6UCSCG0002-29A
September 2010

ADTRAN

Configuration Guide

Using Logs in the NetVanta UC Server

This guide describes the use of logs in the NetVanta Unified Communications (UC) Server system. Logs are accessed through the UC server graphical user interface (GUI) and can be used to track activity and detect problems on the UC server system. Included in this guide is an overview of the UC server logging system, how to access and manage different log types, and how to use logs for troubleshooting purposes. This guide covers logs in all NetVanta UC Server versions, as well as in the Personal Assistant (PA) and Personal Business Assistant (PBA) clients.

This guide consists of the following sections:

Introduction to the NetVanta UC Server Logs

Each NetVanta UC Server edition, and each NetVanta UC Client, has the ability to track and record events that occur within the UC server system. In the UC server administration application, logs are generated to track and record events that occur on managed trunks and user extensions. In the PA and PBA server clients, logs are generated to record events that happen while the client application is enabled on the PA or PBA user's extension. These logs can be viewed, stored for future reference, used for tracking activity, and used to troubleshoot occasional problems. Logs can also be exported as a tab-separated or XML-based file, or used by other reporting applications to provide historical reports. Five types of logs exist in the UC server: audit logs, events log, system errors and warnings logs, sent items logs, and received calls logs. The different log types are described in the following section.

Audit Logs

Audit logs are used by the administrator to track other administrator activity. These logs provide a record of administrative changes made in the software, and keep track of the date and time the changes were made, the author of the changes, the IP address from which the changes were made, the type of changes that were made, and the item(s) that were changed. These logs are useful in maintaining the UC server system and provide an activity trail when changes are made to the system by multiple administrators.

Events Log

The events log tracks information related to mailbox management. These logs track voicemail access and user voicemail management, including every access to the voicemail box and voicemail messages sent by both the UC server and other users. Events logs also contain a message count table and a summary of operations table. These tables are used to monitor the message summary and summary of operations done by all users on the system that are managing their mailboxes. Each PA/PBA user can also view these tables for themselves and for the users they manage.

System Errors and Warnings Logs

System error and warning logs are used to track information that is useful for troubleshooting call answering problems. Errors and warnings occur in instances where the UC server encounters a problem; for example, if the UC server is unable to deliver a message, it generates an error or warning message that includes information about the problem and alerts the administrator of the problem. When an error or warning message occurs, users are notified by an orange bar that appears at the bottom of the UC server GUI. This orange bar is an alert that a problem has been detected and some action may be required, and the alert must be acknowledged for the bar to disappear. In addition to creating a message in the UC server when there is a system error or warning, and notifying the user, the UC server also creates an entry in the Microsoft® Windows® events log to indicate the problem. Error and warning logs thus provide a method for administrators and users to troubleshoot and detect problems within the UC server call answering system.

Sent Items Logs

Sent items logs are logs that track information on outgoing faxes and events related to the use of the pager notification and message delivery. These features are configured using the Notify Pager and Deliver Messages elements in the UC server call service, and the sent items logs record information about each message delivery attempt in order to monitor the function of these two elements. Whenever a message

delivery is attempted, it is recorded in the log along with such information as the date and time of the delivery attempt, the phone number dialed, the port used, and the final outcome of the delivery attempt. This information is useful in monitoring call service configuration for both administrators and PA/PBA users.

Received Calls Logs

Received calls logs track incoming calls regardless of whether the UC server answered them or not. Information included in these logs is the caller's name and phone number, the date, time, and length of the call, whether the call was answered, the port used for the call, and whether a message was left . These logs also aid administrators and PA/PBA users in tracking the use of the UC server call answering system.

Hardware and Software Requirements and Limitations

The audit logs feature was introduced in the NetVanta UC Server version 4.6. Audit logs are only available to the administrator; all other logs are available for both administrators and PA/PBA users.

Audit logs track information for a user-configurable amount of time. The audit log cannot be cleared past the minimum amount of time that the information is collected. In addition, when audit logs are cleared, that action is also recorded in the audit log.

Message count tables (for events logs) are enabled by configuring message summary during voice mailbox management. If message summary is skipped during mailbox management, the message count table is not displayed.

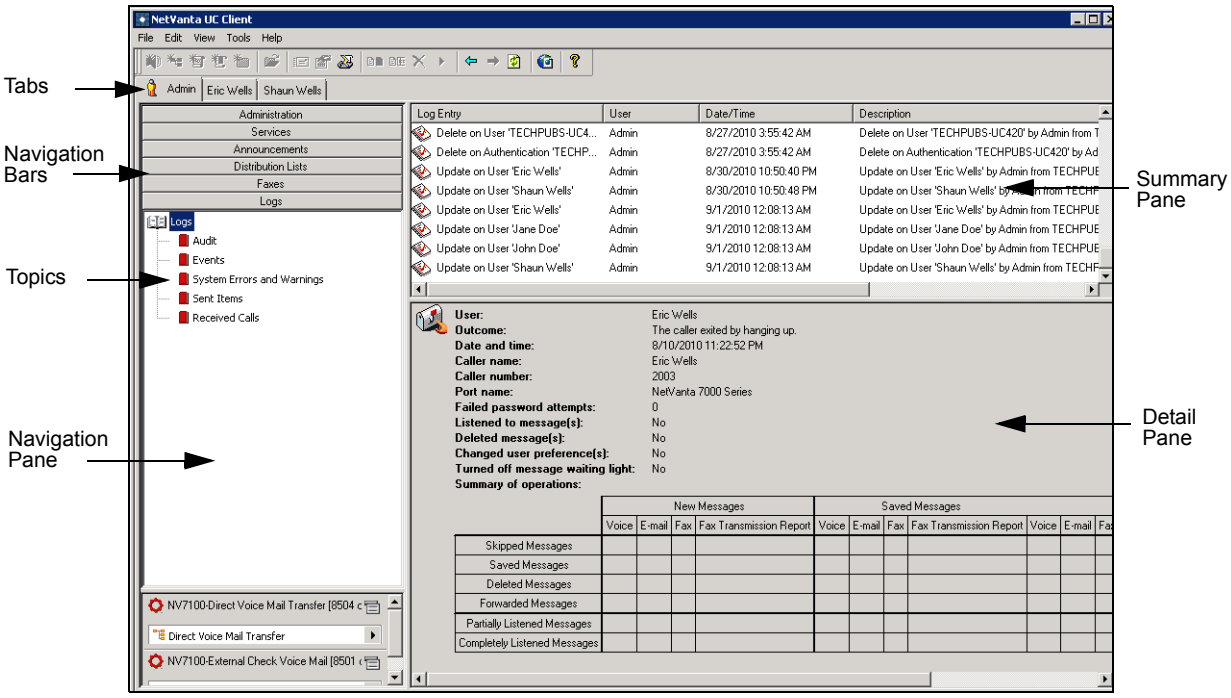
Users must acknowledge error and warning notifications. System errors and warnings log entries cannot be archived or cleared until all errors and warnings are acknowledged.

Users can create custom alerts in the Microsoft Windows Small Business Server (SBS) 2008. This simplifies management so that administrators need not have the NetVanta UC Client open to be aware of error or warning messages. When the UC server is installed on Windows SBS 2008, custom alerts are automatically configured for the SBS 2008 console. If the UC server is not installed on the SBS 2008 system, consult Microsoft documentation for information on creating custom alerts.

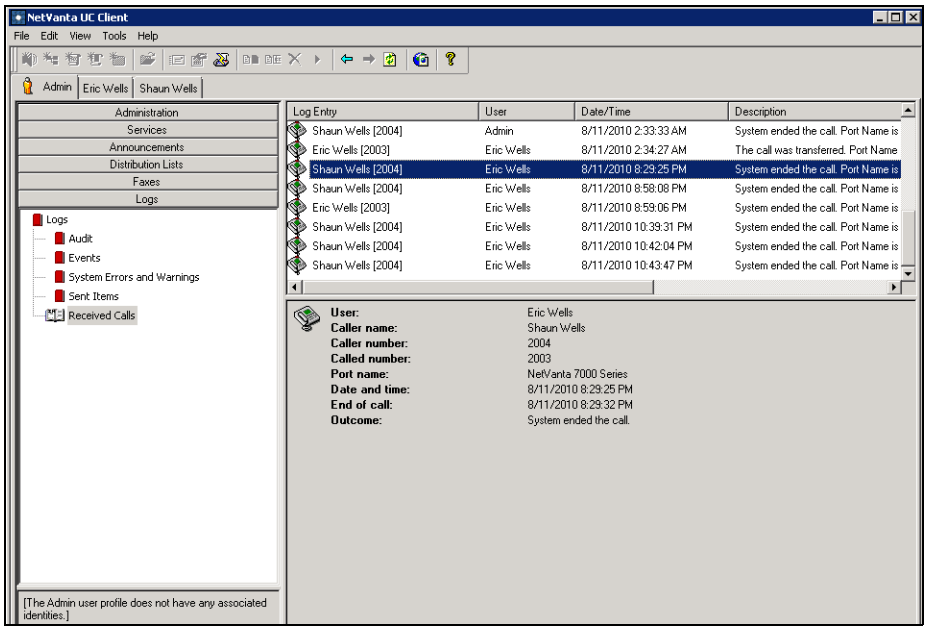
Accessing and Viewing Logs

All logs are available in the **Logs** navigation pane of the NetVanta UC Client. To access and view available logs, follow these steps:

1. Log into the UC server and select the **Logs** navigation bar to access the **Logs** navigation pane.



2. Select the appropriate log from the list in the **Logs** navigation pane. You can select **Events**, **System Errors and Warnings**, **Sent Items**, and **Received Calls** logs if you are a PA/PBA user, and you can additionally select **Audit** logs if you have logged into the system as an administrator. Highlighting the appropriate log type in the list populates the summary pane with each action instance recorded in the log. Selecting an entry in the summary pane provides details for the entry in the detail pane. In the following example, the **Received Calls** log entries are displayed.

