Time (in seconds) before retrying a failed server.
Address	The IP address of the probes.
Receive Timeout	Maximum time in seconds to wait for a reply from real server.
Routed	Displays the check box status, selected or deselected.  Specifies that the probe is routed according to the CSM routing table.
<b>Associated Server Farms</b>	
Name	Server Farm associated with the probe.  All servers in the server farm receive probes of the probe types that are associated with that server farm.  You can associate one or more probe types with a server farm.

From this dialog box, you can do the following:

- Click **Add** to add ICMP probes. For more information, see [“Adding ICMP Probes” section on page 10-46](#).
- Click **Edit** to edit an ICMP probe. For more information, see [“Editing ICMP Probes” section on page 10-47](#).
- Select a ICMP probe, then click **Delete** to delete the probe.

# Adding ICMP Probes

- 
- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > ICMP** in the object selector.
- Step 3** Click **Add**. The Add Probe dialog box appears, displaying the following columns:

Column	Action/Description
Name	Enter the name of the probe.
Type	Type of probe. Here it will be ICMP.
Probe Interval	Enter the time (in seconds) between the probes.
Failed Retry Interval	Enter the time (in seconds) before retrying a failed server.
Receive Time-Out	Enter the maximum time (in seconds) to wait for a reply from real server
Retry Count	Enter the number of probe attempts to wait for before marking a server as failed.
Address	Enter the IP address of the real server.
Routed	Select the check box to specify that the CVDM-CSM route the probe according to its routing table.

---

# Editing ICMP Probes

- 
- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > ICMP** in the object selector.
- Step 3** Click **Edit**. The Edit Probe dialog box appears, displaying the following columns.

Column	Action/Description
Name	Name of the probe.
Type	Type of probe. Here it will be ICMP.
Probe Interval	Enter the time (in seconds) between the probes.
Failed Retry Interval	Enter the time in seconds before retrying a failed server.
Receive Timeout	Enter the maximum time in seconds to wait for a reply from real server
Retry Count	Enter the number of probe attempts to wait for before marking a server as failed.
Address	Enter the IP address of the real server.
Routed	Select the check box to specify that the CVDM-CSM route the probe according to its routing table.

---

# Viewing Script Probes

Probe scripts test the health of a real server by creating a network connection to the server, sending data to the server, and checking the response.

To support a more flexible health-probing functionality, you can upload and execute Toolkit Command Language (TCL) scripts on the CVDM-CSM. You can create a script probe that the CVDM-CSM periodically executes for each real server in any server farm associated with a probe.

- 
- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > Script** in the object selector. The Script Probes dialog box appears, displaying the following columns:

Column	Action/Description
Name	Name of the probe.
Probe Interval	Time (in seconds) between the probes.
Retry Count	Number of probe attempts to wait for before marking a server as failed.

More details about the selected probe appear at the bottom of the table.

Column	Action/Description
Probe Interval	Time (in seconds) between the probes.
Port	Decimal TCP/UDP port number or port name.
Retry Count	Number of probe attempts to wait for before marking a server as failed.
Failed Retry Interval	Time (in seconds) before retrying a failed server.
Receive Time-Out	Maximum time (in seconds) to wait for a reply from real server.
Open Time- Out	Maximum time (in seconds) to wait for a TCP connection.
Associated Health Script	The health-monitoring script associated with the probe.
Script Arguments	The arguments of the script.

From this dialog box, you can do the following:


- Click **Add** to add Script probes. For more information, see [“Adding Script Probes” section on page 10-50](#).
- Click **Edit** to edit an Script probe. For more information, see [“Editing Script Probes” section on page 10-52](#).
- Select a Script probe, then click **Delete** to delete the probe.

# Adding Script Probes

---

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > Script** in the object selector.
- Step 3** Click **Add**. The Add Probe dialog box appears, displaying the following columns:




Field	Action/Description
Name	Enter the name of the probe.
Type	Type of probe. Here it will be Script.
Probe Interval	Enter time (in seconds) between the probes.
Failed Retry Interval	Enter the time (in seconds) before retrying a failed server.
Open Timeout	Enter the maximum time (in seconds) to wait for a TCP connection.
Receive Timeout	Maximum time (in seconds) to wait for a reply from real server.
Port	Enter the decimal TCP/UDP port number or port name.
Retry Count	Enter the number of probe attempts to wait for before marking a server as failed.
Health Script	<p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Health Script</b>—Opens the Select Health Script dialog box and allows you to select from a list of health scripts.</li> <li>• <b>Clear Health Script</b>—Allows you to clear the field.</li> </ul>
Script Arguments	The arguments of the script. You can add up to 5 arguments for the script.

# Editing Script Probes

---

- Step 1** Click **Setup** from the task bar. Click **Probes** in the Setup pane.
- Step 2** Select **Probes > Script** in the object selector.
- Step 3** Click **Edit**. The Edit Probe dialog box appears, displaying the following columns.

Column	Action/Description
Name	Enter the name of the probe.
Type	Type of probe. Here it will be Script.
Probe Interval	Enter time (in seconds) between the probes.
Failed Retry Interval	Enter the time (in seconds) before retrying a failed server.
Open Timeout	Enter the maximum time (in seconds) to wait for a TCP connection.
Port	Enter the decimal TCP/UDP port number or port name.
Receive Timeout	Enter the maximum time (in seconds) to wait for a reply from real server.
Retry Count	Enter the number of probe attempts to wait for before marking a server as failed.
Health Script	<p>Click  and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select Health Script</b>—Opens the Select Health Script dialog box and allows you to select from a list of health scripts.</li> <li>• <b>Clear Header Map</b>—Allows you to clear the field.</li> </ul>
Script Arguments	The arguments of the script. You can add up to 5 arguments for the script.





