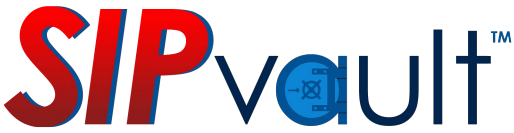


NHI SIPvault Manual

Last Updated: February 2017

When Network Harbor audio software and/or hardware is used as, or in part of, an audio monitoring system, the law may require that the public be given notice of audio recording on the premises. Decals, signs and/or placards can be used for this purpose.

In the United States:
United States Codes, Title 18, Section 2510 (2) states in part:
"oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation…"

United States Codes, Title 18, Section 2511 goes on to state that intercepting an "oral communication" as defined above without due legal purpose as defined in Title 19 Section 2511 is a federal crime.

By definition of the code section, a person cannot have an expectation of privacy, nor can he or she expect that communication will not be intercepted, if there are public signs posted, indicating that the communication is being monitored.
In order to comply with the law, decals, signs and/or placards stating that audio monitoring is being conducted on premises must be displayed as a disclaimer. These disclaimers must be affixed, in plain view, to all entrances to areas where the microphones and/or other audio surveillance devices are installed.

Table of Contents

Installation - Prerequisites

NHI SIPvault Server has the following prerequisites:

- Supported Windows Operating Systems: Windows 7, Windows Server 2003 R2 (32-Bit x86), Windows Server 2003 R2 x64 editions, Windows Server 2003 Service Pack 2, Windows Server 2003 Service Pack 2 x64 Edition, Windows Server 2008 R2, Windows Server 2008 Service Pack 2, Windows Vista Service Pack 2, Windows XP Service Pack 3
- Microsoft .NET Framework 4
- Microsoft SQL Server Compact 3.5 Service Pack 2

Service Installation

To begin the service installation, run the file 'SIPvaultInstaller.msi' as a Windows user that has sufficient permissions to install an Windows Application and Windows Service.

Figure 1: SIPvault Installation Dialog

Click the 'Next' button to continue.

Select the location to which the SIPvault service will be installed and then click the ‘Next’ button.

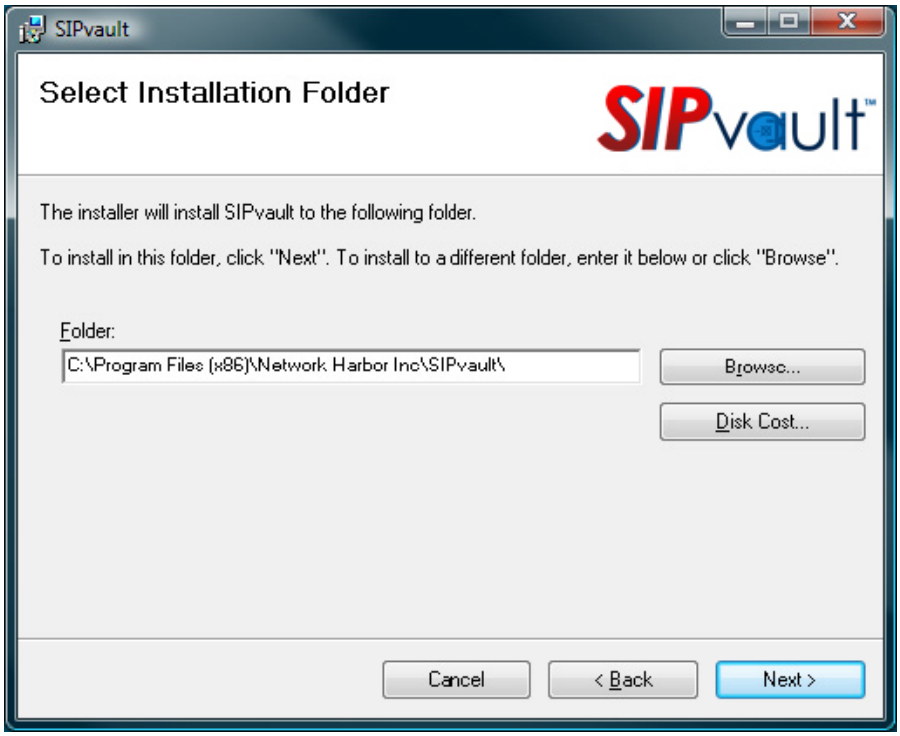


Figure 2: Select the Install Location

The installer will now be asked to agree to the SIPvault End User License Agreement. A portion of this agreement is dedicated to ensuring that the installer/end user is aware of some of the legalities involving audio recording. As the statutes governing audio recording do differ based on legal jurisdiction, it is highly suggested that the installer/end user ensure that their operation of the system is legal according to any applicable local, state, or federal laws.

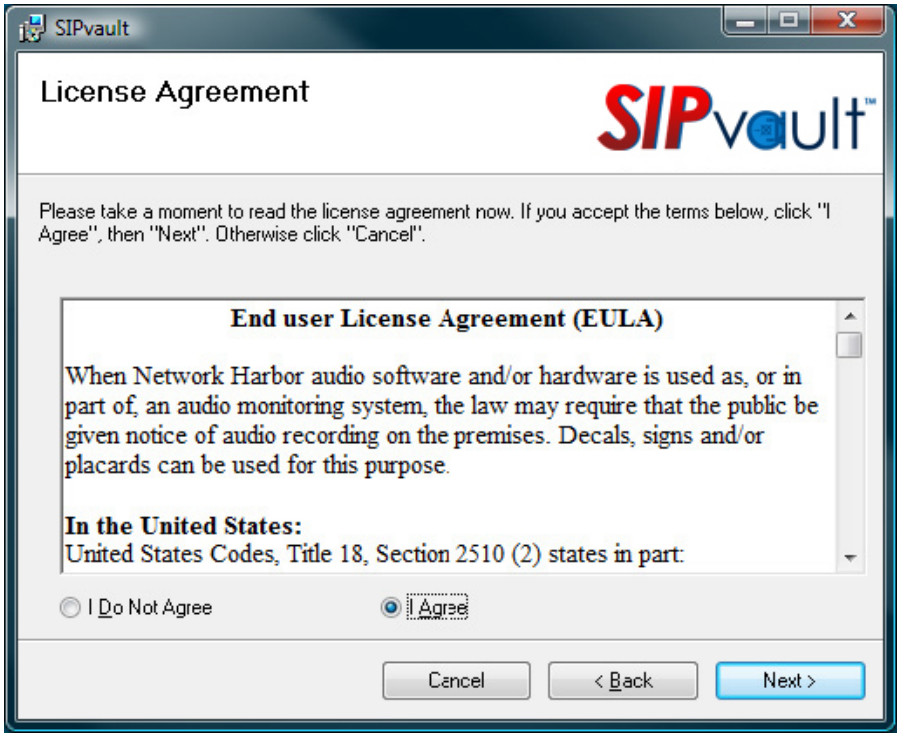


Figure 3: SIPvault EULA

If the given agreement is satisfactory, select the 'I Agree' option, and then click the 'Next' button.

The installer will now be shown a confirmation screen. This is the last opportunity to change a previously entered setting before continuing with the installation. Click ‘Back’ to make changes, or ‘Next’ to start the installation.

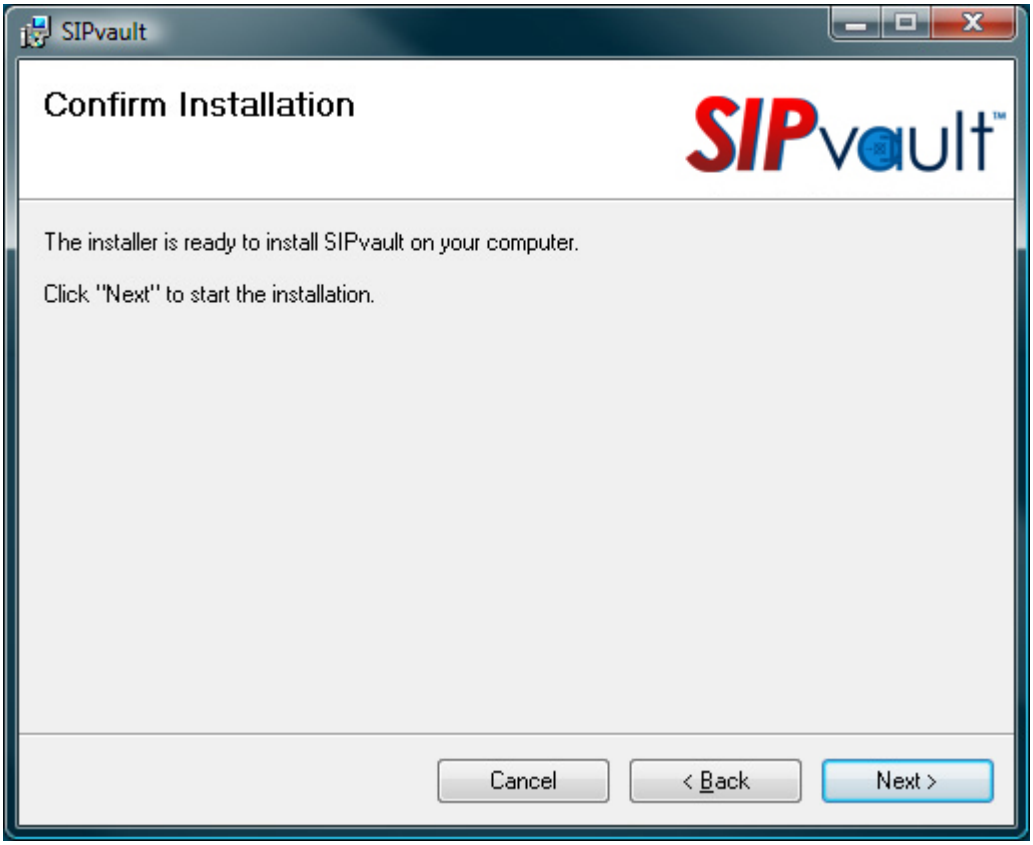


Figure 4: Confirm Installation

Once installation is completed, the dialog showing in Figure 5. Click the ‘Close’ button to exit the installation process.

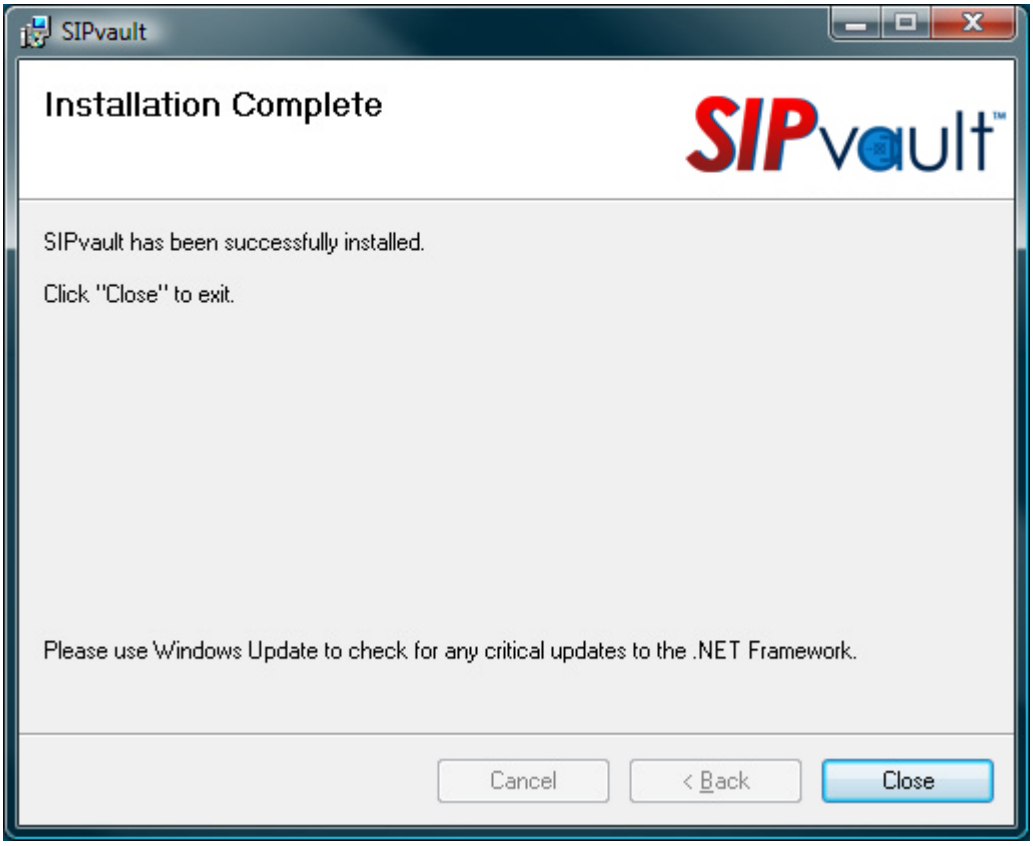


Figure 5: Installation Complete

Service Configuration

After installation, the SIPvault Configuration application should be launched automatically within a few seconds. It is also available at any point after initial configuration using the launcher link named *Configure SIPvault*.

The SIPvault Configuration application consists of six tabs.

Basic

- Basic SIPvault service configuration

Backup/Restore

- Provides the ability to backup and restore the SIPvault endpoint configuration.

RTSP

- Configuration of RTSP conference streaming.

SIP Peers

- Configuration of SIPvault Peer Servers.

Miscellaneous

- Additional SIPvault configuration options.

Certificates

- Host and Trusted certificate configuration for TLS operation.

The Cancel and Save buttons on this tab are used to cancel and save the entirety of the configuration application. These functions are available on any tab of the configuration utility.

Service Configuration - Basic Tab

The Basic configuration tab has three four configuration options: SIP Agent Binding, Admin Passphrase, License, and Service Status.

SIP Agent Binding defines the network interface URI for SIPvault server communications. The binding has two components – transport protocol and hostname.

Transport Protocol allows the administrator to specify which protocols the SIPvault server should use when communicating with endpoints. A simple description of each option is presented in text below the combo box.

