Status and System Information

Status Overview

The Overview page (**Status** > **Overview**) provides an overview of the current status of the Expressway (or Expressway cluster, if applicable). This page is displayed by default after logging in to the Expressway as an administrator.

The following information is displayed:

Field	Description
System Information: many of the items in this section are configurable. Click on an item name to go to its configuration page.	

Field	Description
System name	Name assigned to the Expressway
Up time	Time elapsed since the system last restarted
Software version	Software version currently installed on the Expressway
IPv4 address	Expressway's IPv4 addresses
IPv6 address	Expressway's IPv6 addresses
Options	Maximum limits for calls and registrations are controlled by option keys. Depending on the software version, a few additional features may also be controlled by option keys, although we are phasing out this approach

Resource usage

This section provides statistics about current and cumulative license usage for calls and registrations.

Shows current and peak usage broken down by:

- Rich media sessions
- Registrations (including Unified CM remote sessions)

  Registrations shows the total count of devices registered with Expressway, which includes TelePresence Room, Desktop System, and Conference System.

Also displays resource and license usage information:

- Monitored resource usage, expressed as a percentage of the system capacity.
- Current and peak license usage, expressed as a percentage of the available licenses for each license type. Each rich media session license allows either 1 video call or 2 audio-only SIP traversal calls. Hence, a 100 rich media session license would allow, for example, 90 video and 20 SIP audio-only simultaneous calls. Any other audio-only call (non-traversal, H.323 or interworked) will consume a rich media session license.

To view details of current calls or registrations, click the relevant item in the section.

Note All statistics are based on data since the system was last restarted; values are set to zero after a restart. The information auto-refreshes every 5 seconds.

You can go to the **Resource usage** page to see more details, including total usage statistics.

MRA deployments

If you deploy the Cisco Unified Communications Mobile and Remote Access feature with Expressway, from Expressway X12.6.1 the Expressway-E also displays usage information about SIP devices that are currently registered over MRA. (The MRA service must be enabled for the Expressway in question.) The information shows the count of current active MRA devices, and the peak count for MRA registrations since the last Expressway restart.

Clustered systems

If the Expressway is part of a cluster, then details for each peer are shown as well as totals for the entire cluster.

System Information

The **System information** page (**Status** > **System** > **Information**) provides details of the software, hardware, and time settings of the Expressway.

Many of the items in the **System information** and **Time information** sections are configurable; click on the item name to be taken to its configuration page.

The following information is displayed:

Field	Description
System information section	
System name	The name that has been assigned to the Expressway
Product	This identifies the Expressway
Software version	The version of software that is currently installed on the Expressway
Software build	The build number of this software version
Software release date	The date on which this version of the software was released
Software name	The internal reference number for this software release
Software options	The maximum number of calls, and the availability of some additional Expressway features are controlled through option keys. This section shows any optional features currently installed.
Hardware version	The version number of the hardware on which the Expressway software is installed
Serial number	The serial number of the hardware or virtual machine on which the Expressway software is installed
VM size	(Virtual machine-based systems only) Size of the VM hardware platform - small, medium or large
Time information section	
Up time	The time that has elapsed since the system last restarted

Field	Description
System time (UTC)	The time as determined by the NTP server.If no NTP server is configured, this shows *Time Not Set*.
Time zone	The time zone that has been configured on the **Time** page
Local time	If an NTP server is configured, the system time is shown in local time (UTC adjusted according to the local time zone). If no NTP server is configured, the time according to the Expressway's operating system is shown.
Active sessions section:	
Administrator sessions	The number of current active administrator sessions. Click on the link to see the list of active sessions
User sessions	The number of current user sessions. Click on the link to see the list of active sections.

Ethernet Status

The **Ethernet** page (**Status** > **System** > **Ethernet**) shows the MAC address and Ethernet speed of the Expressway.

The page displays the following information for the LAN 1 port and, if the Advanced Networking option key has been installed, the LAN 2 port:

Field	Description
MAC address	The MAC address of the Expressway's Ethernet device for that LAN port.
Speed	The speed of the connection between the LAN port on the Expressway and the Ethernet switch.

The Ethernet speed can be configured via the Ethernet page.

IP Status

The **IP status** page (**Status** > **System** > **IP**) shows the current IP settings of the Expressway.

The following information is displayed:

Field	Description
IP section	

Field	Description
Protocol	Indicates the IP protocol supported by the Expressway: • *IPv4 only:* it only accepts registrations from endpoints using an IPv4 address, and only takes calls between two endpoints communicating via IPv4. It communicates with other systems via IPv4 only. • *IPv6 only:* it only accepts registrations from endpoints using an IPv6 address, and only takes calls between two endpoints communicating via IPv6. It communicates with other systems via IPv6 only. • *Both:* it accepts registrations from endpoints using either an IPv4 or IPv6 address, and takes calls using either protocol. If a call is between an IPv4-only and an IPv6-only endpoint, the Expressway acts as an IPv4 to IPv6 gateway. It communicates with other systems via either protocol.
IPv4 gateway	The IPv4 gateway used by Expressway
IPv6 gateway	The IPv6 gateway used by Expressway
Advanced Networking	Indicates whether the second LAN port has been enabled. This is done by installing the **Advanced Networking** option key.
LAN 1	Shows the IPv4 address and subnet mask, and IPv6 address of the LAN 1 port.
LAN 2	If the **Advanced Networking** option key has been installed, this shows the IPv4 address and subnet mask, and IPv6 address of the LAN 2 port.
DNS section:	
Server 1..5 address	The IP addresses of each of the DNS servers that are queried when resolving domain names. Up to 5 DNS servers may be configured.
Domain	Specifies the name to be appended to the host name before a query to the DNS server is executed.

The IP settings can be configured via the IP page.

