Diagnostics and Troubleshooting

Network Utilities

This section provides information about how to use the network utility tools:

- Ping: allows you to check that a particular host system is contactable from the Expressway and that your network is correctly configured to reach it.
- Traceroute: allows you to discover the details of the route taken by a network packet sent from the Expressway to a particular destination host system.
- Tracepath: allows you to discover the path taken by a network packet sent from the Expressway to a particular destination host system.
- DNS Lookup: allows you to check which domain name server (DNS server) is responding to a request for a particular hostname.
- SRV Connectivity Tester: allows you to check DNS for specific service records, and verify connectivity to the returned hosts.

Ping

The **Ping** tool (**Maintenance** > **Tools** > **Network utilities** > **Ping**) can be used to assist in troubleshooting system issues.

It allows you to check that a particular host system is contactable and that your network is correctly configured to reach it. It reports details of the time taken for a message to be sent from the Expressway to the destination host system.

To use this tool:

1. In the **Host** field, enter the IP address or hostname of the host system you want to try to contact.
2. Click **Ping**.

A new section will appear showing the results of the contact attempt. If successful, it will display the following information:

Host	The hostname and IP address returned by the host system that was queried.
Response time (ms)	The time taken (in ms) for the request to be sent from the Expressway to the host system and back again.

Traceroute

The **Traceroute** tool (**Maintenance** > **Tools** > **Network utilities** > **Traceroute**) can be used to assist in troubleshooting system issues.

It allows you to discover the route taken by a network packet sent from the Expressway to a particular destination host system. It reports the details of each node along the path, and the time taken for each node to respond to the request.

To use this tool:

1. In the **Host** field, enter the IP address or hostname of the host system to which you want to trace the path.
2. Click **Traceroute**.

A new section will appear with a banner stating the results of the trace, and showing the following information for each node in the path:

TTL	(Time to Live). This is the hop count of the request, showing the sequential number of the node.
Response	This shows the IP address of the node, and the time taken (in ms) to respond to each packet received from the Expressway. *** indicates that the node did not respond to the request.

The route taken between the Expressway and a particular host may vary for each traceroute request.

Tracepath

The **Tracepath** tool (**Maintenance** > **Tools** > **Network utilities** > **Tracepath**) can be used to assist in troubleshooting system issues.

It allows you to discover the route taken by a network packet sent from the Expressway to a particular destination host system.

To use this tool:

1. In the **Host** field, enter the IP address or hostname of the host system to which you want to trace the route.
2. Click **Tracepath**.

A new section will appear with a banner stating the results of the trace, and showing the details of each node along the path, the time taken for each node to respond to the request, and the maximum transmission units (MTU).

The route taken between the Expressway and a particular host may vary for each tracepath request.

DNS Lookup

The **DNS lookup** tool (**Maintenance** > **Tools** > **Network utilities** > **DNS lookup**) can be used to assist in troubleshooting system issues.

It allows you to query DNS for a supplied hostname and display the results of the query if the lookup was successful.

To use this tool:

1. In the **Host** field, enter either:
   - the name of the host you want to query, or
   - an IPv4 or IPv6 address if you want to perform a reverse DNS lookup
2. In the **Query type** field, select the type of record you want to search for:

   (for reverse lookups the **Query type** is ignored - the search automatically looks for PTR records)

Note To facilitate proper reverse lookup, give the domain in the form of 152.50.10.in-addr.arpa (the subnet of addresses would be 10.50.152.0/24) and the target DNS server in the address. This sends all requests in the subnet to the target DNS server instead of the default server.

Option	Searches for...
All	any type of record
A (IPv4 address)	a record that maps the hostname to the host's IPv4 address
AAAA (IPv6 address)	a record that maps the hostname to the host's IPv6 address
SRV (services)	SRV records (which includes those specific to H.323, SIP, Unified Communications and TURN services, see below)
NAPTR (Name authority pointer)	a record that rewrites a domain name (into a URI or other domain name for example)

3. By default the system will submit the query to all of the system's default DNS servers (**System** > **DNS**). To query specific servers only, set **Check against the following DNS servers** to *Custom* and then select the DNS servers you want to use.
4. Click **Lookup**.