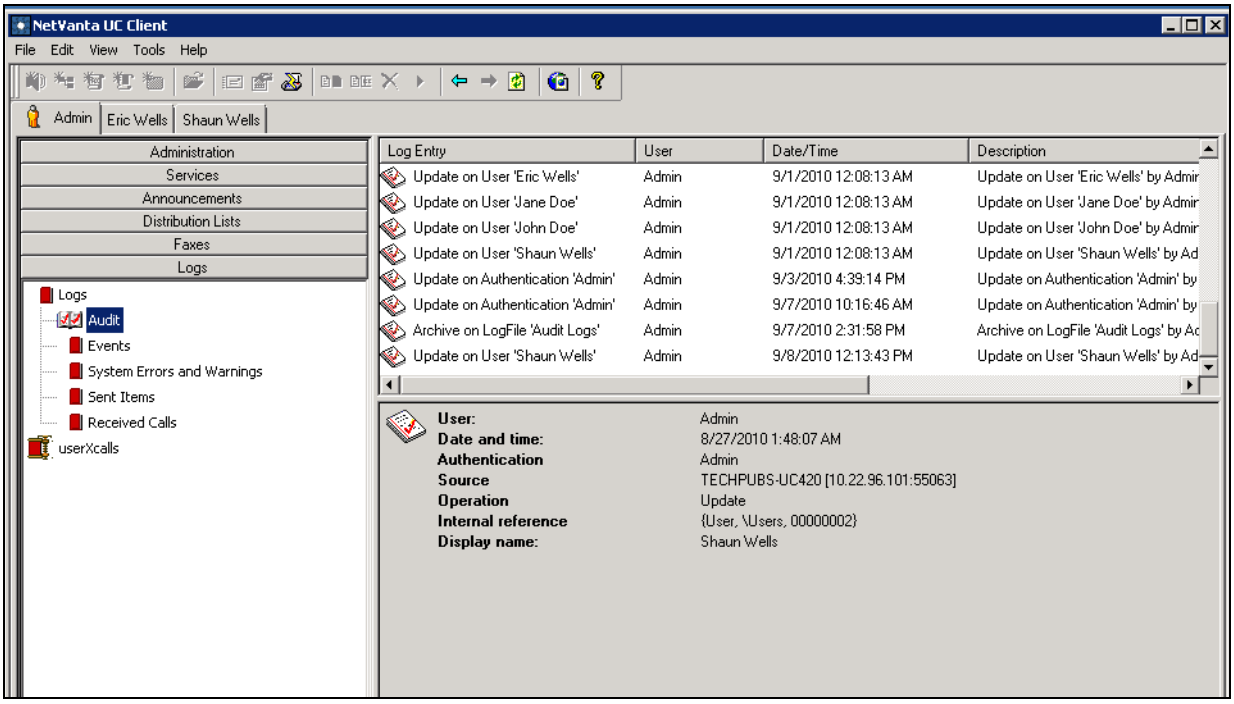


Detailed Log Information

Each type of log gives you different information about the operation and configuration of the UC server system. The following sections outline the specific information collected by each log type and give examples of each.

Audit Log

The audit log provides tracking for administrative actions. Each administrative action is recorded, and in the record is included the date and time of the action, the authenticated identity (user) performing the action, the source of the authenticating login (IP address, reverse Domain Naming System (DNS) lookup, etc.), the action performed, and the object that received the action. The following illustration includes detailed information about audit log records and displays typical auditing information.



Events Logs

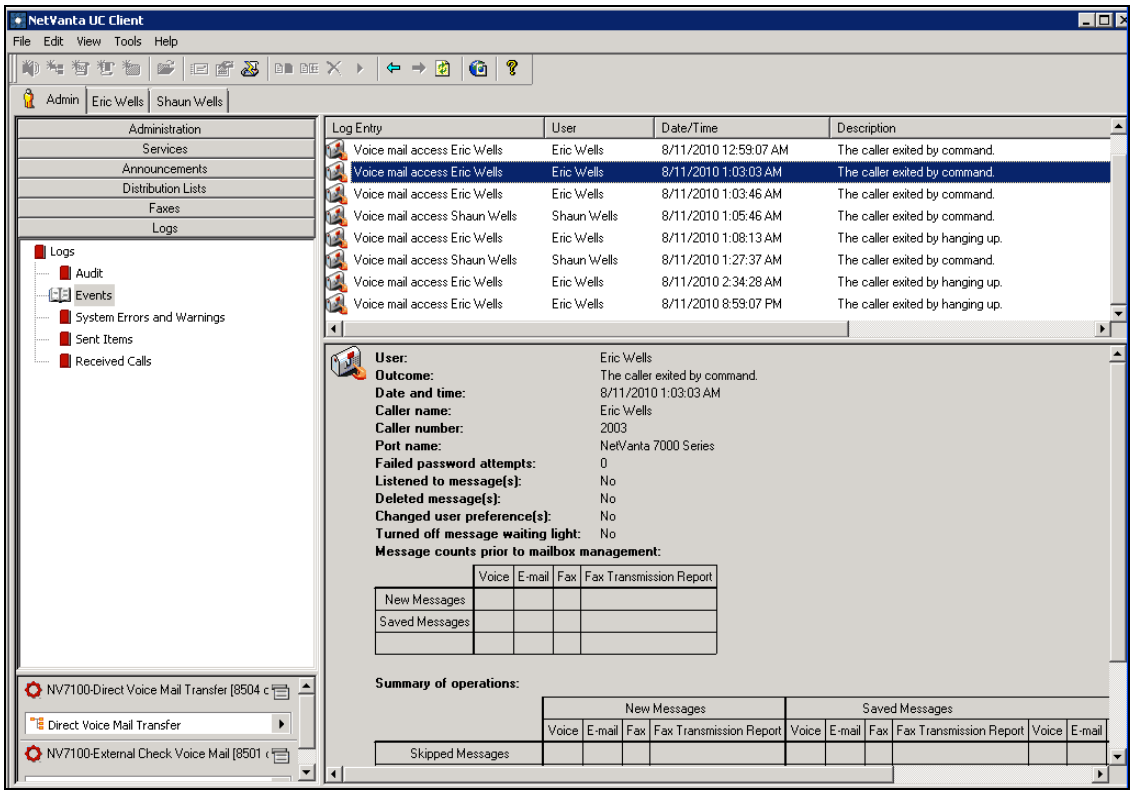
Events logs are used to track system events and user mailbox management. Each event recorded includes an entry describing the event itself (for example, “voicemail access by User X”), the user involved, the date and time of the event, and a brief description of the event outcome (for example, “the caller exited by hanging up”). Also included in the description of the entry are the caller’s name and number, the port, the number of failed login attempts, and any mailbox management actions taken.

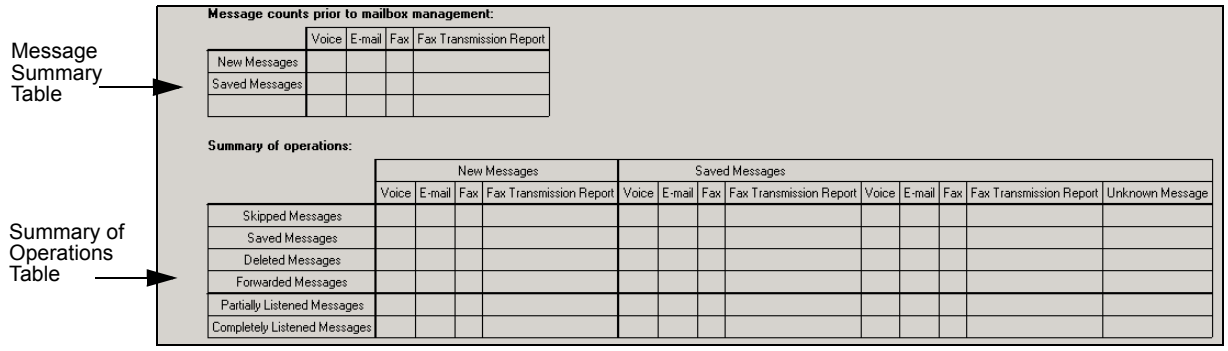
In addition, events logs generate two tables that include mailbox management statistics for each user. The **Message Summary** table includes the number and types of messages for the user, and the **Summary of Operations** table includes message actions, as well as the number and types of both saved and new messages for the user.