Resource Usage

The **Resource usage** page (**Status** > **System** > **Resource usage**) provides statistics about the current and cumulative license usage for calls and registrations.

Shows current and peak usage broken down by:

- Rich media sessions
- Registrations (including Unified CM remote sessions)

  Registrations shows the total count of devices registered with Expressway, which includes TelePresence Room, Desktop System, and Conference System.
- **Webrtc Sessions**: Displays the Webrtc session count on the Web Interface of Expressway-E. The Webrtc sessions count are displayed only when Webrtc is enabled.

Also displays resource and license usage information:

- Monitored resource usage, expressed as a percentage of the system capacity.
- Current and peak license usage, expressed as a percentage of the available licenses for each license type. Each rich media session license allows either 1 video call or 2 audio-only SIP traversal calls. Hence, a 100 rich media session license would allow, for example, 90 video and 20 SIP audio-only simultaneous calls. Any other audio-only call (non-traversal, H.323 or interworked) will consume a rich media session license.

To view details of current calls or registrations, click the relevant item in the section.

Note All statistics are based on data since the system was last restarted; values are set to zero after a restart. The information auto-refreshes every 5 seconds.

Clustered Expressway Systems

If the Expressway is part of a cluster, details for each peer are shown as well as totals for the entire cluster. See About Clusters for more information.

Registration Status

Registration status information can be displayed for both current and historic registrations. If the Expressway is part of a cluster, all registrations that apply to any peer in the cluster are shown.

- The **Registrations by device** page (**Status** > **Registrations** > **By device**) lists each device currently registered with the Expressway, and allows you to remove a device's registration. If the Expressway is part of a cluster, all registrations across the cluster are shown.
- The **Registrations by alias** page (**Status** > **Registrations** > **By alias**) lists all the aliases, E.164 numbers and prefixes used by all endpoints and systems currently registered with the Expressway.

- The **Registration history** page (**Status** > **Registrations** > **History**) lists all the registrations that are no longer current. It contains all historical registrations since the Expressway was last restarted.

The following information is displayed:

Field	Description
Name	For SIP devices, this is its SIP AOR.
Number	For SIP devices this will always be blank because they cannot register E.164 numbers. (This is shown in the **Alias** column in the registration by alias view.)
Alias	The SIP AOR registered by a device. (Registration by alias view only.)
Type	Indicates the nature of the registration. This will most commonly be Endpoint, MCU, Gateway, or SIP UA.
Protocol	Indicates whether the registration is for a SIP device.
Creation time	The date and time at which the registration was accepted. If an NTP server has not been configured, this will say *Time not set*.
Address	For SIP UAs this is the Contact address presented in the REGISTER request.
Device type	Indicates the type of the registered device. The possible types are: *TelePresence Room*, *Desktop System*, or *Conference Systems*.
End time	The date and time at which the registration was terminated. (Registration history view only.)
Duration	The length of time that the registration was in place. (Registration history view only.)
Reason	The reason why the registration was terminated. (Registration history view only.)
Peer	Identifies the cluster peer to which the device is registered.
Action	Click **View** to go to **Registration details** page to see further detailed information about the registration.

Registration details

The information shown on the **Registration details** page depends on the device's protocol, and whether the registration is still current. For example, SIP registrations include the AOR, contact and, if applicable, public GRUU details. It also provides related tasks that let you **View active calls involving this registration** and **View previous calls involving this registration**; these options take you to the **Calls by registration** page, showing the relevant current or historic Call Status information filtered for that particular registration.

Unregistering and blocking devices

The registration status pages provide options to manually unregister and block devices.

- Click **Unregister** to unregister the device. Note that the device may automatically re-register after a period of time, depending on its configuration. To prevent this, you must also use a registration restriction policy such as an Allow List or Deny List.
- Click **Unregister and block** to unregister the device and add the alias to the Deny List page, thus preventing the device from automatically re-registering. (This option is only available if the **Restriction policy** is set to *Deny List*.)

Note If your Expressway is part of a cluster you have to be logged into the peer to which the device is registered, to unregister it.

Call Status

Call status information can be displayed for both current and completed calls:

- **Current calls:** The **Call status** page (**Status** > **Calls** > **Calls**) lists all calls currently taking place to or from devices registered with the Expressway, or passing through the Expressway.
- **Completed calls:** The **Call history** page (**Status** > **Calls** > **History**) lists all calls that are no longer active. The list is limited to the most recent 500 calls--or less if calls used multiple components (see below). It only includes calls that have taken place since the Expressway was last restarted.

The same set of call status information is also shown on the **Calls by registration** page (accessed via the **Registration details** page).

If the Expressway is part of a cluster, all calls that apply to any peer in the cluster are shown, although the list is limited to the most recent 500 calls per peer.

Call summary information

The following summary information is displayed initially:

Field	Description
Start time	The date and time when the call was placed.
End time	The date and time when the call ended (completed calls only).
Duration	The length of time of the call.
Source	The alias of the device that placed the call. (If the call passes through more than one Expressway and User Policy is enabled, the caller's FindMe ID may be displayed instead.)

Field	Description
Destination	The alias dialed from the device. This may be different from the alias to which the call was placed, which may have been transformed (due to pre-search transforms, zone transforms or User Policy).
Type	Indicates the type of call.
SIP variant	*Standards-based*, *Microsoft AV*, *Microsoft SIP IM&P*, or *Microsoft Share* to distinguish between the different implementations of SIP and SDP that can be routed by the Expressway. Does not display for H.323 calls.
Protocol	Shows whether the call used H.323, SIP, or both protocols. For calls passing through the B2BUA, this may show “Multiple components”; you can view the call component summary section to see the protocol of each individual call component.
Status	The reason the call ended (completed calls only).
Peer	Identifies the cluster peer through which the call is being made.
Actions	Click **View** to see further information about the call, including a list of all of the call components that comprise that call.

