



Cisco TelePresence Supervisor 2.3

Online help (printable format)

D15005.02

August 2014

Contents

Introduction	5
Using the web interface	6
Logging into the web interface	7
Failing to log into the web interface	8
Invalid passwords	8
Configuring the Cisco TelePresence Supervisor MSE 8050	9
Getting started with the Cisco TelePresence Supervisor MSE 8050	10
Activating the Cisco TelePresence Supervisor MSE 8050	12
Configuring network settings	14
IP configuration settings	14
IP status	15
Ethernet configuration	16
Ethernet status	16
Automatic IPv6 address preferences	17
Configuring DNS settings	19
View DNS status	19
Configuring IP routes settings	21
Port preferences	21
IP routes configuration	21
Configuring IP services	24
Configuring SNMP settings	26
System information	26
Configured trap receivers	26
Access control	27
Configuring QoS settings	28
QoS tags	28
Displaying and resetting system time	30
System time	30
NTP	30
Configuring security settings	32
Advanced account security mode	32
Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050	35
Upgrading the main Cisco TelePresence Supervisor MSE 8050 software image	35
Upgrading the loader software image	35
Backing up and restoring the configuration	36
Enabling Cisco TelePresence Supervisor MSE 8050 features	36
Backing up the Cisco TelePresence Supervisor MSE 8050 blade to the compact flash	37
Shutting down and restarting the Cisco TelePresence Supervisor MSE 8050	39
Managing users	40
System defined users	41
Displaying the user list	42
Deleting users	42
Adding and updating users	43
Adding a user	43
Updating a user	43
Updating your user profile	46
Changing your password	47

Displaying Cisco TelePresence Supervisor MSE 8050 status	48
Displaying general status	49
Displaying hardware health status	51
Displaying security status	52
Monitoring the chassis	53
Displaying the blades overview	54
Blades' status	54
Displaying the fan status	57
Fan trays status	57
Configuring the power supply monitoring	59
Supply voltage monitoring	59
Power shelf monitoring	60
Configuring the power status monitoring	61
Displaying the chassis status	62
MSE 8000 chassis information	62
Monitoring the blades	63
Displaying an individual blade's status	64
Blade status	64
Blade health	64
MCU and Telepresence Server tables	65
IP VCR tables	67
ISDN Gateway tables	68
IP Gateway tables	68
Individual blade ports configuration	70
IP configuration settings	70
IP status	71
Ethernet configuration	72
Ethernet status	72
Individual blade routes configuration	74
Port preferences	74
IP routes configuration	74
Current routes table	76
Individual blade services configuration	77
Individual blade shutdown	81
Monitoring port licenses	82
Displaying the port license summary	83
Port license status	83
License key management	85
Adding a new license key	85
Allocating port licenses to blades	86
Viewing a summary of current license usage	87
Allocating additional media port licenses by converting TS screen licenses	88
Allocating additional TS screen licenses by converting media port licenses	88
Clustering	90
Understanding clustering	91
About clustering	91
Displaying the clustering summary	93
Cluster warnings	93

Configuring clustering	96
Reviewing cluster configuration	98
Alarms	99
Displaying the alarm status	100
Displaying the alarm log	101
Configuring alarm levels	104
Advanced topics	105
Working with the event logs	106
Event log	106
Audit log	107
Working with the audit log	108
Audit log	108
Understanding security warnings	109
Logging using syslog	112
Syslog settings	112
Using syslog	113
Management event receivers	115
Feedback receivers	116
Individual blade backup configuration	117
Backing up a configuration	117
Restoring a configuration	117
Customizing the user interface	118
Configuring welcome messages for the Login and Home pages	118
Adding headers and footers	118
Network connectivity testing	120
Configuring SSL certificates	121
Prerequisites	121
Managing the local certificate	121
Managing trust stores	122
Configuring HTTPS verification	123
OCSP checks for client certificate revocation	124
Certificate details reference	126
Transitioning to certificate-based security	127
Enabling client certificates and certificate login (HTTPS connections)	127
Enabling OCSP checking	127
Requiring certificate-based login (all connections)	128
Further information	130

Introduction

This document contains the text of the online help for the Cisco TelePresence Supervisor MSE 8050 Version 2.3 web user interface. It is provided so that the help text can be viewed or printed as a single document.

Using the web interface

This section describes how to sign in to the Cisco TelePresence Supervisor MSE 8050.

Logging into the web interface	7
Failing to log into the web interface	8

Logging into the web interface

The TANDBERG Codian Cisco TelePresence Supervisor MSE 8050 web interface is used for administering the MSE 8000 chassis including all its blades, fans and power supplies. Depending on the blades that you have fitted, you can manage conferences, recordings and IP to ISDN and ISDN to IP calls.

When connecting to the TANDBERG Codian Cisco TelePresence Supervisor MSE 8050 web interface, you must log in so that the Cisco TelePresence Supervisor MSE 8050 can associate the session with your configured user and a set of access privileges. The Cisco TelePresence Supervisor MSE 8050 has a set of configured users, and each user has a username and password that are used for logging in.

1. Using a web browser, enter the host name or IP address of the Cisco TelePresence Supervisor MSE 8050.
2. To log in as the administrator, click **Log in** and enter your assigned **Username** and **Password**.
3. Click **OK**

The main menu appears, restricting the available options based on your access privileges. Administrators have full access; List only users can only see the list of installed hardware, including blades, fan trays, power supplies and chassis information.

The **Login** page of the Cisco TelePresence Supervisor MSE 8050 displays a welcome banner which administrators can configure to display text relevant to your organization. For more information, refer to [Customizing the user interface \[p.118\]](#).

Related topics

- [Failing to log into the web interface \[p.8\]](#)

Failing to log into the web interface

When connecting to the Cisco TelePresence Supervisor MSE 8050 web interface, you must log in so that the Cisco TelePresence Supervisor MSE 8050 can associate the session with your configured user and a set of access privileges. The Cisco TelePresence Supervisor MSE 8050 has a set of configured users, and each user has an ID and password that are used for logging in.

If you see the **Access denied** page, you have not been able to log in for one of the following reasons:

- **Invalid username/password:** you have typed the incorrect username and/or password.
If Advanced account security mode is enabled and you incorrectly type the username and/or password three times and if this is an admin account, it is disabled for 30 minutes; for any other account, it is disabled indefinitely (or until you, the administrator, re-enable the account from the **User** page)
- **No free sessions:** the maximum number of sessions allowed simultaneously on the Cisco TelePresence Supervisor MSE 8050 has been exceeded
- **Your IP address does not match that of the browser cookie you supplied:** try deleting your cookies and log in again
- **You do not have access rights to view this page:** you do not have the access rights necessary to view the page that you attempted to see
- **Page expired:** the **Change password** page can expire if the Cisco TelePresence Supervisor MSE 8050 is not entirely happy that the user who requested to change password, is actually the user submitting the change password request. (This may happen if you use a new browser tab to submit the request.)

Invalid passwords

If Advanced account security mode has been enabled, the Cisco TelePresence Supervisor MSE 8050 will disable a user's account if that user incorrectly enters a password three times consecutively. If this is an admin account, it is disabled for 30 minutes; for any other account, it is disabled indefinitely (or until you, the administrator, re-enable the account from the **Users** page)

Related topics

- [Configuring security settings \[p.32\]](#)

Configuring the Cisco TelePresence Supervisor MSE 8050

This section describes how to perform basic configuration tasks for the Cisco TelePresence Supervisor MSE 8050.

Getting started with the Cisco TelePresence Supervisor MSE 8050	10
Activating the Cisco TelePresence Supervisor MSE 8050	12
Configuring network settings	14
Configuring DNS settings	19
Configuring IP routes settings	21
Configuring IP services	24
Configuring SNMP settings	26
Configuring QoS settings	28
Displaying and resetting system time	30
Configuring security settings	32
Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050	35
Shutting down and restarting the Cisco TelePresence Supervisor MSE 8050	39

Getting started with the Cisco TelePresence Supervisor MSE 8050

Ensure you have correctly completed the physical setup of the Cisco TelePresence MSE 8000 chassis following the instructions contained in the Getting Started Guide that accompanied the chassis and on the web site.

Before you can start using the chassis, you need to log in to the web interface of the Cisco TelePresence Supervisor MSE 8050 blade using the IP address you found or set using the Getting Started Guide and complete the setup of the blade as follows using the online help for each web interface page to guide you:

1. If you see the *New supervisor inserted* banner, follow the Activation wizard (for more information, refer to [Activating the Cisco TelePresence Supervisor MSE 8050 \[p.12\]](#)). This only appears if you are using Supervisor software version 1.1(1) or later: these versions support port licensing.
2. We recommend that you change the admin account to use a password as soon as possible. To do that, go to **Settings > Users**, click the admin link, and provide the required user information.
3. Go to **Hardware > Blades** and the Status column. For every slot in which there is a blade fitted, the status should be *Blade OK*. If not, go to **Alarms** to see more information about the problem. If necessary, refit any blades to resolve the alarms.
4. Set up the Cisco TelePresence Supervisor MSE 8050 blade.
 - a. Go to **Network > Port** and choose DHCP or static IP for the Cisco TelePresence Supervisor MSE 8050 - and Ethernet settings.
 - b. Go to **Network > Routes**, **Network > Services** and **Network > SNMP** in turn and set up appropriately.
 - c. Go to **Settings > User** and set a password for the admin user account. Choose a password that you will remember and that is not easy to guess, and keep the password confidential.
 - d. Go to **Settings > Time** and set system time or set up NTP server.
 - e. Go to **Hardware** and select your blade.
 - f. Go to **Backup** and configure automatic backups.
 - g. Go to **Alarms > Alarm levels** and chose settings.
 - h. Configure the capture and display filters for events and configure syslog servers if you intend to use them.
5. Set up the other blades. For each blade:
 - a. Go to **Hardware > Blades** and check the Status column. For every slot in which there is a blade fitted, the status should be *Blade OK*. If not, go to **Alarms** to see more information about the problem.
 - b. Go to **Hardware > Blades**, click on the slot number and then click **Port A** tab.
 - c. Choose DHCP or static IP for the blade - and set the Ethernet settings.
 - d. Go to **Hardware > Blades**, click on the slot number, and click the **Backup** tab and configure the backup of each individual blade.
6. As a final check, go to **Hardware > Blades**, **Hardware > Fan trays**, and **Hardware > Power supplies** in turn and check the Status column in each case.

Related topics

- [Activating the Cisco TelePresence Supervisor MSE 8050 \[p.12\]](#)
- [Displaying the alarm status \[p.100\]](#)
- [Displaying the blades overview \[p.54\]](#)
- [Displaying the fan status \[p.57\]](#)

- [Configuring the power supply monitoring \[p.59\]](#)
- [Displaying the chassis status \[p.62\]](#)

Activating the Cisco TelePresence Supervisor MSE 8050

The **New Supervisor blade inserted** page allows you to choose a backup configuration file with which to activate a new Supervisor blade in the chassis. The page also allows you to check port license allocation and clustering configuration before you activate the Cisco TelePresence Supervisor MSE 8050. This page will appear for both a new Cisco TelePresence Supervisor MSE 8050 and for a Cisco TelePresence Supervisor MSE 8050 that has been taken from another chassis and inserted into this chassis.

The **New Supervisor blade inserted** page is in the style of a 'wizard'. Follow the steps below to activate the new Supervisor blade:

1. Do you want to load a backup configuration? Choose from:
 - **Load master backup:** This is the most recent master backup that is stored on the Cisco TelePresence Supervisor MSE 8050. An administrator makes a master backup by clicking the **Create master backup** button on the **Hardware > Blades > Blade 1** page in the Cisco TelePresence Supervisor MSE 8050's user interface. If you choose this option, when you click **Activate** the Cisco TelePresence Supervisor MSE 8050 will be configured with this backup and will not retain any existing settings.
 - **Load automatic backup:** This is the most recent automatically-created backup stored on the Cisco TelePresence Supervisor MSE 8050. For information about automatic backups, refer to [Individual blade backup configuration \[p.117\]](#). If you choose this option, when you click **Activate** the Cisco TelePresence Supervisor MSE 8050 will be configured with this backup and will not retain any existing settings.
 - **Do not restore any backup:** The Cisco TelePresence Supervisor MSE 8050 will not restore a backup and when you click **Activate**, the Cisco TelePresence Supervisor MSE 8050 will be activated with its existing configuration. For a new Cisco TelePresence Supervisor MSE 8050, this will be default factory settings; for a Cisco TelePresence Supervisor MSE 8050 moved from another chassis, this will be its last configuration.
2. Inspect port license allocation. Click **Inspect port license allocation** and check that the port licenses are allocated as you intend. Note that if you have chosen to load a backup configuration, the port license allocation that you are inspecting is from that backup configuration. When you click **Activate**, the Cisco TelePresence Supervisor MSE 8050 will enforce the port licenses as they are allocated in its configuration. In the case of this being a different allocation to the existing allocation, there could be interruption to services on blades that are currently in use.
3. Inspect cluster allocation. Click **Inspect cluster allocation** to see the clustering configuration that the Cisco TelePresence Supervisor MSE 8050 will apply to blades in the chassis. You need to check that this is as you would expect it to be; a new clustering configuration can cause blades to require a restart when you click **Activate**. Note that if you have chosen to load a backup configuration, the clustering allocation that you are inspecting is from that backup configuration.
4. Click **Activate**.

Related topics

- [Getting started with the Cisco TelePresence Supervisor MSE 8050 \[p.10\]](#)
- [Displaying the port license summary \[p.83\]](#)
- [Displaying the clustering summary \[p.93\]](#)
- [Configuring clustering \[p.96\]](#)

- [Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 \[p.35\]](#)
- [Individual blade backup configuration \[p.117\]](#)

Configuring network settings

To configure the network settings on the Cisco TelePresence Supervisor MSE 8050 and check the network status, go to **Network > Port A**.

The Cisco TelePresence Supervisor MSE 8050 has two Ethernet interfaces, Port A and Port B. However, Port B is not supported and cannot be enabled. Therefore, although there is a **Network > Port B** settings page, you cannot change any settings for Port B.

Port A can be configured to be allocated its IP addresses by DHCP (IPv4) or SLAAC/DHCPv6 (IPv6).

On this page:

- [IP configuration settings](#)
- [IP status](#)
- [Ethernet configuration](#)
- [Ethernet status](#)

IP configuration settings

These settings determine the IP configuration for the appropriate Ethernet port of the Cisco TelePresence Supervisor MSE 8050. When you have finished, click **Update IP configuration**.

Field	Field description	Usage tips
IPv4 configuration		
IP configuration	Specifies whether the port should be configured manually or automatically. If set to <i>Automatic via DHCP</i> the Cisco TelePresence Supervisor MSE 8050 obtains its own IP address for this port automatically via DHCP (Dynamic Host Configuration Protocol). If set to <i>Manual</i> the Cisco TelePresence Supervisor MSE 8050 will use the values that you specify in the Manual configuration fields below.	It is not possible to disable a port if it is being used to access the web user interface, however, it can be disabled via the serial connection. To disable a port that is currently being used to access the web interface via this field, change to a different port for web interface access.
Manual configuration		
IP address	The dot-separated IPv4 address for this port, for example 192.168.4.45	You only need to specify this option if you have chosen <i>Manual</i> IP configuration, as described above. If IP configuration is set to <i>Automatic by DHCP</i> this setting will be ignored.
Subnet mask	The subnet mask required for the IP address you want to use, for example 255.255.255.0	
Default gateway	The IP address of the default gateway on this subnet, for example 192.168.4.1	

IPv6 configuration

IP configuration Specifies whether the port should be configured manually or automatically, or disabled. If set to *Automatic via SLAAC/DHCPv6* the Cisco TelePresence Supervisor MSE 8050 obtains its own IP address for this port automatically. The protocol used will be SLAAC, Stateful DHCPv6, or Stateless DHCPv6 as indicated by the ICMPv6 Router Advertisement (RA) messages. If set to *Manual* the Cisco TelePresence Supervisor MSE 8050 will use the values that you specify in the Manual configuration fields below.

Manual configuration

IPv6 address	The (hexadecimal) colon-separated IPv6 address for this port, for example [2001:db8:168:4::45]. See Automatic IPv6 address preferences [p.17] for more information about IPv6 addresses that are assigned automatically.	You only need to specify this option if you have chosen <i>Manual</i> IP configuration, as described above. If IP configuration is set to <i>Automatic via SLAAC/DHCPv6</i> this setting is ignored. When you enter an IPv6 address anywhere in the user interface, the address must be enclosed in square brackets [].
Prefix length	The (decimal) prefix length value for the global IPv6 address for this port. In the above IPv6 address example, the prefix length is 64.	
Default gateway	Optionally, specifies the IPv6 address of the default gateway on this subnet.	The address can be global or link-local.

IP status

Use the IP status fields to verify the current IP settings for the appropriate Ethernet port of the Cisco TelePresence Supervisor MSE 8050, which were obtained using DHCP/SLAAC or configured manually (see [IP configuration settings](#)) including:

- DHCP
- IP address
- Subnet mask
- Default gateway
- DHCPv6
- IPv6 address
- IPv6 default gateway
- IPv6 link-local address

Ethernet configuration

These settings determine the Ethernet settings for the appropriate port of the Cisco TelePresence Supervisor MSE 8050. Refer to the table for assistance with these settings. When you have finished, click **Update Ethernet configuration**.

Field	Field description	Usage tips
Ethernet settings	Specify whether you want this Ethernet port to automatically negotiate its Ethernet settings with the device it is connected to, or if it should use the values that you specify in the Manual configuration fields below.	It is important that your Ethernet settings match those of the device to which this port is connected. For example, both devices must be configured to use automatic negotiation, or both configured with fixed and matching speed and duplex settings (see below).

Manual configuration

Speed	Identifies the connection speed: <i>10 Mbit/s</i> or <i>100 Mbit/s</i> . Use automatic negotiation if a connection speed of <i>1000 Mbit/s</i> is required.	The connection speed must match that of the device to which this port is connected. You only need to select this option if you have chosen <i>Manual</i> Ethernet settings, as described above.
Duplex	Identifies the connection duplex mode: <ul style="list-style-type: none"> ■ <i>Full duplex</i> Both devices can send data to each other at the same time ■ <i>Half duplex</i> Only one device can send to the other at a time 	The duplex setting must match that of the device to which this port is connected. You only need to select this option if you have chosen <i>Manual</i> Ethernet settings, as described above.

Ethernet status

Field	Field description	Usage tips
Link status	Indicates whether this Ethernet port is connected to or disconnected from the network.	
Speed	The speed (<i>10/100/1000 Mbit/s</i>) of the network connection to the MCU on this port.	This value is negotiated with the device to which this port is connected or based on your Manual configuration selected above.
Duplex	The duplex mode (<i>Full duplex</i> or <i>Half duplex</i>) of the network connection to this port.	This value is negotiated with the device to which this port is connected or based on your Manual configuration selected above.
MAC address	The fixed hardware MAC (Media Access Control) address of this port.	This value cannot be changed and is for information only.

Packets sent	Displays a count of the total number of packets sent from this port by the MCU. This includes all TCP and UDP traffic.	When troubleshooting connectivity issues, this information can help you confirm that the MCU is transmitting packets into the network.
Packets received	Displays a count of the total number of packets received by this port of the MCU. This includes all TCP and UDP traffic.	When troubleshooting connectivity issues, this information can help you confirm that the MCU is receiving packets from the network.
Statistics:	<p>These fields display further statistics for this port.</p> <ul style="list-style-type: none"> ■ Multicast packets sent ■ Multicast packets received ■ Total bytes sent ■ Total bytes received ■ Receive queue drops ■ Collisions ■ Transmit errors ■ Receive errors 	Use these fields for advanced network diagnostics, such as resolution of problems with Ethernet link speed and duplex negotiation.

Related topics

- [Configuring DNS settings \[p.19\]](#)
- [Configuring IP routes settings \[p.21\]](#)
- [Configuring IP services \[p.24\]](#)
- [Configuring SNMP settings \[p.26\]](#)
- [Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 \[p.35\]](#)
- [Network connectivity testing \[p.120\]](#)

Automatic IPv6 address preferences

The table below details the address assignment preferences that are applied for IPv6 addressing based on the ICMPv6 Router Advertisements received when port configuration is set to Automatic.

RA flags			Preferred address
a	o	m	
0	0	0	Stateful DHCPv6
1	0	0	SLAAC
0	1	0	Stateful DHCPv6
1	1	0	Stateless DHCPv6
0	0	1	Stateful DHCPv6
1	0	1	Stateful DHCPv6

0	1	1	Stateful DHCPv6
1	1	1	Stateful DHCPv6

a: ICMPv6 prefix information, auto flag

o: ICMPv6, other flag

m: ICMPv6, managed flag

Related topics

- [Configuring network settings \[p. 14\]](#)

Configuring DNS settings

To configure DNS settings on the Cisco TelePresence Supervisor MSE 8050, go to **Network > DNS**. These settings determine the DNS configuration for the Cisco TelePresence Supervisor MSE 8050.

Click **Update DNS configuration** after making any changes.