NOTE

Message count tables are enabled by configuring message summary during voice mailbox management. If message summary is skipped during mailbox management, the message count table is not displayed.

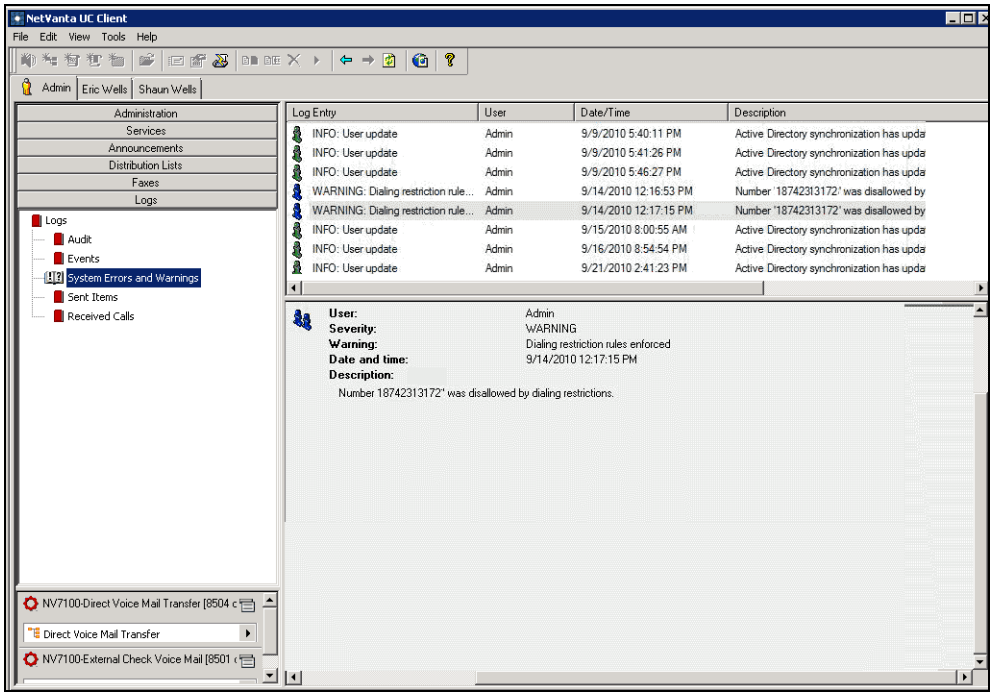
The following illustrations display the events log, the detailed log entry information, and examples of the **Message Summary** and **Summary of Operations** tables from the detail pane.





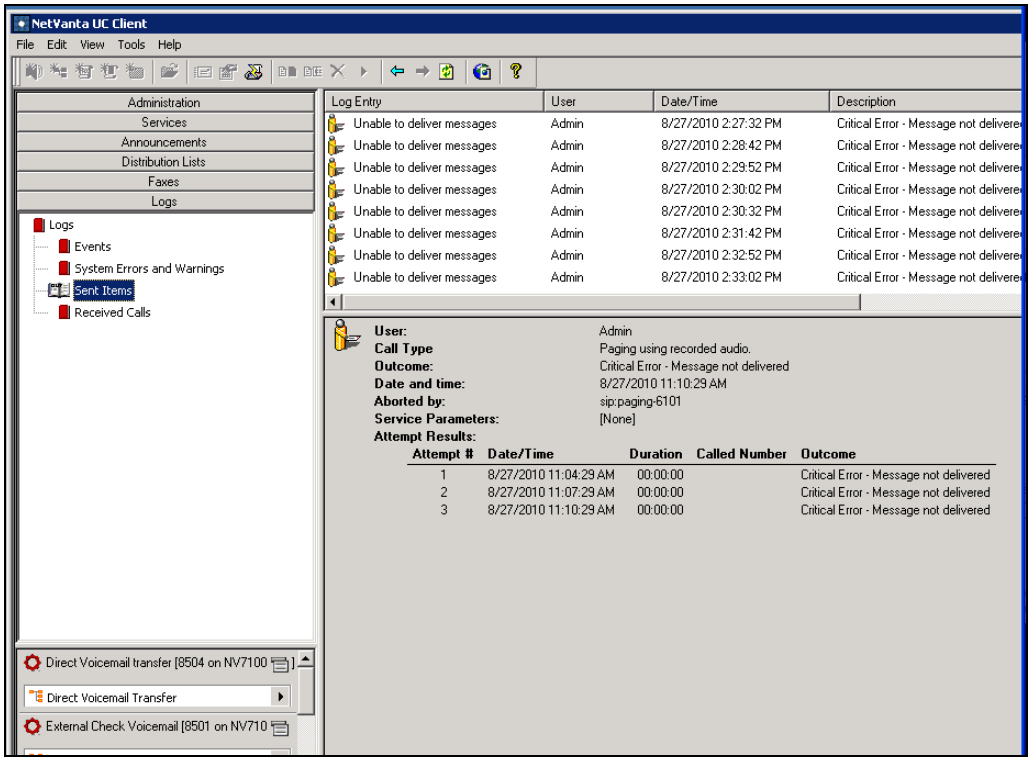
System Errors and Warnings Log

System errors and warnings logs provide significant information related to the overall health of the UC server call answering system. Each log entry records the event that occurred, the user involved, the date and time of the occurrence, and a description of the event. In addition, system log entry details also provide port information along with other specifics related to the individual error or warning. The following illustration displays the errors and warnings log.



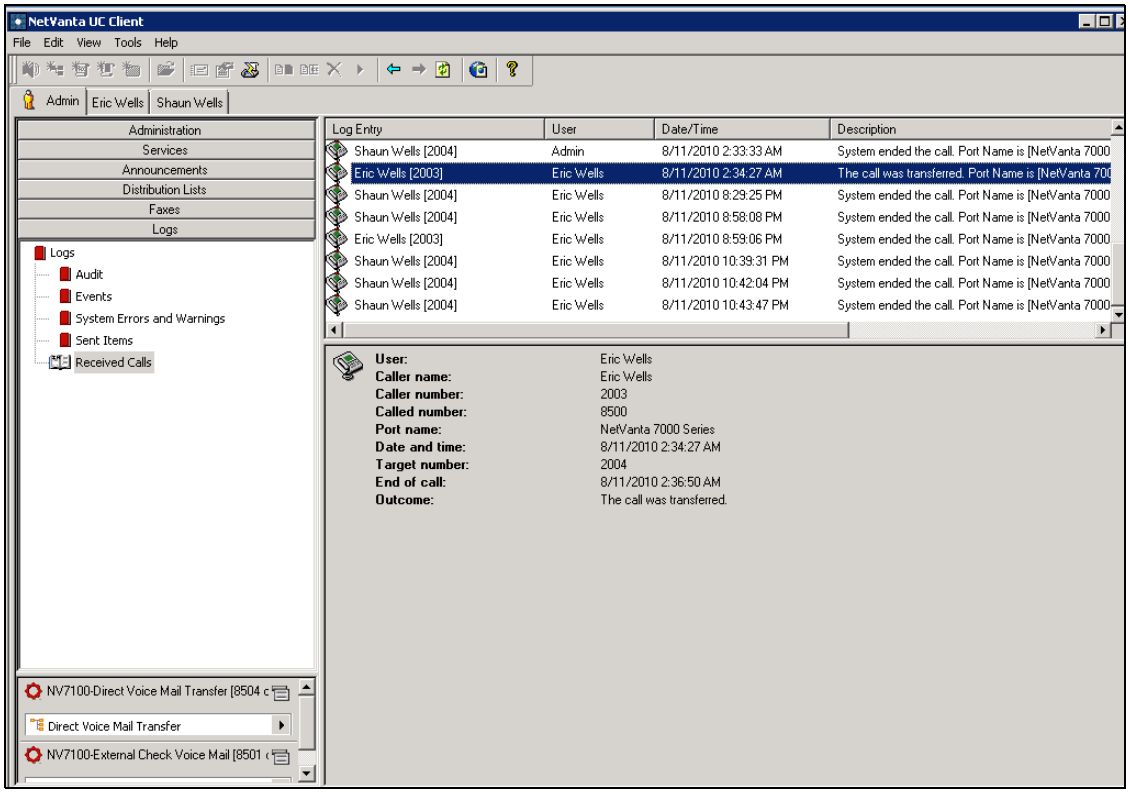
Sent Items Log

Sent items logs are useful in discovering where problems might have occurred in the delivery path of UC server messages. These logs track each outgoing message, whether it is a fax, pager, or voicemail message. Included in these logs are the type of event that occurred, the user involved, the date and time of the occurrence, and a description of the event.The following illustration displays the information typically recorded by the sent items log.



Received Calls Log

The received calls log tracks all incoming calls and gathers information, including the caller's name and phone number, the date, time, and length of the call, whether or not the call was answered, which port was used, and whether or not a message was recorded. These logs can be beneficial in monitoring the UC server's ability to receive and process calls. The following illustration includes the typical information recorded in the received calls log.