Call components summary information

After selecting a call from the primary list (as described above) you are shown further details of that call, including a list of all of the call components that comprise that call.

Each call component may be one of the following types:

- *Expressway*: a standard Expressway call
- *B2BUA*: a call component that is routed through the B2BUA to apply a media encryption policy or ICE messaging support
- *Microsoft Lync B2BUA*: a call component that is routed through the Microsoft Lync B2BUA

To view full details of a call component, click **Local call serial number** associated with it. This opens the **Call details** page for full information about that component, including all call legs and sessions. It also provides further links to the **Call media** page which lists the individual media channels (audio, video, data and so on) for the most relevant session for a traversal call.

If the Expressway is part of a cluster and the call passes through two cluster peers, you can click **View associated call on other cluster peer** to see the details of the other leg of the call.

Call history may reflect fewer than 500 calls

Some calls use multiple components, particularly calls invoked through the B2BUA. In these cases each individual call is actually counted as *three* calls due to the multiple components involved. This means that the number of entries actually listed in the call history may be significantly less than the theoretical 500 limit.

Identifying Mobile and Remote Access (MRA) calls

The call status and call history pages show all call types: Unified CM remote sessions (if MRA is enabled) as well as Expressway RMS sessions.

To distinguish between the call types, you need to drill down into the call components. MRA calls have different component characteristics depending on whether the call is being viewed on the Expressway-C or Expressway-E:

- On the Expressway-C, a Unified CM remote session has three components (as it uses the B2BUA to enforce media encryption). One of the Expressway components routes the call through one of the automatically generated neighbor zones (with a name prefixed by either **CEtcp** or **CEtls**) between Expressway and Unified CM.
- On the Expressway-E, there is one component and that routes the call through the **CollaborationEdgeZone**.

If both endpoints are outside of the enterprise (that is, off premises), you will see this treated as two separate calls.

Rich media sessions (RMA)

If your system has an RMA key installed and thus supports business-to-business calls, and interworked or gatewayed calls to third-party solutions and so on, those calls are also listed on the call status and call history pages.

Disconnecting Calls

Click **Disconnect** to disconnect the selected calls. Note that if your Expressway is part of a cluster you have to be logged into the peer through which the call is associated to be able to disconnect the call.

Call disconnection works differently for H.323 and SIP calls due to differences in the way the protocols work:

- H.323 calls, and interworked H.323 to SIP calls: the **Disconnect** command will actually disconnect the call.
- SIP to SIP calls: the **Disconnect** command will cause the Expressway to release all resources used for the call and the call will appear on the system as disconnected. However, SIP calls are peer-to-peer and as a SIP proxy the Expressway has no authority over the endpoints. Although releasing the resources may have the side-effect of disconnecting the SIP call, it is also possible that the call signaling, media or both may stay up (depending on the type of call being made). The call will not actually disconnect until the SIP endpoints involved have also cleared their resources.
- SIP calls via the B2BUA: as the B2BUA can control the state of a call, if you disconnect the leg of the call that is passing through the B2BUA (where the **Type** is *B2BUA*), the call will fully disconnect. Note that the call may take a few seconds to disappear from the **Call status** page — you may have to refresh the page on your browser.

B2BUA Calls

The **B2BUA calls** page provides overview information about a call routed through the B2BUA. To access this page, go to **Status** > **Calls** > **Calls** or **Status** > **Calls** > **History** and click **View** for a particular B2BUA call.

Calls are routed through the B2BUA in the following cases:

- A media encryption policy applies to the call (any encryption setting other than Auto).
- Expressway is load balancing calls for Cisco Meeting Server. The Expressway B2BUA processes the INVITE messages from the Meeting Server when load balancing is enabled. Note that support for Meeting Server load balancing **may be provided in Preview mode only**, as detailed in the release notes for your current Expressway version.
- ICE messaging is triggered.
- Microsoft interoperability service is enabled and the call routed through the **To Microsoft destination via B2BUA** neighbor zone.

For Microsoft interoperability calls, you can click the **Corresponding Expressway call** link to see details of the leg passing through the Expressway.

Known Limitation

The Send empty INVITE for interworked calls (configured on advanced custom zone profile) is not supported for call that involve B2BUA.

Viewing B2BUA Call Media Details

The **B2BUA call media** page is accessed from the B2BUA Calls page by clicking **View media statistics for this call**. It shows information about the audio and video media channels that made up the call passing through the B2BUA. For calls using the Microsoft interoperability service, this comprises legs between the Expressway, the Microsoft server and any external transcoder (if applicable).

Note B2BUA debug tool connects to media process over ports 13997, 13998 and 13999 on local loopback to get the media statistics. These ports are open for connection and are strictly for internal use only. This is accessible from root only.

Search History

The **Search history** page (**Status** > **Search history**) lists the most recent 255 searches that have taken place since the Expressway was last restarted.

About searches

Before a call can be placed, the endpoint being called must be located. The Expressway sends and receives a series of messages during its attempt to locate the endpoint being called; these messages are each known as searches. An individual call can have one or more searches associated with it, and these searches can be of different types.

The type of search message that is sent depends on whether the call is for SIP or H.323, and whether the call request was received locally or from an external zone, as follows:

- H.323 calls that are placed locally: two messages are sent - the first is an **ARQ** which locates the device being called, and the second is the call **Setup** which sends a request to the device asking it to accept the call. Each message shows up as a separate search in the **Search history** page, but only the **Setup** message is associated with a particular call.
- H.323 searches originating from external zones: an **LRQ** appears in the **Search history** page.
- SIP: a single message is sent to place a call: this is either a SIP **INVITE** or SIP **OPTIONS**.