Hostname allows the administrator to specify the hostname that identifies this SIPvault server on the network. In addition to selecting either all IP addresses assigned to the local machine, the administrator may select a specific IP address or hostname.

In addition to the configuration options above, group boxes are provided which indicate the resulting Binding URI and associated DNS Records. These fields are provided as a convenience, indicating the result of a DNS lookup of the specified URI and consequently, the SIP URIs and IP addresses that will be used by the SIPvault server. Note that changes to relevant DNS records and/or interface configuration may cause these records to change outside of configuration.

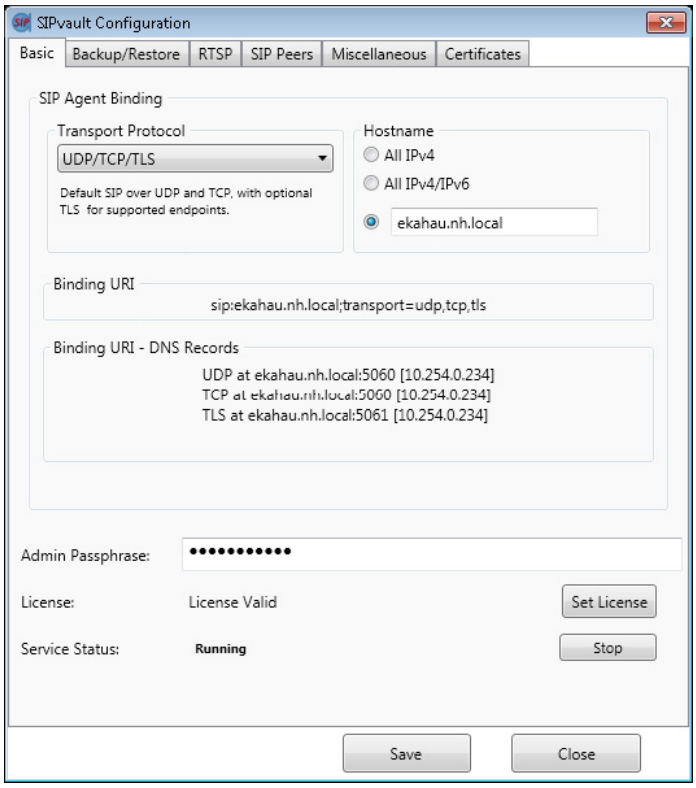


Figure 6: SIPvault Configuration, Basic Tab

> *Note:*
>
> *When configuring FIPS compliant operation, it is highly recommended that the administrator use the "TLS Only (SIPS Scheme)" transport protocol to ensure security is enforced between all network elements.*

Service Configuration - Basic Tab (cont'd)

Admin Passphrase is the authentication token which must be supplied by the SIPvault Client software to authenticate itself to the SIPvault Service.

> *Note:*
>
> *The Admin Passphrase cannot be used for FIPS compliant installations.*

When using a SIPvault Client with an Administration Certificate and TLS transport, a passphrase is not required for authentication; in this case, the admin passphrase field should be left blank.

Licensing is used to authenticate the proper hardware on which the SIPvault service has been licensed, as well as for how many devices this instance of the SIPvault service may support. If the configuration application indicates that the license file does not exist, or is invalid, the license may be updated with the 'Set License' button. Clicking this button will display a file selection dialog, select a new, valid license file using this dialog in order to update the license. If an error is encountered when installing this new license, a message will be displayed indicating the cause of this error. Otherwise, a message will be displayed indicating an accepted license.

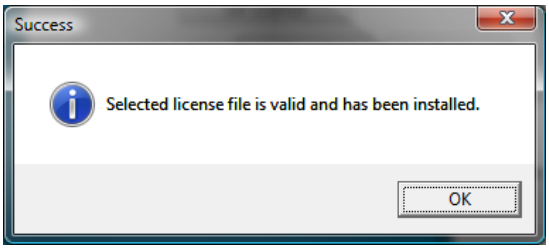


Figure 7: SIPvault Configuration, Valid License Dialog

Service Status displays the current status of the SIPvault service and provides start/stop functionality. It is best practice to restart the service whenever making changes to SIPvault configuration.

Service Configuration - Backup/Restore Tab

The Backup/Restore tab can be used to backup, restore, export, import, and otherwise perform simple manipulations of large groups of stations and groups.

To backup the current list of stations, groups, and alerts to an XML text file, simply click the 'Backup devices to a file.' button. A 'Safe File As…' dialog will be displayed, allowing the user to save this backup to any desired location and file name.

To restore a list of devices from a file, either enter the full file path into the text box, or click the 'Select File' button, to utilize the 'Open File…' dialog. Once a file is selected, a conflict resolution strategy will need to be chosen.

The conflict resolution strategies are as follows:

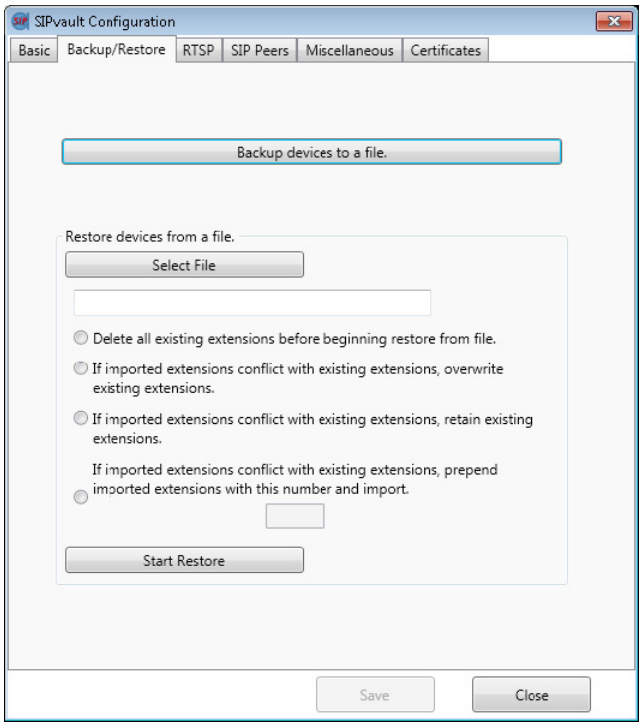


Figure 8: SIPvault Configuration, Backup/Restore

1) **Delete all existing extensions before beginning restore from file.** This option will wipe out the current list of extensions in the local database before performing a restore from the file and will therefore result in a list of extensions identical to that on the system when the backup was made.

2) **If imported extensions conflict with existing extensions, overwrite existing extensions.** In this context, conflict occurs when any two devices (one on the system currently, the other in the backup about to be restored), have the same extension number. This resolution will result in the local database containing all extensions from both the local database, and the backup file, where any objects that have the same extension will have the configuration as defined in the backup file.

3) **If imported extensions conflict with existing extensions, retain existing extensions.** Similar to the previous option, but in this case any objects that have the same extension will have the configuration as defined in the database.

4) **If imported extensions conflict with existing extensions, prepend imported extensions with this number and import.** This option takes devices from the backup, and if they conflict with existing devices, changes that device's extension by adding a given set of digits to the front of it. This method allows a way for all of the current and imported devices to be present on the system. This method is also useful for some odd management scenarios that may appear:

5) **Adding more digits to the standard extension length. Note:** SIPvault can support extensions of any reasonable length, and extension lengths need not be the same between different devices on the same SIPvault server.

   In some cases, a system may start with two- or three-digit extensions, especially when the number of expected devices on that system is very low. If at some later point, growth and a preference for uniformity in extension length forces the administrator to consider moving all users and groups to four-digit extensions, this feature can be helpful. Simply back up the current users/groups and then immediately restore them using this conflict resolution method, and a single digit entered as the prefix. Thus, if all extensions on the system are in the range 100-999, upon restore all of the extensions will conflict, and the devices will be replicated on the range 1100-1999. At this point, both sets of extensions are equally valid. Intercoms and master stations can be moved from one range to another as possible without changing passwords or server URIs, and then the 'old' three-digit range removed from the system when the changeover is complete.

6) **Combining existing SIPvault instances. I**f the extensions on two existing SIPvault instances do not overlap, or do not overlap greatly, then devices from one instance can be backed up and restored onto the other. Intercoms and master stations will need to have their SIP server references changed to point at the new combined server, but extensions and passwords will not change. If there is a conflict between extensions on the two systems, those extensions will have the designated prefix on them, making them easy to find in the extension list, and allowing for manual resolution. A manual resolution would consist of creating a new extension for the imported device on the combined server and changing the configuration on the intercom/master station to point at this new extension.

When a restore file and a conflict resolution strategy have been chosen, click the 'Start Restore' button to begin the restore process. The UI will disable while restoration is ongoing. The success status of the process will be displayed to the user as a message box.

Service Configuration - RTSP Tab

The RTSP interface on SIPvault is used to allow solutions such as NHI Savvault the ability to monitor and record audio which is sent over the SIPvault system.

As this presents obvious legal considerations that for various jurisdictions, it is important that the consequences of enabling recording on SIPvault be well understood before enabling these configuration options. For this reason, these options default to disallowing monitoring/recording.

The option to 'Enable the SIPvault RTSP Interface', when activated, starts an RTSP server running on the SIPvault machine to which requests for audio may be made.

The 'RTSP Server Port' is the TCP port upon which the RTSP server will listen for connections. The default port for the RTSI protocol is TCP 554.

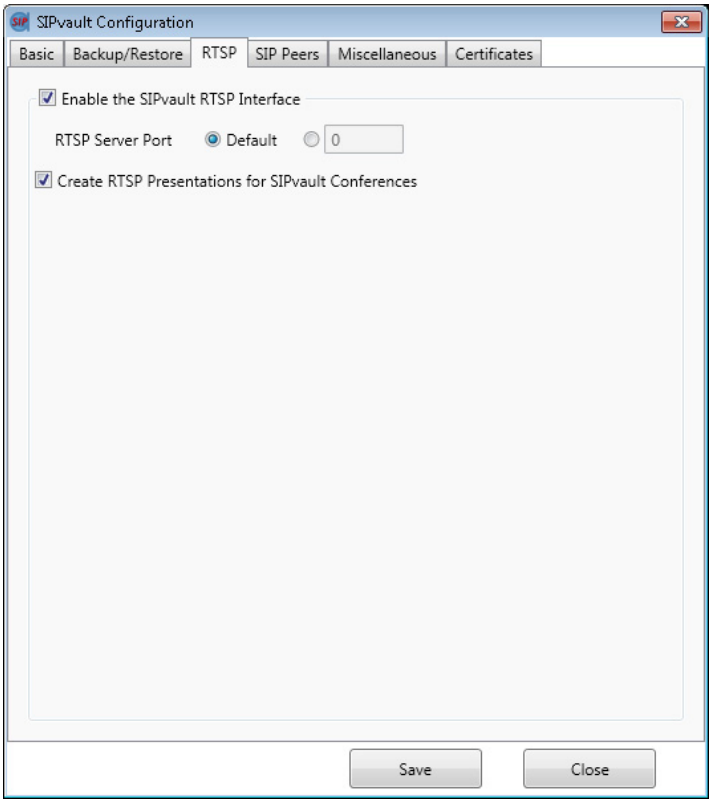


Figure 9: SIPvault RTSP Configuration

The option to 'Create RTSP Presentations for SIPvault Conferences' allows the RTSP server to respond to properly formatted requests for audio from a given conference. If this option is disabled, the RTSP server will be operational, but will not allow for audio recording.

Service Configuration - SIP Peers Tab

SIP Peers are a collection of SIPvault servers which can share resources. Peered SIPvault Servers can perform inter-server calling services, enabling multiple domains of SIP devices. SIPvault Peer servers are a powerful feature that allows consolidated communication between intercom networks at separate physical sites.

The format for a SIP Peer URI entry is similar to the binding URI of each SIPvault server. Specifiy the 'sip:' (or 'sips:') URI, the hostname of the peer, and optionally the port and transport.

Example SIP Peer entries:

- sip:example.com
- sip:server1.example.net:5060
- sip:192.168.1.1:5060;transport=tcp
- sip:192.168.2.1;transport=tls
- sips:server2.example.com

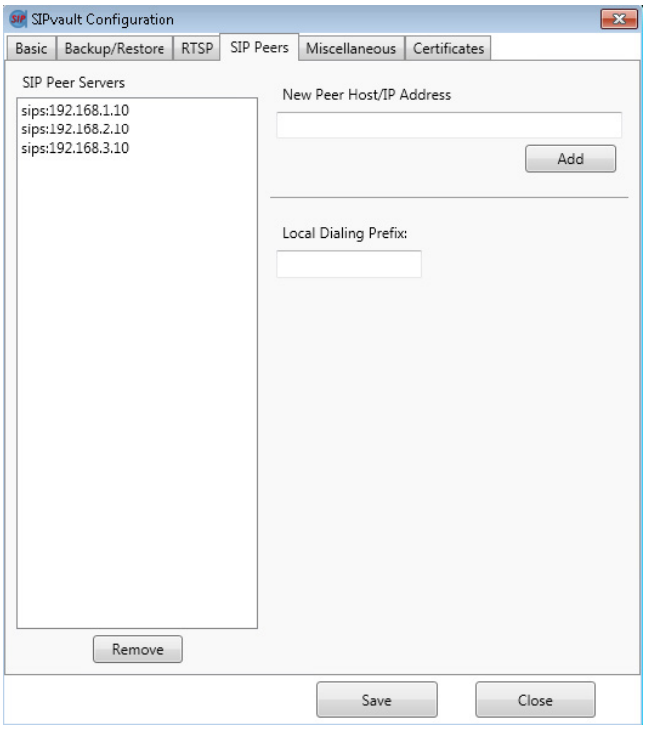


Figure 10: SIPvault Peer Configuration

How it works…

The following conditions must be met to reliably use the SIP Peer feature:

- A matching set of peer servers must be configured on all SIPvault servers.
- Each SIPvault server must be able to resolve the address of all peer URIs.
- Each extension should be configured on exactly one SIPvault peer.

