



## Serviceability

---

Cisco VVB Serviceability provides configuration details for the following functionality:

- Configuring alarms for local and remote Syslogs.
  - Configuration trace settings for VVB components. After these settings are enabled, you can collect and view trace information using the Real-Time Monitoring Tool (RTMT).
  - Configuring and managing log profiles for different VVB components.
  - Managing and controlling network services.
  - Setting parameters for different platform services.
  - Setting Java Virtual Machine (JVM) parameters for different VVB services to collect thread and memory traces.
- 
- [Access Cisco VVB Serviceability, page 1](#)
  - [Alarms, page 1](#)
  - [Traces, page 4](#)
  - [Serviceability Tools, page 6](#)
  - [Simple Network Management Protocol, page 7](#)

## Access Cisco VVB Serviceability

Log in to Cisco VVB with the application user credentials configured during installation.

To access Cisco VVB Serviceability, log in to Cisco Unified VVB and from the navigation drop down select Cisco VVB Serviceability and Click the on the **Go** button.

## Alarms

You can view alarm information by using the SysLog Viewer in Cisco Unified Real-Time Monitoring Tool (RTMT). See “Real-Time Monitoring Tool” section for detailed information on how to view alarm information.

## Alarm Configuration

Use the **Alarm Configuration** web page in Cisco VVB Serviceability to view and configure alarm server settings for different Cisco VVB components.


**Note**

To find more information on the Alarm messages in the system, use **Alarm Definition** page in *Cisco Unified Serviceability*.

## Alarm Configuration Settings

Use the **Alarm Configuration** page to modify alarm settings.

Following table defines the options available on this page:

**Table 1: Alarm Configuration Settings**

Setting	Description
Enable Alarm for Local Syslogs	Enables the alarms to be stored as syslog messages locally. This setting can be viewed in the Application logs within Syslog viewer from the RTMT tool.  For information about viewing logs with the SysLog Viewer, see “Real-Time Monitoring Tool” topic.
Enable Alarm for Remote Syslogs	Enable the alarm messages to be sent to the configured Syslog server.  <b>Server Name</b> field - Provide the IP / hostname of the Syslog server to which the system should send the alarm messages.

Setting	Description
Alarm Event Level	<p>Alarm event level messages range from severity 0 (most severe) to severity 7 (least severe). See the description below for each alarm event level option. When you choose a severity level, all messages of that severity level and higher are sent.</p> <p>For example, if you choose ERROR_ALARM (Severity 3), all messages of severity 3, severity 2, severity 1, and severity 0 are sent. The default is INFORMATIONAL_ALARM (Severity 6), which will send messages on all severity levels starting from 6 to severity level 0.</p> <p>You can choose one of the following alarm event level options from the drop-down list box:</p> <p><b>Emergency</b></p> <p>Systemic failures causing the whole Contact Center to be down. For example, "Cisco VVB engine crashed or went down abruptly".</p> <p><b>Alert</b></p> <p>Multiple components failures on the system. For example, "Telephony and RCM subsystem out of service due to CTI provider failure".</p> <p><b>Critical</b></p> <p>Failures in the Major component of the system. For example "Web chat subsystem out of service".</p> <p><b>Error</b></p> <p>Functionality or certain scenario not working as expected. For example, "Create dialog group failed".</p> <p><b>Warning</b></p> <p>Some limits or threshold about to be breached. For example, "Historical reporting internal queue near capacity".</p> <p><b>Notice</b></p> <p>Trigger of major operation notification. For example, "Engine Shutdown initiated by Administrator"</p> <p><b>Informational</b></p> <p>Information about various minor event occurrences in the system. For example, "Backup Operation completed".</p> <p><b>Debug</b></p> <p>Detailed traces which help in debugging issues. For example, detailed information on some Cisco VVB events.</p>

# Traces

A trace file is a log file that records activity from the Cisco VVB components. Trace files provide detailed information about specific errors and help you troubleshoot the errors.

The Cisco VVB system also generates information about all threads that are running in the system. This information is stored in the thread dump file and is useful for troubleshooting.

## Component Trace Files

The component trace file contains information about each component. You can create a trace file for any of the following Cisco VVB components:

- Administration
- Engine

## Configure Trace Parameters

To update trace file information and to activate and deactivate logging, follow this procedure:

### Procedure

- Step 1** From the Cisco VVB Serviceability menu, choose **Trace > Configuration**.
- Step 2** From the **Select Service** drop-down list box, choose a service or component for which you want to configure trace. Then click **Go**.  
The debug levels for different Cisco VVB subfacilities or services that are displayed may vary depending on the selected service.
- Step 3** Update the debug level for one or more of the libraries or subfacilities for the selected service using the check box provided and click **Save**.
- Step 4** To limit the number and size of the trace files, you can specify the trace output setting using the following table.