Field	Field description	Usage tips
DNS configuration	Select a DNS server preference from the list or select <i>Manual</i> to specify DNS settings manually.	<p>If you select <i>Manual</i>, you must configure the name server(s) on this page. If you select one of the DHCP options, the Cisco TelePresence Supervisor MSE 8050 receives its nameserver address via DHCP on the interface you select.</p> <p>If <i>Automatic via DHCP</i> (IPv4) or <i>Automatic via SLAAC/DHCPv6</i> (IPv6) is selected for IP configuration (on the Ethernet Port's configuration page), no DNS name server will be available until the Cisco TelePresence Supervisor MSE 8050 receives the address via DHCP on that interface.</p> <p>For example, if you select <i>Via Port A DHCPv6</i> for DNS configuration, you must ensure that Port A is configured to use DHCPv6. Do this by going to the Network > Port A page and selecting <i>Automatic via SLAAC/DHCPv6</i> in the IP configuration field of the IPv6 interface.</p> <p>Note that if the DHCP server on your network does not supply DNS configuration information, then the Cisco TelePresence Supervisor MSE 8050 will have no ability to look up names. Additionally, for IPv6 the Router Advertisement packets determine whether or not DHCPv6 is used.</p>
Host name	Specifies a name for the Cisco TelePresence Supervisor MSE 8050.	Depending on your network configuration, you may be able to use this host name to communicate with the Cisco TelePresence Supervisor MSE 8050, without needing to know its IP address.
Name server	The IP address of the name server.	
Secondary name server	Identifies an optional second name server.	The secondary DNS server is only used if the first is unavailable. If the first server returns that it does not know an address, the secondary DNS server will not be queried.
Domain name (DNS suffix)	Specifies an optional suffix to add when performing DNS lookups.	<p>This option can allow you to use non-fully qualified host names when referring to a device by host name instead of IP address.</p> <p>For example, if the domain name is set to <i>cisco.com</i>, then a request to the name server to look up the IP address of host <i>endpoint</i> will actually lookup <i>endpoint.cisco.com</i>.</p>

View DNS status

Use the DNS status fields to verify the current DNS settings for the Cisco TelePresence Supervisor MSE 8050, including:

- Host name
- Name server
- Secondary name server
- Domain name (DNS suffix)

Related topics

- [Configuring network settings \[p.14\]](#)
- [Configuring IP routes settings \[p.21\]](#)
- [Configuring IP services \[p.24\]](#)

Configuring IP routes settings

If the *Video Firewall* feature is enabled (see [Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 \[p.35\]](#)), you will need to set up one or more routing settings to control how IP traffic flows in and out of the Cisco TelePresence Supervisor MSE 8050.

It is important that these settings are configured correctly, or you may be unable to make calls or access the web interface.

To configure the route settings, go to **Network > Routes**.

Note you can also configure individual blade routes by going to **Hardware > Blade > Routes**. For more information, refer to [Individual blade routes configuration \[p.74\]](#).

On this page:

- [Port preferences](#)
- [IP routes configuration](#)

Port preferences

If both Ethernet ports are enabled, it is necessary to specify which port is used in certain special circumstances. Make the appropriate selections described below. Click **Apply changes**.

Field	Field description	Usage tips
IPv4 gateway preference	Select the port whose default gateway setting the Cisco TelePresence Supervisor MSE 8050 will use to send IPv4 traffic in the absence of more specific routing (see IP routes configuration). The Supervisor routes IPv4 packets to the IPv4 default gateway when it does not have a more specific route. Therefore you only need one default IPv4 gateway, even though you may have configured <i>different</i> IPv4 default gateways on the Supervisor's ports.	Ethernet Port B is not supported on the Cisco TelePresence Supervisor MSE 8050 and so the Port B option cannot be selected.
IPv6 gateway preference	Select the port whose default gateway setting the Cisco TelePresence Supervisor MSE 8050 will use to send IPv6 traffic in the absence of more specific routing (see IP routes configuration). The Supervisor routes IPv6 packets to the IPv6 default gateway when it does not have a more specific route. Therefore you only need one default IPv6 gateway, even though you may have configured <i>different</i> IPv6 default gateways on the Supervisor's ports.	Ethernet Port B is not supported on the Cisco TelePresence Supervisor MSE 8050 and so the Port B option cannot be selected.

IP routes configuration

In this section you can control how IP packets should be directed out of the Cisco TelePresence Supervisor MSE 8050. You should only change this configuration if you have a good understanding of the topology of the network(s) to which the Cisco TelePresence Supervisor MSE 8050 is connected.

Configuration of routes is divided into two sections: addition of new routes, and the display and removal of existing routes.

Adding a new IP route

To add a new route, enter the details using the table below for reference. Click **Add IP route** to make the addition. If the route already exists, or aliases (overlaps) an existing route, you will be prompted to correct the problem and try again. The Cisco TelePresence Supervisor MSE 8050 can support up to 128 routes in total.

Field	Field description	Usage tips
IP address / mask length	Use these fields to define the type of IP addresses to which this route applies. IPv4 addresses must be in the dot-separated IPv4 format and IPv6 addresses must be in hexadecimal colon-separated IPv6 address format, while the mask length is chosen in the mask length field. IPv6 addresses must be enclosed in square brackets. The mask field specifies how many bits of the address are fixed; unfixed bits must be set to zero in the address specified.	To route all IP addresses in the range 192.168.4.128 to 192.168.4.255 for example, specify the IP address as 192.168.4.128 and the mask length as 25, to indicate that all but the last seven bits address are fixed.
Route	Use this field to control how packets destined for addresses matching the specified pattern are routed.	You may select <i>Port A</i> , <i>Port B</i> or <i>Gateway</i> . If <i>Gateway</i> is selected, specify the IP address of the gateway to which you want packets to be directed. Selecting <i>Port A</i> results in matching packets being routed to Port A's default gateway (see Configuring network settings [p.14]). Port B is not supported on the Cisco TelePresence Supervisor MSE 8050 so the <i>Port B</i> option should not be selected.

Viewing and deleting existing IP routes

Configured routes are listed below the **Add IP route** section in a separate section each for IPv4 and IPv6. For each route, the following details are shown:

- Destination: The IP address or address block that the route applies to.
- Gateway: The IP address of the gateway where matching packets will be routed through. This can be '-' if the destination is in the local subnets, the IP address of a default gateway of a particular network interface, or the IP address of a user specified gateway.
- Port: Physical network interface that matching packets will be sent through.
- Type: Whether the route has been configured automatically as a consequence of other settings, or added by the user as described above.

The *default* route is configured automatically in correspondence with the *Default gateway preference* field (see [Port preferences](#)) and cannot be deleted. Any packets not covered by manually configured routes will be routed according to this route.

Manually configured routes may be deleted by selecting the appropriate check box and clicking **Delete selected**.

Routes behavior with disabled ports

If you disable the Ethernet port that is currently specifying the default gateway, then there is no default gateway and the only destinations that are reachable are those that are either on the same subnet as the enabled Ethernet port or are covered by an explicit route that uses that port.

Similarly, if you disable the Ethernet port that is used by an explicit route, then destinations that are covered by that route cease to be reachable.

Note: Be very careful when changing routing as it is possible make the Cisco TelePresence Supervisor MSE 8050 unreachable from your PC (or any device used to connect to the web interface). You need to ensure that at all times one of the following is true:

- The Cisco TelePresence Supervisor MSE 8050 has an enabled interface on the same subnet as the PC.
- The Cisco TelePresence Supervisor MSE 8050 has an explicit route that includes the PC's address and goes through an enabled interface.
- The Cisco TelePresence Supervisor MSE 8050 does not have an explicit route that includes the PC's address but does have a default route through an enabled interface that reaches the PC.

Related topics

- [Configuring network settings \[p. 14\]](#)
- [Configuring IP services \[p.24\]](#)
- [Configuring SNMP settings \[p.26\]](#)
- [Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 \[p.35\]](#)
- [Individual blade routes configuration \[p.74\]](#)

Configuring IP services

To configure IP services, go to **Network > Services**.

Use this page to allow or deny access to the listed network services on the Cisco TelePresence Supervisor MSE 8050. Refer to the table below for more details.

You can control which services may be accessed on the unit's Ethernet interface and the TCP/UDP ports through which those services are available.

Check the boxes next to the service names, edit the port numbers if necessary, and then click **Apply Changes**. If the port number for a service is changed, it is necessary to ensure that the new value chosen does not clash with the port number used by any of the other services; it is not, however, normally necessary to use anything other than the pre-configured default values.

You can configure services of an individual blade by going to **Hardware > Blade > Services**. For more information, refer to [Individual blade services configuration \[p.77\]](#).

Note that by default SNMP Traps are sent to port UDP port 162 (on the destination network management station); this is configurable. For more information, refer to [Configuring SNMP settings \[p.26\]](#).

To reset all values back to their factory default settings, click **Reset to default** and then click **Apply changes**.

Field	Field description	Usage tips
TCP services		
HTTP	Enable/disable HTTP access on the specified interface or change the port that is used for this service.	<p>HTTP access is required to view and change the Cisco TelePresence Supervisor MSE 8050 web pages and read online help files. If you disable web access you will need to use the serial console interface to re-enable it.</p> <p>If you require advanced security for the Cisco TelePresence Supervisor MSE 8050, disable web access.</p> <p>If a port is disabled, this option will be unavailable.</p>
HTTPS	Enable/disable secure (HTTPS) web access on the specified interface or change the port that is used for this service.	<p>This field is only visible if the Cisco TelePresence Supervisor MSE 8050 has the <i>Secure management (HTTPS)</i> feature key or an <i>Encryption</i> feature key installed. For more information about installing feature keys, refer to Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 [p.35].</p> <p>By default, the Cisco TelePresence Supervisor MSE 8050 has its own SSL certificate and private key. However, you can upload a new private key and certificates if required. For more information about SSL certificates, refer to Configuring SSL certificates [p.121].</p> <p>If a port is disabled, this option will be unavailable.</p>

FTP	Enable/disable FTP access on the specified interface or change the port that is used for this service.	FTP can be used to upload and download Cisco TelePresence Supervisor MSE 8050 configuration. You should consider disabling FTP access on any port that is outside your organization's firewall. If you require advanced security for the Cisco TelePresence Supervisor MSE 8050, disable FTP access. If a port is disabled, this option will be unavailable.
-----	--	---

UDP services

SNMP	Enable/disable the receiving of the SNMP protocol on this port or change the port that is used for this service.	Note that by default SNMP Traps are sent to port UDP port 162 (on the destination network management station); this is configurable. For more information, refer to Configuring SNMP settings [p.26] . If you require advanced security for the Cisco TelePresence Supervisor MSE 8050, disable the SNMP service.
------	--	--

Related topics

- [Configuring network settings \[p.14\]](#)
- [Configuring IP routes settings \[p.21\]](#)
- [Configuring SNMP settings \[p.26\]](#)
- [Configuring SSL certificates \[p.121\]](#)
- [Individual blade services configuration \[p.77\]](#)

Configuring SNMP settings

To configure monitoring using SNMP, go to **Network > SNMP**.

The Cisco TelePresence Supervisor MSE 8050 sends out an SNMP trap when the device is shut down or started up. The SNMP page allows you to set various parameters; when you are satisfied with the settings, click **Update SNMP settings**.

Note that:

- The 'system uptime' that appears in the trap is the time since SNMP was initialized on the Cisco TelePresence Supervisor MSE 8050 (and therefore will differ from the **Uptime** reported by the Cisco TelePresence Supervisor MSE 8050 on the **Status > General** page).
- The SNMP MIBs are read-only.

System information

Field	Field description	Usage tips
Name	Identifies the Cisco TelePresence Supervisor MSE 8050 in the SNMP system MIB.	Usually you would give every device a unique name. The default setting is: Codian MSE Supervisor
Location	The location that appears in the system MIB.	An optional field. With multiple Cisco TelePresence Supervisor MSE 8050 blades in different offices, it is useful to identify where the blade is located.
Contact	The contact details that appear in the system MIB.	An optional field. The default setting is: <i>Unknown</i> Add the administrator's email address or name to identify who to contact when there is a problem with the device. If SNMP is enabled for a port on the public network, take care with the details you provide here.
Description	A description that appears in the system MIB.	An optional field, by default this will indicate the model number of the blade. Can be used to provide more information on the Cisco TelePresence Supervisor MSE 8050.

Configured trap receivers

Field	Field description	Usage tips
Enable traps	Select this check box to enable the Cisco TelePresence Supervisor MSE 8050 to send traps.	If you do not select this check box, no traps will be sent.
Enable authentication failure trap	Select this check box to enable authentication failure traps.	You cannot select this check box unless you have selected to Enable traps above. Authentication failure traps are generated and sent to the trap receivers when someone tries to read or write a MIB value with an incorrect community string.

Trap receiver addresses 1 to 4	Enter the IP address or hostname for up to four devices that will receive both the general and the authentication failure traps.	The traps that are sent by the Cisco TelePresence Supervisor MSE 8050 are all SNMP v1 traps. You can configure trap receivers or you can view the MIB using a MIB browser. You can set the UDP port number for the trap in the format <IP address>: <port number>. By default the UDP port number is 162.
--------------------------------	--	---

Access control

Field	Field description	Usage tips
RO community	Community string/password that gives read-only access to all trap information.	Note that SNMP community strings are not secure. They are sent in plain text across the network.
RW community	Community string/password that gives read/write access to all trap information.	It is advisable to change the community strings before enabling SNMP as the defaults are well known.
Trap community	Community string/password that is sent with all traps.	Some trap receivers can filter on trap community.

Related topics

- [Configuring DNS settings \[p.19\]](#)
- [Configuring network settings \[p.14\]](#)
- [Configuring IP routes settings \[p.21\]](#)
- [Configuring IP services \[p.24\]](#)

Configuring QoS settings

Quality of Service (QoS) settings are defined on the **Network > QoS** page to set priorities for outbound traffic from the Cisco TelePresence Supervisor MSE 8050. They are specified as 6-bit binary values (tags) in the *Type of Service* header field for IPv4 or the *Traffic Class* header field for IPv6, and can be interpreted by networks as Type of Service (ToS) or Differentiated Services (DiffServ).

QoS tags are supported for the administration packet type transmitted by the Cisco TelePresence Supervisor MSE 8050.

CAUTION: We advise you not to alter QoS settings unless you have specific requirements to do so.

QoS tags

Field (tag)	Defines priority for...
OA&M	Administration packets, including HTTP, HTTPS, FTP, DNS, syslog, OCSP, and NTP traffic.

ToS configuration

ToS uses six out of a possible eight bits. The Cisco TelePresence Supervisor MSE 8050 allows you to set bits 0 to 5, and places zeros for bits 6 and 7.

- Bits 0-2 set IP precedence (the priority of the packet).
- Bit 3 sets delay: 0 = normal delay, 1 = low delay.
- Bit 4 sets throughput: 0 = normal throughput, 1 = high throughput.
- Bit 5 sets reliability: 0 = normal reliability, 1 = high reliability.
- Bits 6-7 are reserved for future use and cannot be set using the Cisco TelePresence Supervisor MSE 8050 interface.

ToS configuration represents a tradeoff between precedence, delay, throughput, and reliability. Ensure that you maintain a balance when prioritizing packets, so that other packets on the network are not subject to undue delay (so for example, do not set every value to 1).

DiffServ configuration

DiffServ uses six out of a possible eight bits to set a codepoint. There are 64 possible codepoints. The Cisco TelePresence Supervisor MSE 8050 allows you to set bits 0 to 5, and places zeros for bits 6 and 7. The codepoint is interpreted by DiffServ nodes to determine how the packet is treated.

Default value

The default QoS setting on the Cisco TelePresence Supervisor MSE 8050 is *000000*.

To revert to the default value, click **Reset to default**.

Changes to QoS settings require a reboot to take effect.

More information

For more information about QoS, including ToS and DiffServ values, see the relevant RFCs on the Internet Engineering Task Force web site www.ietf.org:

- RFC 791
- RFC 2474
- RFC 2597
- RFC 3246

Related topic

- [Configuring network settings \[p. 14\]](#)

Displaying and resetting system time

The system date and time for the Cisco TelePresence Supervisor MSE 8050 can be set manually or using the Network Time Protocol (NTP).

To configure Time settings, go to [Settings > Time](#).

System time

The current system date and time is displayed.

If you do not have NTP enabled and need to update the system date and/or time manually, type the new values and click **Change system time**.

NTP

The Cisco TelePresence Supervisor MSE 8050 supports the NTP protocol. Configure the settings using the table below for help, and then click **Update NTP settings**.

The Cisco TelePresence Supervisor MSE 8050 re-synchronizes with the NTP server via NTP every hour.

If there is a firewall between the Cisco TelePresence Supervisor MSE 8050 and the NTP server, configure the firewall to allow NTP traffic to UDP port 123.

If the NTP server is local then the Cisco TelePresence Supervisor MSE 8050 will automatically use the appropriate port to communicate with the NTP server. If the NTP server is not local, the Cisco TelePresence Supervisor MSE 8050 will use the port that is configured as the default gateway to communicate with the NTP server, unless a specific IP route to the NTP server's network/IP address is specified. To configure the default gateway or an IP route, go to [Network > Routes](#).

Field	Field description	Usage tips
Enable NTP	If selected, use of the NTP protocol is Enabled on the Cisco TelePresence Supervisor MSE 8050.	
UTC offset	The offset of the time zone that you are in from Greenwich Mean Time.	You must update the offset manually when the clocks go backwards or forwards: the Cisco TelePresence Supervisor MSE 8050 does not adjust for daylight saving automatically.
NTP host	The IP address or hostname of the server that is acting as the time keeper for the network.	

Using NTP over NAT (Network Address Translation)

If NAT is used between the Cisco TelePresence Supervisor MSE 8050 and the NTP server, with the Cisco TelePresence Supervisor MSE 8050 on the NAT's local network (and not the NTP server), no extra configuration is required.

If NAT is used between the Cisco TelePresence Supervisor MSE 8050 and the NTP server, with the NTP server on the NAT's local network, then configure the NAT forwarding table to forward all data to UDP port 123 to the NTP server.

Related topics

- [Configuring IP routes settings \[p.21\]](#)

Configuring security settings

To configure security settings, go to **Settings > Security**.

Field	Field description
User authentication settings	
Advanced account security mode	<p>Advanced account security mode causes the Cisco TelePresence Supervisor MSE 8050 to hash passwords before storing them in the configuration.xml file (see below). Note that hashing user passwords is an irreversible process.</p> <p>Before you enable advanced account security mode, we recommend that you back up your configuration. The Cisco TelePresence Supervisor MSE 8050 gives you the option to do that after you have enabled Advanced account security mode.</p> <p>If you enable advanced account security mode, all current passwords (created when the Cisco TelePresence Supervisor MSE 8050 was not in advanced account security mode) will expire and users must change them.</p> <p>Advanced account security mode is described in greater detail below.</p>
Redirect HTTP requests to HTTPS	<p>Enable this option to have HTTP requests to the Cisco TelePresence Supervisor MSE 8050 automatically redirected to HTTPS.</p> <p>This option is unavailable if either HTTP (<i>Web</i>) or HTTPS (<i>Secure web</i>) access is disabled on the Network > Services page.</p>
Idle web session timeout	<p>The timeout setting for idle web sessions. The user must log in again if the web session expires. The timeout value must be between 1 and 60 minutes. Note that status web pages that auto-refresh will keep a web session active indefinitely. You can configure the Cisco TelePresence Supervisor MSE 8050 not to auto-refresh those pages; to do so, go to Settings > User interface.</p>
Serial console settings	
Hide log messages on console	<p>The serial console interface displays log messages. If that is considered to be a security weakness in your environment, select this option to hide those messages.</p>
Disable serial input during startup	<p>Select this option for enhanced serial port security.</p>
Require administrator login	<p>Select this option to require an administrator login by anyone attempting to connect to the Cisco TelePresence Supervisor MSE 8050 via the console port. If this is not enabled, anyone with physical access to the MCU (or with access to your terminal server) can potentially enter commands on the serial console.</p>
Idle console session timeout	<p>If you have enabled Require administrator login, you can configure a session timeout period. The timeout setting for idle console sessions. The admin must log in again if the console session expires. The timeout value must be between 1 and 60 minutes.</p>

Advanced account security mode

You can configure the Cisco TelePresence Supervisor MSE 8050 to use advanced account security mode. Advanced account security mode has the following features:

- The Cisco TelePresence Supervisor MSE 8050 will hash passwords before storing them in the configuration.xml file (see [below](#))
- The Cisco TelePresence Supervisor MSE 8050 will demand that passwords fulfill certain criteria, using a mixture of alphanumeric and non-alphanumeric (special) characters (see [below](#))
- Passwords will expire after 60 days
- A new password for an account must be different from the last ten passwords used with that account
- The Cisco TelePresence Supervisor MSE 8050 will disable a user's account if that user incorrectly enters a password three times consecutively. If this is an admin account, it is disabled for 30 minutes; for any other account, it is disabled indefinitely (or until you, the administrator, re-enable the account from the [User](#) page)
- Non-administrator account holders are not allowed to change their password more than once in any 24 hour period
- Administrators can change any user account's password and force any account to change its password by selecting **Force user to change password on next login** on the [User](#) page. Administrators can prevent any non-administrator account from changing its password by selecting **Lock password** on the [User](#) page.
- The Cisco TelePresence Supervisor MSE 8050 will disable any non-administrator account after a 30 day period of account inactivity. To re-enable the account, you must edit that account's settings on the [User](#) page

If you enable advanced security, all current passwords (created when the Cisco TelePresence Supervisor MSE 8050 was not in advanced account security mode) will expire and users must change them.

When using Advanced account security mode, we recommend that you rename the default administrator account. This is especially true where the Cisco TelePresence Supervisor MSE 8050 is connected to the public internet because security attacks will often use "admin" when attempting to access a device with a public IP address. Even on a secure network, if the default administrator account is "admin", it is not inconceivable that innocent attempts to log into the Cisco TelePresence Supervisor MSE 8050 will cause you to be locked out for 30 minutes.

We recommend that you create several accounts with administrator privileges. This will mean that you will have an account through which you can access the Cisco TelePresence Supervisor MSE 8050 even if one administrator account has been locked out.

If there are API applications accessing the Cisco TelePresence Supervisor MSE 8050, we recommend that you create dedicated administrator accounts for each application.

In advanced account security mode, if a user logs in with a correct but expired password the Cisco TelePresence Supervisor MSE 8050 asks that user to change the password. If the user chooses not to change it, that user is allowed two more login attempts to change the password before the account gets disabled.

Hashing passwords

Passwords are always hashed when they are stored on the Supervisor (irrespective of whether advanced account security mode is active), so that they are stored as hash sums and can not be read if the storage is compromised. This also applies to configuration.xml files that are uploaded with plain text passwords; the Supervisor will hash and overwrite the uploaded password.

Hashing is irreversible.

Password format

In advanced account security mode, passwords must have:

- at least fifteen characters
- at least two uppercase alphabetic characters
- at least two lowercase alphabetic characters
- at least two numeric characters
- at least two non-alphanumeric (special) characters
- not more than two consecutive repeating characters. That is, two repeating characters are allowed, three are not

In advanced account security mode, a new password must be different to the previous 10 passwords that have been used with an account.

Expiring passwords

In advanced account security mode, if a user logs in with a correct but expired password the Cisco TelePresence Supervisor MSE 8050 asks that user to change the password. If the user chooses not to change it, that user is allowed two more login attempts to change the password before the account gets disabled.