A separate DNS query is performed for each selected **Query type**. The domain that is included within the query sent to DNS depends upon whether the supplied **Host** is fully qualified or not (a fully qualified host name contains at least one “dot”):

- If the supplied **Host** is fully qualified:
  - DNS is queried first for **Host**
  - If the lookup for **Host** fails, then an additional query for **Host.<system_domain>** is performed (where **<system_domain>** is the **Domain name** as configured on the **DNS** page)
- If the supplied **Host** is not fully qualified:
  - DNS is queried first for **Host.<system_domain>**
  - If the lookup for **Host.<system_domain>** fails, then an additional query for **Host** is performed

For SRV record type lookups, multiple DNS queries are performed. An SRV query is made for each of the following _service._protocol combinations:

- _h323ls._udp.<domain>
- _h323rs._udp.<domain>
- _h323cs._tcp.<domain>
- _sips._tcp.<domain>
- _sip._tcp.<domain>
- _sip._udp.<domain>
- _collab-edge._tls
- _cisco-uds._tcp
- _turn._udp.<domain>
- _turn._tcp.<domain>

In each case, as for all other query types, either one or two queries may be performed for a <domain> of either **Host** and/or **Host.<system_domain>**.

Results

A new section will appear showing the results of all of the queries. If successful, it will display the following information:

Query type	The type of query that was sent by the Expressway.
Name	The hostname contained in the response to the query.
TTL	The length of time (in seconds) that the results of this query will be cached by the Expressway.
Class	`IN` (internet) indicates that the response was a DNS record involving an internet hostname, server or IP address.

Type	The record type contained in the response to the query.
Response	The content of the record received in response to the query for this **Name** and **Type**.

Transport protocols

The Expressway uses UDP and TCP to do DNS resolution, and DNS servers usually send both UDP and TCP responses. If the UDP response exceeds the UDP message size limit of 512 bytes, then the Expressway cannot process the UDP response. This is not usually a problem, because the Expressway can process the TCP response instead.

However, if you block TCP inbound on port 53, and if the UDP response is greater than 512 bytes, then the Expressway cannot process the response from the DNS. In this case you won't see the results using the DNS lookup tool, and any operations that need the requested addresses will fail.

However, if you block TCP inbound on port 53, and if the UDP response is greater than 512 bytes, then the Expressway cannot process the response from the DNS. In this case you won't see the results using the DNS lookup tool, and any operations that need the requested addresses will fail.

SRV Connectivity Tester

The SRV connectivity tester is a network utility that tests whether the Expressway can connect to particular services on a given domain. You can use this tool to proactively test your connectivity while configuring Expressway-based solutions such as Cisco Webex Hybrid Call Service or business-to-business video calling.

You specify the DNS Service Record Domain and the Service Record Protocols you want to query for that domain. The Expressway does a DNS SRV query for each specified protocol, and then attempts TCP connections to the hosts returned by the DNS. If you specify TLS, the Expressway only attempts a TLS connection after the TCP succeeds.

The Expressway connectivity test page shows the DNS response and the connection attempts. For any connection failures, the reason is provided along with advice to help with resolving specific issues.

To troubleshoot connectivity, you can download the TCP data from your test in *.pcap* format. You can selectively download a dump of the DNS query, or a specific connection attempt, or you can get a single *.pcap* file showing the whole test.

To use this tool:

1. Go to **Maintenance** > **Tools** > **Network utilities** > **Connectivity test**
2. Enter a **Service Record Domain** you want to query, for example, `callservice.webex.com`.
3. Enter the **Service Record Protocols** you want to test, for example, `_sips._tcp`.

   Use commas to delimit multiple protocols, for example, `_sip._tcp,_sips._tcp`.
4. Click **Run**

The Expressway queries DNS for SRV records comprised of the service, protocol and domain combinations, for example: `_sip._tcp.callservice.webex.com` and `_sips._tcp.callservice.webex.com`.

By default the system will submit the query to all of the system's default DNS servers (**System** > **DNS**).