Note An individual call can have one or more searches associated with it, and can be of different types. Each search has an individual Search ID; each call has an individual Call Tag (see Identifying Calls).

The Expressway supports up to 500 concurrent searches.

Search history list

The search history summary list shows the following information:

Field	Description
Start time	The date and time at which the search was initiated.
Search type	The type of message being sent.
Source	The alias of the endpoint that initiated the call.
Destination	The alias that was dialed from the endpoint. This may be different from the alias to which the call was actually placed, as the original alias may have been transformed either locally or before the neighbor was queried.
Status	Indicates whether or not the search was successful.
Actions	Allows you to click **View** to go to the Search Details page, which lists full details of this search.

Filtering the list

To limit the list of searches, enter one or more characters in the **Filter** field and click **Filter**. Only those searches that contain (in any of the displayed fields) the characters you entered are shown.

To return to the full list of searches, click **Reset**.

Search Details

The **Search details** page lists full information about either an individual search, or all searches associated with a single call (depending on how you reached the page). The information shown includes:

- the subzones and zones that were searched
- the call path and hops
- any transforms that were applied to the alias being searched for
- the SIP variant used by the call
- use of policies such as Admin Policy or User Policy (FindMe)
- any policy services that were used

Other information associated with the search and (if it was successful) the resulting call can be viewed via the links in the **Related tasks** section at the bottom of the page:

- **View all events associated with this call tag** takes you to the Event Log page, filtered to show only those events associated with the Call Tag relating to this search.
- **View call information associated with this call tag** takes you to the **Call details** page, where you can view overview information about the call.
- **View all searches associated with this call tag** is shown if you are viewing details of an individual search and there are other searches associated with the same call. It takes you to a new **Search details** page which lists full information about all the searches associated with the call's Call Tag.

Local Zone Status

The **Local Zone status** page (**Status** > **Local Zone**) lists the subzones (the Default Subzone and the Traversal Subzone) that make up the Expressway's Local Zone .

The following information is displayed:

Field	Description
Subzone name	The names of each subzone currently configured on this Expressway. Clicking on **Subzone name** takes you to the configuration page for that subzone.

Field	Description
Calls	The number of calls currently passing through the subzone. **Note** A single call may pass through more than one subzone, depending on the route it takes. For example, calls from a locally registered endpoint always pass through the Traversal Subzone, so they will show up twice; once in the originating subzone and once in the Traversal Subzone.
Bandwidth used	The total amount of bandwidth used by all calls passing through the subzone.

Zone Status

The **Zone status** page (**Status** > **Zones**) lists all of the external zones on the Expressway. It shows the number of calls and amount of bandwidth being used by each zone.

The list of zones always includes the Default Zone, plus any other zones that have been created.

The following information is displayed:

Field	Description
Name	The names of each zone currently configured on this Expressway. Clicking on a zone **Name** takes you to the configuration page for that zone.
Type	The type of zone.
Calls	The number of calls currently passing out to or received in from each zone.
Bandwidth used	The total amount of bandwidth used by all calls passing out to or received in from each zone.

Field	Description
H.323 / SIP status	Indicates the zone's H.323 or SIP connection status: • *Off*: the protocol is disabled at either the zone or system level • *Active*: the protocol is enabled for the zone and it has at least one active connection; if multiple connections are configured and some of those connections have failed, the display indicates how many of the connections are *Active* • *On*: indicates that the protocol is enabled for the zone (for zone types that do not have active connections, for example, DNS and ENUM zones) • *Failed*: the protocol is enabled for the zone but its connection has failed • *Checking*: the protocol is enabled for the zone and the system is currently trying to establish a connection
Search rule status	This area is used to indicate if that zone is not a target of any search rules.

Bandwidth

Link Status

The **Link status** page (**Status** > **Bandwidth** > **Links**) lists all of the links currently configured on the Expressway, along with the number of calls and the bandwidth being used by each link.

The following information is displayed:

Field	Description
Name	The name of each link. Clicking on a link **Name** takes you to the configuration page for that link.
Calls	The total number of calls currently traversing the link. **Note** A single call may traverse more than one link, depending on how your system is configured.
Bandwidth used	The total bandwidth of all the calls currently traversing the link.

Pipe Status

The **Pipe status** page (**Status** > **Bandwidth** > **Pipes**) lists all of the pipes currently configured on the Expressway, along with the number of calls and the bandwidth being used by each pipe.

The following information is displayed:

Field	Description
Name	The name of each pipe. Clicking on a pipe **Name** takes you to the configuration page for that pipe.
Calls	The total number of calls currently traversing the pipe. **Note** A single call may traverse more than one pipe, depending on how your system is configured.
Bandwidth used	The total bandwidth of all the calls currently traversing the pipe.

Policy Server Status and Resiliency

You must specify a **Status path** when configuring the Expressway's connection to a policy server. It identifies the path from where the status of the remote service can be obtained. By default this is *status*.

Up to 3 different policy server addresses may be specified. The Expressway polls each address on the specified path every 60 seconds to test the reachability of that address. The Expressway accepts standard HTTP(S) response status codes.

Note The developers of the policy service must ensure that this provides the appropriate status of the service.

If a server does not respond to status requests, Expressway will deem that server's status to be in a failed state and it is not queried for policy service requests until it returns to an active state. Its availability is not checked again until after the 60 second polling interval has elapsed.

When the Expressway needs to make a policy service request, it attempts to contact the service via one of the configured server addresses. It will try each address in turn, starting with **Server 1 address**, and if necessary - and if configured - via the **Server 2 address** and then the **Server 3 address**. The Expressway only tries to use a server address if it is in an active state, based on its most recent status query.

The Expressway has a non-configurable 30 seconds timeout value for each attempt it makes to contact a policy server. However, if the server is not reachable, the connection failure will occur almost instantaneously.