Related topics

- [Working with the audit log \[p.108\]](#)
- [Displaying security status \[p.52\]](#)
- [Understanding security warnings \[p.109\]](#)
- [Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 \[p.35\]](#)
- [Customizing the user interface \[p.118\]](#)

Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050

On this page:

- [Upgrading the main Cisco TelePresence Supervisor MSE 8050 software image](#)
- [Upgrading the loader software image](#)
- [Backing up and restoring the configuration](#)
- [Enabling Cisco TelePresence Supervisor MSE 8050 features](#)

Upgrading the main Cisco TelePresence Supervisor MSE 8050 software image

The main Cisco TelePresence Supervisor MSE 8050 software image is the only firmware component that you will need to upgrade.

To upgrade the main Cisco TelePresence Supervisor MSE 8050 software image:

1. Go to **Settings > Upgrade**.
2. Check the **Current version** of the main software image to verify the currently installed version.
3. Log onto the [support pages](#) to identify whether a more recent image is available.
4. Download the latest available image and save it to a local hard drive.
5. Unzip the image file.
6. Log on to the Cisco TelePresence Supervisor MSE 8050 web browser interface.
7. Go to **Settings > Upgrade**.
8. Click **Browse** to locate the unzipped file on your hard drive.
9. Click **Upload software image**. The browser begins uploading the file to the Cisco TelePresence Supervisor MSE 8050, and a new browser window opens to indicate the progress of the upload. When finished, the browser window refreshes and indicates that the "Main image upgrade completed."
10. The upgrade status displays in the **Cisco TelePresence Supervisor MSE 8050 software upgrade status** field.
11. [Shutting down and restarting the Cisco TelePresence Supervisor MSE 8050 \[p.39\]](#).

Upgrading the loader software image

Upgrades for the loader software image are not typically available as often as upgrades to the main software image.

To upgrade the loader software image:

1. Go to **Settings > Upgrade**.
2. Check the **Current version** of the loader software to verify the currently installed version.
3. Go to the software download pages of the web site to identify whether a more recent image is available.
4. Download the latest available image and save it to a local hard drive.
5. Unzip the image file.
6. Click **Browse** to locate the unzipped file on your hard drive.

7. Click **Upload software image**. The browser begins uploading the file to the Cisco TelePresence Supervisor MSE 8050, and a new browser window opens to indicate the progress of the upload. When finished, the browser window refreshes and indicates that the "Loader image upgrade completed."
8. The upgrade status displays in the **Loader upgrade status** field.
9. [Shutting down and restarting the Cisco TelePresence Supervisor MSE 8050 \[p.39\]](#).

Backing up and restoring the configuration

The Back up and restore section of the **Upgrade (Settings > Upgrade)** page allows you to back up and restore the configuration of the Cisco TelePresence Supervisor MSE 8050 using the web interface. This enables you to either go back to a previous configuration after making changes or to effectively "clone" one unit as another by copying its configuration.

You can backup the configuration of an individual blade by going to **Hardware > Blade > Backup**. See [Individual blade backup configuration \[p.117\]](#) for more information.

To back up the configuration, click **Save backup file** and save the resulting "configuration.xml" file to a secure location.

To restore configuration at a later date, locate a previously-saved "configuration.xml" file and click **Restore backup file**. When restoring a new configuration file to a Cisco TelePresence Supervisor MSE 8050 you can control which parts of the configuration are overwritten:

- If you select **Network settings**, the network configuration will be overwritten with the network settings in the supplied file. Typically, you would only select this check box if you were restoring from a file backed up from the same Cisco TelePresence Supervisor MSE 8050 or if you were intending to replace an out of service Cisco TelePresence Supervisor MSE 8050. If you copy the network settings from a different, active, Cisco TelePresence Supervisor MSE 8050 and there is a clash (for instance, both are now configured to use the same fixed IP address) one or both boxes may become unreachable via IP. If you do not select **Network settings**, the restore operation will not overwrite the existing network settings, with the one exception of the QoS settings. QoS settings are overwritten regardless of the **Network settings** check box.
- If you select the **User settings** check box, the current user accounts and passwords will be overwritten with those in the supplied file. If you overwrite the user settings and there is no user account in the restored file corresponding to your current login, you will need to log in again after the file has been uploaded.

By default, the overwrite controls are not selected, and therefore the existing network settings and user accounts will be preserved.

Enabling Cisco TelePresence Supervisor MSE 8050 features

The Cisco TelePresence Supervisor MSE 8050 requires activation before most of its features can be used. (If the Cisco TelePresence Supervisor MSE 8050 has not been activated, the banner at the top of the web interface will show a prominent warning; in every other respect the web interface will look and behave normally.)

Advanced Cisco TelePresence Supervisor MSE 8050 features (such as *Video Firewall*) are not enabled as standard, and require additional activation. For information about configuring the video firewall, refer to the Knowledge Base section in the support pages of the web site.

If this is a new Cisco TelePresence Supervisor MSE 8050 you should receive the Cisco TelePresence Supervisor MSE 8050 already activated; if it is not, you have upgraded to a newer firmware version, or you

are enabling a new feature, you may need to contact your supplier to obtain an appropriate activation code. Activation codes are unique to a particular Cisco TelePresence Supervisor MSE 8050 so ensure you know the blade's serial number such that you may receive a code appropriate to your Cisco TelePresence Supervisor MSE 8050.

Regardless of whether you are activating the Cisco TelePresence Supervisor MSE 8050 or enabling an advanced feature, the process is the same.

To activate the Cisco TelePresence Supervisor MSE 8050 or enable an advanced feature:

1. Check the **Activated features** (Cisco TelePresence Supervisor MSE 8050 activation is shown in this same list) to confirm that the feature you require is not already activated.
2. Enter the new feature code into the **Activation code** field exactly as you received it, including any dashes.
3. Click **Update features**. The browser window should refresh and list the newly activated feature, showing the activation code beside it. Activation codes may be time-limited. If this is the case, an expiry date will be displayed, or a warning that the feature has already expired. Expired activation codes remain listed, but the corresponding feature will not be activated.
If the activation code is not valid, you will be prompted to re-enter it.
4. We recommend that you record the activation code in case you need to re-enter it in the future.

Successful Cisco TelePresence Supervisor MSE 8050 or feature activation has immediate effect and will persist even if the Cisco TelePresence Supervisor MSE 8050 is restarted.

Note that you can remove some Cisco TelePresence Supervisor MSE 8050 feature keys by clicking the **Remove** link next to the feature key in this page.

Related topics

- [Shutting down and restarting the Cisco TelePresence Supervisor MSE 8050 \[p.39\]](#)

Backing up the Cisco TelePresence Supervisor MSE 8050 blade to the compact flash

The **Backup** page allows you to back up the Cisco TelePresence Supervisor MSE 8050 blade's configuration to an external compact flash card. You can also back up the Cisco TelePresence Supervisor MSE 8050 blade's configuration to a remote secure location (on the **Settings > Upgrade** page); for more information refer to [Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 \[p.35\]](#)

You can configure the back up to the external compact flash card to be either automatic or manual. If the external compact flash card is not fitted, neither backup can occur and an alarm is raised.

For this reason, on the **Backup** page, the Automatic backup section tells you whether there is a compact flash card inserted and whether the blade is writing to or reading from it currently. Automatic backup will occur every 5 minutes if enabled. Use the **Enable** and **Disable** buttons to control automatic backups. You can also restore from the most recent automatic backup. Click **Restore from automatic backup**.

In addition you can start a manual backup, known as a master backup, at any time; for example when you have just made significant configuration changes. There is only one master backup - it is overwritten each time you click **Create master backup** . (Master backups are independent of the automatic backup function.) You can also restore from this master backup rather than from the automatic backup if you wish.

Note: You can also back up the configuration of other blades to the same compact flash card. See [Individual blade backup configuration \[p.117\]](#).

Related topics

- [Individual blade backup configuration \[p.117\]](#)

Shutting down and restarting the Cisco TelePresence Supervisor MSE 8050

It is sometimes necessary to shut down the Cisco TelePresence Supervisor MSE 8050, generally to restart as part of an upgrade (see [Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 \[p.35\]](#)). You should also shut down the Cisco TelePresence Supervisor MSE 8050 before intentionally removing the blade from the chassis or removing power from the chassis.

To shut down the Cisco TelePresence Supervisor MSE 8050:

1. Go to **Settings > Shutdown**.
2. Click **Shut down MSE Supervisor**.
3. Confirmation of shutdown is required; the button changes to **Confirm MSE Supervisor shutdown**.
4. Click again to confirm.
5. The Cisco TelePresence Supervisor MSE 8050 will begin to shut down. The banner at the top of the page will change to indicate this.
When the shutdown is complete, the button changes to **Restart MSE Supervisor**.
6. Click this button a final time to restart the Cisco TelePresence Supervisor MSE 8050.

Related topics

- [Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 \[p.35\]](#)

Managing users

This section describes how to manage user configuration data on the Cisco TelePresence Supervisor MSE 8050.

System defined users	41
Displaying the user list	42
Adding and updating users	43
Updating your user profile	46
Changing your password	47

System defined users

The Cisco TelePresence Supervisor MSE 8050 is pre-configured with two user accounts ("admin" and "guest"), but you can also add other users (see [Adding and updating users \[p.43\]](#)). Refer to the table below for descriptions of the pre-configured users.

User ID	Description	Usage tips
admin	<p>The Cisco TelePresence Supervisor MSE 8050 must have at least one configured user with administrator privileges. By default, the User ID is "admin" and no password is required.</p> <p>If you configure the Cisco TelePresence Supervisor MSE 8050 with advanced account security mode, a password is required. For more information about advanced account security mode, refer to Configuring security settings [p.32].</p>	<p>After logging into the Cisco TelePresence Supervisor MSE 8050 for the first time (see Logging into the web interface [p.7]), you can change the User ID and password for this account. The privilege level is fixed at <i>administrator</i> for the admin user - who can see all the pages and change settings.</p>
guest	<p>The Cisco TelePresence Supervisor MSE 8050 must have at least one configured user with access privileges below <i>administrator</i>. The fixed User ID for this user is "guest" and by default no password is required.</p> <p>If you configure the Cisco TelePresence Supervisor MSE 8050 with advanced account security mode, the guest account requires a password that adheres to secure password criteria. For more information about advanced account security mode, refer to Configuring security settings [p.32].</p>	<p>You cannot change the name of the "guest" User ID. You can add a password.</p> <p>The privilege level is fixed at <i>list only</i> for the guest user. The guest user and other users with list-only privileges can only see the Blades list.</p>

You can modify the system defined user accounts if you need to. For example, for security, you should add a password to the admin account.

Related topics

- [Displaying the user list \[p.42\]](#)
- [Adding and updating users \[p.43\]](#)
- [Configuring security settings \[p.32\]](#)

Displaying the user list

The **User list** page gives you a quick overview of all configured users on the Cisco TelePresence Supervisor MSE 8050 and provides a summary of some of their settings. To view the **User list** page, go to **Users**. Refer to the table below for assistance.

Field	Field description
User ID	The user name that the user needs to access the web interface of the Cisco TelePresence Supervisor MSE 8050. Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters.
Name	The full name of the user.
Privilege	Access privileges associated with this user. There are two privilege levels: admin and list only. List only users can only see the list of installed hardware, including blades, fan trays, power supplies and chassis information.

Deleting users

To delete a user, select the user you want to delete and click **Delete selected users**. You cannot delete the "admin" and "guest" users.

Related topics

- [Adding and updating users \[p.43\]](#)
- [System defined users \[p.41\]](#)

Adding and updating users

You can add users to and update users on the Cisco TelePresence Supervisor MSE 8050. Although most information is identical for both tasks, some fields differ.

Adding a user

To add a user:

1. Go to the **Users** page.
2. Click **Add user**.
3. Complete the fields referring to the table below to determine the most appropriate settings for the user.
4. After entering the settings, click **Add user**.

Updating a user

To update an existing user:

1. Go to the **Users** page.
2. Click the username of the account you want to update.
3. Edit the user settings, referring to the following table as necessary.
4. After changing the settings, click the update button.

Field	Field description	More information
User ID	Identifies the log-in name that the user will use to access the Cisco TelePresence Supervisor MSE 8050 web interface.	Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters.

Password	The required password, if any.	<p>Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters.</p> <p>In advanced account security mode (configured on the Settings > Security page), passwords must have:</p> <ul style="list-style-type: none"> ■ at least fifteen characters ■ at least two uppercase alphabetic characters ■ at least two lowercase alphabetic characters ■ at least two numeric characters ■ at least two non-alphanumeric (special) characters ■ not more than two consecutive repeating characters. That is, two repeating characters are allowed, three are not <p>In advanced account security mode, a password must be different from the previous ten used with that account. Also, a password will expire if it is not changed within 60 days.</p> <p>If the Cisco TelePresence Supervisor MSE 8050 is not using advanced account security mode, any password can be used.</p> <p>Note that passwords are stored in the configuration.xml file as plain text unless the Cisco TelePresence Supervisor MSE 8050 is configured (or has ever been configured) to use advanced account security mode. For more information, refer to Hashing passwords [p.33].</p> <p>Note that this field is only active when adding a new user. If you are updating an existing user and want to change that user's password, click Change password instead.</p>
Re-enter password	Verifies the required password.	
Disable user account	Select to disable this account.	<p>This can be useful if you want to keep an account's details, but do not want anyone to be able to use it at the moment.</p> <p>You cannot disable the system-created admin account.</p> <p>The system-created guest account is disabled by default. If you enable it, the Cisco TelePresence Supervisor MSE 8050 will create a security warning.</p> <p>In advanced account security mode, a non-admin account will expire after 30 days of inactivity; that is, the Cisco TelePresence Supervisor MSE 8050 will disable it. To re-enable a disabled account, clear this option.</p> <p>For more information about advanced account security mode, refer to Configuring security settings [p.32].</p>
Lock password	Prevents user from changing password.	<p>This is useful where you want multiple users to be able to use the same user ID. The system-created guest account has <i>Lock password</i> enabled by default.</p>

Force user to change password on next login	Select this option to force a user to change their password. Next time this user attempts to log in to the Cisco TelePresence Supervisor MSE 8050, a change password prompt will appear.	<p>This option is enabled by default for a newly created account. It is a good idea for new users to set their own secure passwords.</p> <p>This option is not available for accounts where <i>Lock password</i> is selected.</p> <p>When the user changes his password, the Cisco TelePresence Supervisor MSE 8050 clears this check box automatically.</p>
Privilege level	The access privileges to be granted to this user.	The privilege level is fixed at <i>admin</i> for the admin user - who can see all the pages and change settings. The privilege level is fixed at <i>list only</i> for the guest user. The guest user and other users with list-only privileges can only see the list of installed hardware, including blades, fan trays, power supplies and chassis information.

Related topics

- [System defined users \[p.41\]](#)
- [Displaying the user list \[p.42\]](#)
- [Configuring security settings \[p.32\]](#)

Updating your user profile

You can make some changes to your user profile. To do this, go to [User profile](#). Refer to the table below for tips.

Field	Field description	More information
Change password		
Current password	Type your current password.	
Password	Type your new password.	<p>In advanced account security mode, passwords must have:</p> <ul style="list-style-type: none">■ at least fifteen characters■ at least two uppercase alphabetic characters■ at least two lowercase alphabetic characters■ at least two numeric characters■ at least two non-alphanumeric (special) characters■ not more than two consecutive repeating characters. That is, two repeating characters are allowed, three are not <p>In advanced account security mode, a new password must be different to the previous 10 passwords that have been used with an account.</p>
Re-enter password	Verify your new password.	

Changing your password

In advanced account security mode, passwords must have:

- at least fifteen characters
- at least two uppercase alphabetic characters
- at least two lowercase alphabetic characters
- at least two numeric characters
- at least two non-alphanumeric (special) characters
- not more than two consecutive repeating characters. That is, two repeating characters are allowed, three are not

In advanced account security mode, a new password must be different to the previous 10 passwords that have been used with an account.

In advanced account security mode, if a user logs in with a correct but expired password the Cisco TelePresence Supervisor MSE 8050 asks that user to change the password. If the user chooses not to change it, that user is allowed two more login attempts to change the password before the account gets disabled.

In advanced account security mode, users other than administrator users are not allowed to change their password more than once in a 24 hour period.

If the Cisco TelePresence Supervisor MSE 8050 is not in advanced account security mode, there are no criteria for password selection.

If the Cisco TelePresence Supervisor MSE 8050 is in advanced account security mode, the above criteria for passwords are displayed on the **Change password** page.

Related topics

- [Configuring security settings](#)
- [Understanding security warnings \[p.109\]](#)

Displaying Cisco TelePresence Supervisor MSE 8050 status

This section describes how to display system status information for the Cisco TelePresence Supervisor MSE 8050.

Displaying general status	49
Displaying hardware health status	51
Displaying security status	52

Displaying general status

The **General status** page displays an overview of the Cisco TelePresence Supervisor MSE 8050 status. To access this information, go to **Status > General**.

You can display the status of individual blades by going to **Hardware > Blade**. For more information, refer to [Displaying an individual blade's status \[p.64\]](#).

Refer to the table below for details of the information displayed

Field	Field Description
System status	
Model	The specific Cisco TelePresence Supervisor MSE 8050 model.
Supervisor blade serial number	The unique serial number of the Cisco TelePresence Supervisor MSE 8050.
Chassis serial number	The unique serial number of the chassis.
Software version	The installed software version. You will need to provide this information when speaking to Customer support.
Build	The build version of installed software. You will need to provide this information when speaking to Customer support.
Uptime	The time since the last restart of the Cisco TelePresence Supervisor MSE 8050.
Host name	The host name assigned to the Cisco TelePresence Supervisor MSE 8050.
Slot number in chassis	The slot number in the chassis in which the Cisco TelePresence Supervisor MSE 8050 is currently installed. If the Cisco TelePresence Supervisor MSE 8050 displays a message reporting that the blade is missing, ensure that each blade is firmly secured in the chassis. Close both retaining latches on the front of the blade. Using a number 1 Phillips screwdriver, tighten the screws in the retaining latches with a clockwise quarter turn.
IP address	The IP address assigned to the Cisco TelePresence Supervisor MSE 8050.
CPU load	The current processor utilization of the Cisco TelePresence Supervisor MSE 8050.
System time	
Current time	The system time on the Cisco TelePresence Supervisor MSE 8050. Click New time to modify this value. The Time Settings page opens in which you can update the system date and time manually or refresh the time from an NTP server. For more information about the Time Settings page, refer to Displaying and resetting system time [p.30] .

Field	Field Description
Diagnostic information	
Download diagnostic information	If required to do so by Customer support, click Download diagnostic information to save a set of diagnostic files.
Download network trace	If network trace has been enabled on the Cisco TelePresence Supervisor MSE 8050, via the serial console, there is a Download network trace button here. Click this button to download the most recent network trace if it is required by your customer support representative.

Related topics

- [Displaying hardware health status \[p.51\]](#)
- [Displaying and resetting system time \[p.30\]](#)
- [Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 \[p.35\]](#)
- [Shutting down and restarting the Cisco TelePresence Supervisor MSE 8050 \[p.39\]](#)

Displaying hardware health status

The **Health status** page (**Status > Health**) displays information about the hardware components of the Cisco TelePresence Supervisor MSE 8050.

Note: The **Worst status seen** conditions are those since the last time the Cisco TelePresence Supervisor MSE 8050 was restarted.

To reset these values, click **Clear**. Refer to the table below for assistance in interpreting the information displayed.

Field	Field description	Usage tips
Voltages RTC battery	<p>Displays two possible states:</p> <ul style="list-style-type: none"> ■ OK ■ Out of spec <p>States indicate both <i>Current status</i> and <i>Worst status seen</i> conditions.</p>	<p>The states indicate the following:</p> <ul style="list-style-type: none"> ■ <i>OK</i> – component is functioning properly ■ <i>Out of spec</i> – Check with your support provider; component might require service <p>If the <i>Worst status seen</i> column displays <i>Out of spec</i>, but <i>Current status</i> is <i>OK</i>, monitor the status regularly to verify that it was only a temporary condition.</p>
Temperature	<p>Displays three possible states:</p> <ul style="list-style-type: none"> ■ OK ■ Out of spec ■ Critical <p>States indicate both <i>Current status</i> and <i>Worst status seen</i> conditions.</p>	<p>The states indicate the following:</p> <ul style="list-style-type: none"> ■ <i>OK</i> – temperature of the Cisco TelePresence Supervisor MSE 8050 is within the appropriate range ■ <i>Out of spec</i> – Check the ambient temperature (should be less than 34 degrees Celsius) and verify that the air vents are not blocked ■ <i>Critical</i> – temperature of Cisco TelePresence Supervisor MSE 8050 is too high. An error also appears in the event log indicating that the system will shutdown in 60 seconds if the condition persists <p>If the Worst status seen column displays <i>Out of spec</i>, but Current status is <i>OK</i> monitor the status regularly to verify that it was only a temporary condition.</p>

For fan status go to **Hardware > Fan trays** and for information about the power supplies go to **Hardware > Power supplies**.

Related topics

- [Displaying general status \[p.49\]](#)
- [Displaying the blades overview \[p.54\]](#)
- [Displaying the fan status \[p.57\]](#)
- [Configuring the power supply monitoring \[p.59\]](#)
- [Displaying the chassis status \[p.62\]](#)

Displaying security status

The Security status page displays a list of active security warnings for the Cisco TelePresence Supervisor MSE 8050. To access this information, go to [Status > Security](#).

Security warnings identify potential weaknesses in the security of the Cisco TelePresence Supervisor MSE 8050's configuration. Note that some security warnings might not be relevant for your organization. For example if the Cisco TelePresence Supervisor MSE 8050 is inside a secure network, enabling HTTP may not be a security issue. For information about all possible security warnings, refer to [Understanding security warnings \[p.109\]](#).

To acknowledge a security warning, select that warning and click **Acknowledge selected**. Acknowledged warnings will not appear on the Cisco TelePresence Supervisor MSE 8050's Home page. If the Cisco TelePresence Supervisor MSE 8050 reboots, the warnings are reset and previously acknowledged warnings will need re-acknowledging.