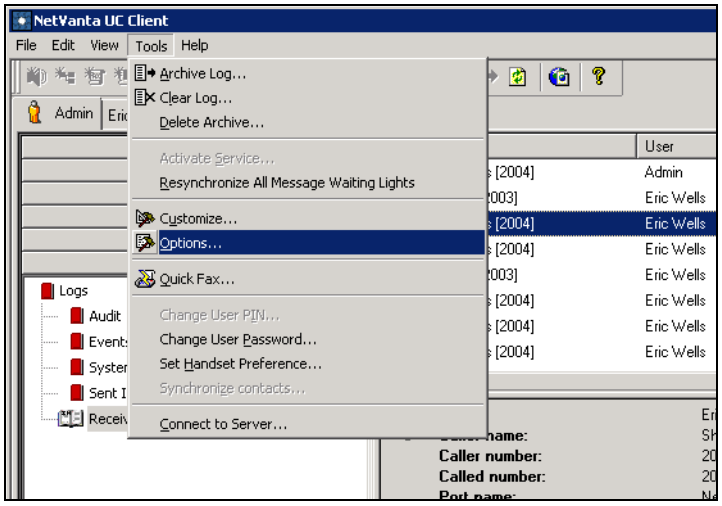
Managing Logs

There are a number of ways logs can be used and managed in the UC server. The following sections discuss basic tasks involved in managing the way logs are recorded and displayed on your UC server system.

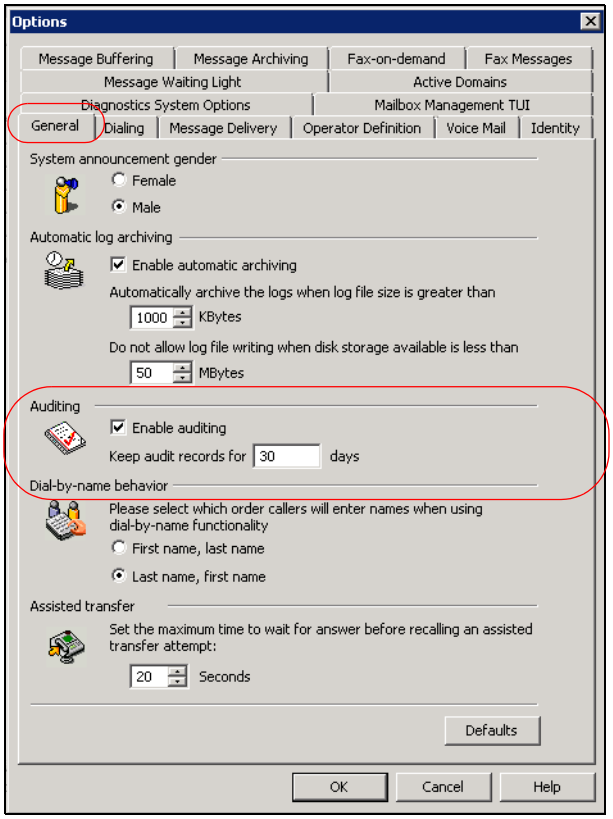
Configuring Audit Logs

Audit logs can be configured by the system administrator to track all administrative actions in the UC server system. These logs can be enabled or disabled, and configured to store collected information for a specified minimum number of days. To configure the auditing log options, follow these steps:

1. Log into the UC server as the administrator. Connect to the UC client and navigate to the **Admin** tab. Next, select **Tools** from the tool menu and select **Options** from the drop-down menu.



2. In the **Options** dialog box, select the **General** tab.



In the **Options** menu, you can enable and disable auditing logs by selecting (or clearing) the checkbox next to **Enable auditing**. In addition, you can specify for how many days records are kept. By default, audit logs keep information for **30** days; however, the valid range is **1** to **9999** days.

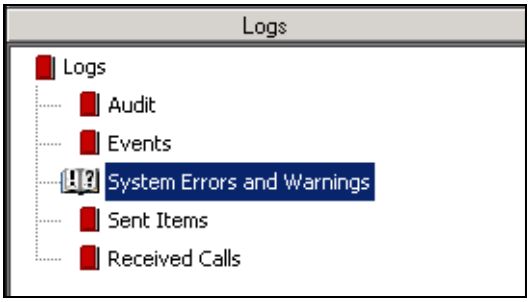
> *When you clear audit logs, you cannot clear the log past the number of days specified here. For example, if records are kept for 15 days, you cannot clear the past 20 days of auditing information. In this case, you could only specify that 15 days of records are cleared.*

3. Once you have enabled auditing and specified the number of days auditing records are kept, select **OK** in the **Options** menu. Audit logs are now configured.

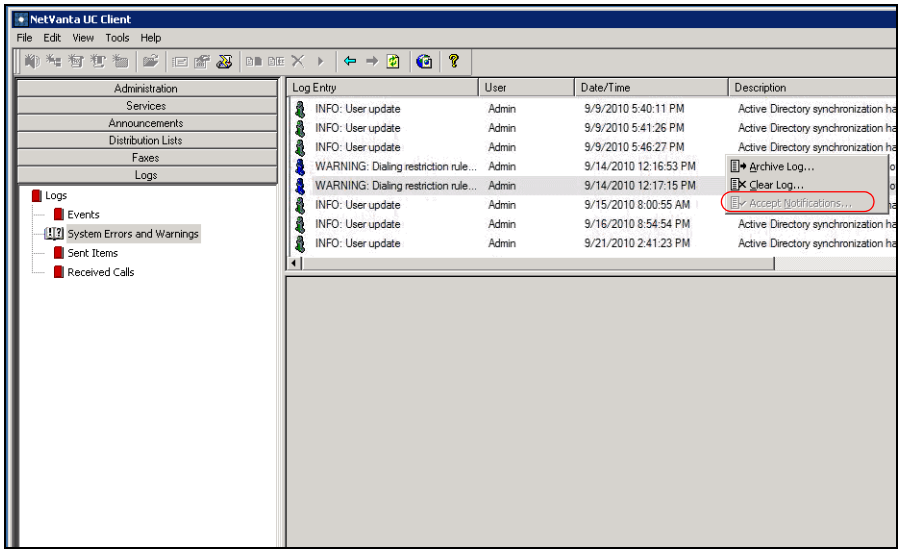
Acknowledging Errors and Warnings

Each time an error or warning log is created, an entry is created in the Microsoft Windows event log. When the Windows entry is created, an orange bar appears at the bottom of the UC client indicating that an error or warning has occurred, and some action might be required. These error and warning alerts must be acknowledged for the orange bar to disappear. To acknowledge an error or warning entry, follow these steps:

1. Select the **System Errors and Warnings** log from the list in the **Logs** navigation pane.



2. In the summary pane of the **System Errors and Warnings** log, right-click on the appropriate log entry and select **Accept Notifications** from the drop-down menu. Select the entry that corresponds to the error or warning notification you just received. Right-clicking on the entry acknowledges the error or warning, and the orange bar disappears from the bottom of the UC server GUI.



Managing Logs with Microsoft Windows SBS 2008

Microsoft Windows SBS 2008 records all unacknowledged errors and warnings in the UC server. When the NetVanta UC Server is installed on Windows SBS 2008, a custom alert is automatically configured for the SBS 2008 console. This effectually alerts you that an error or warning has been detected without having an open UC client window.

If the UC server is not installed on the Windows SBS 2008 system, you should consult Microsoft documentation or support for information on creating custom alerts. You will need to specify the following information for the custom configuration: the path is ***Application****, the provider is* ***UC server****, the SetEventID is* ***256****, and the ClearEventID is* ***512****.*

To access the error and warning alerts from Windows SBS 2008, follow these steps:

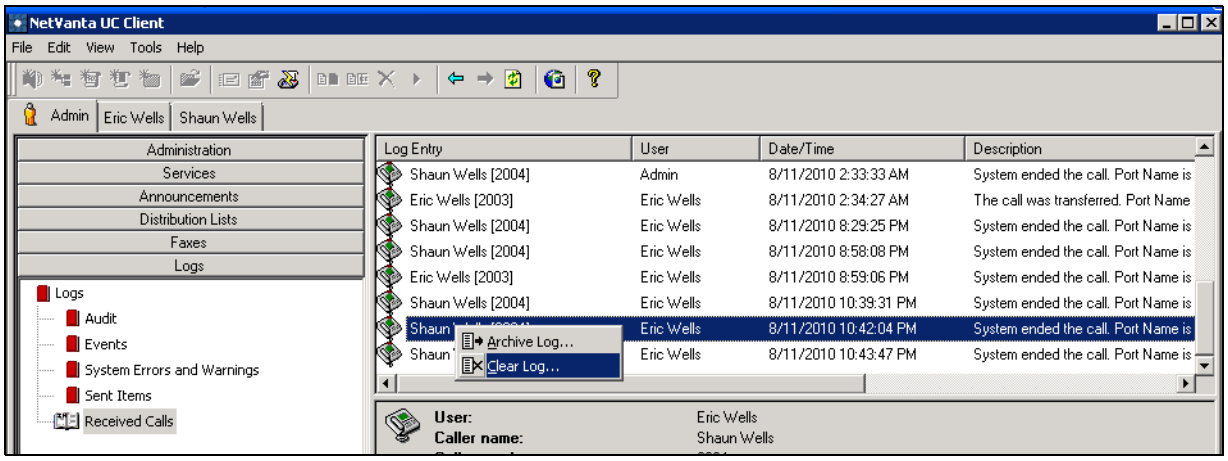
1. Navigate to the Windows **Start** menu and select **Event Viewer**.
2. Open the Windows SBS 2008 console and select the **Network** tab. Under **Computers**, any UC server errors and warnings have not been acknowledged will appear.
3. Follow the steps outlined in *Acknowledging Errors and Warnings on page 12* to acknowledge the errors displayed in Windows SBS 2008.