Note The TCP connection timeout is usually 75 seconds. Therefore, in practice, a TCP connection timeout is unlikely to occur as either the connection will be instantly unreachable or the 30 second request timeout will occur first.

The Expressway uses the configured **Default CPL** if it fails to contact the policy service via any of the configured addresses.

Note This method provides resiliency but not load balancing i.e. all requests are sent to **Server 1 address**, providing that server address is functioning correctly.

Viewing Policy Server Status via the Expressway

A summarized view of the status of the connection to each policy service can be viewed by going to the **Policy service status** page (**Status** > **Policy services**).

The set of policy services includes all of the services defined on the **Policy services** page (**Configuration** > **Dial plan** > **Policy services**), plus a **Call Policy** service if appropriate.

The following information is displayed:

Field	Description
Name	The name of the policy service. Clicking on a **Name** takes you to the configuration page for that service where you can change any of the settings or see the details of any connection problems.
URL	The address of the service. **Note** Each service can be configured with multiple server addresses for resiliency. This field displays the server address currently selected for use by the Expressway.
Status	The current status of the service based on the last attempt to poll that server.
Last used	Indicates when the service was last requested by the Expressway.

TURN Relay Usage

The **TURN relay usage** page (**Status** > **TURN relay usage**) provides a summary list of all the clients that are connected to the TURN server.

Note TURN services are available on Expressway-E systems only; they are configured via **Configuration** > **Traversal** > **TURN**.

The following information is displayed:

Field	Description
Client	The IP address of the client that requested the relay.
Media destinations	The address of destination system the media is being relayed to.

Field	Description
Connection protocol	Indicates if the client is connected over TCP or UDP.
Relays	Number of current relays being used by the client.

Viewing TURN relay details for a client connection

You can click on a specific client to see all of the relays and ports that it is using.

For each relay, its associated relay peer address/port is displayed. It also displays each relay's associated peer address/port (the TURN server relay port from which the media is being sent to the destination system). To see specific statistics about a relay, click **View** to go to the TURN Relay Summary page.

TURN Relay Summary

The **TURN relay summary** page provides overview information about a particular relay, including a summary count of the permissions, channels and requests associated with that relay.

To access this page, go to **Status** > **TURN relay usage**, then click **View** for a TURN client, and then **View** again for the required relay.

Further detailed information about the relay can be viewed by using the links in the **Related tasks** section at the bottom of the page. These let you:

- **View permissions for this relay**: Information about the permissions that have been defined on this relay.
- **View channels for this relay**: Information about the channel bindings that have been defined on this relay.
- **View counters for this relay**: Information about the number of TURN requests received, and the number of TURN success or error responses sent. It also shows counts of the number of packets forwarded to and from the client that allocated this relay.

Unified Communications Status

The **Unified Communications status** page (**Status** > **Unified Communications**) shows the current status of the Unified Communications services including:

- The number of configured Unified CM and IM&P servers (Expressway-C only)
- The current number of active provisioning sessions (Expressway-C only)
- The number of current calls
- All the domains and zones that have been configured for Unified Communications services
- Statistics about SSO access requests and responses

If any configuration or connectivity problems are detected, appropriate messages are displayed with either links or guidelines as to how to resolve the issue.

You can also view some advanced status information, including:

- A list of all current and recent (shown in red) provisioning sessions (Expressway-C only)
- A list of the automatically-generated SSH tunnels servicing requests through the traversal zone

Checking MRA Authentication Statistics

Go to **Status** > **Unified Communications** > **View detailed MRA authentication statistics** to view a summary of requests and responses issued, and more detailed statistics about successful and unsuccessful attempts to authenticate.

If no instances of a particular request or response type exist, then no counter is shown for that type.

SSH Tunnels Status

This page shows the status of the SSH tunnels between this Expressway and its "traversal partner". You can view this status from either side of the tunnel, that is, on the Expressway-C or the Expressway-E.

Here are some reasons why SSH tunnels could fail:

- The Expressway-C cannot find the Expressway-E:
  - Is there a firewall between them? Is TCP 2222 open from the Expressway-C to the Expressway-E?
  - Are there forward and reverse DNS entries for the Expressway-C and Expressway-E?

  Use traceroute and ping to establish if there is a connectivity problem.
- The servers do not trust each other:
  - Are the partners synchronized using NTP servers? A large time difference between the partners could prevent them from trusting each other.
  - Are the server certificates valid and current? Are their issuing CAs trusted by the other side?
  - Is the authentication account added to the local database in the Expressway-E?
  - Is the same authentication account entered on the Expressway-C?

  Try a secure traversal test from the Expressway-C (**Maintenance** > **Security** > **Secure traversal test** and enter the FQDN of the Expressway-E).

Microsoft Interoperability

Microsoft-registered FindMe User Status

The **Status** > **Applications** > **Microsoft-registered FindMe users** page lists the current status of all FindMe IDs being handled by the Microsoft Interoperability service.

It applies to deployments that use both Microsoft clients and FindMe, if they both use the same SIP domain. To enable this feature, **Register FindMe users as clients to Microsoft server** must be set to *Yes* on the Microsoft Interoperability configuration page.

The following information is displayed:

Field	Description
URI	The FindMe ID.
Registration state	Indicates whether the FindMe ID has registered successfully with a Microsoft Front End server. Doing so allows Microsoft infrastructure to forward calls to the FindMe ID. **Note** FindMe users can only register to Microsoft infrastructure if the FindMe ID is a valid user in the Active Directory (in the same way that Microsoft clients can only register if they have a valid account enabled in AD).
Peer	The cluster peer that is registering the URI.

You can view further status information for each FindMe ID by clicking **Edit** in the **Action** column. This can help diagnose registration or subscription failures.