To fix a security issue, click on the **Action** link for the warning message relating to the issue. When you fix a security issue, the security warning disappears from this list (on the [Status > Security](#) page), but it will be logged in the Audit log. For more information about the audit log, refer to [Working with the audit log \[p.108\]](#).

Refer to the table below for details of the information displayed.

Field	Field Description
Warning	The text of the security warning.
State	<p>For every security warning, the state will one of:</p> <ul style="list-style-type: none"> ■ <i>New</i>: A new security warning is one that has been raised by the Cisco TelePresence Supervisor MSE 8050, but you have not acknowledged it. New warnings also appear on the Cisco TelePresence Supervisor MSE 8050 Home page. ■ <i>Acknowledged</i>: An acknowledged security warning is one that you have acknowledged, but have not fixed. <p>When you fix a security issue, the security warning disappears from this list, but it will be logged in the Audit log. For more information about the audit log, refer to Working with the audit log [p.108].</p>
Action	For every security warning, there is a corresponding action that explains how to fix the security issue. Usually this is a link that takes you to the page where you can make the configuration change that will fix the security issue.

Related topics

- [Configuring security settings \[p.32\]](#)
- [Working with the audit log \[p.108\]](#)
- [Understanding security warnings \[p.109\]](#)
- [Displaying hardware health status \[p.51\]](#)

Monitoring the chassis

This section describes how you can use the Cisco TelePresence Supervisor MSE 8050 to monitor the MSE 8000 chassis.

Displaying the blades overview	54
Displaying the fan status	57
Configuring the power supply monitoring	59
Displaying the chassis status	62

Displaying the blades overview

The Cisco TelePresence Supervisor MSE 8050 monitors all the blades in the chassis. Click [Hardware > Blades](#) to view a summary of their status. The Cisco TelePresence Supervisor MSE 8050 also monitors the fan trays, the power supplies and the chassis. Click [Hardware > Fan trays](#), [Hardware > Power supplies](#) and [Hardware > Chassis](#) to view these pages.

Blades' status

The overview page shows the following information for each blade in the Cisco TelePresence MSE 8000 chassis. Click the blade's Slot number or Type to display its detailed status page, or click the IP address to log in to the web interface of the blade.

Field	Field description	Usage tips
Slot	Slots are numbered from left to right as you look at the chassis.	The Cisco TelePresence Supervisor MSE 8050 must be fitted in to slot 1. If it is not, you'll see an error message in the page header. Swap the Cisco TelePresence Supervisor MSE 8050 blade in to slot 1.
Type	The type of blade.	The Cisco TelePresence MSE 8000 chassis may hold the following types of blades: <ul style="list-style-type: none"> ■ Cisco TelePresence Supervisor MSE 8050 (required) ■ Cisco TelePresence MCU MSE 8420 ■ Cisco TelePresence MCU MSE 8510 ■ Cisco TelePresence IP VCR ■ Cisco TelePresence ISDN Gateway ■ Cisco TelePresence IP Gateway ■ Cisco Telepresence Server.
Version	The version number of the software running on the blade.	
Port A/B address	The IPv4 and/or IPv6 addresses of the blade's Ethernet ports.	Click a blade's IP address to log in to its web interface.

Status	<p>The current status of each blade.</p> <hr/> <p>Note: Each slot has two status LEDs. If no blade is fitted, neither LED is on. When you fit a blade, the red LED lights until communication is established with the Supervisor, at which point the green LED lights instead.</p> <p>The red LED lights when the communications link fails. Check that the blade is properly inserted in the slot.</p> <hr/>	<p>Status and troubleshooting:</p> <ul style="list-style-type: none"> ■ <i>Blade OK:</i> this slot contains a blade which is not reporting any problems. ■ <i>Blade removed:</i> no blade is fitted in this slot (somebody has removed a blade from this slot since the last time the Cisco TelePresence Supervisor MSE 8050 restarted). ■ <i>Blade absent:</i> there is no blade in this slot. There has not been a blade in this slot since the last time the Cisco TelePresence Supervisor MSE 8050 restarted. ■ <i>Blade inserted badly:</i> ensure that this blade is firmly secured in the chassis. Close both retaining latches on the front of the blade. Using a number 1 Phillips screwdriver, tighten the screws in the retaining latches with a clockwise quarter turn. ■ <i>Blade shutting down:</i> this blade is shutting down, but has not yet shut down. ■ <i>Attempting restart:</i> the Supervisor is attempting to restart the blade, but the restart has not begun yet. ■ <i>Invalid blade ID:</i> try ensuring that the blade is pushed in firmly, as described above. If you continue to see this status, contact your reseller. ■ <i>Waiting for communications:</i> a blade has failed to make contact with the Cisco TelePresence Supervisor MSE 8050 since being inserted. Go to the web interface of this blade for more information. ■ <i>Lost communication:</i> a blade which was previously communicating with the Cisco TelePresence Supervisor MSE 8050 has now lost contact. ■ <i>Temperature / Voltages / RTC Battery critical:</i> the blade is reporting a problem, as shown on the blade's Health status page. ■ <i>Blade shut down:</i> This blade is currently shut down (or restarting). Note that MCU software earlier than version 4.1 reports <i>Blade shut down</i> for blades that are either shut down or currently restarting. For MCU software 4.1 and later, and for Telepresence Server software 2.0 and later, <i>Blade shut down</i> means that the blade is currently shut down. For other blade types and versions, <i>Blade shut down</i> means either shut down or restarting. ■ <i>Restart required:</i> shut down and restart this blade. A blade requires restarting when you have altered its cluster configuration, when you have allocated/reallocated port licenses, or when you are upgrading the blade. To shut down and restart the blade, go to the web interface of the blade ■ <i>Restarting:</i> this blade is restarting. ■ <i>Blade software version too old: Please upgrade:</i> Upgrade this blade to the latest available software release.
--------	--	--

Related topics

For the Supervisor blade:

- [Displaying general status \[p.49\]](#)
- [Displaying hardware health status \[p.51\]](#)
- [Displaying the fan status \[p.57\]](#)
- [Configuring the power supply monitoring \[p.59\]](#)
- [Displaying the chassis status \[p.62\]](#)

For other blades in the chassis:

- [Displaying an individual blade's status \[p.64\]](#)
- [Individual blade ports configuration \[p.70\]](#)
- [Individual blade backup configuration \[p.117\]](#)

Displaying the fan status

The Cisco TelePresence Supervisor MSE 8050 monitors the upper and lower fan trays and displays this information in the [Hardware > Fan trays](#) page.

For each fan tray you see average fan speed and its status. If a problem is reported, go to [Alarms > Alarms log](#) for more details. The status is also indicated by the Fans LEDs - as explained below.

Fan trays status

The chassis has two fan trays; one at the top and one at the bottom of the chassis. This table provides the status of each tray.

Field	Field description	Usage tips
Tray	Either <i>Upper</i> or <i>Lower</i> .	
Type	The type of fan tray.	
Serial number	The serial number of the fan tray.	You will need this if you have to report a problem with a fan tray to technical support.
Average fan speed	The average fan speed in revolutions per minute.	
Status	The status of each fan tray.	One of: -: the fan tray is not present. <i>OK</i> : the fan tray is present and operating correctly. <i>Initializing</i> : the fan tray has booted and the Cisco TelePresence Supervisor MSE 8050 blade is waiting for its status to be reported. <i>Problem</i> : the fan tray is present but with a problem.

Fans' LEDs

The two fan LEDs indicate whether there is a problem with a fan. The two LEDs cover both fan trays so you must open the Fans status page or the Alarm log to see which fan tray is causing any problems. There is a red and a green LED. The green LED lights when the fans are operating correctly. The red LED:

- Lights continuously when an alarm exists on a fan and it has not been acknowledged or silenced
- Flashes fast when there is a current alarm but it has been silenced
- Flashes slowly to indicate that there was a historic alarm but it has been cleared i.e. the fans are operating correctly now

Related topics

- [Displaying the alarm log \[p.101\]](#)
- [Displaying general status \[p.49\]](#)
- [Displaying hardware health status \[p.51\]](#)

- [Configuring the power supply monitoring \[p.59\]](#)
- [Displaying the chassis status \[p.62\]](#)

Configuring the power supply monitoring

To view information about the power supply to the chassis, go to [Hardware > Power supplies](#).

The chassis can be operated with one or two power supplies, A and B. These feed power independently to every fan tray and blade. The chassis can be fully powered from either supply A or supply B. In the event of failure of either power supply, the chassis will continue to operate by drawing power from the other. TANDBERG recommends that for full redundancy and maximum reliability, the power feeds should be connected to independent power sources - each capable of providing the full electrical load of the unit.

The chassis can be connected to DC power if it is available within the correct range at your facility. Otherwise, use TANDBERG-supplied AC to DC power shelves. For further information about powering the chassis, refer to the chassis Getting Started Guide.

The Cisco TelePresence Supervisor MSE 8050 monitors the voltage received on each power supply.

If the chassis is powered via AC to DC power shelves, and these are connected via the power shelf serial ports on the Cisco TelePresence Supervisor MSE 8050's input/output panel on the rear of the chassis chassis, the Cisco TelePresence Supervisor MSE 8050 can also monitor the state of those power shelves. If the communications fails, then the voltage monitoring is disabled automatically.

The Power supplies page displays the voltage currently being supplied by each power supply. If power shelves are in use and connected to the Cisco TelePresence Supervisor MSE 8050, the Power supplies page also displays the state of the power shelves and allows you to configure the monitoring of the power shelves.

If there is a problem with either the voltages or the communications between the power shelves and the power shelf serial ports, the red Power LED for the appropriate supply lights. Go to [Alarms > Alarms log](#) to see more details.

Supply voltage monitoring

Field	Field description	Usage tips
Supply	Either Power supply A or Power supply B.	
Voltage	The operating voltage actually being supplied to the chassis.	

Status	The status of each power supply.	<p>One of:</p> <ul style="list-style-type: none"> - : power supply is not present OK: power supply is operating between the minimum and maximum voltages set for this power supply in the Monitoring configuration section below <i>Out of range high</i>: voltage is above the maximum supported voltage for this power supply listed in the Monitoring configuration section <i>Out of range low</i>: voltage is below the minimum supported voltage for this power supply listed in the Monitoring configuration section <i>Too high</i>: voltage is above the maximum configured voltage for this power supply configured in the Monitoring configuration section <i>Too low</i>: voltage is below the minimum configured voltage for this power supply configured in the Monitoring configuration section <i>Supply not monitored</i>: voltage monitoring is disabled. To enable voltage monitoring, select Enable voltage monitoring in the Monitoring configuration section of the Power supplies page
--------	----------------------------------	---

Power shelf monitoring

Field	Field description	Usage tips
Shelf	Whether it is the shelf connected to power shelf serial port A or B on the Cisco TelePresence Supervisor MSE 8050's input/output panel on the rear of the MSE 8000 chassis.	
Type	The make and model of the power shelf.	
Reported information	The status of the power supply shelf rectifiers.	<p>For each rectifier, the voltage, current, capacity and status are shown. The voltage is that measured at the power shelf serial port, if connected (see the labeling on the back of the chassis) and may not be identical to that measured by the power supply monitoring.</p> <p>Each AC to DC power shelf can contain up to four rectifiers: for information about determining how many rectifiers are required refer to Cisco TelePresence MSE 8000 Getting Started Guide.</p>

Status	The status of each power supply shelf.	<p>One of:</p> <p><i>OK</i>: the power shelf is present and reporting no problems</p> <p><i>Power shelf reporting fault</i>: the shelf is reporting a fault condition</p> <p><i>Power shelf not monitored</i>: power shelf monitoring has not been enabled. To enable power shelf monitoring, select Enable power shelf monitoring in the Monitoring configuration section of the Power supplies page</p> <p><i>Lost contact with power shelf</i>: the Cisco TelePresence Supervisor MSE 8050 is unable to communicate with the power shelf</p> <p><i>Insufficient current capacity</i>: the power shelf does not have sufficient rectifier capacity to power the chassis under full load</p> <p><i>Authentication failed</i>: you have entered the wrong user name and/or password for serial monitoring of the power shelf</p>
--------	--	---

Configuring the power status monitoring

You can enable monitoring of the power supply voltages and if required, the monitoring of the AC to DC power shelves. Follow these steps for each power supply:

1. Go to **Hardware > Power supplies**.
2. To enable voltage monitoring, select *Enable voltage monitoring*.
3. Type in the lower and upper limits for the operational voltages. (This can be between 40.5 and 72 volts and can be entered to the nearest 0.5 volts. If the measured voltage goes outside this range, an alarm is triggered. Go to **Alarms** for details.)
4. To enable power shelf communications monitoring, select your power supply option from the drop down list.
5. Type in the user name and password for the power supply shelf. (The Cisco TelePresence Supervisor MSE 8050 logs into the power shelf by itself, but requires the correct user name and password to do so. By default, the power shelves ship with a username of Admin and a password of 5001, and the Cisco TelePresence Supervisor MSE 8050 has these set as the defaults. However, if you change these on the web interface, there is no way of automatically retrieving the default values without completely overwriting the configuration.)
If the serial communications between the power supply shelf and the chassis fails, an alarm is raised. Go to **Alarms** for details.
6. Click **Apply changes**.

Note: You might need to supply the user name and password a second time before monitoring can be successfully configured.

Related topics

- [Displaying the alarm log \[p.101\]](#)
- [Displaying general status \[p.49\]](#)
- [Displaying hardware health status \[p.51\]](#)
- [Displaying the fan status \[p.57\]](#)
- [Displaying the chassis status \[p.62\]](#)

Displaying the chassis status

The **Chassis status** page displays the serial number of the chassis and the status of various chassis components. To display the **Chassis status** page go to **Hardware > Chassis**.

MSE 8000 chassis information

The following information is shown.

Field	Field description
Chassis serial number	The serial number of the MSE 8000 chassis.
Backplane serial number	The serial number of the signal backplane PCB.
Backplane revision	The version of the backplane.
Upper power serial number	The serial number of the upper power distribution PCB.
Lower power serial number	The serial number of the lower power distribution PCB.
Supervisor A rear IO card serial number	The serial number of the IO card for the Cisco TelePresence Supervisor MSE 8050 blade A.
Supervisor A rear IO card revision	The revision version of the IO card for the Cisco TelePresence Supervisor MSE 8050 blade A.
Supervisor B rear IO card serial number	The serial number of the IO card for the Cisco TelePresence Supervisor MSE 8050 blade B.
Supervisor B rear IO card revision	The revision version of the IO card for the Cisco TelePresence Supervisor MSE 8050 blade B.

Related topics

- [Displaying the fan status \[p.57\]](#)
- [Configuring the power supply monitoring \[p.59\]](#)
- [Displaying general status \[p.49\]](#)
- [Displaying hardware health status \[p.51\]](#)

Monitoring the blades

This section describes how you can use the Cisco TelePresence Supervisor MSE 8050 to monitor the individual blades in the MSE 8000 chassis.

Displaying an individual blade's status	64
Individual blade ports configuration	70
Individual blade routes configuration	74
Individual blade services configuration	77
Individual blade shutdown	81

Displaying an individual blade's status

Click Hardware to display a list of blades in the chassis and then click the blade type or slot number to show that blade's status.

The blade's status information is summarized in tables that are very similar to those you'll see when you log in to the blade directly. For every type of blade, the status and health are summarized in the first two tables. The other information on the status page depends on the type of blade you are viewing.

Tip: Use the slot number links in the top right corner to view the status of the other blades in the chassis.

On this page:

- [Blade status](#)
- [Blade health](#)
- [MCU and Telepresence Server tables](#)
- [IP VCR tables](#)
- [ISDN Gateway tables](#)
- [IP Gateway tables](#)

Blade status

Field	Field description
Model	The blade model.
Status	The blade's status. For more information about the possible states, refer to the table in Displaying the blades overview [p.54] .
IP address	The IP address(es) assigned to the blade's Ethernet port/s. The blade may have more than one port, and may have an IPv4 address and an IPv6 address on each.
Time inserted	The time that the blade was inserted in to the chassis. Status is <i>present at boot</i> if the blade was resident in the chassis prior to the Supervisor's last reboot.
Uptime	The time since the last restart of the blade.
Serial number	The unique serial number of the blade.
Software version	The installed software version. You need to provide this information when speaking to Technical Support.
Build	The build version of installed software. You need to provide this information when speaking to Technical Support.

Blade health

Field	Field description	Usage tips
-------	-------------------	------------

Temperatures	Each component will report one of these three states:	<ul style="list-style-type: none"> ■ <i>OK</i> – component is functioning properly ■ <i>Out of spec</i> – check with your support provider; the component might require service
Voltages		<p>If the Worst Seen column displays <i>Out of spec</i>, but Current Status is <i>OK</i>, monitor the status regularly to verify that it was only a temporary condition.</p>
RTC battery		
	<ul style="list-style-type: none"> ■ <i>OK</i> ■ <i>Out of spec</i> ■ <i>Critical</i> <p>The table shows the Current Status and the Worst Seen status.</p>	

MCU and Telepresence Server tables

Conference status

Conference status displays an overview of active and completed conferences.

Field	Field description
Active conferences	The number of conferences that are currently configured on the blade.
Active auto attendants	The number of auto attendants that are currently in use. If you dial in with an endpoint to the auto attendant, this will go up by one. It does not reflect the number of configured auto attendants.
Completed conferences	The number of conferences that were once active but are now not.
Completed auto attendants	The total number of calls into an auto attendant, excluding any in progress. If you call an auto attendant and enter into a conference or hang up the call, this number increases by one.
Active conference participants	The number of people currently in conferences.
Previous conference participants	The number of people who were previously participating in a conference (since the last time the blade restarted).
Active streaming viewers	The number of people currently watching conferences via a streaming application, such as Apple QuickTime or RealPlayer.
TCP streaming viewers	The number of streaming sessions out of the Active streaming viewers value shown above which are using TCP media transport rather than UDP.
Video ports in use	<p>This value is shown if the blade is not operating in Port reservation mode, and shows the number of video ports in use. For more information about Port reservation mode, log in to the blade and see the online help.</p> <p>This corresponds to the number of connected participants that are either contributing or being sent video.</p>

Audio-only ports in use	This value is shown if the blade is not operating in Port reservation mode, and shows the number of audio-only ports in use. This corresponds to the number of connected participants that are contributing or being sent audio but not video. For more information about Port reservation mode, log in to the blade and see the online help.
-------------------------	---

Video status

Video status displays an overview of current video resource use.

Field	Field description	Usage tips
Incoming video streams	The number of video streams being received by the blade.	Unicast indicates video streams sent directly to the blade (incoming) or directly to the endpoints (outgoing) rather than multicast streams broadcast to the network and captured or sent by the blade.
Outgoing video streams	The number of video streams being sent by the blade.	
Total incoming video bandwidth	The total video data rate being received by the blade.	
Total outgoing video bandwidth	The total video data rate being sent by the blade.	

Audio status

Audio status displays an overview of current audio resource use.

Field	Field description	Usage tips
Incoming audio streams	The number of audio streams being received by the blade.	Unicast indicates audio streams sent directly to the blade (incoming) or directly to the endpoints (outgoing) rather than multicast streams broadcast to the network and captured or sent by the blade.
Outgoing audio streams	The number of audio streams being sent by the blade.	
Complex (not G.711 or G.722) audio participants	Displays active audio participants using neither G.711 nor G.722.	At most half of the blade's allowable participants are permitted to use complex audio channels. A participant is considered to be using complex audio if <i>either</i> it is transmitting a complex audio channel <i>or</i> the blade is sending complex audio to it.

Slave status

For clustered blades, the video and audio status for the cluster is shown on the master slave's summary page (see [Understanding clustering \[p.91\]](#)).

IP VCR tables

Recording status

Field	Field description
Number of folders	The number of folders on the blade.
Number of stored recordings	The number of recordings currently stored on the blade. This includes recordings made using the blade as well as those uploaded to it.
Number of recordings in progress	The number of recordings that are currently being made.
Number of H.323/SIP playbacks in progress	The number of people currently watching stored recordings using an H.323 or SIP endpoint. This includes auto attendant connections which are showing a preview of a recording.
Number of streaming playbacks in progress	The number of people currently watching stored recordings using conventional streaming via a streaming application such as Apple QuickTime or RealPlayer.
Number of TCP streaming playbacks in progress	The number of people currently watching stored recordings using streaming over TCP.
Number of recording uploads in progress	The number of recordings currently being uploaded to the blade for later playback.
Number of downloads in progress	The number of recordings that are currently being downloaded from the blade.
Number of completed playbacks	The number of people who were once watching stored recordings but are now not. Includes all types of playback, including streaming and playback using an H.323 endpoint.
Number of completed downloads	The number of recordings that have been downloaded from the blade.
Number of completed recordings	The number of recordings that have been made since the blade was last restarted.
Total length of stored recordings	The combined duration of all recordings stored on the blade.
Total size of stored recordings	The combined storage capacity used by all recordings stored on the blade.
Free disk space	The remaining storage capacity of the blade.

ISDN Gateway tables

ISDN port status

Field	Field description	Usage tips
Port	The number of the ISDN port to which this status information relates.	
Enabled	Whether or not the port is enabled.	A port may be disabled because it is not supported by the particular model of blade or because it has been explicitly disabled by the user.
Layer 1	<i>Up</i> when the physical layer is connected. Shows <i>down</i> otherwise.	
Layer 2	<i>Up</i> when the D-channel has established communication with the ISDN network. Shows <i>down</i> otherwise.	

ISDN call status

This table shows the number of currently active calls and the number of completed calls since the blade was last rebooted.

IP Gateway tables

Call status

Call status displays an overview of active and completed calls.

Field	Field description
Through calls	The number of calls currently connected to their final destination. This number does not include calls that are currently with the operator or the auto attendant.
Auto attendant connections	The number of calls currently connected to the auto attendant.
Operator connections	The number of calls currently connected to the operator.
Queued for operator	The number of calls into the IP Gateway that are waiting for the operator to answer.
Video ports in use	The number of video ports in use. This corresponds to the number of connected calls that are either contributing or being sent video.
Audio-only ports in use	The number of audio-only ports in use. This corresponds to the number of connected calls that are contributing or being sent audio but not video.

Video status

Video status displays an overview of current video resource use.