When a call is placed by a SIPvault resource to an extension that is not configured on the local server, SIP Peer server logic is invoked. The unknown extension is combined with the URI of each configured SIP Peer, and calls are placed to each of those peers. Each peer then checks the list of configured resources, and either rejects or completes the call as appropriate.

> *Note:*
>
> *For the best security, use the UDP/ TCP/TLS transport protocol and the 'sips:' URI to identify Peer servers. Each SIPvault server will then require TLS authentication for cross-domain call control.*

Service Configuration – Peer Prefix

The Peer Prefix feature extends the SIPvault SIP Peers functionality adds call routing between peer servers using a dialing prefix.

Peer prefixes are specified for each peer server as part of the SIP Peer URI using the *nhi.prefix* parameter. A local dialing prefix may also be specified, which allows local calls to connect to either the local resource name or the prefixed resource name. In Figure 11, the configured server is shown with a Local Dialing Prefix (84) and three prefixed peer servers (81, 82, and 83).

Example SIP Peer entries:

- sip:example.com;nhi.prefix=5
- sip:10.3.2.1;transport=tls;nhi.prefix=88

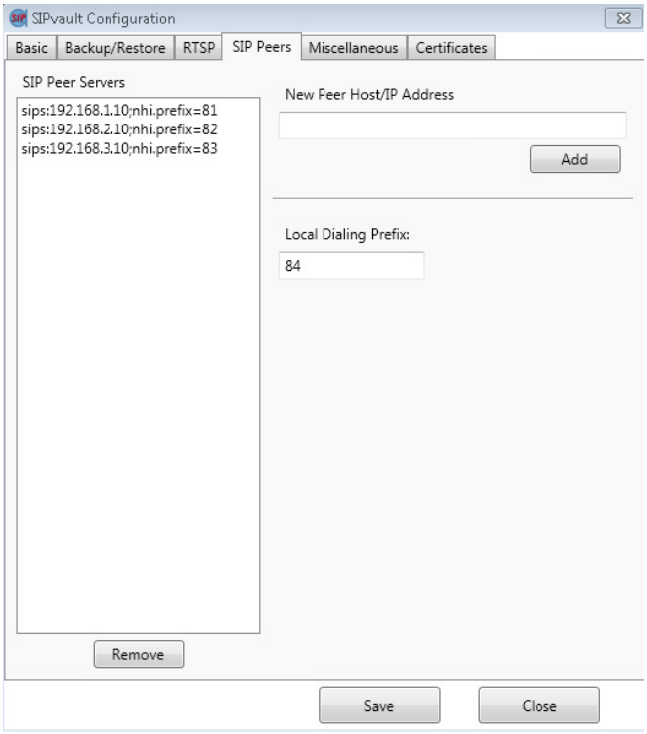


Figure 11: SIPvault Peer Configuration with Prefixes

How it works…

Prefixes may be used to allow consistent numbering schemes across multiple SIPvault instances while ensuring call routing between each instance. When placing calls from a local station, calls can be dialed directly to resources on the current SIPvault instances, or calls can be placed to the same resources by prepending the Local Dialing Prefix. Calls to resources on a SIPvault Peer server with a Prefix must be dialed by concatenating the Peer Prefix with the extension of the target resource.

When a SIP Peer is configured with a Peer Prefix, calls are only sent to that peer if the dialed extension started with the prefix. If a Peer Prefix is found, only the specified SIP Peer will be used to complete the call.

As with normal SIP Peer call routing, local extensions will always take precedence. An administrator may use this characteristic to override certain calls which would otherwise be routed using a prefix.

Note:

When selecting prefixes for your SIPvault instances, allow room for consistency and expansion. We recommend a 2-digit prefix for 2-5 instances, or a 3-digit prefix for 6-50 instances.

Peer Prefixes will match resources names of any length. For a server with the prefix '2', the calls to extension 20 and 220 will be forwarded (to resource 0 and 20, respectively).
Plan accordingly.

Service Configuration - Miscellaneous Tab

The Miscellaneous tab contains various configuration options that modify default SIPvault server behavior. In general, these options assist with device compatibility and general diagnostic.

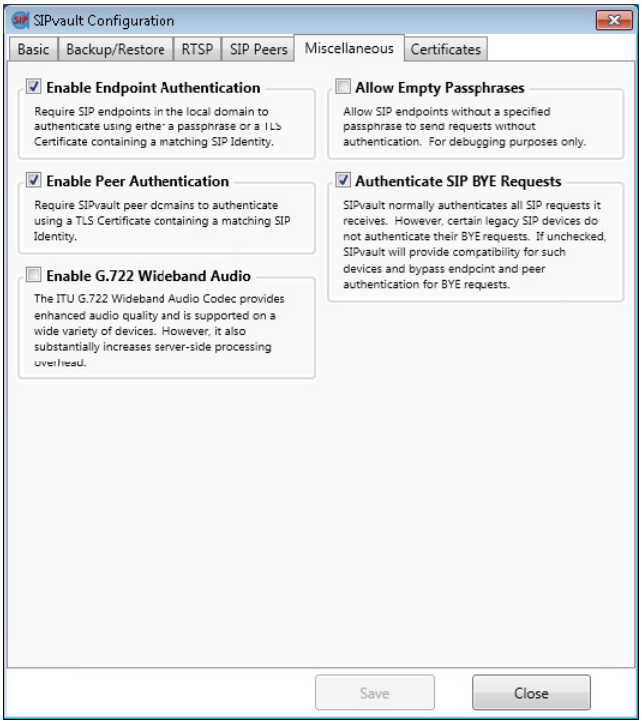


Figure 12: SIPvault Configuration, Miscellaneous Options

Enable Endpoint Authentication – When enabled, SIPvault will challenge requests from configured endpoints to provide a passphrase. The passphrase of each endpoint should be configured using SIPvault Client.

Enable Peer Authentication – When enabled, SIPvault will require that peer domains authenticate themselves with TLS and an X.509 Certificate.

Allow Empty Passphrases – In the case where SIPvault was not configured with a passphrase, allow requests to and from the endpoint without authentication. This applies to both SIPvault administration and SIPvault endpoints. This check is bypassed when authentication is provided by a X.509 certificate.

Authenticate SIP BYE Requests – Some third-party SIP devices do support SIP authentication, but do not apply that authentication when terminating an active call. Disable this mechanism to provide compatibility with such devices.

Enable G.722 Wideband Audio – G.722 is a wideband audio codec which is supported by a wide variety of devices. While it offers better audio quality that the default (G.711) codec, it also requires substantially more server resources to support. For systems with high CPU utilization, disable this feature to decrease system load.

Service Configuration - Certificates Tab

The Certificates tab facilitates configuration of the SIPvault X.509 certificate store. This certificate store contains two types of certificates. Host certificates which identify SIPvault to other SIP resources. Trusted certificates which are used to validate the certificates used by other SIP resources – these are typically CA certificates.

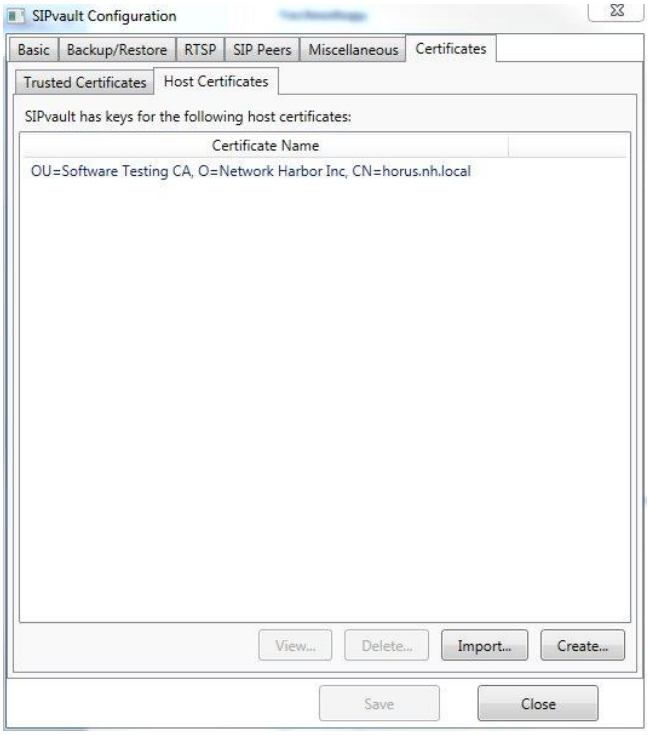


Figure 13: SIPvault Certificates Configuration

Each tab has three functions:

View – Displays basic information about the selected certificate.

Delete – Removes selected certificate from the current certificate store.

Import – Installs pre-generated certificates to the respective certificate store. The required file format of an imported certificate is dictated by the type of certificate. Host certificates must be encoded with the PKCS#12 format using a *.pfx* file extension. Trusted certificates must be Base-64 encoded with a *.cer* or *.crt* file extension. Certificates of either type may be imported directly from an NHI CA Store.

Create – Installs a newly generated certificate to the respective store. For more information, refer to the section titled Using NHI CA Store Files to Create X.509 Certificates.

For additional information about the specific format and extensions of certificates use by SIPvault, please refer to Appendix A – X.509 Certificate Signing Request for SIP.

Note:

The certificates tab will only function when the SIPvault service is running.

Note:

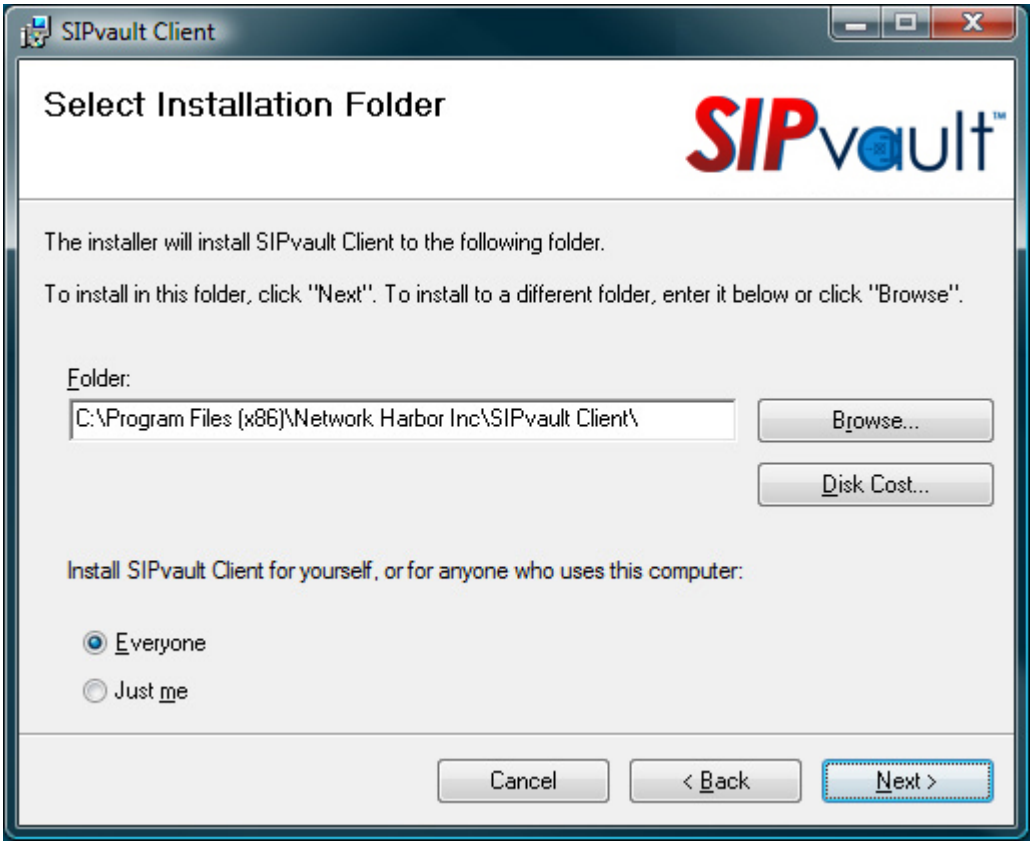
The trusted certificates store is common to all application on the local machine.

Client Installation

The SIPvault Client is installed with the SIPvault Server, therefore the standalone installation described below only needs to take place on machines other than the server machine, on which the user desires to administer the system.

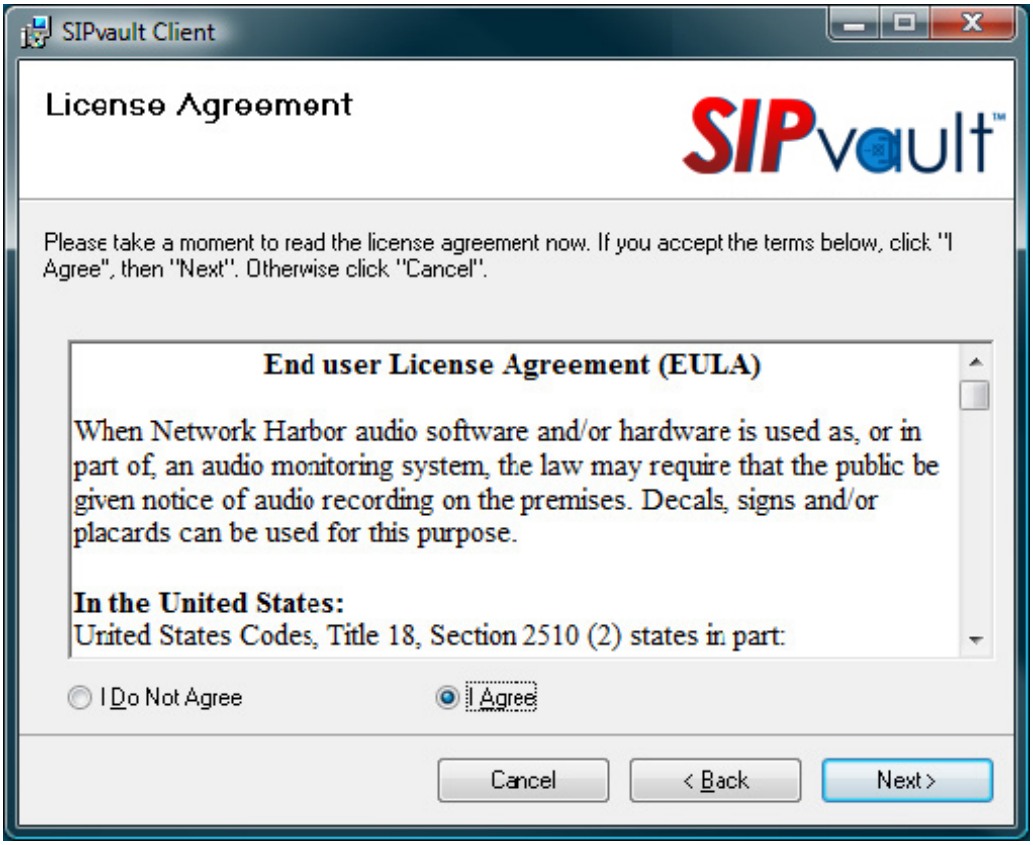
To begin the client installation, run the file 'SIPvaultClientInstaller.msi' as a Windows user that has sufficient permissions to install an application. Click 'Next' to continue.