## Managing Other Features in CVDM-CSM

---

CVDM-CSM provides the following features that you can access from the Miscellaneous page:

- [Understanding Fault Tolerance, page 11-1](#)
- [Understanding Scripts, page 11-6](#)
- [Viewing Environment Variables, page 11-13](#)
- [Understanding XML Configuration, page 11-19](#)

### Understanding Fault Tolerance

From the Fault Tolerance dialog box, you can do the following:

- Configure active and standby CVDM-CSMs, fault tolerant VLANs, and parameters like failover time and heartbeat time.
- Set priority for any CVDM-CSM.

In the secure (router) mode, the client-side and server-side VLANs provide the fault-tolerant (redundant) connection paths between the CVDM-CSM and routers on the client side, and the servers on the server side. In a redundant configuration, two CSMs perform active and standby roles. Each CSM contains the same IP, virtual server, server pool, and real server information. From the client-side and server-side networks, each CSM is configured identically. The network sees the fault-tolerant configuration as a single CSM.

Two CSMs can be configured in a fault-tolerant mode to share state information about user sessions and provide connection redundancy. When the active CSM fails, open connections are handled by the standby CSM without interruption, and users experience hitless failover.

Fault-tolerant configuration can be done with two CSMs in two Cisco Catalyst 6500 Series devices or in a single chassis. Configuration can also be done in either the secure (router) mode or non-secure (bridge) mode.

Configuring fault tolerance requires the following:

- Two CSMs that are installed in the same or different Catalyst 6500 series chassis.
- Identically configured CSMs. One CSM is configured as active; the other is configured as standby.
- Each CSM connected to the same client-side and server-side VLANs.
- Communication between the CSMs provided by a shared private VLAN.
- A network that sees the redundant CSMs as a single entity.

**Related Topics:**

- [Configuring Fault Tolerance, page 11-3](#)
- [Editing Fault Tolerance Configuration, page 11-5](#)

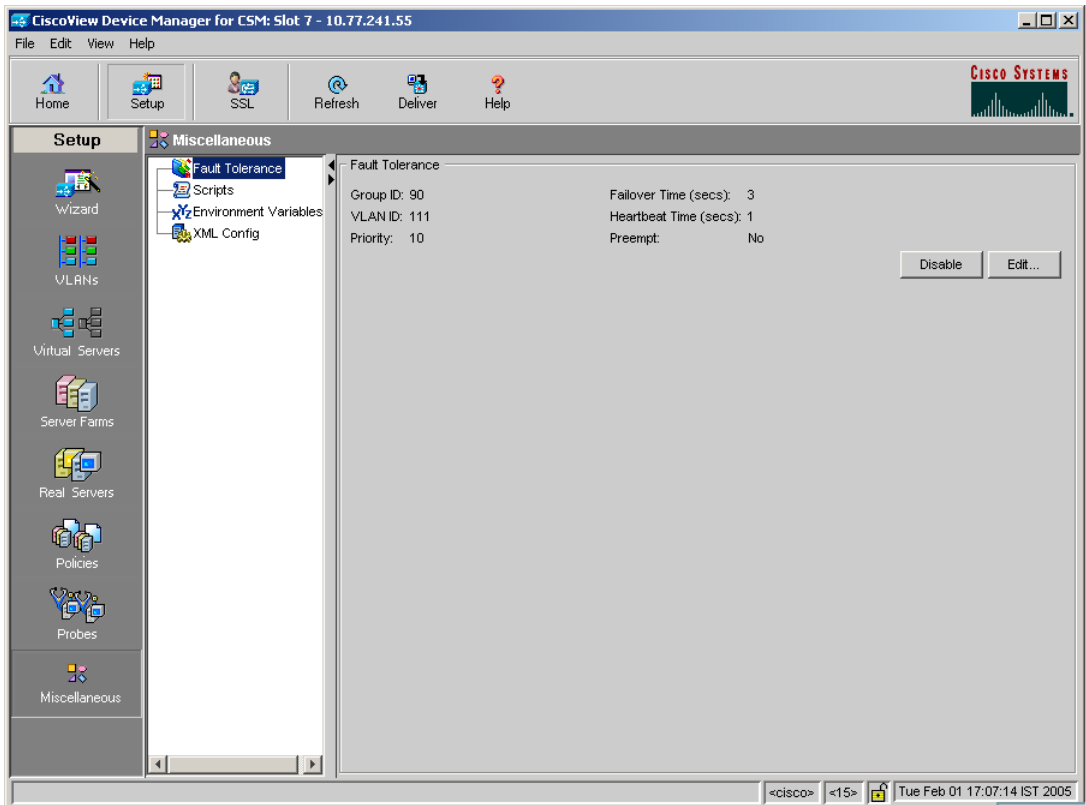
# Configuring Fault Tolerance



## Note

Click the **Enable** button to enable fault tolerance configuration in CVDM-CSM. The Enable button then toggles to **Disable** and the **Edit** button is enabled, allowing changes to the fault tolerance configuration values. To disable fault tolerance configuration, click the **Disable** button.

Figure 11-1 Fault Tolerance Window



130186

- Step 1** Click **Setup** from the task bar, then click **Miscellaneous** in the Setup pane.
- Step 2** Select **Fault Tolerance** from the object selector. The Fault Tolerance dialog box appears, displaying the following columns.

Column	Description
Group ID	ID of the fault-tolerant group. Both CSMs must have the same group ID.
VLAN ID	ID of the VLAN over which heartbeat messages are sent. Both CSMs must have the same VLAN ID.
Failover Time	Amount of time for a standby CSM to wait before becoming active.
Heartbeat Time	Interval (in seconds) between heartbeat transmissions.
Priority	Priority of a CSM.
Preempt	Lets you know that a higher priority CSM will take control of a fault-tolerant group when it comes online.