Service Record Options

Here are some of the _service._protocol combinations you might need to test in your deployments:

- _h323ls._udp.<domain>
- _h323rs._udp.<domain>
- _h323cs._tcp.<domain>
- _sips._tcp.<domain>
- _sip._tcp.<domain>
- _sip._udp.<domain>
- _collab-edge._tls
- _cisco-uds._tcp
- _turn._udp.<domain>
- _turn._tcp.<domain>
- _cms-web._tls.<domain>
- _sipfederationtls._tcp.<domain>

Test Results

A section at the bottom of the page shows the query results and the connectivity test results. Test results will have some or all of the following information:

Table 1: Connectivity Test Results - DNS SRV Lookup

Result field	Description
Stage	The stage of the test; there is one stage for each response to your query and another one for the overall query result.
Service Record	The SRV records that were found, from the set that you queried.
Result	The hosts mapped by the DNS SRV record, if the test succeeded. Also shows the priority, weight, and port of each entry, if they are defined in the DNS record.
Hint	This field holds no value in this table of results.
TCP Dump	For the overall result, you can download a .pcap file that contains the TCP record of the SRV query.

Table 2: Connectivity Test Results - TCP Connections

Result	Description
Stage	The stage of the test; there is one test for each host that was returned for the queried service on TCP protocol. There is also a collective result of all tests.
Target	The hostname returned by DNS SRV query.
Result	Shows that the test completed successfully, or gives the reason for failure, if known.
Hint	A pointer that might help you troubleshoot unsuccessful tests.
TCP Dump	You can download a .pcap file that contains the TCP record of the specific connection attempt.

Table 3: Connectivity Test Results - TLS Connections

Result field	Description
Stage	The stage of the test. For each host, one to three tests are returned for the queried service on TLS protocol. The test is performed using each TLS version that is supported by the host, in the following order: • TLS 1.2 • TLS 1.1 • TLS 1 For example, if the host supports all three versions and the connection is successful using the TLS 1.1 version then the check returns two tests. There is also a collective result of all tests. **Note** If the Expressway cannot establish a TCP connection to a host, it does not attempt a TLS connection to that host.
Target	The hostname returned by DNS SRV query.
Result	Shows that the test completed successfully, or gives the reason for failure, if known.
Hint	A pointer that might help you troubleshoot unsuccessful tests.
TCP Dump	You can download a .pcap file that contains the TCP record of the specific connection attempt.

Diagnostics Tools

This section provides information about how to use Expressway diagnostics tools:

- Configuring Diagnostic Logging
- Creating a System Snapshot
- Configuring Network Log Levels and Configuring Support Log Levels advanced logging configuration tools
- Incident Reporting

Expressway supports SIP "session identifiers". Assuming all devices in the call use session identifiers, the mechanism uses the *Session-ID* field in SIP headers to maintain a unique code through the entire transit of a call. Session identifiers are useful for investigating issues with calls that involve multiple components, as they can be used to find and track a specific call on the Expressway server. Support for session identifiers includes the SIP side of interworked SIP/H.323 calls, and calls to and from Microsoft systems. Session identifiers are defined in RFC 7989.

Configuring Diagnostic Logging

The Diagnostic logging tool (**Maintenance** > **Diagnostics** > **Diagnostic logging**) can assist with troubleshooting. You can generate a diagnostic log of system activity over a period of time, and download it to send to your Cisco customer support representative. You can also obtain and download a *tcpdump* while logging is in progress.

Before You Begin

- Only one diagnostic log can be generated at a time. Creating a new diagnostic log replaces any previously produced log.
- Expressway continually logs relevant system activity. The diagnostic logging function extracts the activity from the start of the diagnostic logging time to when diagnostic logging is stopped and provides a convenient web-based download facility.
- **Restart/Reboot:** Only diagnostic log will be collected; other files will be missing from the bundle.
- When you start a diagnostic log, the relevant system modules have their log levels automatically set to "debug". Ignore any resulting *Verbose log levels configured* alarms, as the log levels will get reset to their original values when you stop logging.
- Diagnostic logging is controlled through the web interface. There is no CLI option.
- When tcpdump option is selected, a maximum of 2 packet 3 packet capture files are created per network interface, each with a maximum size of 20MB (i.e., up to 4 files with a total size of 80MB could be created on an Expressway with dual network interfaces).

Note From X14.0, the number of .pcap files are increased up to 20 per network interface so, the tcpdump can run continuously through web UI. Maximum file size is still 20 MB.

Caution Enabling diagnostic logging can affect the performance of your system. You should only collect diagnostic logs on the advice of Cisco customer support or during periods of lighter traffic load.

Process to Generate the Diagnostic Log

1. Go to **Maintenance** > **Diagnostics** > **Diagnostic logging**
2. (Optional) Select *Take tcpdump while logging*. You can select this option to take a tcpdump while diagnostic logging is in progress. The tcpdump can be downloaded as a separate file on logging completion.