Field	Description
Maximum Number of Files	<p>The maximum number of trace files that can be retained by the system.</p> <p>This field specifies the total number of trace files for a given service. Cisco VVB Serviceability automatically appends a sequence number to the file name to indicate which file it is, for example, Cisco001MADM14.log. When the last file in the sequence is full, the trace data begins writing over the first file. The default value varies by service.</p>

Field	Description
Maximum File Size	This field specifies the maximum size of the trace file in kilobytes depending on the selected service. The default value varies according to the service you select.

**Caution** You should activate additional logging *only* for debugging and remember to *deactivate* logging once the debugging session is complete.

---

## Trace Level Options

A trace file that records all information for a component, such as the Cisco VVB Engine, can become large and difficult to read. To help you manage the trace file, the Cisco VVB system lets you specify the subfacilities for which you want to record information using Trace Level Options page.

For each component, you can select one or more Debugging trace level options. The selections in the Trace Level page specify the level of details in the debugging messages that the system sends to a trace file. For instance, if you select Debugging option, the system sends only the basic error messages, while if you select XDebugging5 option, the system will send errors, warnings, informational, debugging, verbose messages and so on in detail to the trace file.

## Trace File Location

You can collect and view trace information using the Real-Time Monitoring Tool (RTMT).

### Trace File Information

The trace files contain information in standard Syslog format. The file includes some or all of the following information for each event that is recorded:

- Line number
- Date and time the event occurred
- Facility and subfacility (component) name
- Severity level
- Message name
- Explanation
- Parameters and values

## Log Profiles Management

Log profile is an aggregated entity that preserves multiple trace settings of the following Cisco VVB services:

- Cisco VVB Engine (Traces termed as MIVR)
- Cisco VVB Administration (Traces termed as MADM)
- Cisco VVB Cluster View Daemon (Traces termed as MCVD)

Choose **Trace > Profile** from the Cisco VVB Serviceability menu to access the **Log Profiles Management** page.

Log profiles in Cisco VVB can be one of the following two types:

- 1 System Log Profiles: These log profiles are preinstalled with Cisco VVB, and you cannot modify these profiles.
- 2 Custom Log Profiles: If the trace settings generated by system profiles are not sufficient in a particular scenario, you can create custom log profiles for better troubleshooting. You can create and enable these custom log profiles as needed.

**Note**

You cannot delete the profile if the selected log profile is the last-enabled profile in the system.

## Serviceability Tools

### Network Services

Network services include services that the system requires to function and are activated by default.

After you install your application, network services start automatically.

### Manage Network Services

Control Center in Cisco VVB Serviceability lets you perform the following tasks:

- Start, stop, and restart Cisco VVB services
- View and refresh the status of Cisco VVB services

Choose **Tools > Control Center - Network Services** from the Cisco VVB Serviceability menu to manage network services.

**Tip**

You may need to manage services in both Cisco VVB Serviceability and Cisco Unified Serviceability to troubleshoot a problem. The Cisco Unified Serviceability services are described in the *Cisco Unified Serviceability Administration Guide*.

**Note**

You cannot start or stop Cisco VVB Serviceability service using the Cisco VVB Serviceability web interface and you need to use CLI. For a list of services that you can start and stop using the CLI and for detailed instructions, see “Command Line Interface Reference” section.

## Configure Performance Monitoring of Cisco VVB Servers

Use the Performance Configuration and Logging page to configure Java Virtual Machine (JVM) parameters and dump Thread and Memory traces for performance monitoring of Cisco VVB servers.

Use the following procedure to configure JVM parameters for a particular service on a particular server.

### Procedure

- Step 1** Choose **Tools > Performance Configuration and Logging** and select the server and a service for which you want to get the JVM options.
- Step 2** Click **Dump Thread Trace** to dump the thread traces for the selected service in the selected server. You can collect the corresponding `jvm.log` from the log folder for that facility using Real-Time Monitoring Tool (RTMT).
- Step 3** Click **Dump Memory Trace** to dump the memory traces. This creates the following two logs in the log folder for that facility.
  - Memory-<facility name>-<time stamp>.hprof (for heap dump)
  - histo-<facility name> <time stamp>.log (for histogram)
- Step 4** Click **Enable** or **Disable** radio buttons in this page to change the JVM options.
- Step 5** Click **Update JVM Options** to update the new settings for selected service on selected node.

## Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an industry-standard interface for exchanging management information between network devices. SNMP enables you to monitor and manage the Cisco VVB system. You also can set up SNMP traps to automatically notify any high-severity messages and errors that are generated by the Cisco VVB system.

You can configure the SNMP settings using the **Cisco Unified Serviceability** web interface.

## SNMP Management Information Base (MIB)

A Management Information Base (MIB) designates a collection of information that is organized hierarchically. MIBs are made up of managed objects, which are referenced by object identifiers. Managed objects are made up of one or more object instances, which are essentially variables. MIBs provide status monitoring, provisioning, and notification.