From this dialog box, you can do the following:

- Click **Edit** to edit the fault tolerance configuration. For more information, see [“Editing Fault Tolerance Configuration”](#) section on page 11-5.
- Click **Disable** to disable the fault tolerance configuration in CVDM-CSM.



# Editing Fault Tolerance Configuration



**Note** The **Edit** button is enabled only when you enable fault tolerance configuration in CVDM-CSM.

- Step 1** Click **Setup** from the task bar, then click **Miscellaneous** in the Setup pane.
- Step 2** Select **Fault Tolerance** from the object selector.
- Step 3** Click **Edit**. The Fault Tolerance Configuration dialog box appears, displaying the following columns.

Column	Description
Group ID	Enter the ID of the fault-tolerant group. Both CSMs must have the same group ID.
VLAN ID	Enter the ID of the VLAN over which heartbeat messages are sent. Both CSMs must have the same VLAN ID.
Failover Time	Enter the failover time. It is the amount of time for a standby CSM to wait before becoming active.
Heartbeat Time	Enter the interval (in seconds) between heartbeat transmissions.
Priority	Enter the priority of the CSM.
Preempt	Specify Yes or No to allow a higher priority CSM to take control of a fault-tolerant group when it comes online.

# Understanding Scripts

CVDM-CSM allows you to upload and execute Toolkit Command Language (TCL) scripts. You can customize scripts to develop health probes or standalone tasks. The CVDM-CSM executes the scripts at regular intervals.

There are two basic types of scripts in CVDM-CSM:

- Health-monitoring scripts—You can write these scripts using some simple rules. The health-monitoring module controls the execution of these scripts. When a script is a part of a script probe, it executes periodically. The script indicates the relative health and availability of specific real servers.
- Standalone scripts—These are generic TCL scripts which can execute a single task. You can control the execution of these scripts by configuring them.

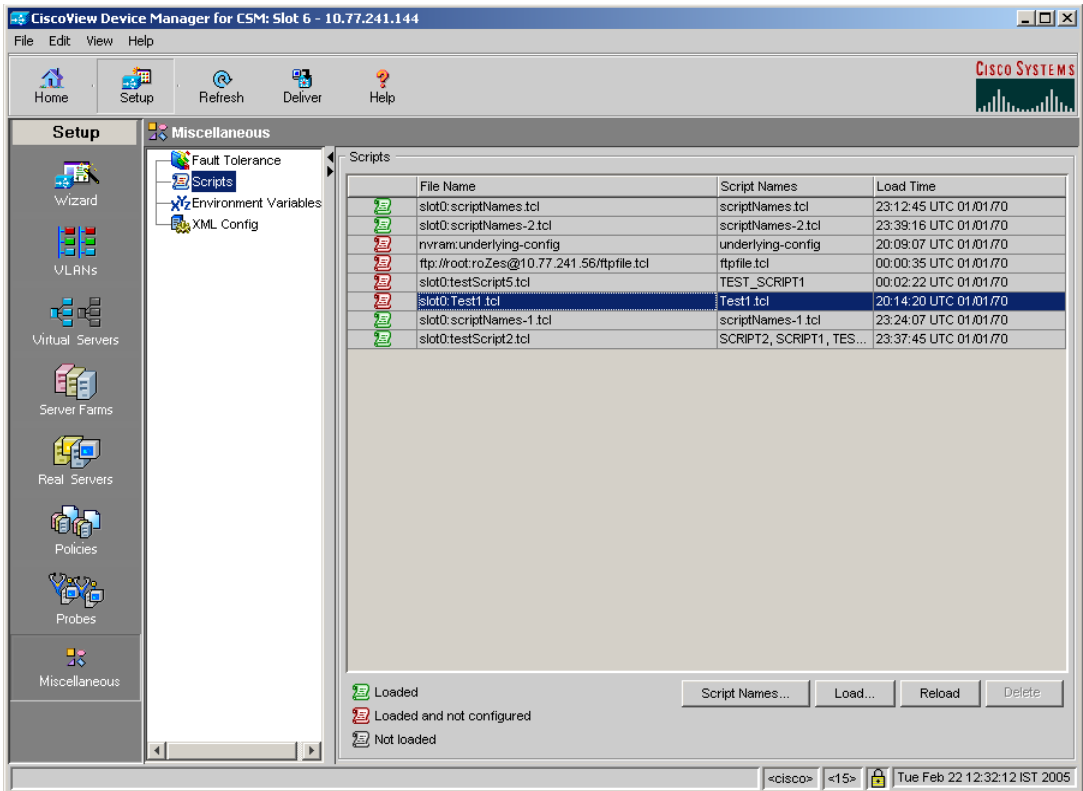
## Related Topics:

- [Viewing Scripts, page 11-7](#)
- [Loading Scripts, page 11-9](#)

## Viewing Scripts

You can load scripts onto the CVDM-CSM through script files. A script file may contain zero, one, or more scripts.

**Figure 11-2** Scripts Window






- Step 1** Click **Setup** from the task bar, then click **Miscellaneous** in the Setup pane.
- Step 2** Select **Scripts** from the object selector. The Scripts dialog box appears, displaying the following columns:

Column	Description
State column (far-left column)	Displays the state of the script. Depending on its state the color of the icon beside the script will change. For more details on what the color of the icon represents, see <a href="#">Table 11-1</a> .
Filename	Specifies the filename of the script
Script Name	Specifies the scripts in the file.
Load Time	Specifies the time at which you loaded the script.

[Table 11-1](#) describes the status of the scripts based on the color of the icons.

**Table 11-1** *Color Scheme for Script Status*

Icon	Color	Description
	Green	Specifies that the script is loaded in CVDM-CSM.
	Red	Specifies that the script is loaded but not configured in CVDM-CSM.
	Gray	Specifies that the script is not loaded in CVDM-CSM.