Field	Field description	Usage tips
Incoming video streams	The number of video streams being received by the blade.	Unicast indicates video streams sent directly to the blade (incoming) or directly to the endpoints (outgoing) rather than multicast streams broadcast to the network and captured or sent by the blade.
Outgoing video streams	The number of video streams being sent by the blade.	
Total incoming video bandwidth	The total video data rate being received by the blade.	
Total outgoing video bandwidth	The total video data rate being sent by the blade.	

Audio status

Audio status displays an overview of current audio resource use.

Field	Field description	Usage tips
Incoming audio streams	The number of audio streams being received by the blade.	Unicast indicates audio streams sent directly to the blade (incoming) or directly to the endpoints (outgoing) rather than multicast streams broadcast to the network and captured or sent by the blade.
Outgoing audio streams	The number of audio streams being sent by the blade.	

Related topics

- [Individual blade ports configuration \[p.70\]](#)
- [Individual blade routes configuration \[p.74\]](#)
- [Individual blade services configuration \[p.77\]](#)
- [Individual blade backup configuration \[p.117\]](#)
- [Individual blade shutdown \[p.81\]](#)
- [Displaying general status \[p.49\]](#)
- [Displaying hardware health status \[p.51\]](#)
- [Displaying security status \[p.52\]](#)

Individual blade ports configuration

To check or modify the network settings on a managed blade, click **Hardware**, select the blade from the summary page, and then click **Port A** or **Port B** to access the settings for that Ethernet port.

The managed blade may have two Ethernet interfaces, Port A and Port B. The configuration pages for the two interfaces look and behave similarly, and so are described together.

Note: These pages are identical to the corresponding pages that you'll see if you log on to the managed blade. The Supervisor immediately updates the managed blade when you make changes to the blade's configuration. However, if you make the same change directly on the managed blade, the blade may take a short while to report the change back to the Supervisor.

Tip: Use the numbered links in the top right corner to switch between the port configuration pages on the numbered blades without returning to the summary page.

On this page:

- [IP configuration settings](#)
- [IP status](#)
- [Ethernet configuration](#)
- [Ethernet status](#)

IP configuration settings

These settings determine the IP configuration for the appropriate Ethernet port of the managed blade. When you have finished, click **Update IP configuration** and then reboot the managed blade.

Field	Field description	Usage tips
IPv4 configuration		
IP configuration	<p>Select Disabled, Manual or Automatic via DHCP.</p> <p>If you select <i>Disabled</i>, the port will not have an IP address and you will not be able to access it through the web interface.</p> <p>If you select <i>Manual</i>, you must also supply the IPv4 address, subnet mask and default gateway.</p> <p>If you select <i>Automatic via DHCP</i>, the blade gets an IPv4 address for this port via DHCP (Dynamic Host Configuration Protocol).</p>	<p>Click Update IP configuration to request a new IP address if you have selected automatic configuration.</p>
IP address	The dot-separated IPv4 address for this port, for example 192.168.4.45.	<p>Specify this option only if you chose <i>Manual IP</i> configuration.</p> <p>For Port A, if the IP configuration setting is set to <i>Automatic by DHCP</i> this setting will be ignored.</p>

Subnet mask	The subnet mask required for the IP address you wish to use, for example 255.255.255.0	Specify this option only if you chose <i>Manual</i> IP configuration.
Default gateway	The IP address of the default gateway on this subnet, for example 192.168.4.1	Specify this option only if you chose <i>Manual</i> IP configuration.
IPv6 configuration		
IP configuration	Select <i>Disabled</i> , <i>Automatic via SLAAC/DHCPv6</i> or <i>Manual</i> . If you select <i>Manual</i> , you must also supply the IPv6 address, prefix length and default gateway. If you select <i>Automatic via SLAAC/DHCPv6</i> , the Supervisor automatically gets an IPv6 address. It uses SLAAC, Stateful DHCPv6 or Stateless DHCPv6 as indicated by the ICMPv6 Router Advertisement (RA) messages (see Automatic IPv6 address preferences below).	Disable IPv6 on the port if the network does not support IPv6.
IPv6 address	If you chose <i>Manual</i> configuration, supply the IPv6 address in CIDR format. Enclose the address in square brackets, for example [IPv6 address], in the user interface.	
Prefix length	If you chose <i>Manual</i> configuration, supply the prefix length.	The prefix length is the (decimal) number of bits that are fixed for this address.
Default gateway	(Optional) Supply the IPv6 address of the default gateway on this subnet.	The address may be global or link-local.

IP status

The IP status section shows the current IP settings for this Ethernet port of the managed blade, as follows, whether they were automatically or manually configured:

IPv4 settings:

- DHCP
- IP address
- Subnet mask
- Default gateway

IPv6 settings:

- DHCPv6
- IPv6 address
- IPv6 default gateway
- IPv6 link-local address

Ethernet configuration

Configure the Ethernet settings for this port of the managed blade, and then click **Update Ethernet configuration**.

Field	Field description	Usage tips
Ethernet settings	Select <i>Automatic</i> or <i>Manual</i> . If you select <i>Manual</i> , you must also supply the speed and duplex settings. Select <i>Automatic</i> if you want this Ethernet port to automatically negotiate its Ethernet settings with the connected device.	It is important that the devices at either end of the Ethernet connection have the same settings. That is, configure both devices to use automatic negotiation, or configure them both with the same fixed speed and duplex settings.
Speed	Set the connection's speed to <i>10 Mbit/s</i> or <i>100 Mbit/s</i> . Select automatic negotiation if you require a connection speed of <i>1000 Mbit/s</i> .	The connection speed setting must be the same for the ports at both ends of this connection.
Duplex	Set the connection's duplex mode to <i>Full duplex</i> or <i>Half duplex</i> .	The connection duplex setting must be the same for the ports at both ends of this connection. Full duplex mode allows simultaneous bidirectional transmission, while half duplex mode only allows bidirectional transmission that is not simultaneous.

Ethernet status

Field	Field description	Usage tips
Link status	Indicates whether or not this Ethernet link is connected.	
Speed	The speed (<i>10/100/1000 Mbit/s</i>) of this Ethernet link.	This value is negotiated with the device to which this port is connected or based on your Manual configuration selected above.
Duplex	The duplex mode (<i>Full duplex</i> or <i>Half duplex</i>) of the network connection to this port.	This value is negotiated with the device to which this port is connected or based on your Manual configuration selected above.
MAC address	The fixed hardware MAC (Media Access Control) address of this port.	You can not change this value, it is for information only.
Packets sent	The total number of packets sent from this port (all TCP and UDP traffic).	This information can help you confirm that the blade is transmitting packets into the network.
Packets received	The total number of packets received by this port (all TCP and UDP traffic).	This information can help you confirm that the blade is receiving packets from the network.

Statistics: More statistics for this port.

- Multicast packets sent
- Multicast packets received
- Total bytes sent
- Total bytes received
- Receive queue drops
- Collisions
- Transmit errors
- Receive errors

This information can assist you with diagnosing network issues, such as link speed and duplex negotiation issues.

Automatic IPv6 address preferences

This table details the address assignment preferences that are applied for IPv6 addressing when port configuration is set to *Automatic*.

RA flags* (Router advertisement)			Preferred address
a	o	m	
0	0	0	NA
1	0	0	SLAAC
0	1	0	NA
1	1	0	Stateless DHCPv6
0	0	1	Stateful DHCPv6
1	0	1	Stateful DHCPv6
0	1	1	Stateful DHCPv6
1	1	1	Stateful DHCPv6

*a: ICMPv6 prefix information, auto flag

*o: ICMPv6, other flag

*m: ICMPv6, managed flag

Related topics

- [Displaying an individual blade's status \[p.64\]](#)
- [Individual blade services configuration \[p.77\]](#)
- [Individual blade routes configuration \[p.74\]](#)
- [Individual blade backup configuration \[p.117\]](#)
- [Displaying the blades overview \[p.54\]](#)

Individual blade routes configuration

To check or modify the route settings on a blade, click **Hardware**, select the blade from the summary page, and then click **Routes**.

To configure the route settings on the Supervisor itself, go to **Network > Routes**.

Note: These pages are identical to the corresponding pages that you'll see if you log on to the managed blade. The Supervisor immediately updates the managed blade when you make changes to the blade's configuration. However, if you make the same change directly on the managed blade, the blade may take a short while to report the change back to the Supervisor.

Tip: Use the numbered links in the top right corner to switch between the Routes pages on the numbered blades without returning to the summary page.

On this page:

- [Port preferences](#)
- [IP routes configuration](#)
- [Current IP status](#)

Port preferences

If both Ethernet ports are enabled, it is necessary to specify which port is used in certain special circumstances. Make the appropriate selections described below, click **Apply changes** to make any changes take effect.

Field	Field description	Usage tips
IPv4 gateway preference	<p>Select the port whose default gateway setting the blade will use to send IPv4 traffic in the absence of more specific routing (see IP routes configuration).</p> <p>The blade routes IPv4 packets to the IPv4 default gateway when it does not have a more specific route. Therefore you only need one default IPv4 gateway, even though you may have configured <i>different</i> IPv4 default gateways on the blade's ports.</p>	<p>If Ethernet Port B is disabled, you cannot specify that port as the default gateway preference.</p> <p>If you select Port B as the default gateway preference, and then disable Port B, the blade's default gateway preference will revert to Port A.</p>
IPv6 gateway preference	<p>Select the port whose default gateway setting the blade will use to send IPv6 traffic in the absence of more specific routing (see IP routes configuration).</p> <p>The blade routes IPv6 packets to the IPv6 default gateway when it does not have a more specific route. Therefore you only need one default IPv6 gateway, even though you may have configured <i>different</i> IPv6 default gateways on the blade's ports.</p>	<p>If Ethernet Port B is disabled, you cannot specify that port as the default gateway preference.</p> <p>Selecting Port B as default gateway preference then disabling Port B will cause the preference to revert to Port A.</p>

IP routes configuration

In this section you can control how IP packets should be directed out of the managed blade. You should only change this configuration if you have a good understanding of the topology of the network(s) to which the

managed blade is connected.

Add a new IP route

To add a new route:

1. Enter the IP address of the target network, and the mask length that defines the range of addresses.
2. Select whether the traffic to those addresses will be routed via port A's default gateway, port B's default gateway, or a gateway that you specify.
3. Click **Add IP route**.
The new route is added to the list. If the route already exists, or aliases (overlaps) an existing route, the interface prompts you to correct the route.

Use the following table for reference:

Field	Field description	Usage tips
IP address / mask length	<p>Use these fields to define the range of IP addresses to which this route applies.</p> <p>IPv4 addressing: Enter the IP address of the target network in dotted quad format, setting any unfixed bits of the address to 0. Use the mask length field to specify how many bits are fixed (and thus how many are unfixed, giving the range of addresses).</p> <p>IPv6 addressing: Enter the IP address of the target network in CIDR format, setting any unfixed bits of the address to 0. Use the mask length field to specify how many bits are fixed (and thus how many are unfixed, giving the range of addresses). Enclose any IPv6 addresses in square brackets.</p>	<p>IPv4 example: To route all IPv4 addresses in the range 192.168.4.128 to 192.168.4.255, specify the IP address as 192.168.4.128 and the mask length as 25. The first 25 bits are fixed, which means that the last seven bits determine the range of addresses.</p> <p>IPv6 example: To route all IPv6 addresses in the range 2001:db8::1234:0000 to 2001:db8::1234:ffff, enter the IP address 2001:db8::1234:0000 and the mask length as 96. The first 96 bits are fixed, which means that the last 32 bits determine the range of addresses.</p>
Route	<p>Use this field to control how packets destined for addresses matching the specified pattern are routed.</p>	<p>You may select <i>Port A</i>, <i>Port B</i> or <i>Gateway</i>. If you select <i>Gateway</i>, specify the IP address of the gateway to which you want packets to be directed.</p> <p>If you select <i>Port A</i>, matching packets will be routed to Port A's default gateway (see Configuring network settings [p.14]).</p> <p>If you select <i>Port B</i>, matching packets will be routed to Port B's default gateway.</p> <p>If Ethernet Port B is disabled, the option to route packets to Port B will be disabled.</p>

To view or delete an existing IP route

The page displays the following details for each route:

- The IP address pattern and mask
- Where matching packets will be routed, with the possibilities being:
 - Port A - meaning the default gateway configured for Port A
 - Port B - meaning the default gateway configured for Port B
 - <IP address> - a specific address has been chosen

- Whether the route has been configured automatically as a consequence of other settings, or manually added by you.

The *default* routes are configured automatically by your choice of *Default gateway preferences* for IPv4 and IPv6 (see [Port preferences](#)) and cannot be deleted. Any packets destined for addresses that are not matched by your manually configured routes will be routed via the default gateway.

You can delete manually configured routes. Select the check boxes next to the routes then click **Delete selected**.

Routes behavior with disabled ports

If the default gateway preference is set to Port B but that port is disabled, the default route will automatically update to route unrecognised addresses via Port A.

If a manually configured route specifies Port B's default gateway but that port is disabled, packets matching that route **will be discarded**. They will not be automatically routed via Port A. You must take care to avoid this situation.

Current routes table

This table shows the IPv4 and IPv6 default gateways for each of the blade's Ethernet ports. If you want to change the default gateways for the Ethernet ports, go to **Hardware > Blades**, select the blade and then click **Port A** or **Port B**.

Related topics

- [Displaying the blades overview \[p.54\]](#)
- [Displaying an individual blade's status \[p.64\]](#)
- [Individual blade services configuration \[p.77\]](#)
- [Individual blade ports configuration \[p.70\]](#)
- [Individual blade backup configuration \[p.117\]](#)
- [Configuring IP routes settings \[p.21\]](#)
- [Configuring network settings \[p.14\]](#)
- [Allocating port licenses to blades \[p.86\]](#)

Individual blade services configuration

To check or modify the service settings on a blade, click **Hardware**, select the blade from the summary page, and then click **Services**.

The tables list the services available on the blade and the Ethernet ports on which those services may be enabled. It also shows the TCP or UDP port number used for each service, and whether the service is enabled for IPv4 or IPv6, or both. The available services, Ethernet ports, and IP addressing scheme shown can vary; these characteristics depend on the type of blade and the version of the software controlling that blade.

Select the services you want to enable, deselect any you want to disable, and then click **Apply changes**.

You may want to have different configurations for each Ethernet port. For example, if one Ethernet port is connected to a network outside your organization's firewall, you might want to disable FTP access on that port.

You can also use this page to specify the TCP or UDP port number on which the blade provides the service. Generally you won't need to change the default port number for a service. If you do, ensure that the port number you choose is not used by another service.

Note: These pages are identical to the corresponding pages that you'll see if you log on to the managed blade. The Supervisor immediately updates the managed blade when you make changes to the blade's configuration. However, if you make the same change directly on the managed blade, the blade may take a short while to report the change back to the Supervisor.

Tip: Use the numbered links in the top right corner to switch between the Services pages on the numbered blades without returning to the summary page.

Field	Field description	Usage tips
TCP service		
HTTP	Enable/disable HTTP access on the specified interface or change the port that is used for this service.	<p>HTTP access is required to view and change the blade's web pages and read online help files. If you disable HTTP access on both Ports A and B, you will need to use the serial console interface to re-enable it.</p> <p>Note that QuickTime uses RTSP by default which is listed as Streaming (other) on the Network > Services page. However, the QuickTime player can be configured to use HTTP instead.</p> <p>If you require advanced security for the blade, enable HTTPS and disable HTTP access.</p> <p>If a port is disabled, this option will be unavailable.</p>

HTTPS	Enable/disable HTTPS access, or change the port number used for HTTPS, on the specified interface.	<p>This field is only visible if the blade has the <i>Secure management (HTTPS)</i> feature key or an <i>Encryption</i> feature key installed. For more information about installing feature keys, refer to Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 [p.35].</p> <p>By default, the blade has its own SSL certificate and private key. However, you can upload a new private key and certificates if required. For more information about SSL certificates, refer to Configuring SSL certificates [p.121].</p> <p>If a port is disabled, this option will be unavailable.</p>
Incoming H.323	Enable/disable the ability to receive incoming calls to the blade using H.323 or change the port that is used for this service.	<p>Disabling this option will not prevent outgoing calls to H.323 devices being made by the blade.</p> <p>That is, the blade will need to dial out to conference participants who are using H.323.</p> <p>If a port is disabled, this option will be unavailable.</p>
SIP (TCP)	Allow/reject incoming calls to the blade using SIP over TCP or change the port that is used for this service.	<p>Disabling this option will not prevent outgoing calls to SIP devices being made by the blade. That is, the blade will need to dial out to conference participants who are using SIP over TCP.</p> <p>Note that if a SIP Outbound connection is negotiated with the registrar, SIP calls incoming via the registrar will still be accepted by the blade.</p> <p>If a port is disabled, this option will be unavailable.</p>
Encrypted SIP (TLS)	Allow/reject incoming encrypted SIP calls to the blade using SIP over TLS or change the port that is used for this service.	<p>Disabling this option will not prevent outgoing calls to SIP devices being made by the blade. That is, the MCU will need to dial out to conference participants who are using SIP over TLS.</p> <p>If a port is disabled, this option will be unavailable.</p>
Streaming (Windows Media Player)	Allow/disable streaming from the blade to Windows Media Player or change the port that is used for this service.	If a port is disabled, this option will be unavailable.
Streaming (other)	Allow/disable RTSP (Real Time Streaming Protocol) streaming from the blade to QuickTime or RealPlayer or change the port that is used for this service.	If a port is disabled, this option will be unavailable.
FTP	Enable/disable FTP access on the specified interface or change the port that is used for this service.	<p>FTP can be used to upload and download blade configuration.</p> <p>You should consider disabling FTP access on any port that is outside your organization's firewall.</p>

ConferenceMe	<p>Enable/disable the ConferenceMe service on the specified interface or change the port that is used for this service.</p> <p>By changing the port, you can block access to the web interface while still allowing users to use ConferenceMe to join conferences.</p>	<p>If a port is disabled, this option will be unavailable.</p>
UDP service		
SNMP	<p>Enable/disable the receiving of the SNMP protocol on this port or change the port that is used for this service.</p>	<p>If a port is disabled, this option will be unavailable.</p> <p>If you want to enable the receiving of the SNMP protocol on Port B, ensure that you have the video firewall as an activated feature (refer to Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 [p.35]) and you have selected the check box for SNMP on Port B.</p> <p>Note that by default SNMP Traps are sent to port UDP port 162 (on the destination network management station); this is configurable. For more information, refer to Configuring SNMP settings [p.26].</p> <p>If you require advanced security for the blade, disable the SNMP service.</p>
SIP (UDP)	<p>Allow/reject incoming and outgoing calls to the blade using SIP over UDP or change the port that is used for this service.</p>	<p>Disabling this option will prevent calls using SIP over UDP.</p> <p>If a port is disabled, this option will be unavailable.</p> <p>If you want to allow incoming and outgoing SIP (UDP) calls on Port B, ensure that you have the video firewall as an activated feature (refer to Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 [p.35]) and you have selected the check box for SIP (UDP) on Port B.</p>
H.323 gatekeeper	<p>Enable/disable access to the built-in H.323 gatekeeper or change the port that is used for the built-in H.323 gatekeeper.</p>	<p>If a port is disabled, this option will be unavailable.</p> <p>If you want to open Port B for the H.323 gatekeeper, ensure that you have the video firewall as an activated feature (refer to Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 [p.35]) and you have selected the check box for H.323 gatekeeper on Port B.</p>
Tunneled media	<p>Enable/disable tunneled media calls to the blade over UDP</p>	<p>This option must be enabled to allow ConferenceMe to connect over UDP. This option is only available if you have the <i>Web Conferencing</i> feature key installed.</p>

Related topics

- [Configuring IP services \[p.24\]](#)
- [Configuring network settings \[p.14\]](#)
- [Displaying an individual blade's status \[p.64\]](#)
- [Individual blade routes configuration \[p.74\]](#)
- [Individual blade ports configuration \[p.70\]](#)

- [Individual blade backup configuration \[p.117\]](#)
- [Displaying the blades overview \[p.54\]](#)

Individual blade shutdown

For some blade types, shut down and restart controls are available on the Supervisor's web interface. To access a blade's shutdown page, go to **Hardware** and click the name of the blade you want to restart. Click on the **Shutdown** tab. The procedure for restarting a blade is to shut down the blade and then restart it.

Field	Field description
Blade status	The current status of the blade. Possible blade statuses are listed in Displaying the blades overview [p.54] .
Slot ID	The number of the slot which houses the blade you want to shut down.
Operational status	The operational status is one of: <ul style="list-style-type: none">■ <i>Inactive – Unit's communications must be available before shut down</i>: The Supervisor has lost communication with the blade. You will be unable to restart the blade from the Supervisor.■ <i>Active – Unit must be shut down before restart</i>: The shutdown and restart process has not started. To restart the blade, click the shut down button.■ <i>Active – Shutdown must be confirmed before restart</i>: You have clicked the shut down button and now you must confirm that you want to shut down the blade. Click the confirm button.■ <i>Shutting down – Please wait</i>: The blade is shutting down. The page will refresh until the blade has shut down at which point the operational status will change to <i>Shutdown</i>.■ <i>Shutdown</i>: The blade is shut down. You must now restart the blade. Click the restart button.■ <i>Sent restart signal – Please wait</i>: You have clicked the restart button and the Supervisor has instructed the blade to restart. The page will refresh until the blade is restarting at which point the operational status will change to <i>Restarting</i>.■ <i>Restarting</i>: The blade is restarting. This can take several minutes.

Related topics

- [Displaying an individual blade's status \[p.64\]](#)
- [Individual blade backup configuration \[p.117\]](#)
- [Displaying the blades overview \[p.54\]](#)

Monitoring port licenses

This section describes how you can use the Cisco TelePresence Supervisor MSE 8050 to monitor and allocate port licenses.

Displaying the port license summary	83
Allocating port licenses to blades	86

Displaying the port license summary

This page provides an overview of port licensing on the chassis and allows you to enter new port license keys.

Port and screen licenses are provided by Cisco so that you can increase the number of ports that are licensed without requiring new hardware (up to the maximum available on a particular blade type). You can also license a number of ports and share the licenses over a number of chassis blades of the same type to provide redundancy. You can also swap a blade with a spare of the same type, as required, without needing to change the port license configuration.