Removing Old Log Entries

In each log type, you can remove old log entries. To remove log entries, follow these steps:

1. Select the appropriate log type from the list in the **Logs** navigation pane.

2. Right-click in the log's summary pane and select **Clear Log** from the drop-down menu.



> NOTE *You can also access the **Clear Log** option by navigating to **Tools** > **Clear Log**.*

3. In the **Purge Log Entries** dialog box that appears, specify the types of entries you want to clear from the system. You can choose to clear all entries (select **everything**), entries created before the current date (select **entries created before today**), entries of the previous months (select **entries created before the beginning of the month**), and entries before a specific date (select **entries created before a specific date** and enter the date in the appropriate field). When you have specified the entries you want to delete, select **OK**.

> NOTE *You cannot delete log entries until all errors and warnings have been acknowledged. For information on acknowledging errors and warnings, refer to Acknowledging Errors and Warnings on page 12.*

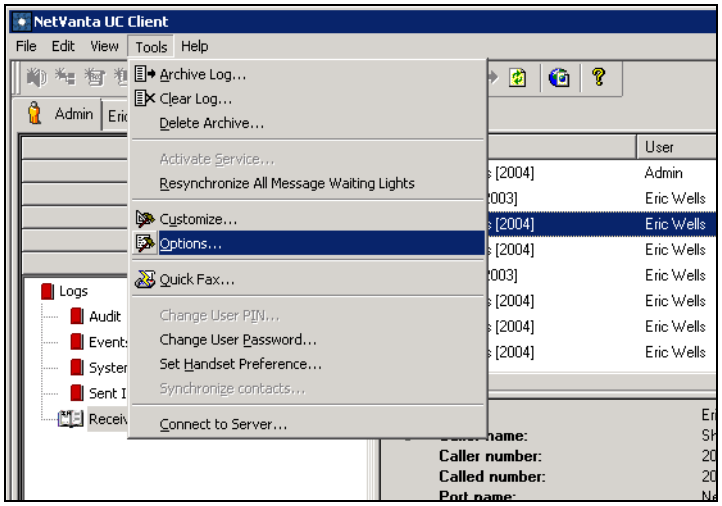
Archiving Logs

Logs can be archived for export and storage. The UC server can be configured to automatically archive logs, or logs can be archived as needed. In addition, archived logs can be renamed as needed. The following sections describe the functions surrounding log archives.

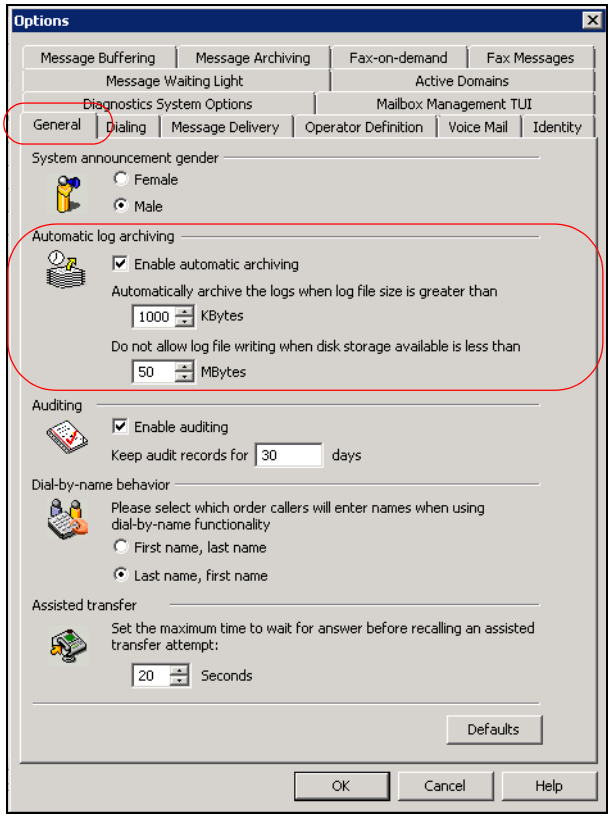
Automatically Archiving Logs

Administrators can set UC server logs to automatically archive based on a configured size limit for the log file. When the size of the log exceeds that threshold, it is automatically archived. To configure logs to archive automatically, follow these steps:

1. Log into the UC server as the local administrator. Connect to the UC client as administrator, and navigate to the **Admin** tab. Select **Tools** from the tool bar and then select **Options** from the drop-down menu.



2. In the **Options** menu, select the **General** tab.

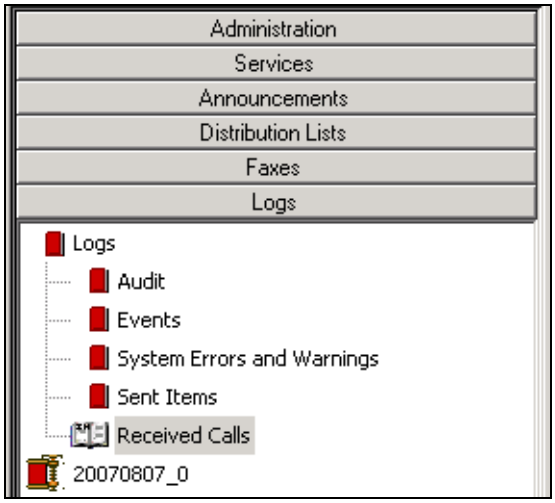


From this menu, you can enable automatic log archiving by selecting the checkbox next to **Enable automatic archiving**. By default, this option is enabled. In addition, you can specify the log file size limit in KBytes. When the log file becomes larger than the number specified here, the log is automatically archived. By default, logs are archived when they become larger than **1000** KBytes.

Lastly, you can specify the amount of disk space you want to devote to log archives. By default, the UC server will not write any more logs to disk once the disk contains **50** MBytes of information.

3. When you have specified the automatic log archiving settings, select **OK** to exit the **Options** menu and apply the settings.

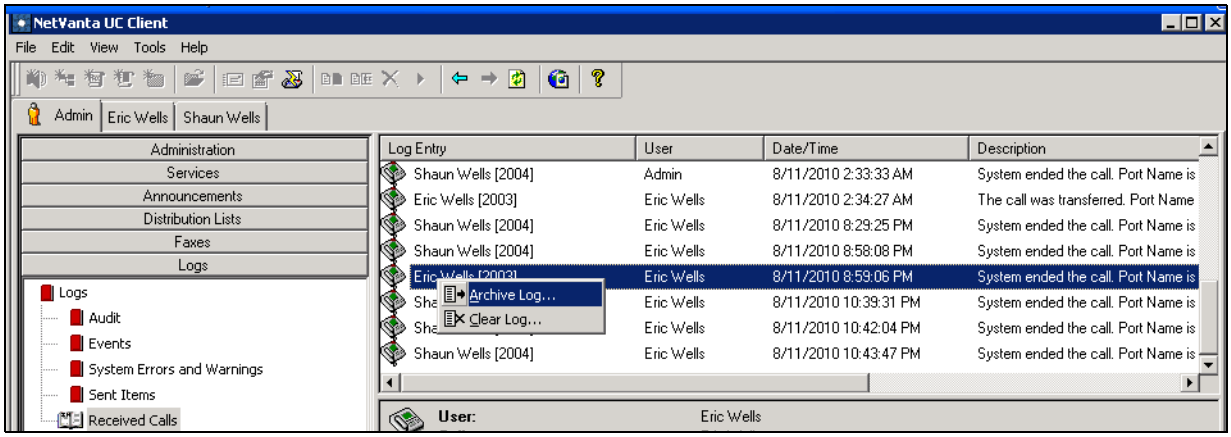
4. As logs are archived, they appear in the topics list in the **Logs** navigation pane. Archived logs are named based on the date the log was created and how many logs have been created for that day (for example, 20070807_0).



Manually Archiving Logs

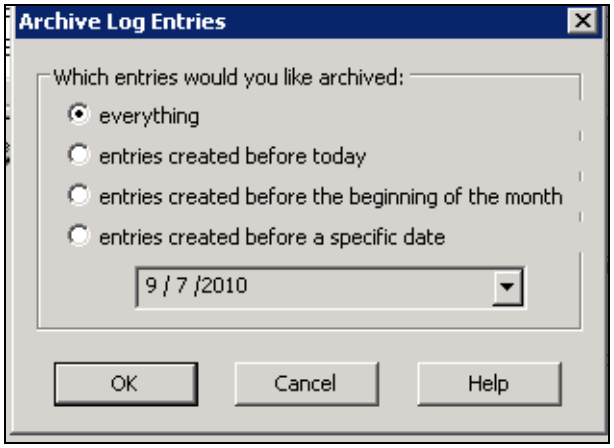
In addition to automatically archiving logs, logs can be archived manually by both PA/PBA users and administrators. Each log type must be archived individually. To manually archive a log, follow these steps:

1. Select the log type that you want to archive from the list in the **Logs** navigation pane.
2. Right-click in the log's summary pane and select **Archive Log** from the drop-down menu.