From this dialog box, you can do the following:

- Select a script from the table and click the **Script Names..** button to see the list of associated script names of the script file.
- Click **Load** to load your scripts. For more information, see [Loading Scripts, page 11-9](#).
- Click **Reload** to reload your scripts. This button will be disabled for the scripts that are not loaded (gray icon) in CVDM-CSM.

When you reload the scripts which are in the green and/or red state, CVDM-CSM prompts you for confirmation and reloads the corresponding scripts.

Based on the commands in the CLI, CVDM-CSM will first remove the configuration of the script and then reconfigure it.

- Click **Delete** to disable the scripts that are in the green and grey states. This button will be disabled for the scripts which are in the red state.



---

**Note** You cannot delete scripts; you can only disable them.

---

When you click **Delete**, CVDM-CSM prompts you for confirmation and disables the corresponding script.

## Loading Scripts

You can load scripts from the switch or from network devices like FTP, TFTP or RCP servers. A script file may contain zero, one, or more scripts. A script remains in the system after you load it. You cannot remove them but you can modify them.



---

**Note** Every script should have a unique name. If two or more scripts have identical names, then the last loaded script will be in the system.

---

- 
- Step 1** Click **Setup** from the task bar, then click **Miscellaneous** in the Setup pane.
- Step 2** Select **Scripts** from the object selector.
- Step 3** Click **Load** to load your scripts. The Load Script dialog box appears with the following tabs:
- Switch (for information on loading scripts from the Switch tab, see [Switch Tab, page 11-10](#)).
  - Network (for information on loading scripts from the Network tab, see [Network, page 11-11](#)).
-

## Switch Tab

**Step 1** Click **Switch** tab to load scripts from the switch.

Do one of the following:

- To load the scripts from bootflash, choose **bootflash** from the list.
- To load the scripts from the switch supervisor engine bootflash, choose **sup-bootflash**.
- To load the scripts from CVDM-CSM hard disk, choose **disk0** from the list.
- To load the scripts from the NVRAM, choose **nvrाम** from the list.

The following columns appear under the Switch tab:

Column	Description
File	Specifies the filename of the script.
Load	Select this check box to load the required script.

## Network

---

**Step 1** Click the **Network** tab to load scripts from network devices like FTP, TFTP, or RCP servers.

The different server types are:

- FTP
- TFTP
- RCP

**Step 2** Do one of the following:

- To load the scripts from the FTP server, choose **FTP** from the list. For information, see [FTP, page 11-11](#).
  - To load the scripts from the TFTP server, choose **TFTP** from the list. For information, see [TFTP, page 11-12](#).
  - To load the scripts from the RCP server, choose **RCP** from the list. For information, see [RCP, page 11-12](#).
- 

## FTP

To load a script from a FTP server, you have to enter the following information:

Column	Description
FTP Server IP Address	IP address of the FTP server.
Username	Name of the credentials user.
Password	Password for the credentials user.
Filename	Specifies the filename of the script.

## TFTP

To load a script from a TFTP server, you have to enter the following information:

Column	Description
TFTP Server IP Address	IP address of the TFTP server.
Filename	Specifies the filename of the script

## RCP

To load a script from an RCP server, enter the following information:

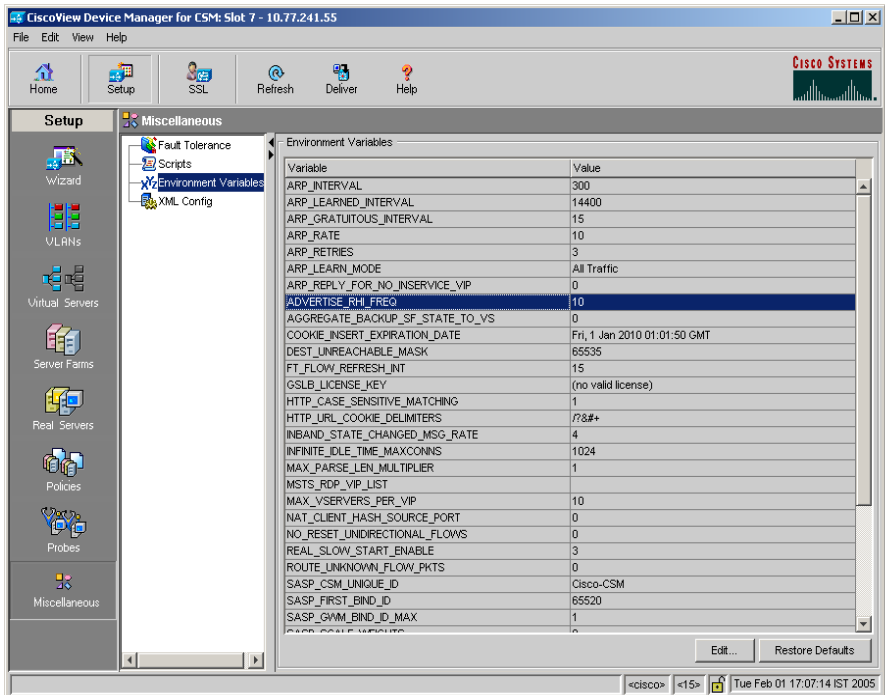
Column	Description
RCP Server IP Address	IP address of the RCP server.
Username	Name of the credentials user.
File Name	Specifies the filename of the script



# Viewing Environment Variables

You can configure CVDM-CSM environment variables and see the values of the configured variables.

**Figure 11-3** Environment Variables Window



To see the list of environment variables used by the CVDM-CSM:

- Step 1** Click **Setup** from the task bar, then click **Miscellaneous** in the Setup pane.
- Step 2** Select **Environment Variables** from the object selector.