Note Now administrator can provide **IP address** and **Port** filters if tcpdump is enabled on the user interface.

The tcpdump filters are used if the administrator wants to see packets coming from a specific host (IP address or Fully Qualified Domain Name (FQDN)) and/or port in pcap files. The administrator can provide the values in the fields identified to get the filtered packets. From version X14.0, tcpdump captures 20 pcap files per LAN and every pcap file is 20MB in size.

The table represents the average time (in seconds) taken to generate 1 pcap file (20MB max) and 20 pcap files depending upon the number of registrations.

Expressway C:

	20MB	**400MB**
5 users	2	40
20 users	2	40
2500 users	10	200

Expressway E:

	20MB	**400MB**
5 users	1	20
20 users	1	20
2500 users	2	40

These numbers are specific to the environment used for troubleshooting. We have used 1 node and Mobile and Remote Access (MRA) video while running this performance test.

3. Enter **Filter tcpdump by IP address**.
4. Enter **Filter tcpdump by port**. Range is 1 to 65536.
5. Click **Start new log**.
6. (Optional) Enter some **Marker** text and click **Add marker**.

- You can use the marker facility to add comment text to the log file before certain activities are performed. This helps to subsequently identify specific sections in the diagnostic log file. Marker text has a `DEBUG_MARKER` tag in the log file.
- You can add as many markers as required, at any time while the diagnostic logging is in progress.

7. Reproduce the system issue you want to trace in the diagnostic log.
8. Click **Stop logging**.
9. Click **Collect log**.
10. When the log collection completes, click **Download log** to save the diagnostic log archive to your local file system.

    You are prompted to save the archive (the exact wording depends on your browser).

Files contained in the diagnostic log archive

- loggingsnapshot_<*system host name*>_<*timestamp*>.txt - containing log messages in response to the activities performed during the logging period
- xconf_dump_<*system host name*>_<*timestamp*>.txt - containing information about the configuration of the system at the time the logging was started
- xconf_dump_<*system host name*>_<*timestamp*>.xml - more complete version of xconfig, in XML format
- xstat_dump_<*system host name*>_<*timestamp*>.txt - containing information about the status of the system at the time the logging was started
- xstat_dump_<*system host name*>_<*timestamp*>.xml - more complete version of xstatus, in XML format
- (if relevant) eth *n*_diagnostic_logging_tcpdump x_<*system host name*>_<*timestamp*>.pcap - containing the packets captured during the logging period
- ca_<*system host name*>_<*timestamp*>.pem
- server_<*system host name*>_<*timestamp*>.pem

These files can be sent to your Cisco support representative if you are asked to do so.

Caution *tcpdump* files may contain sensitive information. Only send *tcpdump* files to trusted recipients. Consider encrypting the file before sending it, and also send the decrypt password out-of-band.

Link to Collaboration Solutions Analyzer tool

You can optionally use the **Analyze log**, to open a link to the Collaboration Solutions Analyzer troubleshooting tool.

To download logs again

To download the logs again, you can re-collect them by using the **Collect log** button. If the button is grayed out, refresh the browser page.

Clustered Systems

If the Expressway is part of a cluster, some activities only apply to the “current” peer (the peer to which you are currently logged in to as an administrator):

- The start and stop logging operations are applied to every peer in the cluster, regardless of the current peer.
- The *tcpdump* operation is applied to every peer in the cluster, regardless of the current peer.
- Each cluster peer maintains its own unified log, and logs activity that occurs only on that peer.
- Marker text is only applied to log of the current peer.
- You can only download the diagnostic log from the current peer.
- To add markers to other peers' logs, or to download diagnostic logs from other peers, you must log in as an administrator to that other peer.

To collect comprehensive information for debugging purposes, we recommend that you extract the diagnostic log for each peer in a cluster.

Creating a System Snapshot

The **System snapshot** page (**Maintenance** > **Diagnostics** > **System snapshot**) lets you create files that can be used for diagnostic purposes. The files should be sent to your support representative at their request to assist them in troubleshooting issues you may be experiencing.