**Table 2: SNMP MIBs**

MIB	Agent Service
CISCO-VOICE-APPS-MIB	Cisco VVB Voice Subagent
CISCO-CDP-MIB	Cisco CDP Agent
CISCO-SYSLOG-MIB	Cisco Syslog Agent
SYSAPPL-MIB	System Application Agent
MIB-II	MIB2 Agent
HOST-RESOURCES-MIB	Host Resources Agent

**Note**

- In Cisco VVB, the SysAppl MIB will not provide the Cisco VVB subsystem information and their status information. You can view the subsystem and their status information through Cisco VVB Serviceability web interface.
- Syslog messages can also be sent as SNMP traps using the CISCO-SYSLOG-MIB. Refer to the section on CISCO-SYSLOG-MIB for details. They can be correlated to the failure of important features of Cisco VVB.

The following section describes CISCO-VOICE-APPS-MIB. For more information about other Cisco VVB supported MIBs, see **Cisco Unified CM SNMP** chapter in the *Cisco Unified Serviceability Administration Guide* available here:

[http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/prod_maintenance_guides_list.html)

**CISCO-VOICE-APPS-MIB**

The CISCO-VOICE-APPS-MIB provides information associated with the installed workflow applications provisioned on the Cisco VVB Server. It also provides information on the supported SNMP Traps on Cisco VVB. You can manage CISCO-VOICE-APPS-MIB through **Cisco VVB Serviceability** web interface.

**Cisco VVB Voice Subagent**

Cisco VVB Voice Subagent service implements the CISCO-VOICE-APPS-MIB. Cisco VVB Voice Subagent Service communicates with the SNMP Master Agent through Cisco VVB SNMP Java Adaptor. The Cisco VVB SNMP Java Adaptor service should be up and running for the Cisco VVB Voice Subagent to work properly.

For more information about the CISCO-VOICE-APPS-MIB, see this URL: <ftp://ftp.cisco.com/pub/mibs/v2/CISCO-VOICE-APPS-MIB.my>.



**Note**

- In Cisco VVB, while exposing the Cisco VVB workflow information through CISCO-VOICE-APPS-MIB, only one trigger per application row will be returned when doing a walk on the workflow table (cvaWorkflowInstallTable object). If there are multiple triggers associated with a Workflow application, these are shown as separate entries (rows).

**SNMP Traps**

Subsystems, which are the functional blocks of Cisco VVB, sends out alarms that are routed to the Syslog or as SNMP Traps. SNMP Traps are generated when any Cisco VVB Subsystem or module or processes start or stop or runtime failure occurs for a module. These failures can be tracked for each major component to track the health of the Cisco VVB system.

The following Traps are supported as part of the CISCO-VOICE-APPS-MIB:

Trap Name	Description
cvaModuleStart	A cvaModuleStart notification signifies that an application module or subsystem has successfully started and transitioned into in-service state.
cvaModuleStop	A cvaModuleStop notification signifies that an application module or subsystem has stopped. If cause of the failure is known then, it will be specified as part of the Trap message.
cvaModuleRunTimeFailure	cvaModuleRunTimeFailure notification signifies that a run time failure has occurred. If cause of the failure is known then it will be specified as part of the Trap message.
cvaProcessStart	A cvaProcessStart notification signifies that a process has just started.
cvaProcessStop	A cvaProcessStop notification signifies that a process has just stopped.

The ModuleStart and ModuleStop traps are generated when the key Cisco VVB services including Cisco VVB Engine, Cisco VVB Cluster View Daemon and, Cisco VVB Administration and their modules/subsystems are started and stopped respectively.

The ProcessStart and ProcessStop traps are generated when the key Cisco VVB services including Cisco VVB Engine, Cisco VVB Administration are started and stopped.

You can configure the notification destinations by using the **SNMP Notification Destination Configuration** page in Cisco Unified Serviceability.

**Note**

SNMP Traps are not generated for events when the Cisco VVB services and/or their subsystems go Out of Service or are In Service. These events are sent as Remote Syslog messages and can be viewed through any third-party Syslog Viewers. You can refer to the list of Cisco VVB services and their subsystems/modules from the Cisco VVB Serviceability under **Tools > Control Center Network Services**.

**Note**

- Cisco VVB does not support SNMP trap V3 notifications.
- CISCO-VOICE-APPS-MIB does not support INFORM notifications.

For all notifications, the system sends traps immediately if the corresponding trap flags are enabled. Before you configure notification destination, verify that the required SNMP services are activated and running. Also, make sure that you configured the privileges for the community string or user correctly.

## More Info on SNMP

For more information related to SNMP such as SNMP Version 1, Version 2C, Version 3, SNMP system group configuration, SNMP informs and SNMP trap parameters, see *Cisco Unified Serviceability Administration Guide* available here:

[http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/prod_maintenance_guides_list.html)