Select the location to which the SIPvault service will be installed, as well as if the shortcuts to the SIPvault Client should be available to all user accounts on the machine, or just the one running the installation and then click the 'Next' button.



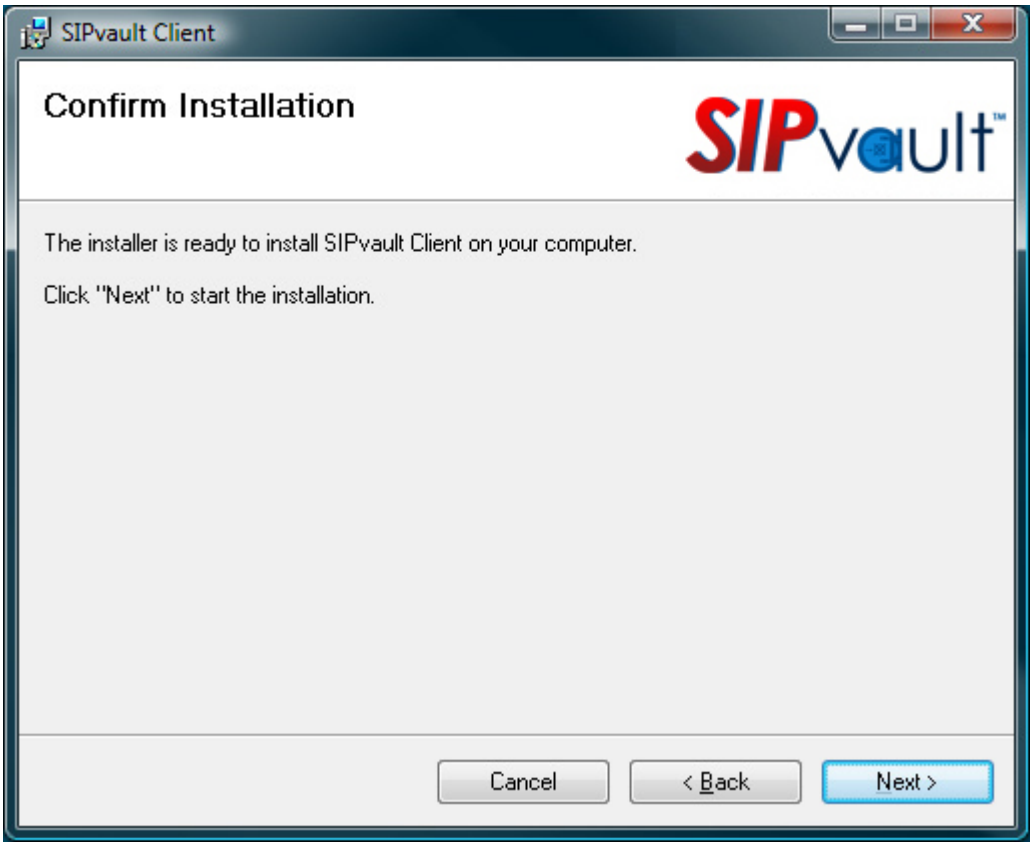
Click the 'Next' button to continue.

The installer will now be asked to agree to the SIPvault End User License Agreement. A portion of this agreement is dedicated to ensuring that the installer/end user is aware of some of the legalities involving audio recording. As the statutes governing audio recording do differ based on legal jurisdiction, it is highly suggested that the installer/end user ensure that their operation of the system is legal according to any applicable local, state, or federal laws.

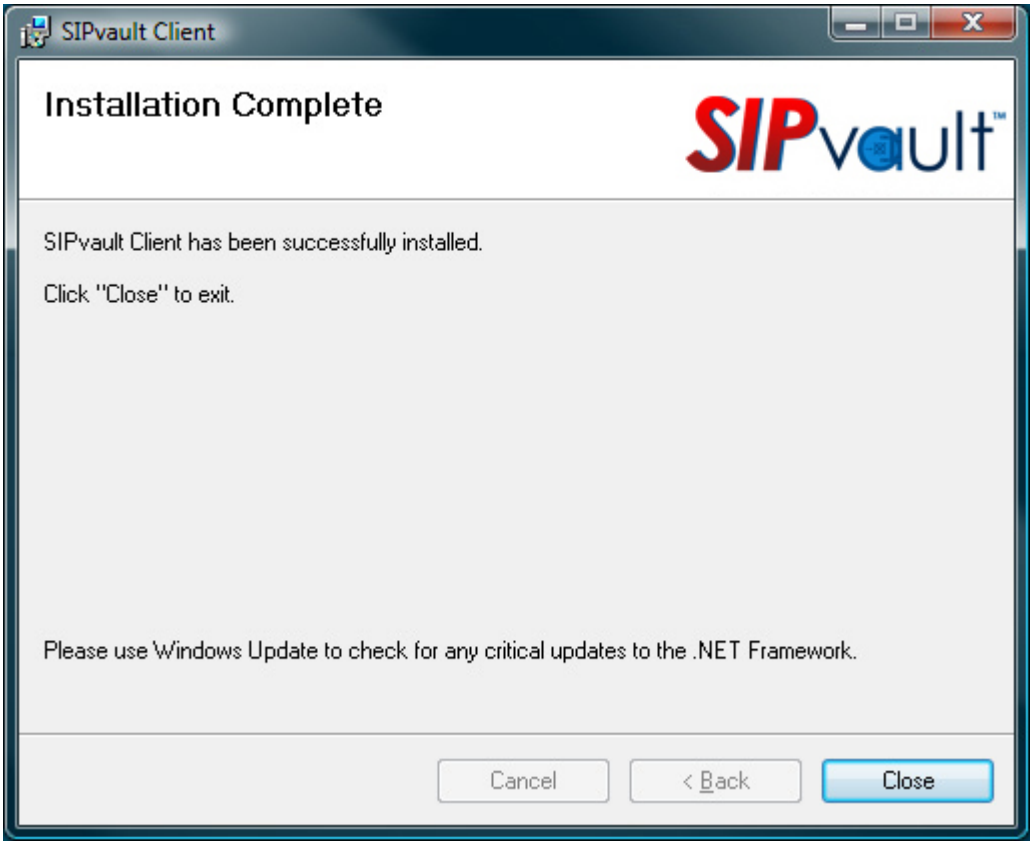


If the given agreement is satisfactory, select the 'I Agree' option, and then click the 'Next' button.

The installer will now be shown a confirmation screen. This is the last opportunity to change a previously entered setting before continuing with the installation. Once any changes have been made, click the 'Next' button on this screen to continue to installation.



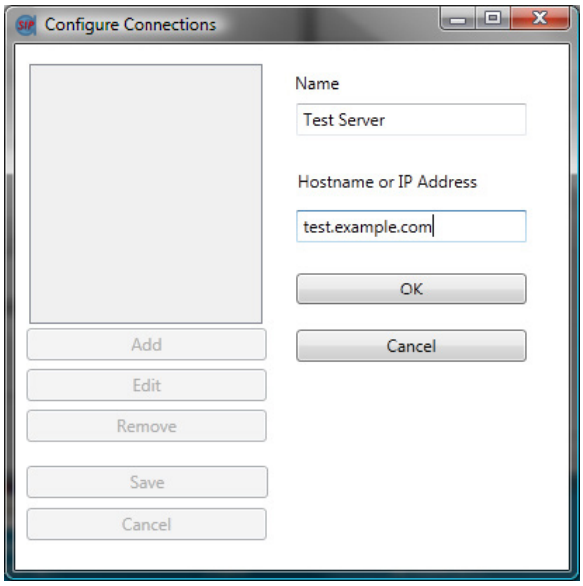
Once installation is completed, the following screen will be displayed. Click the ‘Close’ button to exit the installation process.

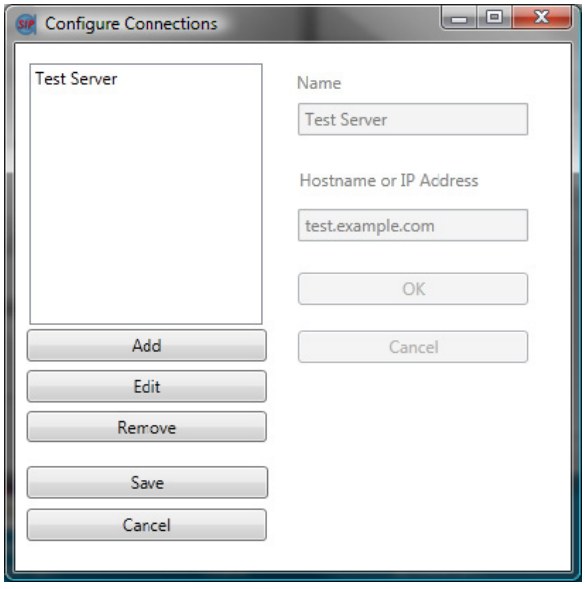


Administration

Connection Setup

When the SIPvault Client is launched, either from the Programs menu (under Network Harbor Inc, SIPvault, SIPvault Client), or from the desktop icon, the 'Log In' window will be automatically displayed, so that the user can select which SIPvault server to connect to. If the 'Log In' window has no configured connections, then the 'Configure Connections' window will be automatically displayed as well.





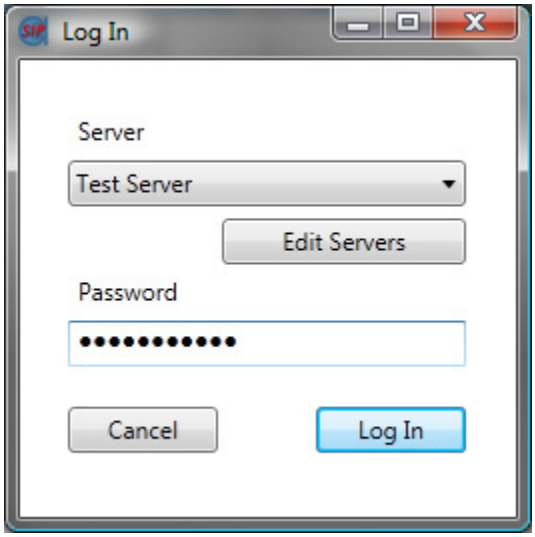
The Configure Connections window allows users to manage a list of SIPvault connections, adding, deleting, or editing items already on the list. If no connections are configured, then the window will be displayed automatically. To add a connection, click the 'Add' button, then fill in the Name (a meaningful label), and a Hostname or IP address for the server in question. Then click the 'OK' button to add this item to the list, or 'Cancel' to cancel the addition.

Connections can also be edited, by selecting an existing connection from the list, clicking the 'Edit' button, and then continuing as above. To delete a connection, simply select that connection in the list and click the 'Remove' button. The user will be asked to confirm that deletion is desired before the item will be removed from the list.

In order to save the changes made to the list and close the window, click the 'Save' button. If the user does not wish to save current changes, the 'Cancel' button may be pressed instead.

Log In

At the ‘Log In’ window, log in by selecting which server to connect to, and then entering a password and clicking the ‘Log In’ button. By default, the password is ‘adminsecret’. To cancel login, click the ‘Cancel’ button. To edit the list of available servers, click the ‘Edit Servers’ button.