Microsoft Interoperability Status

Go to **Status** > **Applications** > **Microsoft interoperability**) to see the status of the Microsoft interoperability service.

This service routes SIP calls between the Expressway and a Microsoft server.

The information shown includes:

- The number of current calls passing through the Microsoft interoperability B2BUA
- Resource usage as a percentage of the number of allowed Microsoft interoperability calls

TMS Provisioning Extension Service Status

The **TMS Provisioning Extension service status** page (**Status** > **Applications** > **TMS Provisioning Extension services** > **TMS Provisioning Extension service status**) shows the status of each of the Cisco TMSPE services to which the Expressway is connected (or to which it is attempting to connect).

Summary details of each service are shown including:

- The current status of the connection.
- When the most recent update of new data occurred.
- When the service was last polled for updates.
- The scheduled time of the next poll.

Click **View** to display further details about a service, including:

- Additional connection status and configuration information, including troubleshooting information about any connection failures.

- Which Expressway in the cluster has the actual connection to the Cisco TMSPE services (only displayed if the Expressway is part of a cluster).
- Details of each of the data tables provided by the service, including the revision number of the most recent update, and the ability to **View** the records in those tables.

You are recommended to use Cisco TMS to make any changes to the services' configuration settings, however you can modify the current configuration for this Expressway from the TMS Provisioning Extension services page (**System** > **TMS Provisioning Extension services**).

See the Provisioning Server section for more information.

Provisioning Server Device Requests Status (Cisco TMSPE)

The **Device requests status** page (**Status** > **Applications** > **TMS Provisioning Extension services** > **Device requests**) shows the status of the Expressway Provisioning Server when using Cisco TMSPE.

If device provisioning is enabled, the Expressway Provisioning Server provides provisioning-related services to provisioned devices, using data supplied by Cisco TMS through the Cisco TMS provisioning mechanism.

Expressway supports only the Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) services to provide the Expressway with provisioning and FindMe data. In this mode all provisioning and FindMe data is managed and maintained exclusively within Cisco TMS.

Provisioning server

This section displays the server's status and summarizes the subscription requests received by the server since the Expressway was last restarted. It shows counts of:

- The total number of subscription requests received
- How many requests were sent a successful provisioning response
- Failed requests because the account requesting provisioning could not be found
- Failed requests because the account requesting provisioning had no provisioned devices associated with it

Model licenses

This section shows the status of the provisioning licenses that are available within your system. Information displayed includes:

- The total license limit and the number of licenses still available (free) for use
- The number of licenses currently being used by devices that are registered to this Expressway (or Expressway cluster); this information is broken down by the device types that can be provisioned by this Expressway

License information is exchanged between Cisco TMS and Expressway by the Cisco TMSPE Devices service. If the Devices service is not active, the Expressway's Provisioning Server will not be able to provision any devices.

The license limit and the number of free licenses indicate the overall number of licenses that are available to all of the Expressways or Expressway clusters that are being managed by Cisco TMS, hence the difference between the license limit and free counts may not equal the sum of the number of used licenses shown for this particular Expressway or Expressway cluster

Phone book server

The phone book server provides phone book directory and lookup facilities to provisioned users.

This section displays the server's status and summarizes the number of phone book search requests received by the server from provisioned users since the Expressway was last restarted.

User Records Provided by Cisco TMSPE Services

You can view the data records provided by the Cisco TMSPE **Users** service by going to **Status** > **Applications** > **TMS Provisioning Extension services** > **Users** > **...** and then the relevant table:

- **Accounts**
- **Groups**
- **Templates**

All the records in the chosen table are listed.

Note Some tables can contain several thousand records and you may experience a delay before the data is displayed.

Filtering the view

The **Filter** section lets you filter the set of records that are shown. It is displayed only if there is more than one page of information to display. Status pages show 200 records per page.

Enter a text string or select a value with which to filter each relevant field, and then click **Filter**.

Only those records that match all of the selected filter options are shown.

Note Text string filtering is case insensitive.

Viewing more details and related records

You can click View to display further details about the selected record. Many views also allow you to click on related information to see the data records associated with that item. For example, when viewing user groups, you can also access the related user templates. When viewing user accounts you can check the data that would be provisioned to that user by clicking Checking Provisioned Data.

FindMe Records Provided by Cisco TMSPE Services

You can view the data records provided by the Cisco TMSPE **FindMe** service by going to **Status** > **Applications** > **TMS Provisioning Extension services** > **FindMe** > **...** and then the relevant table:

- **Accounts**

- **Locations**
- **Devices**

All the records in the chosen table are listed.

Note Some tables can contain several thousand records and you may experience a delay before the data is displayed.

Filtering the view

The **Filter** section lets you filter the set of records that are shown. It is displayed only if there is more than one page of information to display. Status pages show 200 records per page.

Enter a text string or select a value with which to filter each relevant field, and then click **Filter**.

Only those records that match all of the selected filter options are shown. Note that text string filtering is case insensitive.

Viewing more details and related records

You can click **View** to display further details about the selected record. Many views also allow you to click on related information to see the data records associated with that item. For example, when viewing a FindMe user, you can also access the related location and device records.

Phone Book Records Provided by Cisco TMSPE Services

You can view the data records provided by the Cisco TMSPE **Phone books** service by going to **Status** > **Applications** > **TMS Provisioning Extension services** > **Phone book** > **...** and then the relevant table:

- **Folders**
- **Entries**
- **Contact methods**
- **User access**

All the records in the chosen table are listed.

Note Some tables can contain several thousand records and you may experience a delay before the data is displayed.

Filtering the view

The **Filter** section lets you filter the set of records that are shown. It is displayed only if there is more than one page of information to display. Status pages show 200 records per page.