Port/screen licenses apply to a particular blade type and therefore you need different license keys for each type of blade:






- Media port license keys for Media and Media2 blades
- PRI port license keys for ISDN GW blades
- IP GW port license keys for IP GW blades
- Recording port license keys for VCR blades
- TS screen license keys for Telepresence Server blades
- TS screen migration option license key for converting media port licenses to TS screen licenses and vice versa.

For each type of license you can have temporary or permanent licenses, or one of each. Temporary licenses have an expiry date, but if this date is in the future, then the temporary license will be used instead of the permanent one if it allows more ports. The permanent key will be used once more when the temporary one expires. If you enter a second permanent license for a port type that already has a permanent license, the new license key will automatically override the previous one that you used. This is equally true of a second temporary license of the same type, and applies irrespective of whether the number of port licenses in the second license key entered is greater or fewer than in the first license key.

Note: Port and screen licenses are stored on the chassis and tied in to the chassis serial number, not to the Cisco TelePresence Supervisor MSE 8050 blade. Therefore license keys will continue to be valid even if you need to swap Cisco TelePresence Supervisor MSE 8050 blades. Equally, licenses can be allocated to a slot even if the blade currently in that slot is unsuitable for that type of license - or even if there is no blade in that slot. For example, you may want to allocate a number of port licenses of each type to slot 10, and keep the slot empty in normal circumstances, ready for a blade should one of the other blades fail. As soon as the new blade is installed, it will pick up the licenses and be ready to use. (If you ordered the port/screen licenses with the chassis they are pre-installed on the chassis for you.) You cannot transfer port licenses between chassis, even when the blade type is the same. You can add new license keys at any time: on the Supervisor's web interface go to [Port licenses](#) and click **Add key**.

Port license status

Field	Field description	Usage tips
-------	-------------------	------------

Part number	The part number of the license, which depends on the type of blade this license is intended for.	There is one line for each license type for which a license key has been entered. Click on either link to see details of this license and be able to change allocation of ports under this license.
License type	The type of license: <i>Media, Recording, PRI, IP GW</i> or <i>TS screen license</i> .	
Expiry	Never or a date.	Licenses can be permanent or temporary. The temporary key will take precedence, provided that it has not expired and that it is for a greater number of ports than the permanent key for the same license type.
Allocated	The number of port licenses of this type that have been allocated to blades.	
Available	The number of unallocated licenses of this type.	
Allocation	Icons show which blades have been allocated licenses of this type:	Slots 2 to 10 are shown. Hover over the icon to see the number of licenses allocated to the blade and an explanation of the blade's status.
	<p>No licenses of this type are allocated to this slot and there is no blade in this slot capable of using this type of license.</p> <hr/> <p> The blade is capable of using this type of license, but no licenses are allocated.</p> <hr/> <p> The blade is capable of using this type of license, and some have been allocated, but less than the full capacity of the blade.</p> <hr/> <p> The blade is capable of using this type of license, with the number of licenses allocated exactly matching the blade's capacity.</p> <hr/> <p> There are licenses being wasted: either more licenses have been allocated to a slot than the blade in the slot has capacity for, or licenses have been allocated to an empty slot.</p> <hr/> <p> Licenses have been allocated incorrectly: some licenses have been allocated to a slot with a blade, but the blade is incapable of using these licenses.</p>	

License key management

Field	Field description	Usage tips
License key	The license key code that you entered.	
License Type	The type of license: <i>Media</i> , <i>Recording</i> , <i>PRI</i> , <i>IP GW</i> or <i>TS</i> screen license.	Media licenses are intended for Media and Media2 blades, Recording licenses for IP VCR blades, PRI licenses for ISDN GW blades, IP GW for IP GW blades and TS screen licenses for Telepresence Server blades. TS screen migration option licenses allow the conversion of media port licenses to TS screen licenses and vice versa. Note that keys that are not being used are listed but grayed.
Quantity	The number of port licenses that this license gives you permission to use.	
Expiry	The expiry date of this key.	<i>Never</i> or a date. (Expired license keys remain listed.)

Adding a new license key

To enter a new key, type in the key exactly as provided including dashes and click **Add key**. The key is verified against the chassis number. (It is recommended that you keep a record of the key in case you need to re-enter it in the future.)

Related topics

- [Allocating port licenses to blades \[p.86\]](#)

Allocating port licenses to blades

To use the licenses on the Cisco TelePresence Supervisor MSE 8050, you must allocate them to the blades. Even when licenses are pre-installed on the chassis, they need to be allocated to blades.

Note that you can:

- allocate more port licenses than the port capacity (for example, if you are updating the port allocation in anticipation of swapping blades)
- allocate port licenses for a different type to the blade currently in the slot, although a warning will be displayed. The icon and **State** field also change to remind you
- allocate additional port licenses by converting media port licenses to TS screen licenses or vice versa. (Requires the license conversion feature key "TS screen migration option" to be installed and visible on the Port license summary page.) One TS-screen license converts to 5 media port licenses.
- allocate port licenses to empty slots. For example, you may want to allocate a number of port licenses of each type to slot 10, and keep the slot empty in normal circumstances, ready for a blade should one of the other blades fail. As soon as the new blade is installed, it will pick up the licenses and be ready to use






To allocate port licenses to blades:

1. Go to **Port licenses**.
2. Click on the link for the type of port license that you want to allocate (Note that all the Allocation pages have the same layout irrespective of license type).
3. For **New allocation**, enter the number of licenses to allocate to each slot.
4. Click **Update allocation**.

Note: Standard definition ports require one port license per port but high definition ports require more than one port license per port. See the online help on the individual blade for details.

The table below describes the fields on the allocation page.

Field	Field description	Usage tips
Slot	The slot number in the chassis.	All slots are shown, even those of the type not selected.
Blade type	The model number of blade in the slot.	

State	Icons show the current port license status for each slot:	
		No licenses of this type are allocated to this slot.
		The blade has some licenses of this type allocated to it, but less than the full capacity of the blade.
		The number of licenses of this type allocated exactly matches the blade's capacity.
		There are licenses being wasted: either more licenses have been allocated to a slot than the blade in the slot has capacity for, or licenses have been allocated to an empty slot.
		Licenses of this type have been allocated incorrectly: some licenses have been allocated to a slot with a blade, but the blade is incapable of using these licenses.
Port capacity	The number of licenses of this type that the blade can support.	Standard definition ports require one port license per port but high definition ports require more than one port license per port. See the online help on the individual blade for details.
Current allocation	The number of licenses of this type that have been allocated to each slot.	
New allocation	Enter the number of port licenses of this type that you want to allocate to each slot. This number replaces the <i>Current allocation</i> , it does not add to it.	

Viewing a summary of current license usage

Use the License usage summary table below the port allocation table to view license usage information. The information displayed depends on the type of port license you selected when you accessed the Allocations page. If the license conversion feature key "TS screen migration option" is installed and visible on the Port license summary page, the License usage summary table displays information about licenses converted and available for conversion from another license type.

Field	Field description	Usage tips
Sources of <name> ports / Sources of TS screens		
<name> licenses	Number of native licenses.	This row is always displayed.

Converted from <name> licenses	Number of licenses converted from the named license type.	This row is displayed only if licenses have been converted from another license type.
Available from <name> licenses	Number of licenses available for conversion from the named license type.	This row is displayed only if licenses are available to be borrowed from another license type.
Consumers of <name> ports / Sources of TS screens		
Allocated to slots	Total number of licenses allocated to slots.	Identical to the "Total" value in the port allocation table This row is always displayed.
Converted to <name> ports / Converted to TS screens	Total number of converted licenses.	This row is displayed only if licenses have been converted to another license type.
Available <name> ports / Available TS screens		
Sources of <name> ports minus allocations of <name> ports / Sources of TS screens minus allocations of TS screens	The sum of "Sources of ports" minus the sum of "Consumers of ports".	This number is identical to the "Available" value in the port allocation table.

Allocating additional media port licenses by converting TS screen licenses

If all native media port licenses are already allocated and the license conversion feature key "TS screen migration option" is installed, you can allocate additional media port licenses by converting available TS screen licenses as follows:

1. Go to **Port licenses**.
2. In the Port license status table, click the Media port licenses link.
3. Use the information displayed in the License usage summary table to check how many additional media port licenses are available for conversion from TS screen licenses. Each TS screen license equates to five additional media port licenses.
4. For **New allocation**, enter the number of media port licenses to allocate to each slot.
5. Click **Update allocation**.
Conversions are rounded up to meet the required number of licenses. For example, if 49 additional (non-native) media port licenses are required, 10 TS screen licenses are converted, giving a total of 50 converted licenses.

Allocating additional TS screen licenses by converting media port licenses

If all native TS screen licenses are already allocated and the license conversion feature key "TS screen migration option" is installed, you can allocate additional TS screen licenses by converting available media port licenses as follows:

1. Go to **Port licenses**.
2. In the Port license status table, click the TS screen licenses link.
3. Use the information displayed in the License usage summary table to check how many additional TS screen licenses are available for conversion from media port licenses. Five media port licenses equate to one additional TS screen license.
4. For **New allocation**, enter the number of TS screen licenses to allocate to each slot.
5. Click **Update allocation**.
Media ports cannot be rounded up. For example, if you have 49 media port licenses, you can convert to up to 9 TS screen licenses. 10 TS screen licenses would require 50 media port licenses.

Related topics

- [Displaying the port license summary \[p.83\]](#)

Clustering

This section describes how you can use the Cisco TelePresence Supervisor MSE 8050 to configure and manage clusters.

Understanding clustering	91
Displaying the clustering summary	93
Configuring clustering	96
Reviewing cluster configuration	98

Understanding clustering

About clustering

Clusters are configured and managed using the Cisco TelePresence Supervisor MSE 8050. A cluster is a group of blades on the same MSE chassis linked together to behave as a single unit that provides the combined port count of all the blades in the cluster. A larger port count provides flexibility: either conferences with more participants or several smaller conferences. You can configure two types of cluster:

- **MSE 8510 cluster:** MSE Media2 blades running software version 4.1 or later support clustering. Clustering provides you with the combined port count of the blades in the cluster. For example, on an MSE 8510 cluster of three blades each with 20 port licenses, the cluster can have either 30 HD ports or 15 HD+ ports and the master can allocate them to participants in conferences as necessary. This could be one large conference, or several smaller conferences. Note that in a cluster of MSE 8510 blades, SD ports are not available.

The maximum port counts for clusters comprising three MSE 8510 Media2 blades are as follows:

- For HD+ mode, the maximum number of port licenses that a three-blade cluster can utilize is 240. This will provide you with a total of 60 HD+ ports.
- For HD mode, the maximum number of port licenses that a three-blade cluster can utilize is 120. This will provide you with a total of 60 HD ports.

To configure media ports, on the MCU go to **Settings > Media ports**.

- **Telepresence Server 8710 cluster:** Telepresence Server blades running software version 2 or later support clustering. Currently up to three blades can be clustered, with one blade acting as a "master" and the other blades being "slaves" to this master. Clustering provides you with the combined video port count of the blades in the cluster. For example, on an MSE 8710 cluster of three blades each with 16 screen licenses, the cluster has 48 video ports and the master can allocate them to participants in conferences as necessary. This could be one large conference, or several smaller conferences.

Master blades

All of the port or screen licenses allocated to all the blades in a cluster are "inherited" by the master blade; all ports in the cluster are controlled by the master. Therefore, after you have configured a cluster, you must control functionality through the master using either its web interface or through its API. All calls to the cluster are made through the master. For details, see the online help for the type of cluster that you have configured.

Slave blades

Slave blades do not display the full blade web interface. Only certain settings are available, such as network configuration, logging and upgrading. Similarly, a slave blade will only respond to a subset of API methods. For more information, refer to the relevant API documentation (available on the Support pages of www.cisco.com).

General points

Some points to note about clustering:

- To cluster a blade, it requires the cluster support feature key.
- The Supervisor blade must be running software version 2.1 or above to configure clustering.

- You cannot mix the type of blades in a cluster but you can have both types of cluster in the same MSE 8000 chassis.
- All blades in a cluster must be running the same version of software.
- You assign the cluster roles (master/slave) to the slots in the chassis; if a blade fails, you can replace it with a blade of the same type and the cluster configuration will persist; however, what happens to active calls and conferences varies, as described below.
- If you restart or remove the master, the slaves will also restart: all calls and conferences end.
- Blades that do not support clustering can be installed into an MSE 8000 chassis alongside a cluster.
- If the clustering configuration on the Supervisor and a blade disagree, then the Supervisor pushes the clustering configuration to the blade. (This might happen if you replace a slave blade with another blade of the same type.) The clustering configuration only includes clustering information; it does not configure network settings or anything else on the blade. If the Supervisor has pushed a configuration change to a blade, the Supervisor will prompt you to restart the blade.
- Always keep a recent backup of the Supervisor, see [Backing up the Cisco TelePresence Supervisor MSE 8050 blade to the compact flash \[p.37\]](#).
- If the Supervisor restarts or is removed, the cluster continues to function, conferences continue, and the cluster does not restart when the Supervisor reappears.
- Slave blades only have admin logins.

Upgrading clustered blades

If you need to upgrade the blades in a cluster, first upload the new software images to each blade in the cluster and then restart the master. The slaves will automatically restart and the upgrade will be completed.

Related topics

- [Displaying the clustering summary \[p.93\]](#)
- [Configuring clustering \[p.96\]](#)
- [Reviewing cluster configuration \[p.98\]](#)

Displaying the clustering summary

To view the chassis clustering summary, go to [Clustering > Summary](#).

The [Clustering summary](#) page provides an overview of clustered blades in the chassis. There is one table per cluster and one table for unclustered blades.

To configure clusters, go to [Clustering > Configuration](#).

The following fields are shown on the [Clustering summary](#) page.

Field	Field description	Usage tips
Slot	Slots are numbered from left to right as you look at the chassis.	The Cisco TelePresence Supervisor MSE 8050 must be fitted in to slot 1. If it is not, you see an error message in the page header. Swap the Cisco TelePresence Supervisor MSE 8050 in to slot 1. If there is no blade in a slot, you see blade <i>absent</i> .
Type	The type of blade in a slot.	The MSE 8000 chassis can be fitted with Codian Media, Media2, IP VCR, ISDN Gateway, IP Gateway blades and TelePresence Servers in addition to the Cisco TelePresence Supervisor MSE 8050.
Version	The software version of the blade in this slot.	All blades in the same cluster must be running the same software version.
Role	The blade's role in the cluster: Master or Slave	This field only applies to clusters.
Supports clustering	Whether the blade can be part of a cluster or not.	This field only appears in the table for unclustered blades. Only Media2 and TelePresence Server blades installed with the <i>Cluster support</i> feature key can be clustered.
Status	The status of each individual blade. Blade statuses are listed in Displaying the blades overview [p.54] .	Note that each slot has two status LEDs. If there is no blade fitted, neither light is on. When a blade is fitted, the red LED lights until communication is established with the Supervisor, when the green LED lights instead. The red LED also lights subsequently if the communications link fails. (The first thing to check if the red LED is on is that the blade is correctly inserted.)
Cluster warnings		If there is a cluster warning, click the Configuration tab and resolve the conflict. Refer to the list of possible cluster warnings below .
Restart	You'll see a restart button if the blade needs to be restarted.	Any changes to the cluster configuration requires every blade in that cluster to be restarted. This includes the master blade, which means that every conference running on this cluster will stop.

Cluster warnings

Cluster warning	Description
-----------------	-------------

Restart blade to apply new configuration	This blade requires a restart to apply the changes to the configuration.
Blade will require a restart.	You have changed the configuration of this blade. Apply the changes and then restart this blade.
Blade restarting	This blade is currently restarting. You can still configure it as part of a cluster but it will prompt you to restart it again to enable it to join the cluster. You can also configure it as unclustered, or leave it as it is. Any change to the cluster role of the blade will not take effect until the blade completes the current restart and you restart it again.
Configuring blade	The Supervisor is configuring this blade. The Supervisor might prompt you to shut down and restart this blade, depending on the type of configuration changes.
Clustering feature key not present on this blade	This blade supports clustering, but it does not have the <i>Cluster support</i> feature key. To add this blade to a cluster, install the feature key first.
Waiting for communication	This blade is just starting up and the Supervisor is waiting for this blade to provide information about its clustering role.
Absent/removed blade will be set to unclustered	There is no blade in this slot. The slot will automatically be set to unclustered.
Master blade using different software version	This blade is using a different software version to that on the master. This cluster will not be able to use the resources on this blade until you upgrade the blade to the same software version. Every blade in a cluster must be using the same version of software.
Master not configured	This blade is configured to be a slave of another blade, but that other blade is not configured as a master.
Blade can only support <number> slaves	This master has been configured with too many slaves.
Incompatible master	This blade is configured with a master that is of a different product type. A cluster can only include blades of the same product type.
Clustering not supported on this blade	This blade is either of a type that does not support clustering or it is running software that does not support clustering. If you configure this blade, the slot will automatically be set to unclustered.
<type of> blade conflicts with supervisor records	<p>The Supervisor's clustering configuration conflicts with that on this blade; you may have swapped the blade at some point after you configured it as part of a cluster.</p> <p><type of> will be one of:</p> <ul style="list-style-type: none"> ■ <i>Master</i> ■ <i>Slave</i> ■ <i>Unclustered</i> ■ <i>Unclustered (no key)</i>. <p>You must resolve this conflict before you continue.</p>

Invalid blade ID	The blade ID has been incorrectly communicated to the Supervisor. Ensure that the blade is firmly secured in the chassis. Close both retaining latches on the front of the blade. Tighten the screws in the retaining latches, with a clockwise quarter turn, using a number 1 Phillips screwdriver.
New configuration will be set upon Supervisor activation	The Supervisor's clustering configuration is different to that on this blade <i>and</i> you have not yet activated the Supervisor. When you activate the Supervisor, it will apply its clustering configuration to this blade.

Related topics

- [Understanding clustering \[p.91\]](#)
- [Configuring clustering \[p.96\]](#)
- [Displaying the blades overview \[p.54\]](#)
- [Backing up the Cisco TelePresence Supervisor MSE 8050 blade to the compact flash \[p.37\]](#)

Configuring clustering

The **Cluster configuration** page allows you to create a number of clusters on the chassis. To display the page, go to **Clustering > Configuration**.

For more information about clustering, see [Understanding clustering \[p.91\]](#).

To create a cluster:

1. Set up the hardware:
 - a. Put the MSE Media2 Blades in the slots that you want to use for the cluster.
 - b. Ensure that each blade is firmly secured in the chassis. Close both retaining latches on the front of the blade. Using a number 1 Phillips screwdriver, tighten the screws in the retaining latches with a clockwise quarter turn.
2. Go to the Supervisor's web interface and set up the network settings for the blades. (For more information, refer to [Configuring network settings \[p.14\]](#).)
3. Go to the web interface of each blade and install the cluster support feature key.
4. Go to the Supervisor's web interface and allocate the port licenses that you require for the cluster. You can allocate the port licenses as you want to the slots in the cluster (either all to the slot housing the master, or distributed between the slots in the cluster); all ports in the cluster will be controlled by the master. If there are existing port license allocations, you can leave them alone. For new port licenses, you can allocate some to each blade in the cluster (in case you later remove a blade from the cluster).
5. On the Supervisor, go to **Clustering > Configuration**.
6. Check that the software version of all the blades that you want to cluster is the same and check that each supports clustering.
7. Set up the master and slaves as required using the **Change settings** drop-down menu.
8. Click **Review changes**.
9. If the configuration is as you want it, click **Apply changes** (if not, click **Return to configuration** and correct).
10. The **Clustering > Summary** page is displayed. For some blades a **Shutdown** button might display. If this is the case, use this button to restart the blade.
11. On the master blade, go to **Status > Cluster** and check the status of the cluster. For all blades in the cluster the status should be *OK*.

Field	Field description	Usage tips
Slot	The slot number in the chassis. Slots are numbered from left to right as you look at the chassis.	All slots are shown, even those that do not support clustering.
Type	The type of blade in the slot.	
Version	The version number of the software running on the blade.	

Current role	The current role of the blade.	<p>One of:</p> <ul style="list-style-type: none"> ■ <i>Master</i>: This blade is configured as a master blade ■ <i>Slave of slot <slot number></i>: This blade is configured as a slave of the blade in the given slot number ■ <i>Not clustered</i>: This blade is currently not part of a cluster ■ <i>Not supported</i>: This blade does not support clustering. It is either a type of blade that does not support clustering, or it is running software that does not support clustering. For more information, refer to Understanding clustering [p.91]
Change settings	Select the new role for a blade from the drop-down list.	<p>You have the option to configure a blade as a master, or as a slave to any slot, or as an unclustered blade.</p> <p>You cannot change the role of a blade on which clustering is not supported.</p>
Status	The status of the blade. Blade statuses are listed in Displaying the blades overview [p.54] .	Even if the status of the blade is <i>Blade restarting</i> or <i>Lost communication</i> , you can configure the blade to be in a cluster. In these cases, when the blade completes its restart it will prompt you to restart the blade again (a Shutdown button will appear).
Cluster warnings	The Supervisor will list if there is a clustering problem with this blade.	Cluster warnings are described in Displaying the clustering summary [p.93] .

Related topics

- [Understanding clustering \[p.91\]](#)
- [Reviewing cluster configuration \[p.98\]](#)
- [Displaying the clustering summary \[p.93\]](#)
- [Displaying the blades overview \[p.54\]](#)

Reviewing cluster configuration

The **Review clustering** page allows you to review a new cluster configuration on the chassis before you save and apply that new configuration. To display the page, when you have made changes on **Clustering > Configuration**, click **Review changes**.

It is important to review all the configuration changes before you apply the new configuration. In particular, you will need to fix any problems before you apply the configuration. Read carefully and pay attention to any cluster warnings. Refer to [Displaying the clustering summary \[p.93\]](#) for information about cluster warnings.

For more information about clustering, see [Understanding clustering \[p.91\]](#).

For information about configuring clustering, see [Configuring clustering \[p.96\]](#).

Related topics

- [Understanding clustering \[p.91\]](#)
- [Configuring clustering \[p.96\]](#)
- [Displaying the clustering summary \[p.93\]](#)
- [Displaying the blades overview \[p.54\]](#)

Alarms

This section describes how to configure Cisco TelePresence Supervisor MSE 8050 alarms.