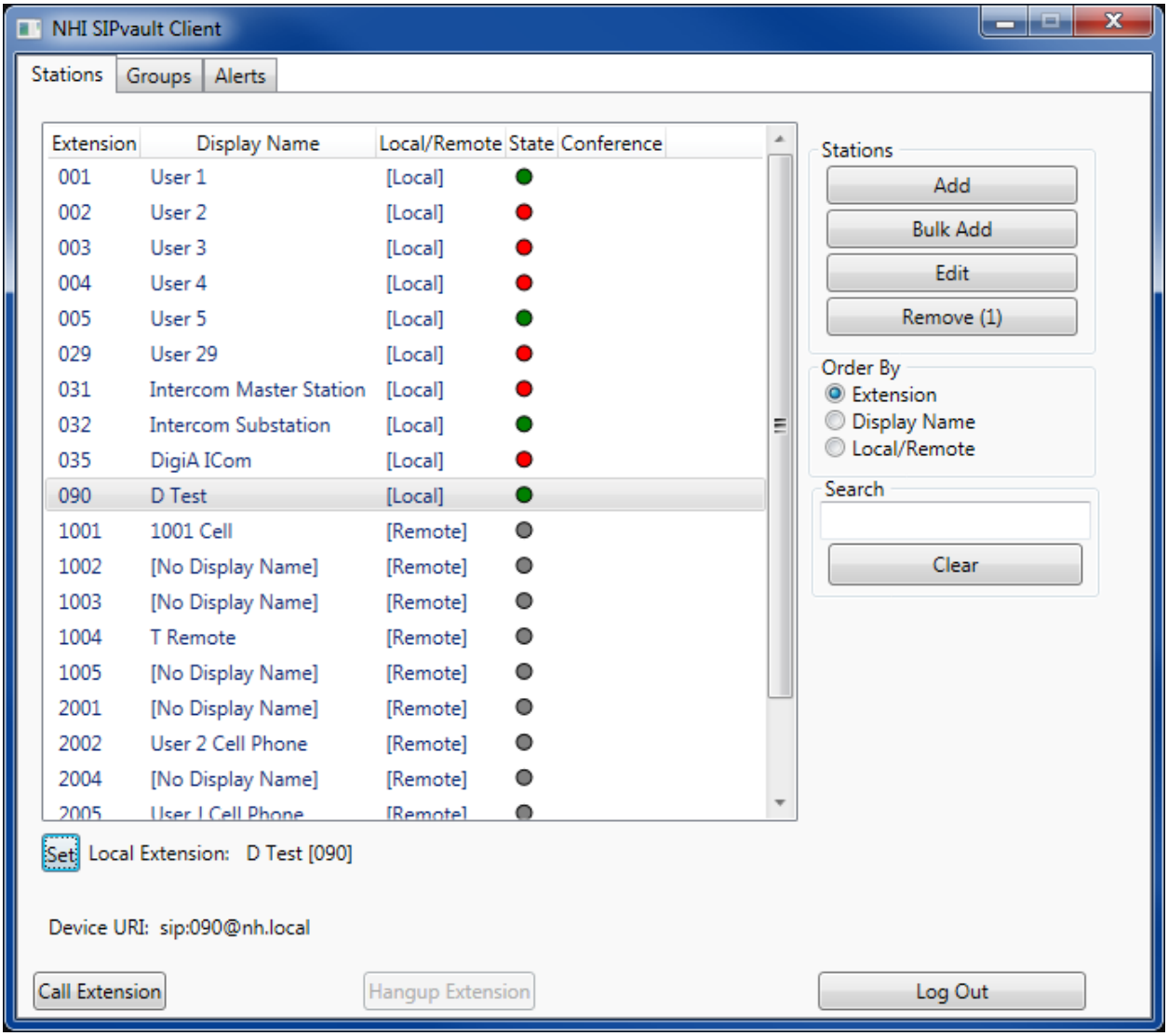


Log Out

The ‘Log Out’ button is located at the bottom-right of the NHI SIPvault Client main interface. Clicking this button at any time will log the client out of the system. The button will then become the ‘Log In’ button, displayign the ‘Log In’ window and allowing reconnection to the previous server, or any other configured server.

The Stations Tab

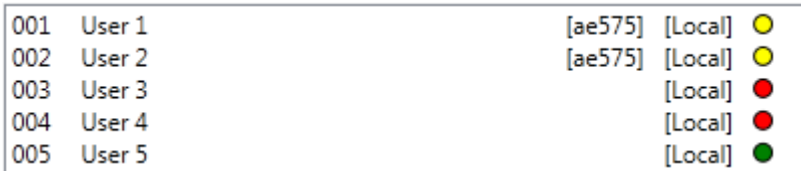
Upon logging into the SIPvault server, the main user interface (UI) will be displayed. The UI consists of three tabs, a 'Stations' tab, a 'Groups' tab, and an 'Alerts' tab. Stations are SIP devices representing a single entity.



Stations are represented in this interface as a short text descriptive line. Take the following example:

This is a station with the name '001'. The name is an identifier unique to this SIP server, and globally unique when combined with the SIP server's domain to produce a SIP URI. Further, the station has a Display Name of 'User 1', is a local station, and is online (green bubble). If this station was not currently registered, their bubble would be red. If the station was currently known to be in a call, the bubble would be yellow, and the first 5 characters of the call's unique identifier would be displayed. All stations that are currently in a call are sorted to the top of the list, and grouped by call.

In the following example, stations ‘User 1’ and ‘User 2’ are in the same call, stations 003 and 004 are not registered/online, and station 005 is online and available.



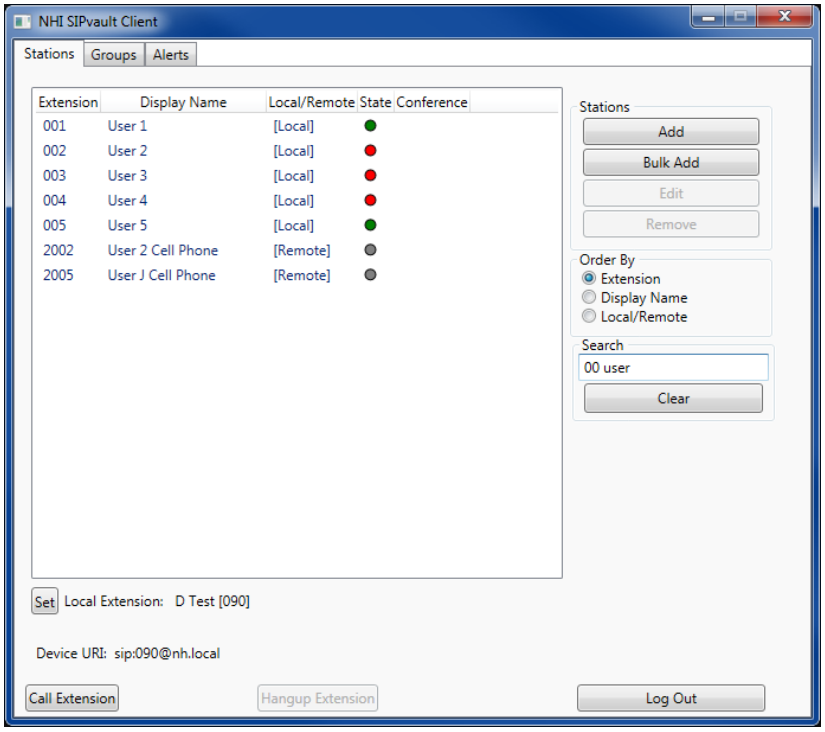
If a station is selected from the list, that station’s SIP URI, of the format ‘sip:002@example.com’ will be displayed in the space underneath the stations list.

Stations come in two types, local and remote. Local stations are SIP devices that register directly to the SIPvault server. These devices register and authenticate to the server directly. Remote stations are aliases that can be used to allow local stations to call SIP devices that are registered to other SIP servers. Because remote stations are registered to other SIP servers, their state cannot be monitored in real time.

Along the right side of this tab is a set of buttons allowing users to add, bulk add, edit, or remove stations. To edit or remove a station, simply select that station from the list and click the appropriate button. To add a station, click the ‘Add’ button. The ‘Bulk Add’ button is used to create a range of stations in a single operation. The ‘Remove’ button can apply to multiple objects at the same time, therefore a running count of the number of selected devices that would be deleted is shown on the button.

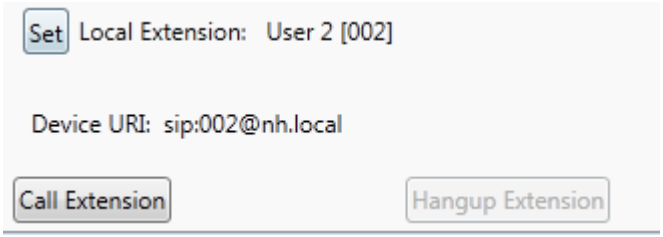
Stations in the list can be sorted in different fashions by selecting the different options under the ‘Order By’ group box. Name is unique and therefore sorts in a descending order on that attribute. Display Name is not necessarily unique. Any two stations with the same display name will be further sorted by Name. Type (local or remote) is also not unique, and devices will therefore be further sorted by Name.

There also exists a ‘Search’ box on the right side of the form, underneath the sorting options. This allows the user to search for a specific object or set of objects by their name or display name. Spaces are used to delimit terms, and only objects that have all of the given terms in their name or display name will be shown in the list. For example, if the text ’00 user’ was entered into the Search box, this would match (and therefore display) only those objects that had ‘00’ in their name or display name **and** have ‘user’ in their name and display name.



This functionality can be useful when searching for a particular object in larger systems. To return to the full object list, simply clear the text from the search box.

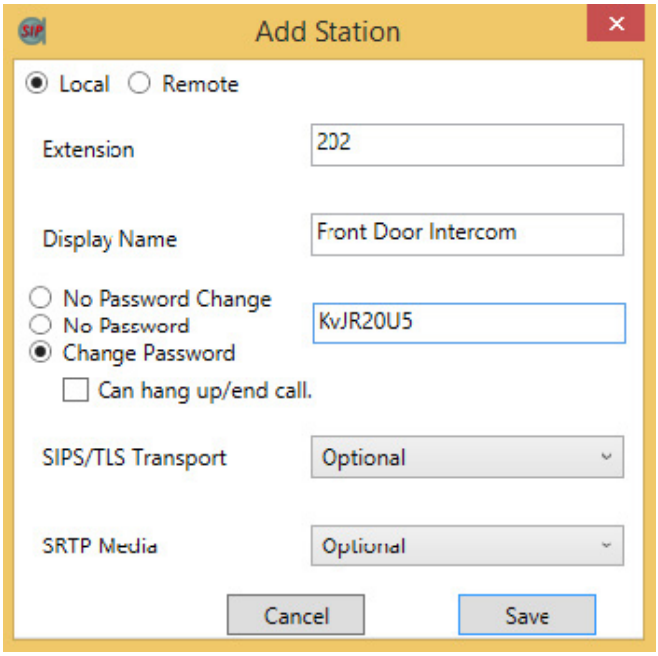
Finally, there is the calling functionality. To begin using call functionality, find the station extension for the SIP enabled phone/master station next to the operator's desk. Select this item, and then click the 'Set' button near the bottom of the form.



When another extension (on either the Stations, Groups, or Alerts tab) is selected, the 'Call Extension' button will be enabled if that extension is available to call (not currently in a call, and not the local extension). When this button is clicked, the device(s) defined as the local extension will ring.

Upon the local station answering this call, the target extension (be it another user, or a group, or an alert) will be called and placed into conference with the local device. If a user extension is selected that is currently in a call, the 'Hangup Extension' button will be enabled instead. Pressing this button will cause that extension to leave the call. If there are insufficient stations left in the conference to continue the call (only one station of any type, or any number of stations where all of them are 'byeless'), then the call will end.

Add/Edit Stations – Local Endpoints



A local station is one in which the SIP device registers to, and is directly managed by SIPvault.

Extension – A unique identifier across all SIPvault resources (Stations, Groups, Alerts) which is generally a number when used for intercom systems to allow for ease in dialing, such as '202'.

Display Name – An optional friendly name which can be used to identify the location or purpose of an intercom (such as 'Front Door Intercom'), which may be displayed during a call on some models of intercom master station/SIP phone.

The password field is used to authenticate messages coming from devices that attempt to represent themselves as this device. The options here consist of:

No Password Change – Preserves the current password configuration for this extension.

No Password – Indicates that if a password currently exists for this device, it should be removed. Messages purporting to originate the associated endpoint device should not be authenticated by means of password authentication.

Change Password – The password for this extension should be replaced with the contents of text box to the right of the password radio buttons.

Can hang up/end call. – This field indicates that this endpoint is not 'byeless'. Byeless endpoints are those stations, such as intercom substations, that cannot hang themselves up or remove themselves from a conference. A conference composed entirely of byeless endpoints is automatically terminated.

SIPS/TLS Transport – Defines the required security policy used for call control by devices at this extension. Possible values are Optional, Required, and Disabled.

Optional – Control communication with endpoint devices at this extension is secured by TLS if possible. SIPvault will automatically fall back to unsecured communication if the endpoint device does not use SIPS or TLS for control communication.

Required – Control communications with endpoint devices at this extension must use SIPS and/or TLS for control communication. SIPvault will forbid communication if the endpoint device does not use SIPS or TLS for control communication.

Disabled – Control communication with endpoint devices at this extension is unsecured. The endpoint device must be configured to use unsecured SIP over UDP or TCP.

SRTP Media – Defines the required security policy for media sent and received for this extension. Possible values are Optional, Required, and Disabled.

Optional – Media communication with endpoint devices at this extension is encrypted and authenticated if possible. SIPvault will automatically fall back to unsecured communication if the endpoint device does not indicate SRTP/SAVP support.

Required – Media communication with endpoint devices at this extension must use encryption and authentication. SIPvault will cancel the call if the endpoint device does not indicate SRTP/ SAVP support.

Disabled – Media communication with endpoint devices at this extension is unsecured. The endpoint device must be configured to allow unsecured media.

Details for the configuration of specific endpoint devices may be found in accompanying device-specific documentation provided by either Network Harbor, Inc and/or the manufacturer of the endpoint device. For general instructions, see the **Endpoint Configuration** section of this document.

Volunteer Call Routing Rules

One special case of configuring a local station is the configuration of a volunteer call routing rule. A volunteer call routing rule allows a user to 'volunteer' to take calls going to a certain extension. An example may make this idea more clear.