The Environment Variables dialog box appears with the following variables.

## ■ Viewing Environment Variables

Name	Default Value	Valid Values	Description
ARP_INTERVAL	300	Integer (15 to 31536000)	Time (in seconds) between ARP requests for configured hosts.
ARP_LEARNED_INTERVAL	14400	Integer (60 to 31536000)	Time (in seconds) between ARP requests for learned hosts.
ARP_GRATUITOUS_INTERVAL	15	Integer (10 to 31536000)	Time (in seconds) between gratuitous ARP requests.
ARP_RATE	10	Integer (1 to 60)	Time (in seconds) between ARP retries.
ARP_RETRIES	3	Integer (2 to 15)	Number of ARP attempts before flagging a host as down.
ARP_LEARN_MODE	1	Integer (0 to 1)	Indicates whether the CSM learns MAC addresses on responses only (0) or all traffic (1).
ARP_REPLY_FOR_NO_INSERVICE_VIP	0	Integer (0 to 1)	Indicates whether the CSM will reply to ARP for an out-of-service virtual server.
ADVERTISE_RHI_FREQ	10	Integer (1 to 65535)	Frequency (in seconds) at which the CSM checks for RHI updates.
AGGREGATE_BACKUP_SF_STATE_TO_VS	0	Integer (0 to 1)	Specifies whether to include the operational state of a backup server farm in the state of a virtual server.
COOKIE_INSERT_EXPIRATION_DATE	Fri, 1 Jan 2010 01:01:50 GMT	String (2 to 63 chars)	Configures the expiration time and date for the HTTP cookie inserted by the CSM.
CSM_FAST_FIN_TIMEOUT	10	Integer (10 to 65535)	Timeout (in seconds) for connection reset after FIN is detected.
DEST_UNREACHABLE_MASK	65535	Integer (0 to 65535)	Bitmask that defines the ICMP destination unreachable codes to be forwarded.

Name	Default Value	Valid Values	Description
FT_FLOW_REFRESH_INT	15	Integer (1 to 65535)	Interval (in seconds) for the FT slow path flow refresh.
GSLB_LICENSE_KEY	(no valid license)	String (1 to 63 chars)	License key string that enables the Global Server Load Balancing (GSLB) feature.
GSLB_KALAP_PROBE_FREQ	45	Integer (45 to 65535)	Frequency of GSLB KAL-AP probes.
GSLB_KALAP_PROBE_RETRIES	3	Integer (1 to 65535)	Maximum number of retries for GSLB KAL-AP probes.
GSLB_KALAP_UDP_PORT	5002	Integer (1 to 65535)	GSLB KAL-AP UDP port number.
GSLB_ICMP_PROBE_FREQ	45	Integer (45 to 65535)	Frequency of GSLB ICMP probes.
GSLB_ICMP_PROBE_RETRIES	3	Integer (1 to 65535)	Maximum number of retries for GSLB ICMP probes.
GSLB_HTTP_PROBE_FREQ	45	Integer (45 to 65535)	Frequency of GSLB HTTP probes.
GSLB_HTTP_PROBE_RETRIES	3	Integer (1 to 65535)	Maximum retries for GSLB HTTP probes.
GSLB_DNS_PROBE_FREQ	45	Integer (45 to 65535)	Frequency of GSLB Domain Name System (DNS) probes.
GSLB_DNS_PROBE_RETRIES	3	Integer (1 to 65535)	Maximum retries for GSLB DNS probes.
HTTP_CASE_SENSITIVE_MATCHING	1	Integer (0 to 1)	Specifies whether the URL (cookie, header) matching and sticky are case sensitive.
HTTP_URL_COOKIE_DELIMITERS	/?&#+	String (1 to 64 chars)	Configures the list of delimiter characters for cookies in the URL string.
INBAND_STATE_CHANGED_MESSAGE_RATE	4	Integer (0 to 32)	Maximum number of log messages per second, when the real server changed state within inband.

## Viewing Environment Variables

Name	Default Value	Valid Values	Description
INFINITE_IDLE_TIME_MAXCONNS	1024	Integer (1 to 4294967295)	Maximum number of connections with infinite idle timeout.
MSTS_RDP_VIP_LIST	—	String (0 to 256 chars)	List of Virtual IP (VIPs) supporting MSTS-RDP protocol.
MAX_PARSE_LEN_MULTIPLIER	1	Integer (1 to 16)	Multiplies the configured maximum parse length by this amount.
MAX_VSERVERS_PER_VIP	10	Integer (7 to 10)	Configures the maximum limit for virtual servers having the same IP address. It is represented in powers of 2.
NAT_CLIENT_HASH_SOURCE_PORT	0	Integer (0 to 1)	Specifies whether to use the source port to select the client NAT IP address.
NO_RESET_UNIDIRECTIONAL_FLOWS	0	Integer (0 to 1)	Specifies that unidirectional flows need not be reset when timed out.
REAL_SLOW_START_ENABLE	3	Integer (0 to 10)	Disables or enables the Slow Start feature with an average number of connections sent to the slow start server. It is represented in powers of 2.
ROUTE_UNKNOWN_FLOW_PACKETS	0	Integer (0 to 1)	Specifies whether to route non-SYN packets that do not match any existing flows
SASP_CSM_UNIQUE_ID	Cisco-CSM	String (3 to 63 chars)	Text identifier of this CSM to GWM running Server/Application State Protocol (SASP).
SASP_FIRST_BIND_ID	65520	Integer (1 to 65525)	Treat Dynamic Feedback Protocol (DFP) bind_ids as SASP IDs starting at this value.
SASP_GWM_BIND_ID_MAX	1	Integer (0 to 8)	Maximum number of GWMS/bind_ids using SASP.