You can create several types of snapshot file:

- **Status snapshot**: contains the system's current configuration and status settings.
- **Logs snapshot**: contains log file information (including the Event Log, Configuration Log and Network Log).
- **Full snapshot**: contains a complete download of all system information. The preparation of this snapshot file may take several minutes to complete and may lead to a drop in system performance while the snapshot is in progress.

To create a system snapshot file:

1. Click one of the snapshot buttons to start the download of the snapshot file. Typically your support representative will tell you which type of snapshot file is required.
   - The snapshot creation process will start. This process runs in the background. If required, you can navigate away from the snapshot page and return to it later to download the generated snapshot file.
   - When the snapshot file has been created, a **Download snapshot** button will appear.
2. Click **Download snapshot**. A pop-up window appears and prompts you to save the file (the exact wording depends on your browser). Select a location from where you can easily send the file to your support representative.

Configuring Network Log Levels

The **Network Log configuration** page (**Maintenance** > **Diagnostics** > **Advanced** > **Network Log configuration**) is used to configure the log levels for the range of Network Log message modules.

Caution Changing the logging levels can affect the performance of your system. You should only change a log level on the advice of Cisco customer support.

To change a logging level:

1. Click on the **Name** of the module whose log level you want to modify.
2. Choose the required **Level** from the drop-down list.
   - A log level of *Fatal* is the least verbose; *Trace* is the most verbose.
   - Each message category has a log level of *Info* by default.
3. Click **Save**.

Configuring Support Log Levels

The **Support Log configuration** page (**Maintenance** > **Diagnostics** > **Advanced** > **Support Log configuration**) is used to configure the log levels for the range of Support Log message modules.

Caution Changing the logging levels can affect the performance of your system. You should only change a log level on the advice of Cisco customer support.

To change a logging level:

1. Click on the **Name** of the module whose log level you want to modify.
2. Choose the required **Level** from the drop-down list.
   - A log level of *Fatal* is the least verbose; *Trace* is the most verbose.
   - Each message category has a log level of *Info* by default.
3. Click **Save**.

XCP Routing Information

This improvement displays content of the Extensible Communications Platform (XCP) routing table. This content is a complete data dump of the XCP routing information contained in Cisco Jabber. This information is useful for debugging from the XCP point of view. It is made available both in the **routing.xml** file on the VCS device and in the **developer.xcp.jabber logs**.

Additionally, the ConnectionManager information is also available as a data dump through developer logs. This information displays the state of ConnectedSockets and FailedRequests counters.

All this information will help administrators to check the routing information, the number of connections, and details of each Jabber client connection.

Implementation

Information is made available in the following files -

- **routing.xml** file under `/tmp/xml` location which contains XCP route information.
- Additional logging for XCP route information in developer logs in **developer.xcp.jabber logs**.

XCP Routing Graph Representation

This section details the structure of the **routing.xml** file. It contains multiple structures. For more information, see Table 4: List of Element(s) and their Description.

XML Syntax

```
> <RoutingGraph>
              > <Edges>
                ...
                </Edges>
              > <RealmsToEdges>
                ...
                </RealmsToEdges>
              > <VersionsToEdges>
                ...
                </VersionsToEdges>
              > <BestHops>
                ...
                </BestHops>
              > <LastHops>
                ...
                </LastHops>
                <Orphans/>
                <from>vmx144-032-p-extend1-corpb-rd-rusc1abs-cisco-com</from>
                <num_edges>2</num_edges>
                <num_vertices>3</num_vertices>
              > <Connections>
                ...
                </Connections>
              > <RealmsToConnections>
                ...
                </RealmsToConnections>
              > <CompToDomains>
                ...
                </CompToDomains>
               > <DomainToComps>
                  ...
                 </DomainToComps>
               > <IdRealms>
                  ...
                 </IdRealms>
            </RoutingGraph>
```

The table describes the various elements used in the *routing.xml* file.

Table 4: List of Element(s) and their Description

Element(s)	Description
Edges	Associate JIDs of local and remote Realms
RealmsToEdges	Multimap of JID to Edges
VersionsToEdges	Multimap of Version to Edges
BestHops	Hash map of Realm JID to JID distance
LastHops	The result when BestHops was last computed successfully
Orphans	Vertices without edges
from	The last vertex that BestHops are computed from
num_edges	Number of edges
num_vertices	Number of nodes
Connections	Associate remote Realm JID and corresponding component
RealmsToConnections	Map of connection JID to component that supports it
CompToDomains	Map of component JID to set of routable JIDs
DomainToComps	Map of routable JID to set of component JIDs
IdRealms	Map of component JID to pair of Realm JID and available type

Incident Reporting

The incident reporting feature for Expressway automatically saves information about critical system issues such as application failures. This section describes how to view incident reports.