Displaying the alarm status	100
Displaying the alarm log	101
Configuring alarm levels	104

Displaying the alarm status

To display the **Alarm status** page for the chassis, go to **Alarms**. This page shows the status of a number of conditions that can cause an alarm; divided by whether the condition raises a Critical, Major or Minor alarm. (This is set in the [Configuring alarm levels \[p.104\]](#) page.)

The following statuses are available for each condition:

- *OK*: everything is operating satisfactorily
- *Alarm*: there is a current alarm for this condition. See the [Displaying the alarm log \[p.101\]](#) for more details, which also lists the possible alarms
- *Muted*: the alarm condition still exists but the alarm has been silenced by pressing the **Silence** button on the chassis. See the [Displaying the alarm log \[p.101\]](#) for more details
- *Historic alarm*: there was an alarm for this condition previously, but the alarm condition has been resolved. See the [Displaying the alarm log \[p.101\]](#) for more details

If there are alarms present, these will also be shown by LEDs and, for *Major* and Critical alarms, the sounder activates. If there are no alarms, then the Status LED is green.

To clear the historic alarms from this page, click **Clear historic alarms**. This:

- Clears the alarm LEDs
- Does *not* affect the entries in the Alarms log
- Does *not* clear the alarms where the condition that caused the alarm still exists, even if the sounder has been silenced using the Silence button beside the LEDs

Note: Some alarms are instantaneously set and resolved, and therefore you see the status as a Historic alarm; for example, the Power on alarm is always a historic alarm.

Related topics

- [Configuring alarm levels \[p.104\]](#)
- [Displaying the alarm log \[p.101\]](#)

Displaying the alarm log

To display the **Alarm log** page for the chassis, go to **Alarms > Alarms log**. The Alarm log shows up to 2000 alarms with the most recent alarms at the bottom of the list.

Field	Field description	Usage tips
Time	The time that the alarm event occurred.	
Alarm	The type of alarm (see the Possible alarms [p.102] below).	Which component raised the alarm and why.
Action	The status of the alarm when this entry occurred.	One of: <i>Set</i> : an alarm condition occurred <i>Muted</i> : the alarm was silenced by pressing the Silence button on the chassis <i>Cleared</i> : the alarm was cleared because the component started operating normally again. <i>Revised</i> : this alarm has already been set previously, but has recurred. For example, if the Blade communication failure occurs on one blade, the log shows which blade this is. If the error occurs on a second blade while the first error is still set, then the Blade communication failure appears as a new entry but says "multiple blades". Go to Logs > Events log and see which blades are in error.
Severity	Whether the alarm was a Critical, Major or Minor alarm.	The severity with which an alarm condition is reported is set in the Alarm levels page.

You can:

- Sort the log by any column heading: for example to see all critical alarms at the top
- Display the log as text in a file by clicking **Download as text**
- Click **Clear log** to empty the log
- Change the level of detail collected in the traces in the **Alarms > Alarm levels** page

Note that if you update the alarm levels; for example, changing a condition from a Minor to a Major alarm, the **Alarm status** page is updated to reflect this change - even for historical alarms - but the **Alarm log** page always shows the alarm level that applied when the alarm occurred.

If an alarm occurs repeatedly and you cannot discover the reason for this, contact Technical support.

Possible alarms

The following table shows the alarms that are monitored by the Cisco TelePresence Supervisor MSE 8050. The status of these alarms is displayed in the [Displaying the alarm status \[p.100\]](#) page. You can change the severity with which an alarm is reported in the [Configuring alarm levels \[p.104\]](#) page.

Alarm	Default severity	Seen when
Power on	No alarm	The Supervisor blade boots.
Fan failure	Minor alarm	The fan speed is detected as too low or too high.
Fan tray(s) absent	Major alarm	Immediately when the fan tray is not detected.
Fan tray communication failure	Major alarm	The fan tray has not communicated for 60 seconds.
Filter blocked	Minor alarm	The filter check fails.
Blade unexpectedly removed	Minor alarm	A blade is removed without proper shutdown.
Blade unexpectedly rebooted	Minor alarm	A blade has rebooted without proper shutdown.
Blade communication failure	Major alarm	A blade has not communicated for an extended time period.
Blade temperature critical	Critical alarm	The blade temperature is above safe levels.
Power supply out of range	Major alarm	The input voltages to the chassis are outside the specification.
Internal voltages out of range	Major alarm	The low voltage supervisor / chassis supplies are outside of the specification.
Power supply reporting fault	Major alarm	The Valere power supply reports "not ok" status.
Lost contact with power supply	Major alarm	The Valere power supply is not responding to communication within 15 seconds, or on an authentication failure.

No compact flash card inserted	Minor alarm	No CompactFlash card is inserted in the Supervisor blade.
Port licenses automatically deallocated	Major alarm	A port license expires causing port licenses to be removed from a blade.
Supply under capacity	Major alarm	One or both of the power shelves reports insufficient capacity.
New supervisor inserted	Major alarm	Someone has replaced the Supervisor blade with another Supervisor blade.
Blade badly seated	Minor alarm	The blade is incorrectly installed. Ensure that the blade is firmly secured in the chassis. Close both retaining latches on the front of the blade. Using a number 1 Phillips screwdriver, tighten the screws in the retaining latches with a clockwise quarter turn.

Related topics

- [Displaying the alarm status \[p.100\]](#)
- [Configuring alarm levels \[p.104\]](#)

Configuring alarm levels

To display the **Alarm levels** page, go to **Alarms > Alarm levels**. This page displays the conditions that can cause alarms to be raised and their current severity level. Each alarm is assigned a default severity level of None (not reported in the Alarms log), Minor, Major, or Critical depending on how the cause of the alarm affects the services provided by the chassis. The default setting for each condition is shown in bold.

Note: Only Major and Critical alarms activate the sounder.

Changing an alarm level changes the level shown on the **Alarms status** page immediately: alarms occurring after the change are reported with the new level. But historic alarms are also affected; for example, if you change an Alarm level setting from Minor to Major and this alarm occurred previously and therefore was reported as Minor, it will now be reported as Major on the **Alarms status** page. However, levels are not updated in the Alarms log - here you see the level that was assigned to each alarm at the time it occurred.

After you have set the alarm levels, click **Apply changes**.

Related topics

- [Displaying the alarm status \[p.100\]](#)
- [Displaying the alarm log \[p.101\]](#)

Advanced topics

This section describes advanced configuration tasks for the Cisco TelePresence Supervisor MSE 8050.

Working with the event logs	106
Working with the audit log	108
Understanding security warnings	109
Logging using syslog	112
Management event receivers	115
Feedback receivers	116
Individual blade backup configuration	117
Customizing the user interface	118
Network connectivity testing	120
Configuring SSL certificates	121
Transitioning to certificate-based security	127

Working with the event logs

If you are experiencing complex issues that require advanced troubleshooting, you may need to collect information from the Cisco TelePresence Supervisor MSE 8050 logs. Typically, you will be working with Customer support who can help you obtain these logs.

Event log

The last 2000 status messages generated by the Cisco TelePresence Supervisor MSE 8050 are displayed in the **Event log** page (**Logs > Event log**).

In general these messages are provided for information, and occasionally *Warnings* or *Errors* may be shown in the Event log. The presence of such messages is not necessarily cause for concern; if you are experiencing a specific problem with the operation or performance of the Cisco TelePresence Supervisor MSE 8050, Customer support can interpret logged messages and their significance for you.

You can:

- Change the level of detail collected in the traces by editing the **Capture filter** page. You should not modify these settings unless instructed to do so by Customer support.
- Display the log as text: go to **Logs > Event log** and click **Download as text**.
- Change which of the stored Event log entries are displayed by editing the **Display filter** page
- Send the event log to one or more syslog servers on the network for storage or analysis. The servers are defined in the **Syslog** page.
For more information, refer to [Logging using syslog \[p.112\]](#)
- Click **Clear log** to empty the log

Event capture filter

The Event capture filter allows you to change the level of detail to collect in the Event log traces.

Note: You should not modify these settings unless instructed to do so by Customer support. You may impair the performance of your Cisco TelePresence Supervisor MSE 8050 if you modify these settings.

Normally, the capture filter should be set to the default of *Errors, warnings and information* for all logging sources. There is no advantage in changing the setting of any source without advice from Customer support. There is a limited amount of space available to store logged messages and enabling anything other than *Errors, warnings and information* could cause the log to become full quickly.

Event display filter

Use the Event display filter to view or highlight stored Event log entries. Normally, you should not need to view or modify any of the settings on this page.

Syslog

You can configure the Cisco TelePresence Supervisor MSE 8050 to send event messages to up to four syslog servers. To add or remove a syslog server, go to **Logs > Syslog** to make the changes you require.

See [Logging using syslog \[p.112\]](#).

Audit log

The audit log records any user action on the Cisco TelePresence Supervisor MSE 8050 which might compromise the security of the unit, of its functions, or of the network. For more information, refer to [Working with the audit log \[p. 108\]](#).

Related topics

- [Logging using syslog \[p. 112\]](#)

Working with the audit log

The audit log records any user action on the Cisco TelePresence Supervisor MSE 8050 which might compromise the security of the unit, of its functions, or of the network.

By enabling auditing, all network settings, security settings, and any changes to the audit log itself are logged on the Cisco TelePresence Supervisor MSE 8050.

All relevant actions on the Cisco TelePresence Supervisor MSE 8050 are logged, including those made through the serial console, a supervisor blade (for MSE blades), the API, FTP, and the web interface. The module that has caused a log is listed within the details of that log and will be one of:

- **Web:** For configuration changes made through the web interface.
- **Serial:** For configuration changes made through the serial interface.
- **API:** For configuration changes made through the API.
- **Supervisor:** For configuration changes made through the Supervisor Blade (only applies to MSE blades).
- **System:** For audit messages from the Cisco TelePresence Supervisor MSE 8050.
- **FTP:** For audit messages recording requests made to the Cisco TelePresence Supervisor MSE 8050 over FTP.

Each log also has a severity associated with it (Error, Severe Warning, Warning, Info, or Status Warning).

You must enable the audit log for it to record these actions.

To enable and view the audit log, go to [Logs](#) and select the **Audit log** tab.

Audit log

The last 2000 audit messages generated by the Cisco TelePresence Supervisor MSE 8050 are displayed in the **Audit log** page.

The last 100,000 audit messages are stored on the compact flash if there is one; otherwise, the last 100,000 audit messages are stored internally. You can only view the last 2000 through the web interface, but you can download all stored audit messages (up to the 100,000) as XML.

You can delete audit messages, but you cannot delete the most recent 400 audit messages. If you delete any audit messages, that will be audited in a new audit message.

You cannot send the audit log to a syslog server.

Related topics

- [Configuring security settings \[p.32\]](#)
- [Understanding security warnings \[p.109\]](#)

Understanding security warnings

The **Security status** page displays a list of active security warnings for the Cisco TelePresence Supervisor MSE 8050. To access this information, go to **Status > Security**. Security warnings identify potential weaknesses in the security of the Cisco TelePresence Supervisor MSE 8050's configuration. For more information on configuring security settings, refer to [Configuring security settings \[p.32\]](#). For more detailed information on the security status, refer to [Displaying security status \[p.52\]](#).

The table below details the warnings that appear, and the relevant actions needed to rectify them.

Warning	Action	Explanation
Advanced password security is disabled	Enable advanced account security mode in security settings	If advanced account security mode is not enabled, passwords will be stored in plain text in the configuration file, and therefore be unsecure. To enable advanced account security mode, go to Settings > Security and enable <i>Advanced account security mode</i> .
Hide log messages on console is disabled	Enable hide log messages on console in serial console settings	To hide log messages on the console, go to Settings > Security and select Hide log messages on console . This will stop event messages appearing on the console.
Require administrator login to console is disabled	Enable require administrator login in serial console settings	You must log in using an admin account to access serial console commands, in this way the serial console will be more secure. To do this, go to Settings > Security and select Require administrator login .
Guest account is enabled	Disable the guest account.	By default the guest user account is assigned the privilege of 'conference list only', meaning that users who log in as guest can view the list of active conferences and change their own profile. Disabling the guest account makes the Cisco TelePresence Supervisor MSE 8050 more secure. To disable the guest account, go to Users > User list and select Guest . Select Disable user account .
Admin account has default username	Change the admin account username	The Cisco TelePresence Supervisor MSE 8050 must have at least one configured user with administrator privileges. By default, the User ID is "admin" and no password is required. To change the admin account username, go to Users > User list and select admin . Enter a new username in the User ID field and click Update user settings .
Unsecured FTP service is enabled	Disable FTP in network TCP services	Information sent using FTP is unencrypted and sent in plain text; therefore, it is possible for people to discover usernames and passwords easily. To disable FTP, go to Network > Services and deselect the FTP check box.

Unsecured HTTP service is enabled	Disable HTTP in network TCP services	Information sent using HTTP (Web) is unsecured and not encrypted. To disable HTTP, go to Network > Services and deselect Web . We recommend that you enable Secure web .
Unsecured SNMP service is enabled	Disable SNMP in network UDP services	Information sent using SNMP is unencrypted and sent in plain text; therefore, it is possible for people to discover usernames and passwords easily. To disable SNMP, go to Network > Services and deselect SNMP .
Auto-refresh of web pages is enabled	Change auto-refresh interval to "No auto-refresh"	If your Cisco TelePresence Supervisor MSE 8050 is set to auto-refresh it could mean that on an idle Cisco TelePresence Supervisor MSE 8050 a session will never time out. To turn off auto-refresh, go to Settings > User interface and change Status page auto-refresh interval to <i>No auto-refresh</i> .
Audit logging of configuration changes is disabled	Enable the audit log	If the audit log is disabled, the Cisco TelePresence Supervisor MSE 8050 will not create an audit log. To enable audit logs, go to Logs > Audit log and select Enable auditing . For more information on the audit log, refer to Working with the audit log [p.108] .
Audit logs hash check failed, audit system integrity compromised	Check system configuration for possible security changes	If audit logs checks fail, it is possible that your Cisco TelePresence Supervisor MSE 8050 has been compromised. For example, someone may have taken the compact flash card out and deleted some audit logs. For more information on the audit log, refer to Working with the audit log [p.108]
Compact flash card not present, audit logs will not be saved	Insert a compact flash card or check whether the existing compact flash card is functional	If no compact flash card is installed in the Cisco TelePresence Supervisor MSE 8050, logs are only stored up to a maximum of 200 events. The 200 events do not 'wrap', and therefore when the maximum is reached the log is deleted and started over again. The Cisco TelePresence Supervisor MSE 8050 will give you this warning when you are nearing the 200 maximum. To rectify this problem, insert a compact flash card.
Call encryption is disabled	Enable call encryption	When encryption status is <i>Disabled</i> , no calls on the Cisco TelePresence Supervisor MSE 8050 will be able to use encryption. To enable encryption, go to Settings > Encryption . For Encryption status , select <i>Enabled</i> .
Audit log above 75% capacity	Download and delete audit logs	The audit log has a maximum capacity of 100,000 audit events, or the size limit of the compact flash card. When you are nearing either of these limits, the Cisco TelePresence Supervisor MSE 8050 will give you this warning. If you reach full capacity of the compact flash card, the Cisco TelePresence Supervisor MSE 8050 will 'wrap' meaning that older logs will be deleted. To rectify this problem download and clear the audit log. To do this, go to Logs > Audit log and select Download as XML . Once this has completed, click Delete all records .

Audit log above 90% capacity	Download and delete audit logs.	<p>The audit log has a maximum capacity of 100,000 audit events, or the size limit of the compact flash card. When you are nearing either of these limits, the Cisco TelePresence Supervisor MSE 8050 will give you this warning. If you reach full capacity of the compact flash card, the Cisco TelePresence Supervisor MSE 8050 will 'wrap' meaning that older logs will be deleted. To rectify this problem download and clear the audit log.</p> <p>To do this, go to Logs > Audit log and select Download as XML. Once this has completed, click Delete all records.</p>
Shell not secured for startup	Disable the serial input during startup.	<p>If Disable serial input during startup isn't selected, the serial console is not protected during application startup. This means users will have access to debug services in the operating system.</p> <p>To disable this, go to Settings > Security, and select Disable serial input during startup.</p>

Related topics

- [Configuring security settings \[p.32\]](#)
- [Working with the audit log \[p.108\]](#)
- [Displaying security status \[p.52\]](#)

Logging using syslog

You can send the [Working with the event logs \[p.106\]](#) to one or more syslog servers on the network for storage or analysis.

To configure the syslog facility, go to **Logs > Syslog**.

On this page:

- [Syslog settings](#)
- [Using syslog](#)

Syslog settings

Refer to this table for assistance when configuring Syslog settings:

Field	Field description	Usage tips
Host address 1 to 4	Enter the IP addresses of up to four Syslog receiver hosts.	The number of packets sent to each configured host will be displayed next to its IP address.

Facility value	<p>A configurable value for the purposes of identifying events from the Cisco TelePresence Supervisor MSE 8050 on the Syslog host.</p> <p>Choose from the following options:</p> <ul style="list-style-type: none"> ■ <i>0 - kernel messages</i> ■ <i>1 - user-level messages</i> ■ <i>2 - mail system</i> ■ <i>3 - system daemons</i> ■ <i>4 - security/authorization messages (see Note 1)</i> ■ <i>5 - messages generated internally by syslogd</i> ■ <i>6 - line printer subsystem</i> ■ <i>7 - network news subsystem</i> ■ <i>8 - UUCP subsystem</i> ■ <i>9 - clock daemon (see Note 2)</i> ■ <i>10 - security/authorization messages (see Note 1)</i> ■ <i>11 - FTP daemon</i> ■ <i>12 - NTP subsystem</i> ■ <i>13 - log audit (see Note 1)</i> ■ <i>14 - log alert (see Note 1)</i> ■ <i>15 - clock daemon (see Note 2)</i> ■ <i>16 - local use 0 (local0)</i> ■ <i>17 - local use 1 (local1)</i> ■ <i>18 - local use 2 (local2)</i> ■ <i>19 - local use 3 (local3)</i> ■ <i>20 - local use 4 (local4)</i> ■ <i>21 - local use 5 (local5)</i> ■ <i>22 - local use 6 (local6)</i> ■ <i>23 - local use 7 (local7)</i> 	<p>Choose a value that you will remember as being the Cisco TelePresence Supervisor MSE 8050.</p> <hr/> <p>Note: Various operating system daemons and processes have been found to utilize Facilities 4, 10, 13 and 14 for security/authorization, audit, and alert messages which seem to be similar.</p> <p>Various operating systems have been found to utilize both Facilities 9 and 15 for clock (cron/at) messages.</p> <hr/> <p>Processes and daemons that have not been explicitly assigned a Facility value may use any of the "local use" facilities (16 to 21) or they may use the "user-level" facility (1) - and these are the values that we recommend you select.</p>
----------------	---	---

Using syslog

The events that are forwarded to the syslog receiver hosts are controlled by the event log capture filter.

To define a syslog server, simply enter its IP address and then click **Update syslog settings**. The number of packets sent to each configured host is displayed next to its IP address.

Note: Each event will have a severity indicator as follows:

- 0 - Emergency: system is unusable (unused by the Cisco TelePresence Supervisor MSE 8050)
 - 1 - Alert: action must be taken immediately (unused by the Cisco TelePresence Supervisor MSE 8050)
 - 2 - Critical: critical conditions (unused by the Cisco TelePresence Supervisor MSE 8050)
 - 3 - Error: error conditions (used by Cisco TelePresence Supervisor MSE 8050 *errorevents*)
 - 4 - Warning: warning conditions (used by Cisco TelePresence Supervisor MSE 8050 *warningevents*)
 - 5 - Notice: normal but significant condition (used by Cisco TelePresence Supervisor MSE 8050 *infoevents*)
 - 6 - Informational: informational messages (used by Cisco TelePresence Supervisor MSE 8050 *traceevents*)
 - 7 - Debug: debug-level messages (used by Cisco TelePresence Supervisor MSE 8050 *detailed traceevents*)
-

Management event receivers

If the Cisco TelePresence Supervisor MSE 8050 is being managed by a remote management system, for instance TANDBERG TMS, information on that remote system may be shown on this page. In certain circumstances you may need to remove the link between the external system and the Cisco TelePresence Supervisor MSE 8050. To do so, click **Clear**.

Related topics

- [Working with the event logs \[p.106\]](#)

Feedback receivers

The Supervisor publishes feedback events so that any receivers listening to the Supervisor can take action when something changes. To see the list of feedback receivers, click [Logs > Feedback receivers](#).

Each receiver in the list has the following details:

Field	Field description	Usage tips
Index	The position of the receiver in the list of receivers.	
Receiver URI	The fully qualified URI of the receiver.	The receiver may be a software application, for example TMS, that can respond to the feedback events with an appropriate API call to retrieve the list of changes from the feedback source.
Source identifier	A string that the source will provide to the receiver when it is queried or when it publishes feedback events.	The string is optional and defaults to port A's MAC address on the source.
Notification events subscribed to	The list of source feedback events that the receiver is subscribing to.	The receiver can subscribe to some or all of the feedback events published by the source. By default, the receiver subscribes to all of the source's feedback events.

The Supervisor publishes the following feedback events under the conditions listed:

Field	Field description	Usage tips
restart	The source publishes this event when it starts up.	
configureAck	The source publishes this event to acknowledge that an application has successfully configured a feedback receiver.	
alarmChanged	The Supervisor publishes this event when an alarm status changes.	

Related topics

- [Displaying the alarm status \[p.100\]](#)

Individual blade backup configuration

You can copy the configuration from a blade to the external compact flash disk on the Cisco TelePresence Supervisor MSE 8050 blade either automatically or manually. If the external compact flash card is not fitted, neither backup can occur and an alarm is raised.

For this reason, the Automatic backup section tells you when there is no compact flash card inserted and whether the blade is writing to or reading from it currently. Automatic backup occurs every 5 minutes when it is enabled. Use the **Enable** and **Disable** buttons to control automatic backups. You can also restore from the most recent automatic backup: click **Restore from automatic backup**.

In addition you can start a manual backup (known as a master backup) at any time, for example when you have just made significant configuration changes. There is only one master backup - it is overwritten each time you click **Create master backup**. (Master backups are independent of the automatic backup function.) You can also restore from this master backup rather than from the automatic backup.