Enter a text string or select a value with which to filter each relevant field, and then click **Filter**.

Only those records that match all of the selected filter options are shown.

Note Text string filtering is case insensitive.

Viewing more details and related records

You can click **View** to display further details about the selected record. Many views also allow you to click on related information to see the data records associated with that item. For example, when viewing a phone book entry, you can also access the related contact method or folder.

Provisioned Devices

The **Provisioned device status** page (**Status** > **Applications** > **TMS Provisioning Extension services** > **Provisioned device status**) displays a list of all of the devices that have submitted provisioning requests to the Expressway's Provisioning Server.

Filtering the view

The **Filter** section lets you filter the set of records that are shown. It is displayed only if there is more than one page of information to display. Status pages show 200 records per page.

Enter a text string or select a value with which to filter each relevant field, and then click **Filter**.

Only those records that match all of the selected filter options are shown.

Note Text string filtering is case insensitive.

The list shows all current and historically provisioned devices. A device appears in the list after it has made its first provisioning request. The **Active** column indicates if the device is currently being provisioned (and is thus consuming a provisioning license).

Checking Provisioned Data

The **Check provisioned data** page is used to check the configuration data that the Expressway's Provisioning Server will provision to a specific user and device combination.

You can get to this page only through the **User accounts status** page (**Status** > **Applications** > **TMS Provisioning Extension services** > **Users** > **Accounts**, locate the user you want to check and then click **Check provisioned data**).

Step 1 Verify that the **User account name** is displaying the name of the user account you want to check.

Step 2 Select the **Model** and **Version** of the user's endpoint device.

If the actual **Version** used by the endpoint is not listed, select the nearest earlier version.

Step 3 Click **Check provisioned data**.

The **Results** section will show the data that would be provisioned out to that user and device combination.

Managing Alarms

Alarms occur when an event or configuration change has taken place on the Expressway that requires some manual administrator intervention, such as a restart. Alarms may also be raised for hardware and environmental issues such as faulty disks and fans or high temperatures.

The **Alarms** page (**Status** > **Alarms**) provides a list of all the alarms currently in place on your system (and, where applicable, their proposed resolution). When there are unacknowledged alarms in place on the Expressway, an alarm icon ⚠ appears at the top right of all pages. You can also access the **Alarms** page by clicking on the alarm icon.

Each alarm is identified by a 5-digit **Alarm ID**, shown in the rightmost column in the alarms list. The alarms are grouped into categories as follows:

Alarm ID prefix	Category
10nnn	Hardware issues
15nnn	Software issues
20nnn	Cluster-related issues
25nnn	Network and network services settings
30nnn	Licensing / resources / option keys
35nnn	External applications and services (such as policy services or LDAP/AD configuration)
40nnn	Security issues (such as certificates, passwords or insecure configuration)
45nnn	General Expressway configuration issues
55nnn	B2BUA issues
6nnnn	Hybrid Services alarms
60000-60099	Management Connector alarms
60100-60199	Calendar Connector alarms
60300-60399	Call Connector alarms
9nnnn	Significant Event alarms

All alarms raised on the Expressway are also raised as Cisco TMS tickets. All the attributes of an alarm (its ID, severity and so on) are included in the information sent to Cisco TMS.

Alarms are dealt with by clicking each **Action** hyperlink and making the necessary configuration changes to resolve the problem.

Acknowledging an alarm (by selecting an alarm and clicking on the **Acknowledge** button) removes the alarm icon from the web UI, but the alarm will still be listed on the **Alarms** page with a status of *Acknowledged*. If a new alarm occurs, the alarm icon will reappear.

- You cannot delete alarms from the **Alarms** page. Alarms are removed by the Expressway only after the required action or configuration change has been made.
- After a restart of the Expressway, any *Acknowledged* alarms that are still in place on the Expressway will reappear with a status of New, and must be re-acknowledged.
- The display indicates when the alarm was first and last raised since the Expressway was last restarted.
- If your Expressway is a part of a cluster, the **Alarms** page shows all of the alarms raised by any of the cluster peers. However, you can acknowledge only those alarms that have been raised by the “current” peer (the peer to which you are currently logged in to as an administrator).
- You can click the Alarm ID to generate a filtered view of the Event Log, showing all occurrences of when that alarm has been raised and lowered.

See the alarms list for further information about the specific alarms that can be raised.

Logs

Event Log

The **Event Log** page (**Status** > **Logs** > **Event Log**) lets you view and search the Event Log, which is a list of the events that have occurred on your system since the last upgrade.

The Event Log holds a maximum of 2GB of data; when this size is reached, the oldest entries are overwritten. However, only the first 50MB of Event Log data can be displayed through the web interface.

Filtering the Event Log

The **Filter** section lets you filter the Event Log. It is displayed only if there is more than one page of information to display. Log pages show 1000 records per page.

Enter the words you want to search for and click **Filter**. Only those events that contain all the words you entered are shown.

To do more advanced filtering, click **more options**. This gives you additional filtering methods:

- **Contains the string**: Only includes events containing the exact phrase entered here.
- **Contains any of the words**: Includes any events that contain at least one of the words entered here.
- **Not containing any of the words**: Filters out any events containing any of the words entered here.

Note Use spaces to separate each word you want to filter by.

Click **Filter** to reapply any modified filter conditions. To return to the complete log listing, click **Reset**.

Reconfiguring the log settings

Clicking **Configure the log settings** takes you to the Logging configuration page. From this page, you can set the level of events that are recorded in the Event Log, and also set up a remote server to which the Event Log can be copied.

Saving the results to a local disk

Click **Download** this page if you want to download the contents of the results section to a text file on your local PC or server.

Results section

The **Results** section shows all the events matching the current filter conditions, with the most recent being shown first.