It also describes how to send incident reports to Cisco customer support, either manually or automatically. The information in the reports can then be used by Cisco customer support to diagnose the cause of the failures. All information gathered during this process will be held in confidence and used by Cisco personnel for the sole purpose of issue diagnosis and problem resolution.

Incident Reporting Caution: Privacy-Protected Personal Data

IN NO EVENT SHOULD PRIVACY-PROTECTED PERSONAL DATA BE INCLUDED IN ANY REPORTS TO CISCO.

Privacy-Protected Personal Data means any information about persons or entities that the Customer receives or derives in any manner from any source that contains any personal information about prospective, former, and existing customers, employees or any other person or entity. Privacy-Protected Personal Data includes,

without limitation, names, addresses, telephone numbers, electronic addresses, social security numbers, credit card numbers, customer proprietary network information (as defined under 47 U.S.C. § 222 and its implementing regulations), IP addresses or other handset identifiers, account information, credit information, demographic information, and any other information that, either alone or in combination with other data, could provide information specific to a particular person.

PLEASE BE SURE THAT PRIVACY-PROTECTED PERSONAL DATA IS NOT SENT TO CISCO WHEN THE EXPRESSWAY IS CONFIGURED TO AUTOMATICALLY SEND REPORTS.

IF DISCLOSURE OF SUCH INFORMATION CANNOT BE PREVENTED, PLEASE DO NOT USE THE AUTOMATIC CONFIGURATION FEATURE. Instead, copy the data from the Incident Report Details page and paste it into a text file. You can then edit out any sensitive information before forwarding the file on to Cisco customer support.

Incident reports are always saved locally, and can be viewed via the Viewing Incident Reports page.

Enabling Automatic Incident Reporting

Read the Incident Reporting Caution: Privacy-Protected Personal Data before you decide whether to enable automatic incident reporting.

To configure the Expressway to send incident reports automatically to Cisco customer support:

1. Go to **Maintenance** > **Diagnostics** > **Incident reporting** > **Configuration**.
2. Set the **Incident reports sending mode** to *On*.
3. Specify the **Incident reports URL** of the web service to which any error reports are to be sent. The default is `https://cc-reports.cisco.com/submitapplicationerror/`.
4. Optional. Specify a **Contact email address** that can be used by Cisco customer support to follow up any error reports.
5. Optional. Specify a **Proxy server** to use for the connection to the incident reporting server. Use the format (http|https)://address:port/ such as `http://www.example.com:3128/`.
6. Ensure that **Create core dumps** is *On*; this is the recommended setting as it provides useful diagnostic information.

Note If the **Incident reports sending mode** is *Off*, incidents will not be sent to any URL but they will still be saved locally and can be Viewing Incident Reports from the **Incident detail** page.

Sending Incident Reports Manually

Read the Incident Reporting Caution: Privacy-Protected Personal Data before you decide whether to send an incident report manually to Cisco.

To send an incident report manually to Cisco customer support:

1. Go to **Maintenance** > **Diagnostics** > **Incident reporting** > **View**.
2. Click on the incident you want to send. You will be taken to the **Incident detail** page.

3. Scroll down to the bottom of the page and click **Download incident report**. You will be given the option to save the file.
4. Save the file in a location from where it can be forwarded to Cisco customer support.

Removing Sensitive Information from a Report

The details in the downloaded incident report are Base64-encoded, so you will not be able to meaningfully view or edit the information within the file.

If you need to edit the report before sending it to Cisco (for example, if you need to remove any potentially sensitive information) you must copy and paste the information from the **Incident detail** page into a text file, and edit the information in that file before sending it to Cisco.

Viewing Incident Reports

The **Incident view** page (**Maintenance** > **Diagnostics** > **Incident reporting** > **View**) shows a list of all incident reports that have occurred since the Expressway was last upgraded. A report is generated for each incident, and the information contained in these reports can then be used by Cisco customer support to diagnose the cause of the failures.