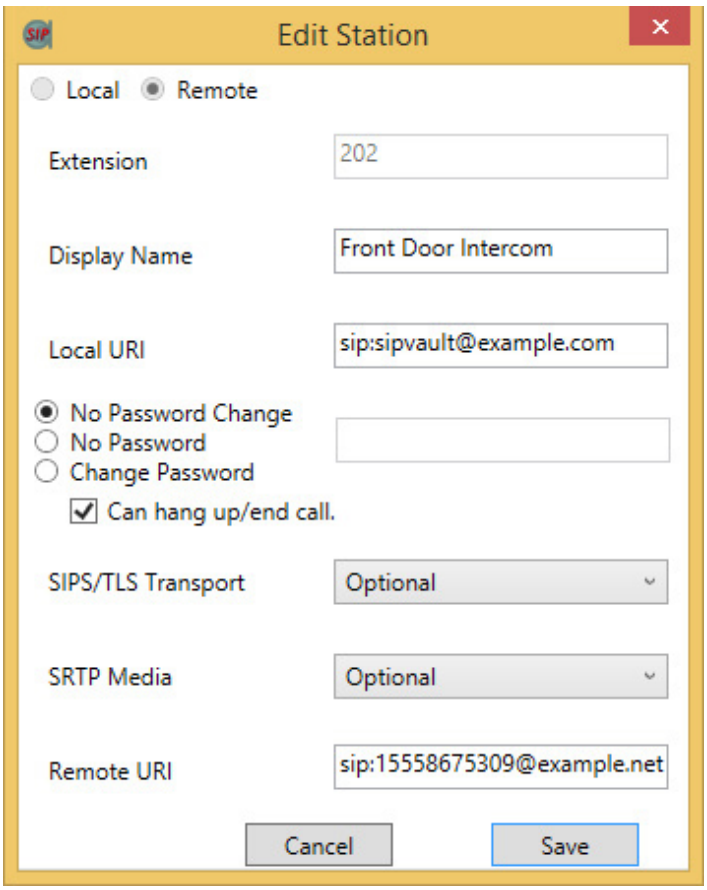
As a 'for instance', the installer wishes calls to extension 1001 to go to their security offices. However, they only want one security office to get the call, as the two offices are manned on different shifts. Suppose that office 1 has an extension of 9000, and office 2 has an extension of 8000. When configuring the local station that represents this rule, the installer will set the Extension as '1001', and the display name as '9000~8000'. What this means is that once the system starts, it will route calls made to extension 1001 (from any extensions other than 8000 and 9000) to extension 9000 (office 1). If office 2 calls extension 1001, their call will be automatically rejected – but now all calls to 1001 will be routed to 8000 (office 2). Should office 1 call 1001, their call will likewise be automatically rejected, but now incoming calls will be routed to 9000 (office 1). If calls are being routed to office 2, but office 2 calls 1001 again, they will receive a 'busy' notification. This means that the rule has been set to return to default behavior – in this case, routing to office 1.

In the general case, it may make sense to have the first entry in the list be an all-call group of all security offices (so if no one has currently volunteered to handle all calls, all security offices get it), OR a remote extension dialing an external resource. In these cases, once someone volunteers, the only way for the call routing to go back to default is if the volunteer cancels their request by calling again and getting a busy notification (as there is no way for an all-call extension, or a remote extension to call the 1001 extension).

If a user at another location has volunteered their extension to receive notifications but is no longer present to either take those calls or cancel their request, any other valid extension may dial the route extension twice to return to default operation. The first time, the extension will have the call rejected, indicating that they are now the target, and the second time they will receive a busy signal indicating that default operation is now in effect.

The system will also return to default operation after a system restart.

Add/Edit Stations – Remote Endpoints



A remote station is one which has a local URI, but does not register to, and is not managed by the SIPvault service. Instead, the device(s) represented by the remote station are registered to and managed by another SIP server.

Extension – A unique identifier and will represent the local URI which locally registered devices may use to call this remote device.

Display Name – An optional friendly name which can be used to identify the location or purpose of an endpoint (such as 'Front Door Intercom'), which may be displayed during a call on some models of intercom master station/SIP phone.

Local URI – The SIP URI of the call originator in the remote domain. SIPvault will use the local URI to 'call into' the SIP server managing the remote device. In this case, it is assumed that there is a SIP server at 'example.com', which we can call into as 'sip:sipvault@example.com'.

Password – The remote station is a different than that of a local station. When SIPvault 'calls into' the remote SIP device, that remote device may require authentication information. The password for 'Remote' stations is therefore the password required on the remote SIP system to authenticate as the 'Local URI' to that system.

Remote URI – The SIP URI of the call target in the remote domain. This may be another SIP station, or it could be a normal phone line if the remote domain has SIP->POTS connectivity. For more information regarding using SIPvault to call outward to POTS endpoints, email support@networkharbor.com.

SIPS/TLS Transport – Defines the required security policy used for call control by devices at this extension. Possible values are Optional, Required, and Disabled.

> **Optional** – Control communication with endpoint devices at this extension is secured by TLS if possible. SIPvault will automatically fall back to unsecured communication if the endpoint device does not use SIPS or TLS for control communication.

Required – Control communications with endpoint devices at this extension must use SIPS and/or TLS for control communication. SIPvault will forbid communication if the endpoint device does not use SIPS or TLS for control communication.

Disabled – Control communication with endpoint devices at this extension is unsecured. The endpoint device must be configured to use unsecured SIP over UDP or TCP.

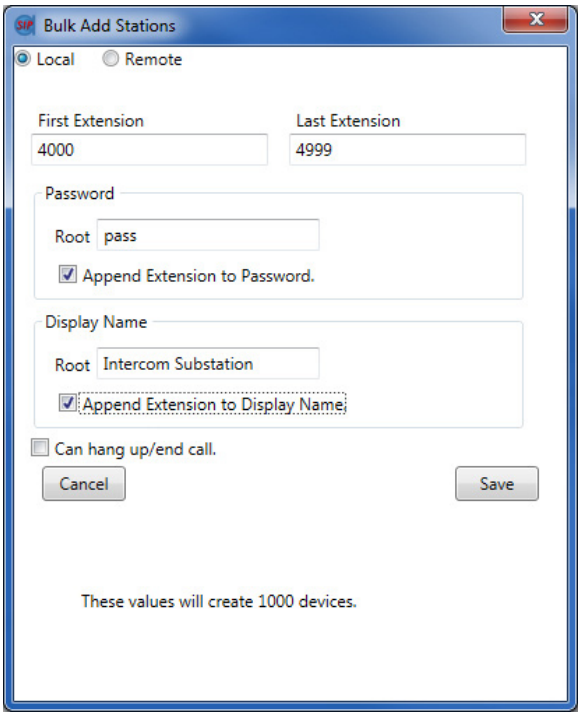
SRTP Media – Defines the required security policy for media sent and received for this extension. Possible values are Optional, Required, and Disabled.

Optional – Media communication with endpoint devices at this extension is encrypted and authenticated if possible. SIPvault will automatically fall back to unsecured communication if the endpoint device does not indicate SRTP/SAVP support.

Required – Media communication with endpoint devices at this extension must use encryption and authentication. SIPvault will cancel the call if the endpoint device does not indicate SRTP/ SAVP support.

Disabled – Media communication with endpoint devices at this extension is unsecured. The endpoint device must be configured to allow unsecured media.

Bulk Add Local Stations



When the 'Bulk Add' button is pressed on the 'Stations' tab, the following control will be displayed on screen. This is the 'Bulk Add Local Stations' control, and as the name suggests, it can be used to add a large number of devices to the system at a time, a convenience when configuring new systems, or adding large numbers of devices to an existing system.

The first two entries are required. The First Extension is the extension number of the first local station to be created. The Last Extension is the extension number of the last local station to be created. Both numbers must have the same number of digits in them so that the numbering format for the created block is consistent.

At the bottom, a piece of text will inform the user of how many devices the given range will create. If the input given is incorrect or not sufficient to generate a block of devices, this area will turn red and display an error message detailing what is wrong.

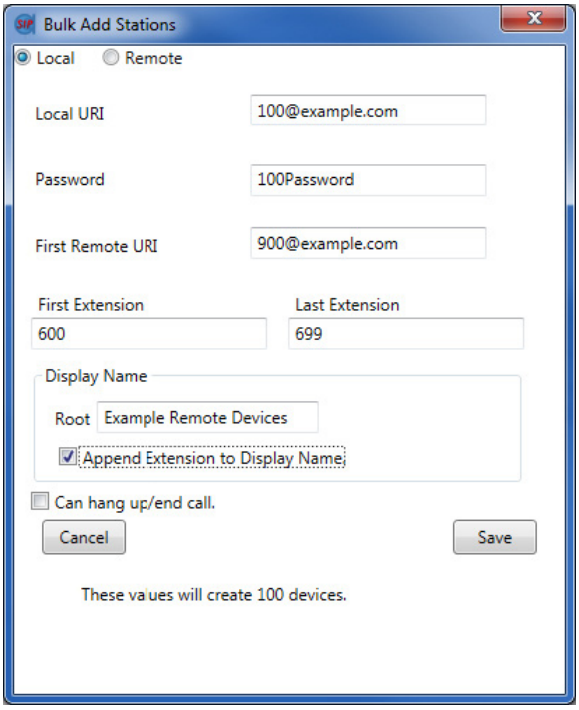
If it is desired to set a password for the devices to be created, that password can be typed into the 'Password Root' text box. If it is desired that each password be slightly different, the 'Append Extension to Password' checkbox may be activated. In this example, with a root of 'pass', and the checkbox activated, the generated local station with extension '4505' would have a password of 'pass4505'.

If it is desired to set a display name for the devices to be created, that display name can be typed into the 'Display Name Root' text box. Because this would generate a large block of devices with the same display name, it is possible to activate the 'Append Extension to Display Name' checkbox. This will append a space, and then the extension number to the display name. In this example, with a root of 'Intercom Substation', the generated local user with extension 4505' would have a display name of 'Intercom Substation 4505'.

When the user is satisfied with the given settings, click the 'Save' button. This will disable the UI, and show a progress bar showing progress in device creation. The 'Cancel' button may be clicked in order to exit without performing bulk station addition.

Local stations created in the Bulk Add Local Users window can be edited/changed like any other local user. All extensions configured with this mechanism use 'Optional' control and media security settings.

Bulk Add Remote Stations



If the 'Remote' type is selected on the 'Bulk Add Stations' window, it is possible to create a range of remote stations. Configuration here is similar to that of adding a single remote station.

The 'Local URI' is the resource identifier of an account on a remote SIP exchange, which the local SIP exchange can use as an origin to initiate calls to the remote SIP exchange's stations.

The 'Password' is the password of the resource identifying as the Local URI, and is used to authenticate as the Local URI to the remote SIP exchange.

The 'First Remote URI' indicates the base of the remote URI range. In this case, that number is '900@example.com'.

The First Extension is the extension number of the first local station to be created. The Last Extension is the extension number of the last local station to be created. Both numbers must have the same number of digits in them so that the numbering format for the created block is consistent.

When saved, the first extension (600) will be a remote station, pointed at the first remote URI (900@example.com). The next extension, (601), will point at 901@example.com, and so on, until the last extension (699) points at 999@example.com.

At the bottom, a piece of text will inform the user of how many devices the given range will create. If the input given is incorrect or not sufficient to generate a block of devices, this area will turn red and display an error message detailing what is wrong.

If it is desired to set a display name for the devices to be created, that display name can be typed into the 'Display Name Root' text box. Because this would generate a large block of devices with the same display name, it is possible to activate the 'Append Extension to Display Name' checkbox. This will append a space, and then the extension number to the display name. In this example, with a root of 'Example Remote Devices', the generated remote user with extension 605 would have a display name of 'Example Remote Devices 605'.

The checkbox for 'Can hang up/end call' is used to indicate if endpoints generated in this range will be 'Byeless' or not. Byeless endpoints are those stations, such as intercom substations, that cannot hang themselves up or remove themselves from a call. A call composed entirely of byeless endpoints is invalid and will be ended. Therefore, for a call to be valid, at least one participant must have the capability to hang up.

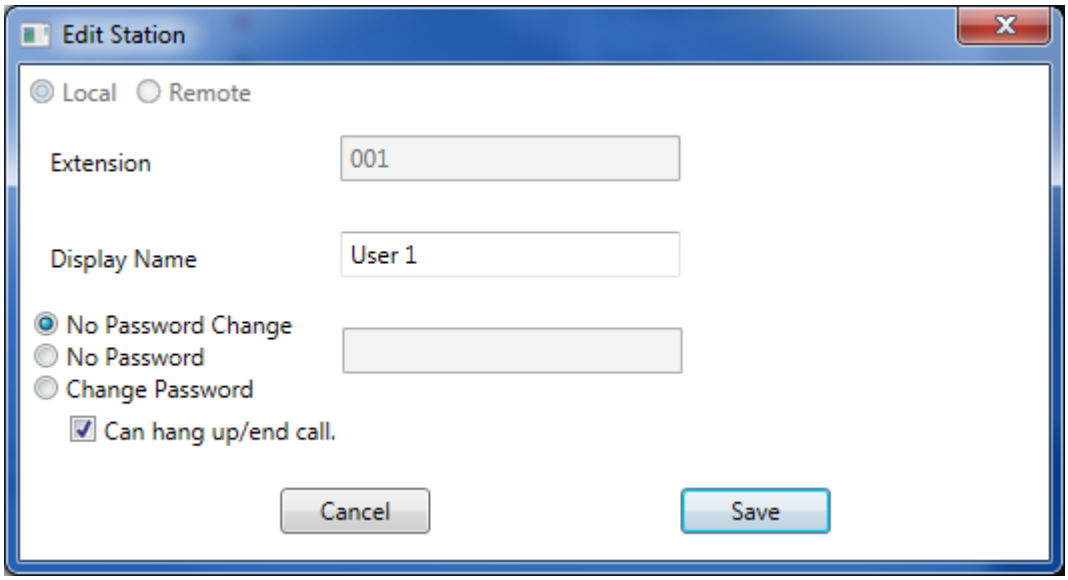
When the user is satisfied with the given settings, click the ‘Save’ button. This will disable the UI, and show a progress bar showing progress in device creation. The ‘Cancel’ button may be clicked in order to exit without performing bulk station addition.

Local stations created in the Bulk Add Local Users window can be edited/changed like any other local user. All extensions configured with this mechanism use ‘Optional’ control and media security settings.

Examples

This is an example of an edit being performed on a local SIPvault station object. The extension is '001', meaning that the devices registered as this station (assuming that the SIPvault server is 'example.com') will have the URI <sip:001@example.com>. The display name of 'User 1' will be displayed as caller information on capable SIP master stations/phones. As the 'No Password Change' option has been selected, saving this station will not change their previous password configuration, regardless of what it is.

Note: The Local and Remote radio buttons are disabled. Once a station has been created, these options cannot be modified during station edit. If necessary, delete the existing station of a given type before creating a new station of the other type.