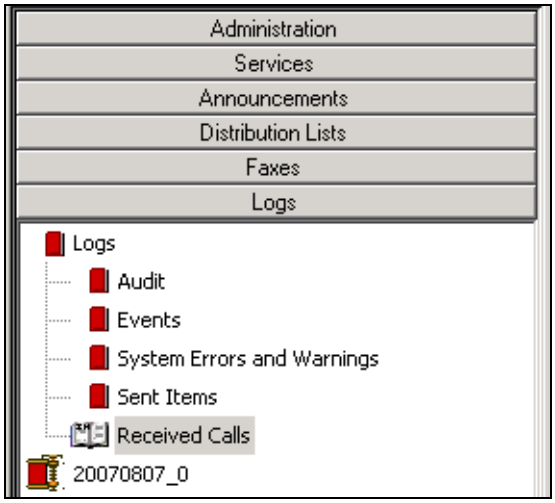
NOTE *You can also access the **Archive Log** option by navigating to **Tools** > **Archive Log**.*

3. In the **Archive Log Entries** dialog box that appears, specify the types of entries you want to archive. You can choose to clear all entries (select **everything**), entries created before the current date (select **entries created before today**), entries of the previous months (select **entries created before the beginning of the month**), and entries before a specific date (select **entries created before a specific date** and enter the date in the appropriate field). When you have specified the entries you want to delete, select **OK**.



> NOTE *You cannot archive log entries until all errors and warnings have been acknowledged. For information on acknowledging errors and warnings, refer to Acknowledging Errors and Warnings on page 12.*

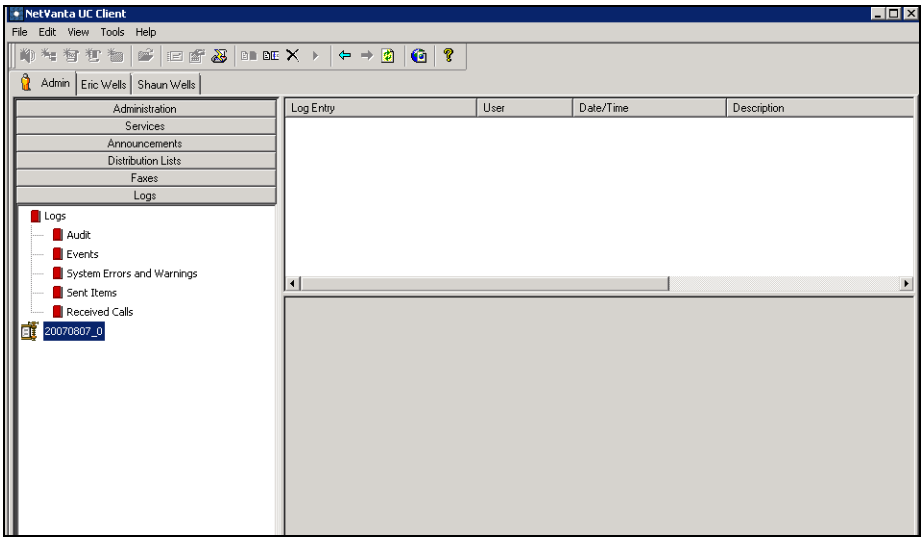
4. As logs are archived, they appear in the topics list in the **Logs** navigation pane. Archived logs are named based on the date the log was created and how many logs have been created for that day (for example, 20070807_0).



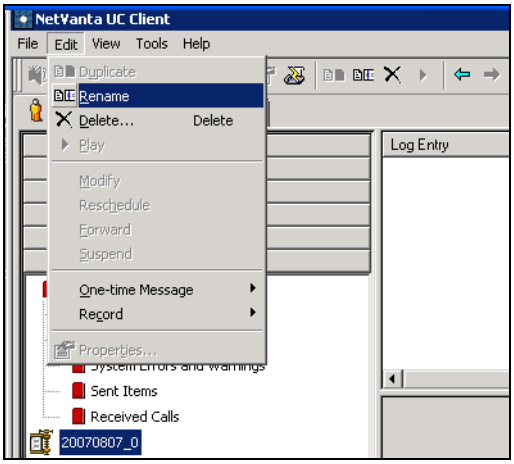
Renaming Archived Logs

When logs are archived, the files are named based on the date the archive was made. To rename these files, follow these steps:

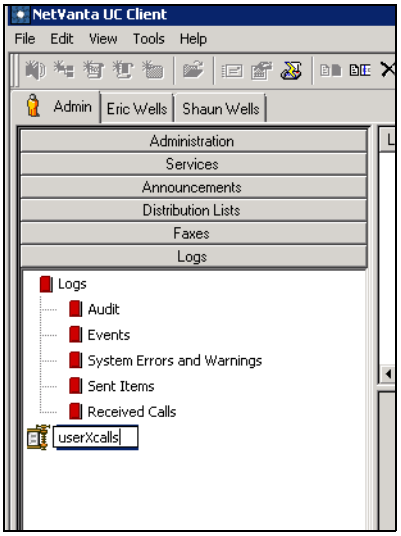
1. Select the archived log that you want to rename from the list in the **Logs** navigation pane.



2. Select **Edit** from the tool bar and select **Rename**.



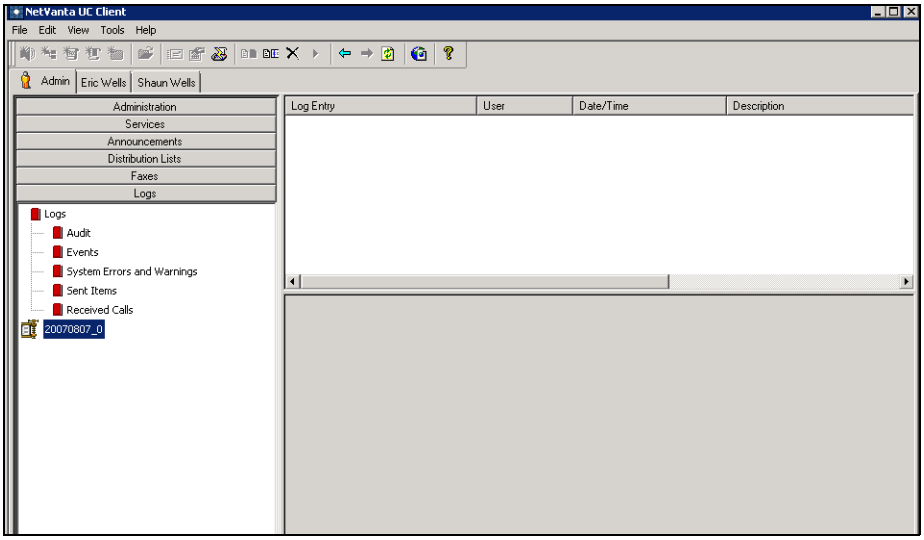
3. Enter the new name for the archive into the appropriate field and select **Enter**.



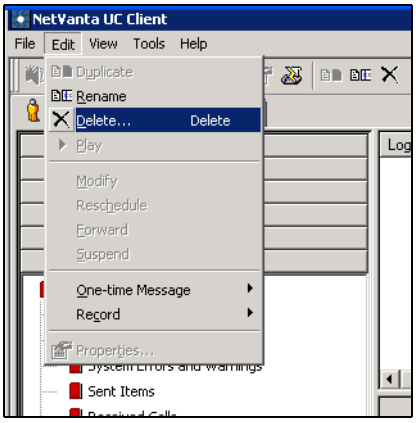
Deleting Archived Logs

To delete an archived log, follow these steps:

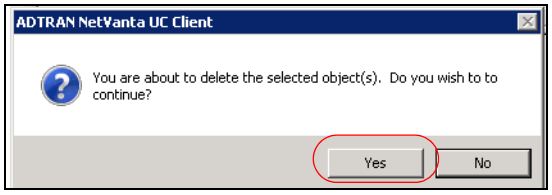
1. Select the archived log that you want to delete from the topics list in the **Logs** navigation pane.



2. Select **Edit** from the tool bar and select **Delete**.



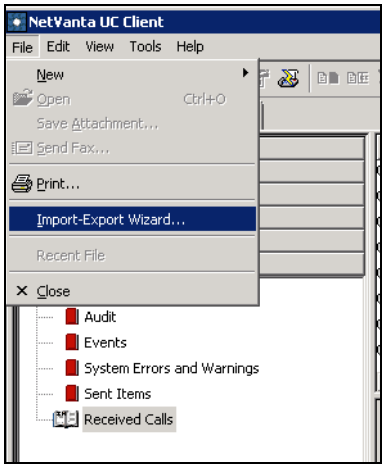
3. Next, select **Yes** to confirm the deletion.