Name	Default Value	Valid Values	Description
SASP_SCALE_WEIGHTS	0	Integer (0 to 12)	Scale SASP weights by <i>N</i> ; a value of 12 means the range corresponds with the CVDM-CSM range.
SECURE_HTTP_PORT	443	Integer (1 to 65535)	HTTPS server port number.
SECURE_HTTP_PRIV_KEY_FILE	—	String (0 to 256 chars)	Private key file used by the HTTPS server.
SECURE_HTTP_SSL_METHOD	0	Integer (0 to 3)	SSL version used by the HTTPS server.
SECURE_HTTP_TFTP_HOST_IP_ADDRESS	—	String (0 to 16 chars)	IP address of TFTP server that contains the HTTP server certificates.
SECURE_HTTP_SERVER_CERTIFICATE	—	String (0 to 256 chars)	Certificate file used by the HTTPS server.
SECURE_SASP_ENABLE	0	Integer (0 to 1)	Enables secure SASP.
SECURE_SASP_PRIV_KEY_FILE	—	String (0 to 256 chars)	Private key file used by the SASP client.
SECURE_SASP_SSL_METHOD	0	Integer (0 to 3)	SSL version used by the secure SASP client.
SECURE_SASP_SERVER_CERTIFICATE	—	String (0 to 256 chars)	Certificate file used by the SASP client.
SECURE_SASP_TFTP_HOST_IP_ADDRESS	—	String (0 to 16 chars)	IP address of TFTP server that contains the SASP client certificates.
SSL_DEFAULT_STICKY	0	Integer (0 to 1)	Stick to source IP sticky upon receipt of an unknown or BAD SSL format.
SWITCHOVER_RP_ACTION	0	Integer (0 to 1)	Specifies whether to recover (0) or halt/reboot (1) after a supervisor engine Route Processor (RP) switchover occurs.

## Viewing Environment Variables

Name	Default Value	Valid Values	Description
SWITCHOVER_SP_ACTION	0	Integer (0 to 1)	Specifies whether to recover (0) or halt/reboot (1) after a supervisor engine SP switchover occurs.
SYN_COOKIE_INTERVAL	3	Integer (1 to 60)	Specifies the interval (in seconds at which a new syn-cookie key is generated.
SYN_COOKIE_THRESHOLD	5000	Integer (0 to 1048576)	Specifies the threshold (in number of pending sessions) at which syn-cookie is engaged.
TCP_ACCEPT_RST_EQU_NEXT_GET_SEQ	0	Integer (0 to 1)	Specifies if CVDM-CSM will immediately close connections, when it receives Reset (RST) that has Sequence# equal (but not less than) the Sequence# of the next expected HTTP request header.
TCP_MSS_OPTION	1460	Integer (1 to 65535)	Specifies the maximum segment size (MSS) value sent by CSM for layer 7 processing.
TCP_WND_SIZE_OPTION	8192	Integer (1 to 65535)	Specifies the window size value sent by CSM for layer 7 processing.
VSERVER_ICMP_ALWAYS_RESPOND	false	String (1 to 5 chars)	If the response is true, the CSM responds to ICMP probes regardless of the state of the virtual server.
XML_CONFIG_AUTH_TYPE	Basic	String (5 to 6 chars)	Specifies the HTTP authentication type for xml-config. It can be: <ul style="list-style-type: none"> <li>• Basic</li> <li>• Digest</li> </ul>

From this dialog box, you can do the following functions:

- Select an environment variable and click **Edit** to edit its value.
- Click **Restore Defaults** to set the environment variable values to their defaults values.

# Understanding XML Configuration

With XML, you can configure the CVDM-CSM using a Document Type Definition (DTD) rather than the IOS command line interface (CLI).

**Related Topics:**

- [Viewing XML Configuration, page 11-20](#)
- [Editing XML Configuration, page 11-21](#)

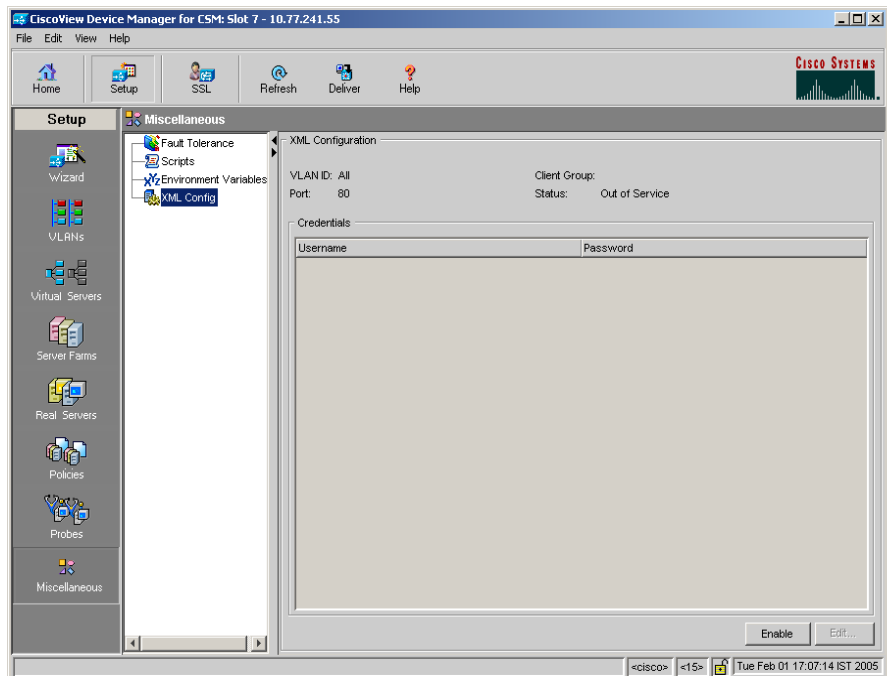
## Viewing XML Configuration



### Note

Click the **Enable** button to enable XML configuration in CVDM-CSM. The **Enable** button then toggles to Disable and the Edit button is enabled, allowing changes to the XML configuration values. To disable XML configuration, click the **Disable** button.