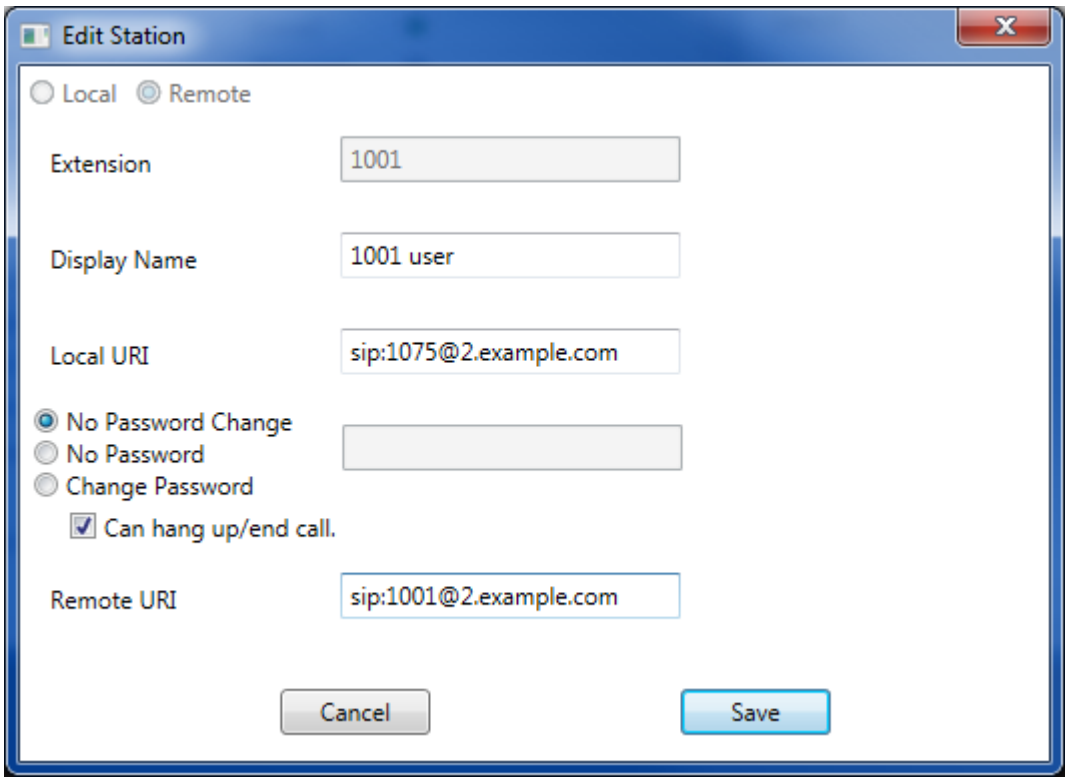
This is an example of an edit being performed on a remote SIPvault station object. The station is '1001', meaning that the devices registered to the SIPvault server (assuming that the SIPvault server is 'example.com') will have call the uri 'sip:1001@example.com' in order to contact this device. The display name of 'Test remote user' will be displayed as caller information on capable SIP master stations/phones.

The 'Local URI' given is 'sip:1075@2.example.com'. This means that after the call is routed through SIPvault, the call will go to 2.example.com and will be 'from' 1075@2.example.com. This allows SIPvault to perform cross-domain calls with other SIP systems that allow registration.

The 'Change Password' option is selected and set to '1075Password', indicating that if the remote server '2.example.com' requires authentication when SIPvault sends messages to it as '1075@2.example.com', SIPvault should use the password '1075Password' to authenticate itself.

The 'Remote URI' of 'sip:1001@2.example.com' indicates that the purpose of this remote station is to allow local endpoints to call the device(s) identified by the URI 'sip:1001@2.example.com'.

Thus, if a local user dials '1001', the call will then be bridged to the remote SIP server '2.example.com', and represented there as a call between 1075 (which has the password '1075Password'), to 1001.

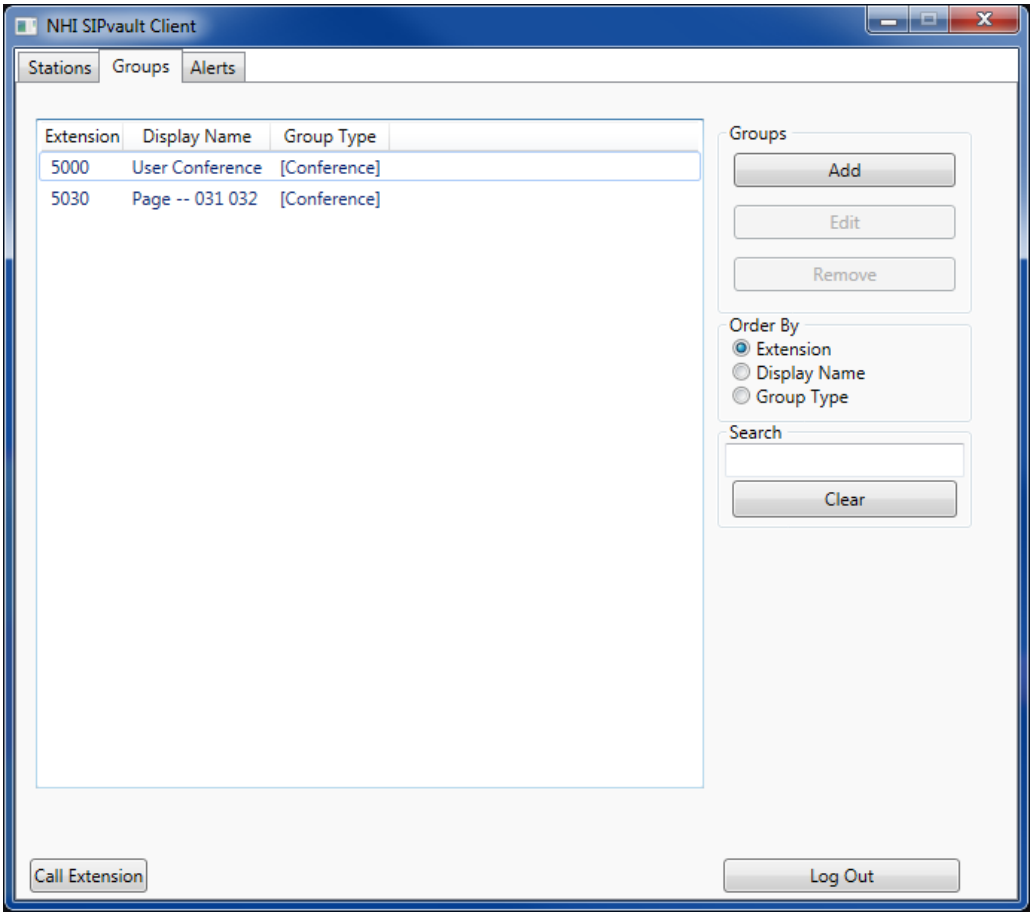


The Groups Tab

The other tab in the SIPvault Client UI is for viewing and administrating groups. Groups are calling functions that are associated with a collection of users, and can be used to make simplified calling rules. The Groups tab, similar to the Users tab, contains a list of objects, buttons to create, edit, or remove objects, and a few sorting options.

In the example below, there are five groups. A group's extension is what number a device should dial in order to activate the group call. This must not collide with a user extension. The display name is a user-friendly name intended to give some information about that purpose or configuration of the group call, but has no technical meaning. The Group Type describes what group call function this group uses. Groups have no state. The available group types are Conference, AllCall, Paging, and Tour. The functions of these types are described in the section below on adding and editing groups.

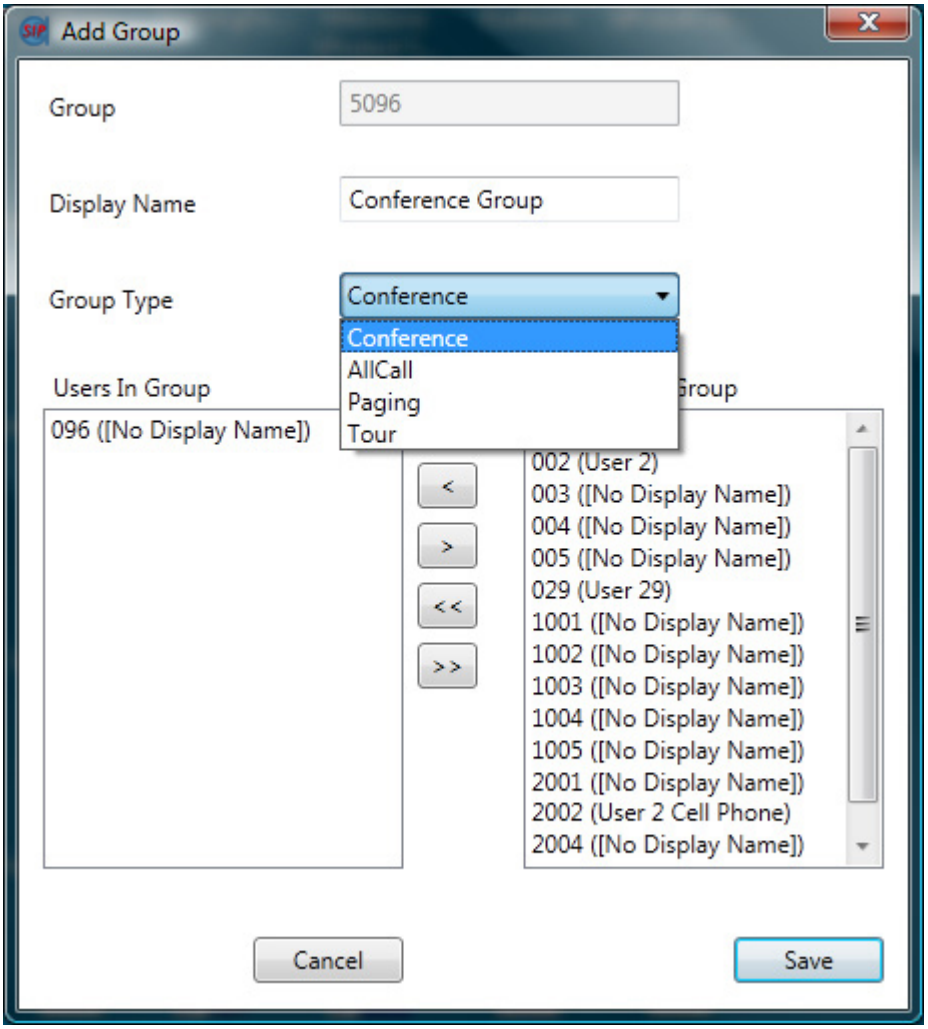
Along the right side of this tab is a set of buttons allowing users to add, edit, or remove groups. To edit or remove a group, simply select that group from the list and click the appropriate button. To add a group, click the 'Add' button.



The Search box works in the same way as that for Users, filtering results based upon name and display name.

Add/Edit Groups

When adding or editing a new group, the following control will be displayed. If editing an existing group, the 'Group' field will be disabled.



The 'Group' name is a field designating what number is used to address this group. This number must be unique on this SIPvault server between groups, stations, and alerts.

The 'Display Name' is a meaningful label used to describe the function or members of a group to the user.

The 'Group Type' determines the functionality of the group.

> 'Conference' – Performs a conference call into which all included stations are invited. All endpoints in a group will ring, and when the call is received will be added to the conference where all users can speak and be heard. This type is most useful for groups of master stations, as everyone has the ability to pick up and hang up the phone/master station.

'AllCall' – Performs a call to which all included stations are invited. When the first device picks up, that station is connected to the station which called this group, and the invitations to all other members of the All Call group are cancelled. This function is sometimes used for 'night transfer'. As the first individual picking up is placed into the call and all others cancelled, it makes little sense to include intercom substations (which pick up automatically) in this type of call group.

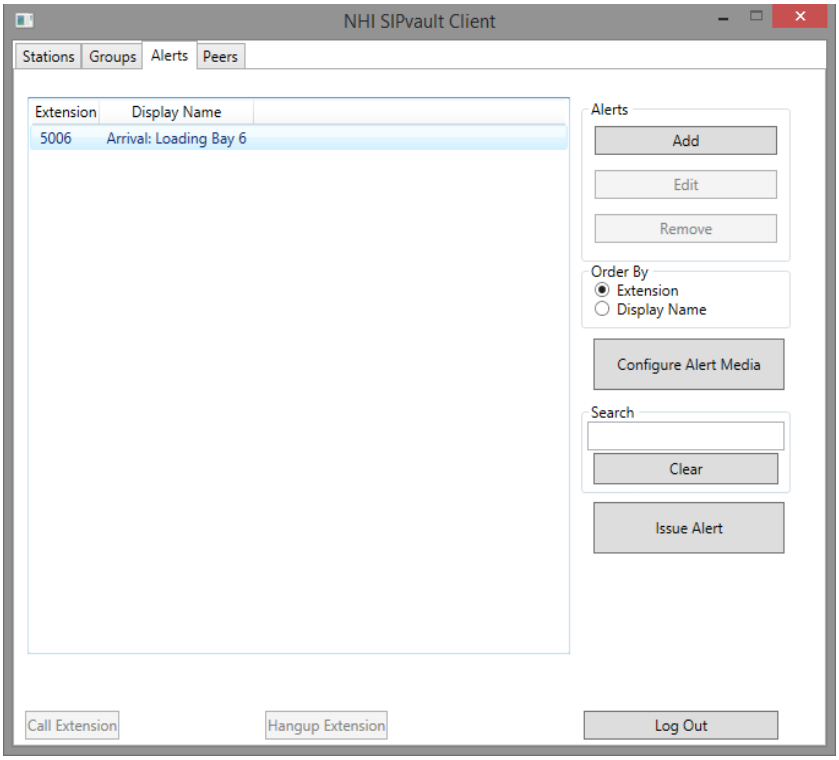
'Paging' – Much like Conference, performs a call to which all included stations are invited. All endpoints in the group will ring, and when the call is received will be added to the call. The difference is that in a paging call, only the intercom that initiated the conference can talk. All of the called stations can only receive, but not send audio. This is useful for paging in public areas and is ideal for groups of intercoms, as they pick up automatically.