Most **tvcs** events contain hyperlinks in one or more of the fields (such fields change color when you hover over them). You can click on the hyperlink to show only those events that contain the same text string. For example, clicking on the text that appears after **Event=** filters the list to show all the events of that particular type. Likewise, clicking on a particular **Call-Id** shows just those events that contain a reference to that particular call.

Event Log color coding

Certain events in the Event Log are color-coded so that you can identify them more easily. These events are as follows:

Green events:

- System Start
- Admin Session Start/Finish
- Installation of <item> succeeded
- Call Connected
- Request Successful
- Beginning System Restore
- Completed System Restore

Orange events:

- System Shutdown
- Intrusion Protection Unblocking

Purple events:

- Diagnostic Logging

Red events:

- Registration Rejected

- Registration Refresh Rejected
- Call Rejected
- Security Alert
- License Limit Reached
- Decode Error
- TLS Negotiation Error
- External Server Communications Failure
- Application Failed
- Request Failed
- System Backup Error
- System Restore Error
- Authorization Failure
- Intrusion Protection Blocking

For more information about the format and content of the Event Log see Event Log Format and Events and Levels.

Configuration Log

The **Configuration Log** page (**Status** > **Logs** > **Configuration Log**) provides a list of all changes to the Expressway configuration.

The Configuration Log holds a maximum of 30MB of data; when this size is reached, the oldest entries are overwritten. The entire Configuration Log can be displayed through the web interface.

Filtering the Configuration Log

The **Filter** section lets you filter the Configuration Log. It is displayed only if there is more than one page of information to display. Log pages show 1000 records per page.

Enter the words you want to search for and click **Filter**. Only those events that contain all the words you entered are shown.

To do more advanced filtering, click **more options**. This gives you additional filtering methods:

- **Contains the string**: Only includes events containing the exact phrase entered here.
- **Contains any of the words**: Includes any events that contain at least one of the words entered here.
- **Contains any of the words**: Includes any events that contain at least one of the words entered here.

Note Use spaces to separate each word you want to filter by.

Click **Filter** to reapply any modified filter conditions. To return to the complete log listing, click **Reset**.

Results section

The **Results** section shows all the web-based events, with the most recent being shown first.

Most events contain hyperlinks in one or more of the fields (such fields change color when you hover over them). You can click on the hyperlink to show only those events that contain the same text string. For example, clicking on the text that appears after Event= filters the list to show all the events of that particular type. Likewise, clicking on a particular **user** shows just those events relating to that particular administrator account.

All events that appear in the Configuration Log are recorded as Level 1 Events, so any changes to the logging levels will not affect their presence in the Configuration Log.

Configuration Log events

Changes to the Expressway configuration made by administrators using the web interface have an Event field of *System Configuration Changed*.

The **Detail** field of each of these events shows:

- The configuration item that was affected
- What it was changed from and to
- The name of the administrator user who made the change, and their IP address
- The date and time that the change was made

Network Log

The **Network Log** page (**Status** > **Logs** > **Network Log**) provides a list of the call signaling messages that have been logged on this Expressway.

The Network Log holds a maximum of 2GB of data; when this size is reached, the oldest entries are overwritten. However, only the first 50MB of Network Log data can be displayed through the web interface.

Filtering the Network Log

The **Filter** section lets you filter the Network Log. It is displayed only if there is more than one page of information to display. Log pages show 1000 records per page.

Enter the words you want to search for and click **Filter**. Only those events that contain all the words you entered are shown.

To do more advanced filtering, click **more options**. This gives you additional filtering methods:

- **Contains the string**: Only includes events containing the exact phrase entered here.
- **Contains any of the words**: Includes any events that contain at least one of the words entered here.
- **Not containing any of the words**: Filters out any events containing any of the words entered here.

Note Use spaces to separate each word you want to filter by.

Click **Filter** to reapply any modified filter conditions. To return to the complete log listing, click **Reset**.

Reconfiguring the log settings

Clicking **Configure the log settings** takes you to the Network Log configuration page. From this page, you can set the level of events that are recorded in the Network Log.

Saving the results to a local disk

Click **Download this page** if you want to download the contents of the results section to a text file on your local PC or server.

Results Section

The **Results** section shows the events logged by each of the Network Log modules.

Most events contain hyperlinks in one or more of the fields (such fields change color when you hover over them). You can click on the hyperlink to show only those events that contain the same text string. For example, clicking on the text that appears after **Module=** filters the list to show all the events of that particular type.

The events that appear in the Network Log are dependent on the log levels configured on the Network Log configuration page.

Common Criteria Changes

The following are the changes -

- **Audit Log for Login Banner** - Editing the Login Banner will now create an Event Log displaying the changes made, the user who made them, and the time they were made.
- **SSH Logging Enhancement** - SSH logs are added.
- **CLI Session Timeout** - Local CLI Sessions will now timeout as intended.
- **Event Logging** - **TLS Handshake**, **Failed Connection**, and many more –
  - A new log level is included for the Apache Web Server called "developer.apache2."
  - Log Level change for "developer.apache2" will trigger the Apache Web Server to restart.
  - In the **Maintenance** > **Diagnostics** > **Advanced** > **Support Log configuration** section, the "Reset to info" button is renamed to "Reset Defaults.”

Hardware Status

The **Hardware** page (**Status** > **Hardware**) provides information about the physical status of your Expressway appliance.

Information displayed includes:

- Fan speeds
- Component temperatures
- Component voltages

Any appropriate minimum or maximum levels are shown to help identify any components operating outside of their standard limits.

Warning Do not attempt to service the apparatus yourself as opening or removing covers may expose you to dangerous voltages or other hazards, and will void the warranty. Refer all servicing to qualified service personnel.

Note Hardware status information is not displayed if the Expressway is running on VMware.