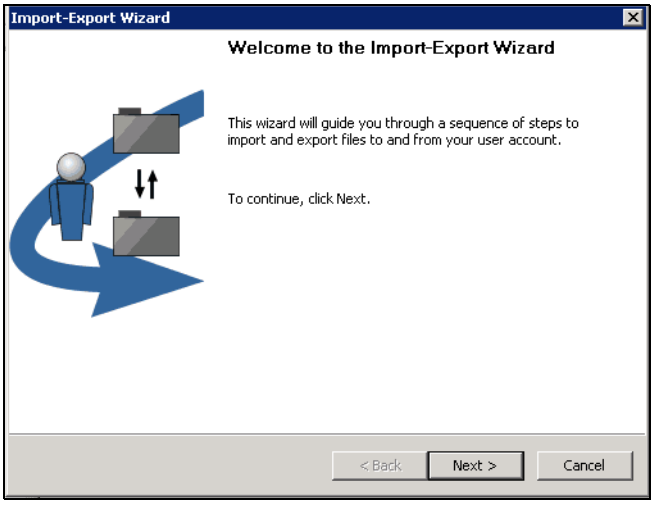
Exporting Logs

Logs can be exported as tab-separated or XML-based files using the **Import/Export** wizard. The log files can then be used by other reporting applications to provide historical reports on UC server activity. To export a log, follow these steps:

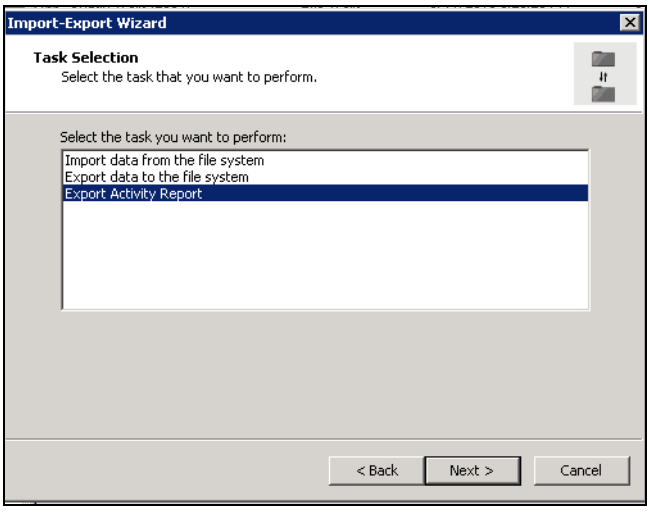
1. Navigate to **File** > **Import-Export Wizard** in the UC client tool bar.



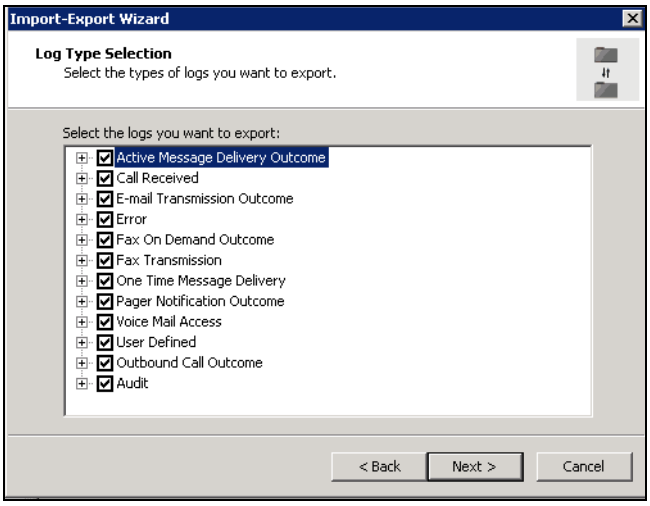
2. Select **Next** on the first **Import-Export Wizard** dialog box.



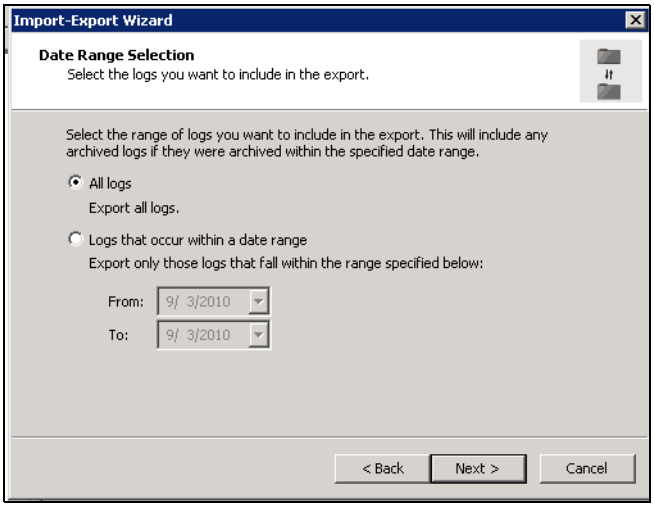
3. Select **Export Activity Report** and select **Next**.



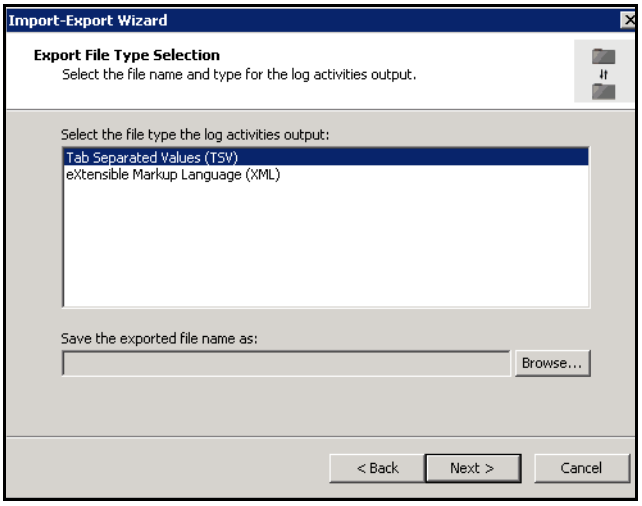
4. Select the types of logs that you want to export, and select **Next**.



5. Now, specify whether you want to export all logs or only logs from a specific date range. If you only want to export logs within a date range, enter the dates in the appropriate field. Then select **Next**.



6. Select the file type (tab-separated or XML-based) for the log that you want to export. Additionally, specify a name for the log file in the appropriate field. Once you have entered the file type and name, select **Next** to export the log.



7. Once the log is exported, select **Close** to exit the **Import-Export Wizard**.

Using the Errors and Warnings Log for Troubleshooting

The logs recorded by the UC server provide significant information about the configuration, operation, and use of the UC server. The following table outlines specific log entries that you might encounter, and possible causes, and solutions for those errors or warnings.

> NOTE
>
> *The following log entries are example entries and use the **%** symbol to indicate variables. For example, **%s** indicates a string variable (for example, user name), **%d** represents an integer variable, and **0x%08x** represents a 8-digit hexadecimal integer.*

Table 1. Potential Error and Warning Log Entries, Causes, and Solutions

Log Entry	Severity	Possible Causes and Solutions
Failed to create identity %s. Internal error %d.	Serious Error	Verify that all UC server processes are started, and retry creating that identity.
Failed to deliver a message to user %.	Serious Error	This error can be caused by messages that were queued for delivery but attempted delivery has failed. When this occurs, messages are delivered to the system defined default mailbox. Verify the connection and permissions to the message store.
Failed to get server object for user %.	Serious Error	Verify the network connectivity and the UC server's service accounts file permissions in the .\UC Server folder.

Table 1. Potential Error and Warning Log Entries, Causes, and Solutions *(Continued)*

Log Entry	Severity	Possible Causes and Solutions
Failed to update Active Directory user's extensions (hr=0x%08x).	Serious Error	Verify the network connectivity, the connection to Active Directory, and the UC server's service accounts file permissions in the .\UC Server folder. Rerun the Server Configuration wizard.
Internal error finding the Exchange Server message store.	Serious Error	Verify the connection to Microsoft's Exchange Server and validate that the UC server's service account has the appropriate permissions configured.
System diagnostics has detected a potential problem with port %s.	Serious Error	This error indicates the port auditing system has detected a problem with one or more of the system ports. These problems can include a bad private branch exchange (PBX) port or that the wiring is connected to the wrong port on the PBX. To verify the wiring, call each port individually and monitor them in the UC server **Ports Manager** to validate that calls are being received on the expected port.
The minimum disk storage threshold has been exceeded. New voice messages will not be saved until the problem is corrected.	Serious Error	Increase the disk storage or remove any files that are not required.
Application Services have been restarted to recover from an error condition.	Fatal Error	In most cases, the system will operate normally after this occurs. However, if this log entry appears regularly or frequently, you should investigate further. This message can potentially be caused by the following: Microsoft Exchange Server is not responding in a timely manner, Microsoft Active Directory responses are slow, the UC server system CPU is overloaded, other activities are slowing down operation (such as virus scanning), or there are software issues. To investigate these possible causes, validate the following: voicemail and auto attendants are operating correctly, the UC client is connected to the server, and that user mailboxes are accessible from all mail servers. In addition, review previous logs to see if there is a pattern (for example, they all occur at 3:00 a.m.). If there is a pattern, consider the possibility of other activities interfering (such as virus scanning, updates, etc.). If the logs occur rapidly or frequently, there is likely a problem in the configuration or operation and you should contact technical support. If logs occur infrequently, continue with normal operation.

