Audit Logging

The VPT audit logs provide a record of activity on the system, including information about who performed an action and when he or she performed it. Audit log entries are generated for login and logout attempts, provisioning operations, configuration changes, and the startup and shutdown of the VPT application.

This chapter contains the following information:

Audit Log Information

Each audit log file starts with a header row that contains a comma-separated list of field names, followed by a row for each audit entry. Table 6-1 lists the fields that display in the log and a description of the content that is logged for each field.

Table 6-1 Audit Log Field Descriptions

Field	Description
Task ID	An alphanumeric identifier, which can be used to correlate multiple operations when a particular task (such as adding a new user) involves multiple back-end operations (such as adding the user profile on a Cisco CallManager server and adding the subscriber account on a Cisco Unity server).
Task Name	The name of the high-level task to which the operation belongs (for example, Add User).
Event ID	An alphanumeric identifier, which can be used to correlate multiple audit log events, if a particular back-end operation generates multiple events before completing.
Date/Time	The timestamp at which the audit record was generated.
Event	The name of the back-end operation or the type of the event being logged.
Product System(s)	The name(s) of the product system(s) on which the task was executed.

Table 6-1 Audit Log Field Descriptions (continued)

Field	Description
Outcome	The outcome of the operation or event. The possible values follow: • Initiated—A back-end operation began execution. • Completed—A back-end operation finished execution. • Success—The event or operation completed successfully. • Failure—The event or operation did not complete successfully.
Severity	Indicates whether the event or outcome that occurred is normal (an expected event or outcome) or severe (an error condition). Severe events also are logged in the Windows application event log.
Admin	The admin ID of the administrator who requested or performed the operation.
Data	A detailed listing of the data involved in an operation or event. This field usually contains a list of attribute-value pairs that are involved in the operation. Sensitive information such as passwords and PINs are not recorded. If no relevant data is involved, this field stays empty.
Remarks	Any additional information relevant to understanding the outcome of the operation—for example, when an "Add User" operation fails, this field may include further information, such as "Product System not responding."

In the following example, the superadmin adds a user with the alias kbader as a subscriber on the Cisco Unity server c-unity1 and as a user on the Cisco CallManager server c-callmanager1. In this example, you can see that the task ID, E97BEB7A-D04E-E5AB-3656-D931B92DF18A, remains the same throughout the Add User Task operation; however, the entire operation requires a series of individual steps on each product system, which can be linked together based on the event ID.

```
E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
Task,BB9655AB-107F-A888-9274-4E7A2BC06933,Thu Jun 09 12:51:03 EDT 2005,Get System
Dependent User Task Data,c-unity1,Initiated,Normal,superadmin,,,

E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
Task,BB9655AB-107F-A888-9274-4E7A2BC06933,Thu Jun 09 12:51:04 EDT 2005,Get System
Dependent User Task Data,c-unity1,Success,Normal,superadmin,
[Message System = c-unity1],,

E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
Task,BB9655AB-107F-A888-9274-4E7A2BC06933,Thu Jun 09 12:51:04 EDT 2005,Get System
Dependent User Task Data,c-unity1,Completed Successfully,Normal,superadmin,,,

E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
Task,03BCB50E-2C3C-713C-4258-C049251139C7,Thu Jun 09 12:52:30 EDT 2005,Add
User,c-callmanager1;c-unity1,Initiated,Normal,superadmin,,,

E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
Task,03BCB50E-2C3C-713C-4258-C049251139C7,Thu Jun 09 12:52:30 EDT 2005,Add
User,c-callmanager1,Success,Normal,superadmin,[First Name = Kelly]
[Locale = English UnitedStates] [Default Profile = ] [Telephone No. = ]
[User ID = kbader] [Last Name = Bader] [Primary Extension = ]
[Call Park Retrieval = false] [Calling Party Number Modification = false]
[Authentication Proxy = false] [Manager's User Id = ] [CTI Application Use = false]
[Dept. = Marketing] ,,

E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
```

```
Task,03BCB50E-2C3C-713C-4258-C049251139C7,Thu Jun 09 12:52:39 EDT 2005,Add
User,c-unity1,Success,Normal,superadmin,[Message Extension = 3003]
[First Name = Kelly] [Exchange Server = c-exch1] [Fax Id = ]
[Display name = Kelly Bader] [User ID = kbader] [Message System = c-unity1]
[Subscriber Type = unity_user_subscriberTypes_exchange] [Last Name = Bader] ,,

E97BEB7A-D04E-E5AB-3656-D931B92DF18A,Add User
Task,03BCB50E-2C3C-713C-4258-C049251139C7,Thu Jun 09 12:52:40 EDT 2005,Add
User,c-callmanager1;c-unity1,Completed Successfully,Normal,superadmin,,,
```