**Figure 11-4** XML Configuration Window



**Step 1** Click **Setup** from the task bar, then click **Miscellaneous** in the Setup pane.

**Step 2** Select **XML Config** from the object selector.

The XML Configuration dialog box appears, displaying the following columns.



Column	Description
VLAN ID	ID of the VLAN.
Client Group	Client-group can be either standard access-list name or ID (from 1 to 99).
Port	Specifies the TCP port on which the CVDM-CSM HTTP server listens.
Status	Status of XML service.
<b>Credentials</b>	
User Name	Name of the credentials user.
Password	Password of the credentials user.

From the XML Configuration dialog box, you do the following:

- Click **Edit** to edit the XML Configuration. For more information, see [“Editing XML Configuration” section on page 11-21](#).
- Click **Disable** to disable the XML Configuration in CVDM-CSM.

## Editing XML Configuration



### Note

The Edit button will be enabled only when you enable XML configuration in the CVDM-CSM module.

To edit the XML configuration:

- Step 1** Click **Setup** from the task bar, click Miscellaneous in the Setup pane.
- Step 2** Select **XML Config** from the object selector.
- Step 3** Click **Edit**. The Edit XML Configuration dialog box appears, displaying the following columns.

Column	Description
VLAN ID	Enter the ID of the VLAN.
Client Group	Enter the name or ID of the client group.
Port	Enter the TCP port on which the CVDM-CSM HTTP server listens.
Status	Specify, from the list, the status of XML service. You can choose between In Service or Out of Service.
<b>Credentials</b>	
User Name	Name of the credentials user.
Password	Password of the credentials user.

From this dialog box, you can do the following:

- Click **Add** to add the credentials by entering the username and the password.
- Select a row and click **Delete** to delete the corresponding credential.



---

## A

- action buttons, understanding [1-19](#)
- Advanced Setup wizard [2-13](#)
  - policy setup [2-14](#)
  - Welcome page [2-14](#)
- audience for this document [xiii](#)

---

## B

- Basic Setup wizard [2-3](#)
  - client VLAN
    - setup [2-4](#)
    - static routes, adding [2-8](#)
  - default policy [2-11](#)
  - server side VLAN
    - setup [2-4](#)
    - static routes, adding [2-8](#)
  - summary, displaying [2-12](#)
  - virtual server setup [2-9](#)
  - Welcome page [2-4](#)

---

## C

- client groups in policy nodes, viewing [7-21](#)

- configuring CSM [2-1](#)
  - Advanced Setup wizard [2-13](#)
    - policy setup [2-14](#)
    - Welcome page [2-14](#)
  - Basic Setup wizard [2-3](#)
    - client VLAN setup [2-4](#)
    - default policy [2-11](#)
    - server side VLAN setup [2-4](#)
    - summary, displaying [2-12](#)
    - virtual server setup [2-9](#)
    - Welcome page [2-4](#)
  - scenarios [2-15](#)
    - virtual server with default policy [2-16](#)
    - virtual server with L7 policy [2-17](#)
  - wizards, understanding [2-2](#)
- configuring CVDM-CSM with XML
  - viewing the configuration dialog [11-20](#)
- cookie maps, viewing
  - cookie maps [8-8](#)
  - cookie maps in policy nodes [7-18](#)
- cookie sticky groups, managing
  - adding [9-10](#)
  - editing [9-11](#)
  - viewing [9-8](#)

**D**

device transport log, viewing [1-31](#)  
 documentation  
   audience for this [xiii](#)  
   related to this product [xv](#)  
   specific to this product [xiv](#)  
   typographical conventions used in [xiii](#)  
 dual mode setup wizard, about [1-5](#)

**F**

fault tolerance, managing [11-1](#)  
   editing [11-5](#)  
   viewing, configuring [11-3](#)  
 fault tolerant group identification feature,  
   about [1-7](#)

**G**

getting started [1-1](#)  
   (see also configuring CSM) [2-1](#)  
   CLI commands, delivering to the device [1-32](#)  
   device transport log, viewing [1-31](#)  
   homepage [1-20](#)  
   key features [1-5](#)  
   navigating [1-13](#)  
     action buttons, understanding [1-19](#)  
     desktop, understanding [1-14](#)  
   preferences, modifying [1-30](#)

refreshing CVDM-C6500 [1-32](#)  
 setup page [1-25](#)  
 starting CVDM-CSM [1-8](#)

**H**

header maps, managing  
   adding [8-23](#)  
   viewing  
     header maps [8-20](#)  
     header maps in policy nodes [7-19](#)  
 health-monitoring configuration probes feature,  
   about [1-7](#)  
 homepage, about [1-20](#)

**K**

key features in CVDM-CSM [1-5](#)  
   dual mode setup wizard [1-5](#)  
   fault tolerate group identification [1-7](#)  
   health-monitoring configuration probes [1-7](#)  
   map configuration [1-6](#)  
   policy configuration [1-6](#)  
   real server configuration [1-6](#)  
   server farm configuration [1-6](#)  
   sticky group configuration [1-7](#)  
   virtual server setup [1-5](#)  
   VLAN setup [1-5](#)  
   XML configuration [1-7](#)