Although the Backup page displays for the blade you selected from the summary page, you can swap between blades for backing up and restoring without returning to the summary page. Click the numbered links on the top right of the page to switch between slots in the chassis.

Backing up a configuration

To back up a configuration from a blade:

1. Go to **Hardware > Blades**.
2. Select the blade for which you want to back up the configuration.
3. Open the **Backup** tab.
4. To start automatic regular backups of this blade's configuration click **Enable**.
5. To create a master backup, click **Create master backup**.
6. To configure backups for a different blade, click on the numbered link representing the slot that the blade is in and return to step 4.

Restoring a configuration

To retrieve a configuration from the external compact flash disk to a blade, follow these steps:

1. Go to **Hardware > Blades**.
2. Select the blade for which you want to restore the configuration.
3. Click the **Backup** tab.
4. Click either **Restore from automatic backup** or **Restore from master backup**, as appropriate.

Related topics

- [Displaying an individual blade's status \[p.64\]](#)
- [Individual blade ports configuration \[p.70\]](#)
- [Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 \[p.35\]](#)
- [Shutting down and restarting the Cisco TelePresence Supervisor MSE 8050 \[p.39\]](#)

Customizing the user interface

The Cisco TelePresence Supervisor MSE 8050 provides you with options for customizing the text of the welcome messages and for controlling the auto-refreshing of user interface pages.

Controlling the auto-refreshing of status pages on the Cisco TelePresence Supervisor MSE 8050

Some pages on the Cisco TelePresence Supervisor MSE 8050 auto-refresh to ensure that the information displayed is current. Auto-refreshing pages keep web sessions alive indefinitely meaning that an administrator login will never timeout. This may be considered to be a security weakness, and if necessary you can disable all auto-refreshing.

To control the auto-refreshing of status pages on the Cisco TelePresence Supervisor MSE 8050:

1. Go to **Settings > User interface**.
2. Choose the time interval for page auto-refreshes or, to stop pages from auto-refreshing, choose **No auto-refresh**.

The status pages affected by this control are as follows:

- **Status > General**
- **Status > Health**
- **Hardware > Blades**
- **Hardware > Fan trays**

3. Click **Apply changes**.

Configuring welcome messages for the Login and Home pages

You can configure a message banner to appear on the Login page of the Cisco TelePresence Supervisor MSE 8050. For example, some organizations might require some legal text on the login page of the Cisco TelePresence Supervisor MSE 8050. You can also configure a message banner to appear on the Home page. You can configure a separate title (maximum: 100 characters) and text (maximum: 1500 characters) for each banner. To configure the message banners:

1. Go to **Settings > User interface**.
2. In the **Welcome messages** section, enter the text you require for the titles and the text of the messages.

Adding headers and footers

You can optionally configure header and footer text, with up to 100 characters each. The headers and footers will display on each page of the web user interface (except the help):

1. Go to **Settings > User interface**.
2. In the **Header and footer messages** section, enter the required text for the header and/or footer.
3. Click **Apply changes**.

Changes to headers or footers are recorded in the **Event log** and the **Audit log**.

Related topics

- [Upgrading and backing up the Cisco TelePresence Supervisor MSE 8050 \[p.35\]](#)

Network connectivity testing

The Network connectivity page can be used for troubleshooting issues that arise because of problems in the network between the Cisco TelePresence Supervisor MSE 8050 and a remote video conferencing device being called (or a device from which a user is attempting to call the Cisco TelePresence Supervisor MSE 8050).

The Network connectivity page enables you to attempt to 'ping' another device from the Cisco TelePresence Supervisor MSE 8050's web interface and perform a 'traceroute' of the network path to that device. The results show whether or not you have network connectivity between the Cisco TelePresence Supervisor MSE 8050 and another device. You can see from which port the Cisco TelePresence Supervisor MSE 8050 will route to that address. For a hostname, the IP address to which it has been resolved will be displayed.

To test connectivity with a remote device, go to **Network > Connectivity**. In the text box, enter the IP address or hostname of the device to which you want to test connectivity and click **Test connectivity**. Note that IPv6 addresses must be enclosed in square brackets.

For each successful 'ping', the time taken for the ICMP echo packet to reach the host and for the reply packet to return to the Cisco TelePresence Supervisor MSE 8050 is displayed in milliseconds (the round trip time). The TTL (Time To Live) value on the echo reply is also displayed.

For each intermediate host (typically routers) on the route between the Cisco TelePresence Supervisor MSE 8050 and the remote device, the host's IP address and the time taken to receive a response from that host is shown. Not all devices will respond to the messages sent by the Cisco TelePresence Supervisor MSE 8050 to analyse the route; routing entries for non-responding devices is shown as <unknown>. Some devices are known to send invalid ICMP response packets (e.g. with invalid ICMP checksums); these responses are not recognized by the Cisco TelePresence Supervisor MSE 8050 and therefore these hosts' entries are also shown as <unknown>.

Note: The ping message is sent from the Cisco TelePresence Supervisor MSE 8050 to the IP address of the endpoint that you enter. Therefore, if the Cisco TelePresence Supervisor MSE 8050 has an IP route to the given IP address, the ping will be successful. This feature allows the Cisco TelePresence Supervisor MSE 8050's IP routing configuration to be tested, and it has no security implications.

If you are unable to ping the device then check your network configuration especially any firewalls using NAT.

Related topics

- [Configuring network settings \[p. 14\]](#)

Configuring SSL certificates

The Cisco TelePresence Supervisor MSE 8050 supports certificate-based user authentication over HTTPS, and is capable of mutual TLS authentication with the client. The client presents a certificate, signed by a certificate authority (CA), which the Cisco TelePresence Supervisor MSE 8050 trusts if it recognizes the CA from its trust store. Similarly, the client requests the Cisco TelePresence Supervisor MSE 8050's local certificate and checks the signing CA against its own trust store.

To manage the Cisco TelePresence Supervisor MSE 8050's local certificate and its trust store for HTTPS TLS, and optionally to configure OCSP checks (Online Certificate Status Protocol) for HTTPS connections, go to [Network > SSL certificates](#).

The SSL certificates page is also used to allow or enforce certificate-based login in place of standard, password-based login. Any attempts to authenticate with a revoked certificate are recorded in the Cisco TelePresence Supervisor MSE 8050's [Audit log](#).

In this topic:

- [Prerequisites](#)
- [Managing trust stores](#)
- [Configuring HTTPS verification](#)
- [Configuring client certificate security](#)
- [Configuring server certificate security](#)
- [OCSP checks for client certificate revocation](#)
- [Certificate details reference](#)

Prerequisites

You should have your own local certificate and trust store, which must be in .pem format (Base64 encoded text).

HTTPS access to the web user interface requires the following prerequisites:

- The *Secure management (HTTPS) or Encryption* feature key must be installed on the Cisco TelePresence Supervisor MSE 8050.
- HTTPS must be enabled on the [Network > Services](#) page.

CAUTION: A local certificate and private key are pre-installed on the Cisco TelePresence Supervisor MSE 8050 and are used by default for HTTPS access. As all Cisco TelePresence Supervisor MSE 8050s have identical default certificates and keys, to ensure security we recommend that you replace it with your organization's own certificate and private key (see below).

Managing the local certificate

Uploading a local certificate and private key

1. Go to [Network > SSL certificates](#).
2. Go to the [Local certificate configuration](#) section.
3. Click **Browse** for the Certificate field to navigate to the certificate .pem file.

4. Click **Browse** for the Private key field to navigate to the private key file that accompanies your certificate. You must upload the certificate and its key simultaneously.
5. In the **Private key encryption password** field, type the relevant password.
6. Click **Upload certificate and key**.
The uploaded certificate overwrites the previously held certificate.
7. Restart the Cisco TelePresence Supervisor MSE 8050.

Deleting a local certificate and private key

1. Go to the **Local certificate** section.
2. Click **Delete custom certificate and key**.

Managing trust stores

A trust store is a collection of certificates from intermediate and root certificate authorities against which the Cisco TelePresence Supervisor MSE 8050 can attempt to verify client certificates it receives. The Cisco TelePresence Supervisor MSE 8050 can hold a trust store file for HTTPS TLS; when you upload a new one, the previously held file is overwritten.

Putting multiple CA certificates in a trust store

1. Open the first certificate in a text editor, and save it as *yourfilename.pem*.
2. Open the next certificate in your text editor, and copy all the lines from `-----Begin Certificate-----` to `-----End Certificate-----` (inclusive).
3. Paste the text block at the end of *yourfilename.pem*.
Repeat this to copy as many certificate blocks into your .pem file as you need to, making sure not to modify any of the pasted text.
4. Save the resulting file.

Uploading a trust store

1. Go to **Network > SSL certificates**.
2. Go to the **HTTPS trust store** section.
3. Click **Browse** to navigate to your trust store .pem file (eg. *yourfilename.pem*).
4. Click **Upload trust store**.
5. Confirm that you wish to proceed.
The trust store is uploaded, replacing the previous one (if it existed).
Each certificate in the trust store appears in its own table row that shows pertinent certificate details in plain text.

Deleting a trust store

1. Go to **Network > SSL certificates**.
2. Go to the **HTTPS trust store** section.
3. Click **Delete trust store**.

4. Confirm that you wish to proceed.
The trust store is deleted.

Configuring HTTPS verification

The **HTTPS trust store** section is where you can configure certificate-based authentication for users logging in to the web interface and for applications interacting with the API. This section also lets you configure whether the Cisco TelePresence Supervisor MSE 8050 should verify server certificates, presented by an OCSP server or by feedback receivers, before allowing these connections.

CAUTION: If you transition from solely password-based client authentication to *any* level of certificate-based client authentication (including those that permit but do not require certificates), it is possible inadvertently to block client access to the Cisco TelePresence Supervisor MSE 8050. This can happen if HTTP is disabled or if HTTP to HTTPS redirection is enabled. In such cases, a certificate that is trusted by the Cisco TelePresence Supervisor MSE 8050 must be presented by the client side (typically you the administrator) in order to log in. If no such client certificate exists then no one can log in.

We strongly recommend that you first review the option descriptions below and then follow the process in [Transitioning to certificate-based security \[p.127\]](#).

Configuring client certificate security

1. Go to **Network > SSL certificates**.
2. Go to the **HTTPS trust store** section.
3. Select one of the options from the Client certificate security field.
4. Click **Apply changes**.

Client certificate security options	
Not required	Certificate-based client authentication is not required (default) and client certificates are ignored. Password-based authentication is required for all client access, whether by users over HTTPS or applications making API calls.
Verify certificate	Incoming HTTPS connections are only permitted if the client certificate is signed by an authority that the Cisco TelePresence Supervisor MSE 8050 trusts, but password-based login is <i>still required</i> to authenticate the client, for HTTPS, API, and other client connections.
Certificate-based authentication allowed	Incoming HTTPS connections are only permitted if the client certificate is signed by an authority that the Cisco TelePresence Supervisor MSE 8050 trusts and, if the certificate identity matches a stored username, the client logs in as that user. However, if the certificate is trusted and the identity does not match, the client may log in with username and password.

Certificate-based authentication required Incoming HTTPS connections are only permitted if the client certificate is signed by an authority that the Cisco TelePresence Supervisor MSE 8050 trusts. The identity of the certificate must also match a stored username and password-based client authentication is not allowed. HTTP and FTP logins are blocked. If Require administrator login is checked (on [Settings > Security](#)), then console access is restricted to functions that do not require a login.

Note: The Cisco TelePresence Supervisor MSE 8050 requires every user account to have a password, even if *Certificate-based authentication required* is selected and thus clients may not use their passwords. Furthermore, if the Cisco TelePresence Supervisor MSE 8050 is in advanced account security mode, passwords must be replaced every 60 days. Users are not prompted to change their passwords when they log in using certificate-based authentication, so the passwords will expire and generate security warnings.

For the purpose of any timed access restrictions that exist on user accounts (typically password change intervals and inactive account expiry rules) any log in using a certificate is treated as a standard password-based login and will reset the timer accordingly.

For information about how these options affect the API interface, see the *Cisco TelePresence Cisco TelePresence Supervisor MSE 8050 API Reference Guide*.

Configuring server certificate security

1. Go to [Network > SSL certificates](#).
2. Go to the [HTTPS trust store](#) section.
3. Select one of the options from the Server certificate security field.
4. Click **Apply changes**.

Server certificate security options

No verification	The Cisco TelePresence Supervisor MSE 8050 does not verify the server's certificate (if one is presented) when it makes an OCSP request or when it sends HTTPS feedback messages.
Verify certificate	The Cisco TelePresence Supervisor MSE 8050 requires a server certificate from the OCSP server or feedback receiver, and must be able to verify that the certificate is trusted by one of the authorities in its HTTPS trust store, before it sends the OCSP request or feedback message.

OCSP checks for client certificate revocation

You can optionally configure an external OCSP server, which the Cisco TelePresence Supervisor MSE 8050 will use to check the revocation status of client certificates presented with incoming HTTPS connection requests. The following details describe the Cisco TelePresence Supervisor MSE 8050's OCSP checking mechanism.

- For chained certificates the OCSP check is performed only against the leaf certificate.
- The Cisco TelePresence Supervisor MSE 8050 supports SHA-1 hashing for OCSP.
- If the response from the OCSP server is anything other than 'good' (that is, invalid, revoked, unknown, or any other error condition) the Cisco TelePresence Supervisor MSE 8050 rejects the associated connection request.
- No further OCSP checking takes place after the connection is established. An active session will continue if a certificate is revoked during that session, but any subsequent connection attempts with the revoked certificate will be rejected.

CAUTION: If you enable OCSP checking for the Cisco TelePresence Supervisor MSE 8050 it is possible inadvertently to block *all* login access (including administrators) to the Cisco TelePresence Supervisor MSE 8050. If you want to enable OCSP checking, we strongly recommend that you first review the option descriptions below and then follow the process in [Transitioning to certificate-based security \[p. 127\]](#).

Configuring the OCSP connection

1. Go to **Network > SSL certificates**.
2. Go to the **Online certificate status protocol (OCSP)** section.
3. Select *HTTPS certificates* in the Certificates to check field.
When you click **Apply changes**, the OCSP check for HTTPS certificates will be enabled; if you select *None* you will disable the check.
4. Enter the server address in the OCSP server field.
5. Check the Require nonce checkbox if this feature is supported by the OCSP server.
6. Enter the Maximum clock skew of OCSP server, in seconds.
7. Enter the Maximum age of OCSP server records, in days.
8. Click **Apply changes**.

OCSP details reference

Online certificate status protocol (OCSP) field descriptions

Certificates to check	<i>None</i> to disable OCSP checks or <i>HTTPS client certificates</i> to enable OCSP checks of HTTPS client certificates' revocation status.
OCSP server	The URL of the external OCSP server. <ul style="list-style-type: none"> ■ If the default port allocation is sufficient (port 80 for HTTP and port 443 for HTTPS) use one of these formats, as appropriate: <i>http://example.com</i>; <i>https://example.com</i>; <i>http://example.com/examplepath</i>; <i>https://example.com/examplepath</i> ■ To send to a non-standard port number (port 88 is used in the examples here) use one of these formats, as appropriate: <i>http://example.com:88</i>; <i>https://example.com:88</i>; <i>http://example.com:88/examplepath</i>; <i>https://example.com:88/examplepath</i>
Require nonce	Determines whether OCSP queries must include a nonce extension (to prevent replay attacks). <ul style="list-style-type: none"> ■ If enabled, the Cisco TelePresence Supervisor MSE 8050 includes a nonce in each OCSP request, and requires the nonce to be returned in the corresponding response. If the nonce is not returned, the associated connection request is rejected. ■ If disabled, the Cisco TelePresence Supervisor MSE 8050 does not send a nonce in OCSP requests.
Maximum clock skew of OCSP server	Specifies the maximum acceptable time (in seconds) for clock skew in OCSP responses. In this context the skew is the divergence between the respective system clocks on the Cisco TelePresence Supervisor MSE 8050 and on the OCSP server. If the skew exceeds this setting, then the OCSP responses may be treated as invalid.

Maximum age of OCSP server records	<p>Specifies the maximum acceptable age (in days) for certificates. The certificate age is derived from the response field <i>'thisUpdate'</i> which indicates when the returned status was last known to be correct. How this value is determined depends on the OCSP server configuration (often it is the last time the server was updated with a new Certificate Revocation List).</p> <p>The Cisco TelePresence Supervisor MSE 8050 rejects any response where the value of <i>'thisUpdate'</i> is later in the past than the time derived by counting back from current time by the number of days specified here (after accounting for clock skew).</p>
------------------------------------	--

Certificate details reference

Field	Description
Subject	<p>The business to which the certificate has been issued:</p> <ul style="list-style-type: none"> ■ C Country where the business is registered ■ ST State or province where the business is located ■ L Locality or city where the business is located ■ O Legal name of the business ■ OU Organizational unit or department ■ CN Certificate common name, or the domain name
Issuer	The issuer of the certificate. Where the certificate has been self-issued, these details are the same as for Subject.
Issued	Date on which the certificate was issued.
Expires	Date on which the certificate will expire.
Private key	<p>Your web browser uses the SSL certificate public key to encrypt the data that it sends back to the Cisco TelePresence Supervisor MSE 8050. The private key is used by the Cisco TelePresence Supervisor MSE 8050 to decrypt that data.</p> <p>The private key field is only present for the local certificate.</p>

Related topics

- [Configuring security settings \[p.32\]](#)
- [Configuring IP services \[p.24\]](#)
- [Transitioning to certificate-based security \[p.127\]](#)

Transitioning to certificate-based security

Certificate-based security methods carry a risk of inadvertently blocking all login access to the Cisco TelePresence Supervisor MSE 8050. (If problems occur with the client certificate or the trust store, you will need to fall back to HTTP. If you cannot fall back — because HTTP is disabled or because HTTP to HTTPS redirection is set — then all access methods will be blocked.) We strongly recommend that you follow the procedure below when implementing certificate-based security:

- [Enabling client certificates and certificate login \(HTTPS connections\)](#)
- [Enabling OCSP checking](#)
- [Requiring certificate-based login \(all connections\)](#)

Enabling client certificates and certificate login (HTTPS connections)

To transition access handling for HTTPS connections from standard, password-based access to client certificate validation and optionally to allow certificate-based login, do the following:

1. Ensure that an appropriate HTTPS trust store is installed on the Cisco TelePresence Supervisor MSE 8050 (**Network > SSL certificates**) and that the web browser(s) to be used when accessing the Cisco TelePresence Supervisor MSE 8050 are configured with a valid client certificate.
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and disable **Redirect HTTP requests to HTTPS** (uncheck the check box). This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**.
 - a. Scroll to the **HTTPS trust store** section.
 - b. Set **Client certificate security** to *Verify certificate* (to have client certificate validation but no certificate login) or *Certificate-based authentication allowed* (to have client certificate validation and to allow certificate-based login).
 - c. Click **Apply changes**.
5. Now test that you are able to log in to the Cisco TelePresence Supervisor MSE 8050 over an HTTPS connection.
 - a. First verify that you can log in using the standard password login mechanism.
 - b. If you specified *Verify certificate* in the previous step, verify that you can log in using the standard password login mechanism.

Note: Provided that this procedure is successful, you can now disable HTTP (**Network > Services**) or enable redirection from HTTP to HTTPS (**Settings > Security**) if either are required by your configuration.

Enabling OCSP checking

CAUTION: The Cisco TelePresence Supervisor MSE 8050 will only perform OCSP checking if client certificate security mode is enabled. To do this go to **Network > SSL certificates** and set the **Client certificate security** option. When you first enable OCSP checking, set **Client certificate security** to one of the 'lesser' modes (*Verify certificate* or *Certificate-based authentication allowed*). If you want to set it to *Certificate-based authentication required*, only do so after you have completed the procedure for [Requiring certificate-only login \(all connections\)](#) and you are certain that OCSP checking is working correctly.

To enable OCSP checking for the Cisco TelePresence Supervisor MSE 8050, do the following:

1. Ensure that an appropriate HTTPS trust store has been installed on the Cisco TelePresence Supervisor MSE 8050 (**Network > SSL certificates**).
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and *disable Redirect HTTP requests to HTTPS*. This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**.
 - a. Scroll to the **Online certificate status protocol (OCSP)** section.
 - b. Set **Certificate to check** to *HTTPS client certificates*.
 - c. Enter the URL of the external OCSP server and set any options you require.
 - d. Click **Apply changes**.
5. Now test that you are able to log in to the Cisco TelePresence Supervisor MSE 8050 over an HTTPS connection. Only proceed to the next step if you can successfully log in.
6. Do one of the following, as appropriate for your configuration:
 - Go to **Network > Services** and disable HTTP.
 - Go to **Settings > Security** and enable **Redirect HTTP requests to HTTPS**.

Requiring certificate-based login (all connections)

To transition from password-based authentication to required certificate-based authentication for *all* connection types, do the following:

1. Ensure that an appropriate HTTPS trust store is installed on the Cisco TelePresence Supervisor MSE 8050 (**Network > SSL certificates**) and that the web browser(s) to be used to access the Cisco TelePresence Supervisor MSE 8050 are configured with a valid client certificate.
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and *disable Redirect HTTP requests to HTTPS* (uncheck the check box). This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**:
 - a. Scroll to the **HTTPS trust store** section.
 - b. Set **Client certificate security** to *Certificate-based authentication allowed*.
Do NOT set **Client certificate security** to *Certificate-based authentication required yet*.
 - c. Click **Apply changes**.
5. Now test that you are able to log in to the Cisco TelePresence Supervisor MSE 8050 over an HTTPS connection *using a certificate*. Only proceed to the next step if you can successfully log in with a certificate.
6. Assuming the previous step succeeded, go to the **Client certificate security** option again and this time set it to *Certificate-based authentication required*.
7. Click **Apply changes** and confirm at the prompt.
8. Do one of the following, as appropriate for your configuration:
 - Go to **Network > Services** and disable HTTP.
 - Go to **Settings > Security** and enable **Redirect HTTP requests to HTTPS**.

Related topics

- [Configuring SSL certificates \[p. 121\]](#)
- [Configuring security settings \[p.32\]](#)
- [Configuring IP services \[p.24\]](#)

Further information

Refer to the online help for details of software licenses that relate to this product.

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2014 Cisco Systems, Inc. All rights reserved.