For each report the following information is shown:

Field	Description
Time	The date and time when the incident occurred.
Version	The Expressway software version running when the incident occurred.
Build	The internal build number of the Expressway software version running when the incident occurred.
State	The current state of the incident: *Pending*: indicates that the incident has been saved locally but not sent. *Sent*: indicates that details of the incident have been sent to the URL specified in the Incident Reporting page.

To view the information contained in a particular incident report, click on the report's **Time**. You will be taken to the Incident Report Details page, from where you can view the report on screen, or download it as an XML file for forwarding manually to Cisco customer support.

Incident Report Details

The **Incident detail** page (**Maintenance** > **Diagnostics** > **Incident reporting** > **View**, then click on a report's **Time**) shows the information contained in a particular incident report.

This is the information that is sent to the external web service if you have enabled **Incident reports sending mode** (via **Maintenance** > **Diagnostics** > **Incident reporting** > **Configuration**). It is also the same information that is downloaded as a Base64-encoded XML file if you click **Download incident report**.

The information contained in the report is:

Field	Description
Time	The date and time when the incident occurred.
Version	The Expressway software version running when the incident occurred.
Build	The internal build number of the Expressway software version running when the incident occurred.
Name	The name of the software.
System	The system name (if configured), otherwise the IP address.
Serial number	The hardware serial number.
Process ID	The process ID the Expressway application had when the incident occurred.
Release	A true/false flag indicating if this is a release build (rather than a development build).
Username	The name of the person that built this software. This is blank for release builds.
Stack	The trace of the thread of execution that caused the incident.
Debug information	A full trace of the application call stack for all threads and the values of the registers.

Caution For each call stack, the Debug information includes the contents of variables which may contain some sensitive information, for example alias values and IP addresses. If your deployment is such that this information could contain information specific to a particular person, read the Incident Reporting Caution: Privacy-Protected Personal Data regarding privacy-protected personal data before you decide whether to enable automatic incident reporting.

Developer Resources

The Expressway includes some features that are intended for the use of Cisco support and development teams only. Do not access these pages unless it is under the advice and supervision of your Cisco support representative.

Caution Incorrect usage of the features on these pages could cause the system operation to become unstable, cause performance problems and cause persistent corruption of system configuration.

These features are:

- Debugging and System Administration Tools
- Experimental Menu

Debugging and System Administration Tools

Caution These features are not intended for customer use unless on the advice of a Cisco support representative. Incorrect usage of these features could cause the system operation to become unstable, cause performance problems and cause persistent corruption of system configuration.

The Expressway includes a number of debugging and system admin tools that allow administrators to inspect what is happening at a detailed level on a live system, including accessing and modifying configuration data and accessing network traffic.

To access these tools:

1. Open an SSH session.
2. Log in as admin or root as required.
3. Follow the instructions provided by your Cisco support representative.

Experimental Menu

The Expressway web interface contains a number of pages that are not intended for use by customers. These pages exist for the use of Cisco support and development teams only. Do not access these pages unless it is under the advice and supervision of your Cisco support representative.

Caution Incorrect usage of the features on these pages could cause the system operation to become unstable, cause performance problems and cause persistent corruption of system configuration.

To access these pages:

1. Go to `https://<Expressway host name or IP address>/setaccess`.

   The **Set access** page appears.
2. In the **Access password** field, enter `qwertsys`.
3. Click **Enable access**.

A new top-level **Experimental** menu will appear to the right of the existing menu items.

Enabling or Disabling CDB API Access

Considering the Security of the Expressway product, access to CDB API has been disabled by default. They can be enabled or disabled using the Web User Interface or through REST API. Enabling or Disabling of CDB API Access is implemented across the cluster.

Caution Enabling this feature provides access to numerous experimental Database Rest APIs with exposure to Security vulnerabilities. These are not intended for use on a production system. Use of this feature will be at your own risk.

CDB REST APIs are available in the **Experimental** menu -> **API** -> **DATABASE REST API**. Here the status of CDB REST API Access is displayed which is disabled by default.

Enable CDB API Access

In the **Experimental** menu -> **API** -> **DATABASE REST API** page, click **Enable CDB API Access**.

This will enable the CDB API Access (across the cluster if applicable).

Disable CDB API Access

In the **Experimental** menu -> **API** -> **DATABASE REST API** page, click **Disable CDB API Access**.

This will disable the CDB API Access (across the cluster if applicable).