---

**M**

- maps, managing [8-1](#)
  - adding [8-7](#)
  - cookie maps
    - adding [8-9](#)
    - viewing [8-8](#)
  - header maps
    - adding [8-23](#)
    - viewing [8-20](#)
  - map configuration feature, about [1-6](#)
  - match conditions for return code maps
    - adding [8-16](#)
  - return code maps
    - adding [8-13](#)
    - viewing [8-11](#)
  - URL maps
    - adding [8-19](#)
    - viewing [8-18](#)
  - viewing
    - maps [8-2](#)
    - maps in policy nodes [7-18](#)

---

**N**

- netmask sticky groups, managing
  - adding [9-20](#)
  - editing [9-21](#)

---

**P**

- policies, managing [7-1](#)
  - (see also policy nodes, managing) [7-16](#)
  - adding [7-5](#)
  - editing [7-11](#)
  - policy configuration feature, about [1-6](#)
  - viewing [7-3](#)
- policy nodes, managing
  - (see also policies, managing) [7-1](#)
  - viewing [7-16](#)
  - viewing with action options selected [7-21](#)
    - server farms, backup server farms [7-22](#)
    - sticky groups [7-23](#)
  - viewing with condition options selected [7-17](#)
    - client group [7-21](#)
    - cookie maps [7-18](#)
    - header maps [7-19](#)
    - maps [7-18](#)
    - URL maps [7-20](#)
    - virtual servers [7-21](#)
- preferences, modifying [1-30](#)
- probes, managing [10-1](#)
  - adding [10-5](#)
  - editing [10-6](#)
  - viewing [10-3](#)

---

**R**

- real servers, managing **6-1**
  - adding **6-9**
  - editing **6-10**
  - real server configuration feature, about **1-6**
  - viewing
    - named real servers **6-2**
    - named real servers node **6-4**
    - unnamed real servers **6-6**
    - unnamed real servers node **6-7**
- Redirect virtual servers, managing
  - adding
    - to server farm nodes **5-35**
    - to server farms **5-10**
  - editing
    - in server farm nodes **5-37**
    - in server farms **5-18**
- refreshing CVDM-C6500 **1-32**
- return code maps, managing
  - adding **8-13**
  - match conditions for
    - adding **8-16**
  - viewing **8-11**
- named real servers, adding **5-23**
- real servers, editing **5-30**
- Redirect virtual servers
  - adding **5-35**
  - editing **5-37**
- unnamed real servers, adding **5-27**
- viewing **5-19**
- server farms, managing **5-1**
  - (see also server farm nodes, managing) **5-19**
  - adding **5-5**
  - editing **5-12**
  - health checkup details
    - adding **5-9**
    - editing **5-16**
  - NAT pools
    - adding **5-42**
    - editing **5-43**
    - viewing **5-40**
  - real server details
    - adding **5-8**
    - editing **5-15**
  - Redirect virtual server details
    - adding **5-10**
    - editing **5-18**
  - server farm configuration feature, about **1-6**
  - viewing
    - server farms **5-3**
    - server farms in policy nodes **7-22**
- SSL stick groups, managing

adding [9-23](#)  
 editing [9-24](#)  
 viewing [9-22](#)  
 starting CVDM-CSM [1-8](#)  
 sticky groups, managing [9-1](#)  
   adding [9-6](#)  
   cookie sticky groups  
     adding [9-10](#)  
     editing [9-11](#)  
     viewing [9-8](#)  
   editing [9-7](#)  
   netmask sticky groups  
     adding [9-20](#)  
     editing [9-21](#)  
   SSL stick groups  
     adding [9-23](#)  
     editing [9-24](#)  
     viewing [9-22](#)  
   sticky group configuration feature, about [1-7](#)  
   viewing  
     sticky groups [9-3](#)  
     sticky groups in policy nodes [7-23](#)

---

## T

typographical conventions used in this document [xiii](#)

---

## U

unnamed real servers, managing  
   adding to server farms [5-27](#)  
   unnamed real server nodes, viewing [6-7](#)  
   viewing [6-6](#)  
 URL maps, managing  
   adding [8-19](#)  
   viewing  
     URL maps [8-18](#)  
     URL maps in policy nodes [7-20](#)

---

## V

virtual servers, managing [4-1](#)  
   adding [4-5](#)  
   basic configuration details, adding [2-19](#), [4-6](#)  
   basic configuration details, editing [4-18](#)  
   clients, restricting [2-24](#), [4-11](#)  
   clients, restricting, editing [4-22](#)  
   default policy, viewing [4-36](#)  
   editing [4-17](#)  
   performance and other details, adding [2-28](#), [4-14](#)  
   performance and other details, editing [4-24](#)  
   policies, adding [2-21](#), [4-8](#)  
   policies, editing [4-20](#)  
   policies, viewing [4-34](#)  
   policy nodes, viewing in [7-21](#)  
   server farms, adding to [2-22](#), [4-9](#)

server farms, editing in [4-20](#)  
sticky connection details, adding [2-25, 4-12](#)  
sticky connection details, editing [4-23](#)  
viewing [4-3](#)  
virtual servers, individual, viewing [4-26](#)  
virtual server setup feature, about [1-5](#)

## VLANs, managing [3-1](#)

adding [3-4](#)  
editing [3-6](#)  
viewing [3-2](#)  
VLAN client, viewing [3-7](#)  
VLAN server, viewing [3-8](#)  
VLAN setup feature, about [1-5](#)

---

## W

### wizards

Advanced Setup wizard [2-13](#)  
    policy Setup [2-14](#)  
    Welcome page [2-14](#)  
Basic Setup wizard [2-3](#)  
    client VLAN and server side VLAN  
        setup [2-4](#)  
    default policy [2-11](#)  
    summary, displaying [2-12](#)  
    virtual server setup [2-9](#)  
    Welcome page [2-4](#)

wizards, understanding [2-2](#)

---

## X

XML, configuring CVDM-CSM with  
    viewing the configuration dialog [11-20](#)  
XML configuration feature, about [1-7](#)