Audit Log File Storage

The Cisco Voice Provisioning Tool automatically controls the size and number of audit log files that are stored for the tool based on configurable audit log settings. If your account has sufficient permissions, you can configure the location of the logs; you can also control the total amount of disk space that can be taken up by the logs and the number of backup log files that should be kept. The log files automatically roll over based on these two parameters.

For example, if you set the total disk space allowed for the logs to 5 MB, and you set the number of backup files to 4, then an individual audit log file will be written until it reaches 1 MB (5 MB divided by 5 possible files) in size; at that point, a new log file will be created, and the old file will be renamed AuditLog.csv.1. Each time the audit log reaches 1 MB, a new file will be opened, and the file names of the old logs will be renumbered from newest (.1) to oldest (.4). When four backup files are saved, and the total disk space taken up by the current file and the four backup files reaches 5MB, the oldest file is deleted, and once again, a new file will be opened, and the older backup files will be renumbered.

Configuring Audit Log Settings

You can configure the parameters that control where and how audit logs are stored via the VPT administrative interface.

Note To configure audit log settings, your administrator account must belong to a role that has Audit Log Modify permissions for the VPT application. If you do not see the VPT Administration > Configuration option in the VPT navigation menu, your account does not have the applicable permissions.

To Configure Audit Log Settings

Step 1 In the Cisco Voice Provisioning Tool, choose **VPT Administration > Configuration**.

The Configuration window displays.

Step 2 In the Audit section, enter the **Audit Log Location**.

Specify the full path to the directory where audit logs will be stored. The directory must already exist and should reside on the VPT server (you should not specify a network drive or path to a directory on another server).

Step 3 Enter the **Total Disk Space for Audit**.

This total specifies the maximum disk space (in megabytes) that can be in use by all audit log files. When audit log information exceeds this size, the oldest audit log file is removed, and a new file is created.

Step 4 Enter the **Number of Audit Backup Files**.

This number specifies the maximum number of backup audit files to create. Enter a value from 1 to 99. An audit log will be written until it reaches a size equal to the total disk space for audit logs divided by the total possible number of audit files (the current log file plus the backup files). At this point, a new audit log file is created. When all audit log files are full, the oldest file is removed and a new file is created.

Step 5 Click **Save**.

Accessing Audit Logs

Note To access audit logs through the VPT Administrator interface, your administrator account must belong to a role that has Audit Log Access permissions for the VPT application. If you do not see the VPT Administration > View Audit Log option in the VPT navigation menu, your account does not have the applicable permissions.

To Access Audit Logs

Step 1 In the Cisco Voice Provisioning Tool, choose **VPT Administration > View Audit Log**.

The View Audit Log window displays a list of audit log files that are currently stored on the system, the time when each file was last updated, and the size of each file in bytes.

Step 2 Click the name of the audit log that you want to view.

Depending on your browser settings, you may be prompted to open or save the file, or the browser may launch an external viewer. All audit logs are stored in comma-separated value (CSV) format. Using an external viewer or application, you can view, sort, or filter the audit log after downloading it.