Table 1. Potential Error and Warning Log Entries, Causes, and Solutions *(Continued)*

Log Entry	Severity	Possible Causes and Solutions
Call reason code %s is invalid in key: %s	Warning	An analog PBX configuration file has been edited manually and a specified call reason code for an in-band signaling key doesn't exist in the valid call reasons defined in the same file.
Cannot write to file xxx.	Warning	Verify the UC server's service accounts file permissions in the .\UC Server folder and rerun the Server Configuration wizard.
Configuration file could not be copied: %s	Warning	This warning occurs when the PBX-specific configuration file doesn't exist and the template configuration file cannot be copied. Verify the UC server's service accounts file permissions in the .\UC Server folder and rerun the Server Configuration wizard.
Configuration file does not exist: %s	Warning	The file .\UC Server\Data\System\ CallInfoOverride.cfg has been edited manually and one or more of the entries in this file are invalid. Consult the inline documentation for details about valid syntax rules.
Duplicate override spec: %s in key %s	Warning	An analog PBX configuration file has been edited manually and an in-band signaling key's match pattern has been duplicated.
Duplicate pattern type %c in match pattern: %s in key %s	Warning	An analog PBX configuration file has been edited manually and an in-band signaling key's match pattern has been duplicated.
Error: '%s' compiling regular expression: %s in key %s	Warning	An analog PBX configuration file has been edited manually and an in-band signaling key's match pattern cannot be converted to a regular expression.
Exception %s caught, wrong format in override rule file on line: %s	Warning	The file .\UC Server\Data\System\ CallInfoOverride.cfg has been edited manually and one or more of the entries in this file are invalid. Consult the inline documentation for details about valid syntax rules.
Exception caught, wrong format in override rule file on line: %s	Warning	The file .\UC Server\Data\System\ CallInfoOverride.cfg has been edited manually and one or more of the entries in this file are invalid. Consult the inline documentation for details about valid syntax rules.

Table 1. Potential Error and Warning Log Entries, Causes, and Solutions *(Continued)*

Log Entry	Severity	Possible Causes and Solutions
Failed to retrieve server address	Warning	The UC server is unable to find the network address on the associated network adapter. This commonly occurs if the files were copied from one UC server machine to another. To correct this, navigate to the appropriate **Communication System** and reselect the adapter that you want to bind to the UC server. Select **OK**.
Failed to update %s's database with the received fax. The fax will be saved instead to the default mailbox.	Warning	This warning indicates a problem communicating with the database defined in the **Receive Fax** element. Check your database connection parameters and ensure that the database is available.
Incompatible match pattern: %s or overrides in key %s	Warning	An analog PBX configuration file has been edited manually and an in-band signaling key's match pattern is invalid.
Input file xxx does not exist	Warning	Verify the UC server's service accounts file permissions in the .\UC Server folder and rerun the Server Configuration wizard.
Invalid call progress tone spec: %s	Warning	A PBX configuration file has been edited manually, and "StandardTone[x]" (where [x]=1 to 9) is defined and formatted incorrectly.
Invalid disconnect spec: %s	Warning	An analog PBX configuration file has been edited manually and there is an error with the value for the tag "disconnectType." It must match one of the following values: positive, disconnectTone, disconnectDTMFSequence, or disconnectSilence.
Invalid disconnect tone spec: %s	Warning	An analog PBX configuration file has been edited manually and the tag "disconnectType" has a value of disconnectTone and the required corresponding tag "disconnectTone" is missing from the same configuration file.
Invalid override spec: %s in key %s	Warning	An analog PBX configuration file has been edited manually and an in-band signaling key's match pattern is invalid.
Key 'disconnectType' not defined: %s	Warning	An analog PBX configuration file has been edited manually and the tag 'disconnectType' is not present.
No key is defined in section: %s	Warning	An analog PBX configuration file has been edited manually and all keys are missing from the section 'In Band Signaling.'

Table 1. Potential Error and Warning Log Entries, Causes, and Solutions *(Continued)*

Log Entry	Severity	Possible Causes and Solutions
No match pattern is defined in key: %s	Warning	An analog PBX configuration file has been edited manually and an in-band signaling key is missing a match pattern.
No reason codes are defined in key: %s	Warning	An analog PBX configuration file has been edited manually and the reason code for an in-band signaling key is missing.
Pattern type %d not supported yet	Warning	A PBX configuration file has been edited manually, and an in-band signaling protocol definition was added that is not yet supported.
System did not receive caller ID information from the modem and hence, could not transmit it to your pager. Ensure that your phone rings at least twice before answering otherwise you will not receive caller ID information.	Warning	Verify that caller ID is available when attempting to send a pager notification that includes sending the caller ID.
The current number of ports has exceeded the number of licensed ports.	Warning	Verify that you have enough ports or application server channels licensed. To verify the licensing, navigate to **Help** > **Licensing Information** to refer to the existing licensing capabilities. Contact your sales representative to purchase additional ports or application server media channels.
The data source, %s, referenced in the element, %s, is unknown.	Warning	ServiceStateMachine when an element refers to a data source that no longer exists. Verify the following: that the open database connectivity (ODBC) data source (if applicable) and the fields in the reference data source are configured correctly.
The specified number was disallowed by dialing restrictions.	Warning	This warning occurs when the application server attempts to dial a number that matches a dial restriction entry (configured in **Tools** > **Options** > **Dialing**). Verify the application server toll restrictions.
Unable to communicate with remote agent %s	Warning	This warning indicates the application server could not communicate with the IP Office remote agent. Verify the remote agent properties, IP address, port, and network connection state.
Unable to deliver a message to user %s	Warning	This warning indicates there was a problem delivering a voice or fax message to a user. Verify your message store and network connection states to ensure that the connection to the message store is available. This error occurs on the first message delivery failure.

Table 1. Potential Error and Warning Log Entries, Causes, and Solutions *(Continued)*

Log Entry	Severity	Possible Causes and Solutions
Unrecognized character %c in match pattern: %s in key %s	Warning	An analog PBX configuration file has been edited manually and an in-band signaling key's match pattern has an invalid character.
Wrong format in override rule file on line: %s...	Warning	The file .\UC Server\Data\System\ CallInfoOverride.cfg has been edited manually and one or more of the entries in this file are invalid. Consult the inline documentation for details about valid syntax rules.

Table 2. Potential Error and Warning Log Entries When Integrating with an Avaya Definity PBX

Log Entry	Severity	Possible Causes and Solutions
%s display pattern not defined	Warning	The Definity PBX configuration file in use has been edited manually and a required display pattern is missing.
Error in repeat count after '_' in: %s	Warning	The Definity PBX configuration file in use has been edited manually and an error was encountered in parsing a 'display format' entry.
Error in repeat count after '%c' in: %s	Warning	The Definity PBX configuration file in use has been edited manually and an error was encountered in parsing a 'display format' entry.
Display format definition error, no matching '\' found: %s	Warning	The Definity PBX configuration file in use has been edited manually and an error was encountered in parsing a 'display format' entry.
Display format error, illegal character '%c' is found: %s	Warning	The Definity PBX configuration file in use has been edited manually and an error was encountered in parsing a 'display format' entry.
Error: '%s' compiling regular expression '%s' from display rule '%s'	Warning	The Definity PBX configuration file in use has been edited manually and an error was encountered in parsing a 'display format' entry.
Error in reason code translation, at most two characters are allowed in each field: %s	Warning	The Definity PBX configuration file in use has been edited manually and a reason code translation has more than two characters in a field (fields are separated by a comma).
Error in repeat count after '_' in: %s	Warning	The Definity PBX configuration file in use has been edited manually and an error was encountered in parsing a 'display format' entry.
Error in repeat count after '%c' in: %s	Warning	The Definity PBX configuration file in use has been edited manually and an error was encountered in parsing a 'display format' entry.

Table 2. Potential Error and Warning Log Entries When Integrating with an Avaya Definity PBX *(Continued)*

Log Entry	Severity	Possible Causes and Solutions
Failed to parse pattern line '%s', ignoring	Warning	The Definity PBX configuration file in use has been edited manually and a display pattern has an invalid value.
Illegal characters found in allowedNondigitCharactersInExternalNumber%	Warning	The Definity PBX configuration file in use has been edited manually and the "allowedNondigitCharactersInExternalNumber" tag has one or more invalid characters.
Illegal characters found in literals in %s	Warning	The Definity PBX configuration file in use has been edited manually and an error was encountered in parsing a 'display format' entry.
Pattern length (%d) differs from display length (%d) in pattern: %s	Warning	The Definity PBX configuration file in use has been edited manually and an error was encountered in parsing a 'display format' entry.