'Tour' – Calls the included stations in sequence, with a delay between stations. When a device picks up, the call is connected between the caller and the station that picked up only. This type of group can be used for access, where an intercom substation calls a tour which first rings the nearest guard station, then a different guard station, then main security. As the first individual picking up is placed into the call, it makes little sense to include intercom stations (which pick up automatically) in this type of call group.

Note: When the 'Tour' group type is selected, another field labeled 'Tour Delay' is shown. This is used to allow the operator to describe how long SIPvault should wait (in seconds) between invites to successive target stations. The maximum value is 120 seconds (two minutes).

It should be noted that many SIP endpoints will only ring for a set period of time, often less than two minutes. In these cases, the phone will ring for as long as it is configured to do so, but SIPvault will wait for the entire delay time before ringing another station. If for instance, the first station on the list rings for a maximum of 30 seconds, but the 'Tour Delay' is set to 60 seconds, the first station will ring, cease ringing, and only 30 seconds after that will the next station on the list begin ringing. It is therefore important to configure this time period in a fashion that works will with the hardware SIP devices selected.

The Alerts Tab



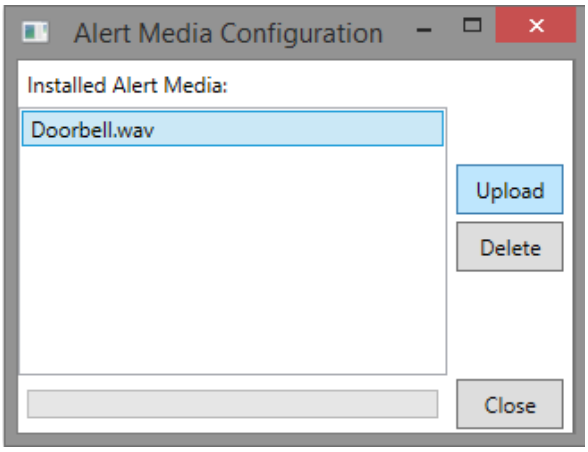
The Alerts Tab is used to create and issue alerts or announcements. An alert is a type of resource, like a station or group, which is primarily identified by its extension. As in all other cases, the extension must be unique upon the SIPvault Server it is created upon. Each alert also has a Display Name, which is utilized by users to identify the purpose of the alert.

Alerts have two possible delivery mechanism, which depends upon whether the target is disconnected or is in a conference when the announcement operation is requested. If the target resource is in a conference, the announcement is injected into the existing conference, and the conference persists after the alert has played. If the target is disconnected, it is connected to a temporary conference for the duration of the announcement.

Announcement operations have three modes of failure. Announcements which target a Group Resource are all-inclusive and only play to a conference that contains all members of that group – if the members are in separate conferences, the announcement will fail or be deferred. Also, if the announcement target is not in the disconnected or established state, it is excluded from the operation, and an announcement will fail if no valid endpoints are found. Finally, announcements will not play concurrently, so any ongoing announcement will block or defer new announcement requests.

The purposes of the Add, Edit, and Remove buttons, as well as the OrderBy, Search, Call Extension, and Log Out sections of the Alerts Tab are identical in purpose to those on the Station and Groups Tabs.

Configure Alert Media



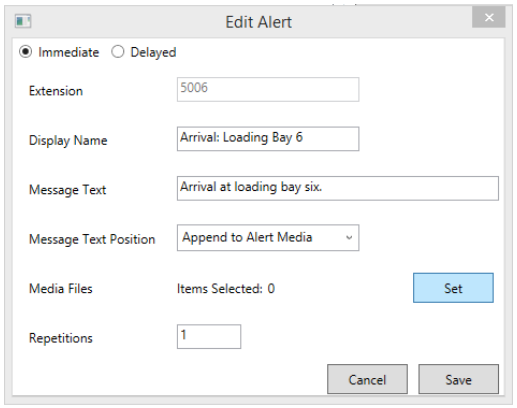
The Alert Media Configuration window can be accessed from a button on the Alerts tab. This window contains a list of all alert media sound files currently stored on the SIPvault server instance. It also allows the user to upload new WAVE files from the client, and files that are stored on the server.

The upload mechanism allows the user to uplaod a WAVE file from the local computer to a SIPvault instance for use with an audio Alert.

The audio file should be single channel audio sampled at 8Khz or 16Khz. The maximum size of an uploaded audio file is 67108864 bytes (64 MB).

Instructions for creating a WAVE file for use as an Alert are beyond the scope of this document. Many applications such as Microsoft Sound Recorder may be used; refer to the documentation for your sound recording/editing software to find instructions for creating WAVE format sound files.

Add and Edit Alerts

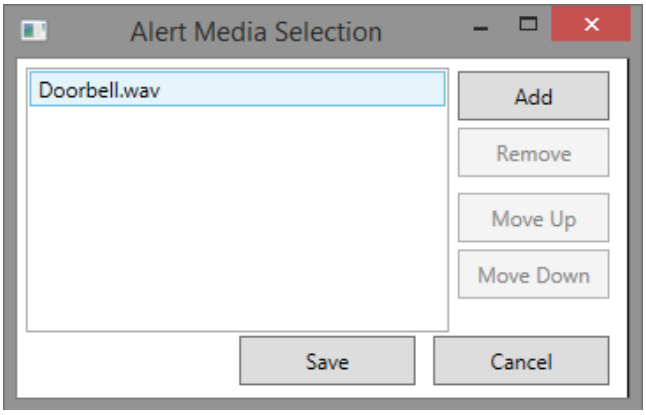


The Add and Edit buttons display the Add/Edit Alert dialog, which is used to create new or modify existing audio alerts. The Extension and Display Name fields are identical to those used for Stations and Groups.

The Immediate or Delayed radio buttons indicate desired behavior if the alert target is currently in a call. Immediate alerts are conditional upon the current state of the endpoint – if the announcement cannot be delivered immediately, the announcement operation will fail. Delayed alerts will enqueue the announcement request until the target resource is in a state that allows for the announcement to play, and then deliver the announcement using whichever delivery mechanism is appropriate.

The Message Text is a piece of text that will be converted to audio using the server hosts' text to speech engine and read to the endpoint. The behavior of this component of an alert is dependent upon the configuration of the Message Text Position and the selection of Media Files.

The Message Text Position indicates the whether the text-to-speech component will precede or follow an alert media file, or if the text will be reserved as fallback in case no media file is specified or available.



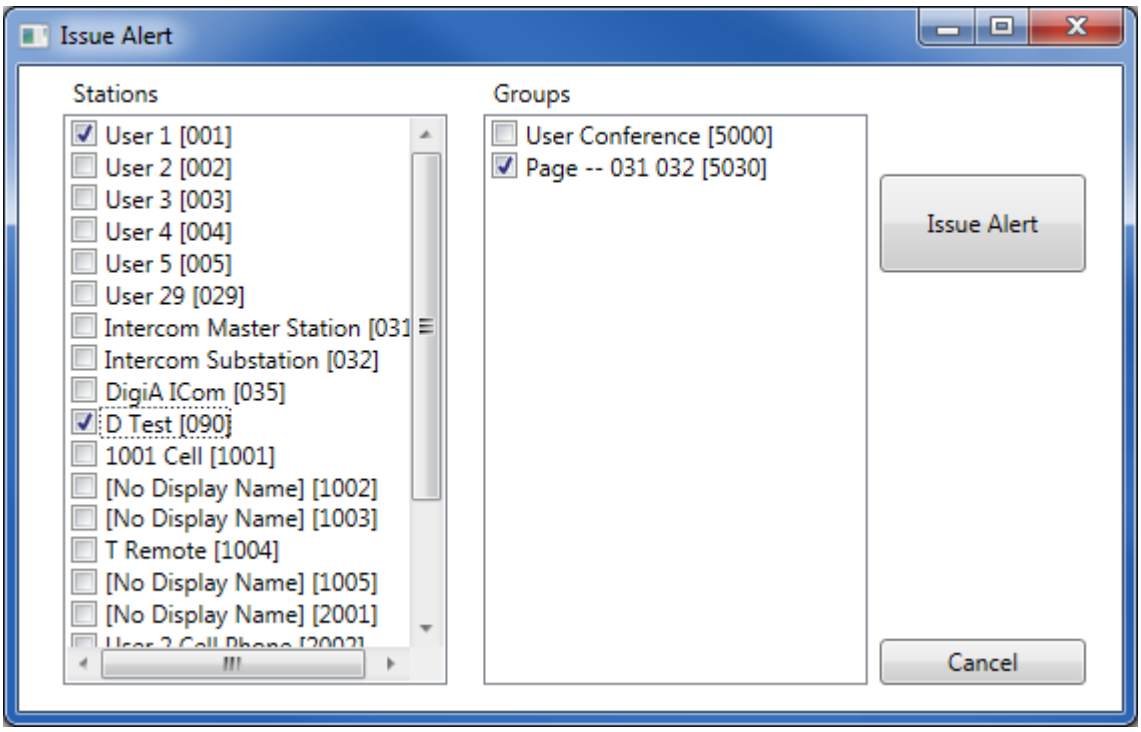
The Media Files field indicates the number of individual audio clips that will be combined to form the alert, not including the Message Text. To select media files, click the *Set* button in the Edit Alert window. The administrator can then select from media files stored on the server and order the sound clips as desired.

The Repetitions field (default 1) indicates how often this should be repeated before the alert hangs up on the target station. One second of silence is played before each message repetition. A repetition count of zero indicates that the alert should repeat forever, until the target station hangs up. An alert with a repetition count of zero is invalid for byeless stations as they are unable to hang up and will otherwise receive the repeating alert indefinitely.

Note: With the above mechanisms, it is possible to create a wide variety of static and dynamic audio alerts for use with a SIPvault audio system. ***Be sure to test every alert*** *to ensure correct and desired operation.*

Issuing Alerts

The Issue Alert button on the Alerts Tab is used to target one or more stations or groups with a selected alert. To issue and alert, an alert must be selected from the alerts list. Then click the 'Issue Alert' button.



In the Issue Alert dialog, simply select the stations and groups that should hear the alert message. Stations will be invited to a call, and when the alert is completed, will be hung up upon. A group which is targeted shall behave in the manner assigned to the group. Therefore group types such as All Call will ring all stations, but only the first group member to accept the call will hear the message.

Clicking the 'Issue Alert' button in this dialog will cause all targeted resources to be called. If there is an issue placing an alert for any of the resources, a message box will inform the user of this once all alert issues have been attempted.

The Peers Tab

The Peers tab is used to review and modify the list of SIP Peer Servers used by the connected SIPvault Server instance. This replicates the configuration functionality found in the service configuration utility.

SIPvault Client also provides an indication of connectivity between the current SIPvault Server instance and each configured peer. The status icon indicates the following conditions:

Green – The remote server is responding and correctly configured as a SIP Peer Server.
Yellow – The remote server is not configured to peer with the connected SIPvault server.
Red – The remote peer server is not responding to requests.

See *Service Configuration – SIP Peers* for additional information about SIPvault Peer Server configuration.

Station Configuration

SIPvault is implemented with SIP standards compliance as a principal design goal. Implementers can expect SIPvault compatibility with most SIP-compliant endpoints. In general, SIP station configuration should be performed in accordance with the SIP station manufacturer's instructions. This section provides generic instructions for configuring SIP Master Stations and SIP Substations.

Device-specific instructions can be found for certain hardware in these supplementary documents:

- SIPvault Endpoint Guide – NHI-IS-100 Security Intercom
- SIPvault Endpoint Guide – Yealink T2x Enterprise IP Phone

Before proceeding with station configuration, ensure that SIPvault is configured, any relevant DNS changes have been made, and extensions for each station have been defined with SIPvault Client.

Station Configuration: Network Parameters

Configuration of network parameters for each substation is installation specific. SIPvault supports IPv4 and IPv6 addressing mechanisms, and optionally makes use of the Domain Name System (DNS) to provide location services. Consult your network administrator for your installation's addressing guidelines and network traffic is routable between the SIPvault server and each station.

All stations are expected to require these minimum parameters for configuration:

- Station IP Address and Netmask
- DNS Server IP Address
- Default Gateway IP Address

Station Configuration: SIP Master Stations

SIP Master Stations are broadly defined as endpoints with a dialing pad. These stations can be used to dial specific extensions on-demand. For most deployments, generic SIP telephones fill the role of a master station. Master stations are also capable of removing themselves from established calls.

SIP devices must be minimally configured with an account name, account password, and SIP registrar for correct operation. The account name and account password must match the parameters configured with the SIPvault Client. The registrar is the hostname of the SIPvault server, as entered in Hostname group box in the SIPvault Configuration Utility.

Several additional configuration parameters are common, although usually optional. An Outbound proxy identifies a specific address for outbound communication; this is should be configured with the IP address of the SIPvault server. A separate authentication username field may be available; this should match the account name.

Finally, if your installation is making use of TLS security, each station must be configured with the Authority Certificate that authenticates the SIPvault server. Use of certificates for client authentication is supported as a replacement for password authentication.

Station Configuration: SIP Substations

SIP Substations are application specific endpoints with limited input options. They are pre-configured to call a master station or master group on an event trigger; typically, pressing a call button. Substations usually cannot remove themselves from established calls.

The configuration of a SIP substation uses all the parameters described in Station Configuration: SIP Master Stations, with the addition of pre-configured master station extension. If a SIP URI is required for this field, refer to the device-specific URI of the preferred master station as displayed in the SIPvault Client.

> *Installer's Note:*
>
> *It may be expedient to configure a single-repetition alert on the master station's extension during the installation process. This will allow the installer to test each station during configuration.*
>
> *The alert can be replaced with a master station calling group once installation is complete.*

Using NHI CA Store Files to Create X.509 Certificates

Network Harbor Inc encourages everyone to make use of TLS to secure network communications in all applications. To use TLS for SIPvault communications, X.509 certificates must be created and distributed to all connected devices.

To simplify the creation and storage of X.509 certificates for SIPvault Server, the SIPvault Configuration Utility provides a proprietary mechanism to manage a unified certificate issuing authority. This mechanism uses NHI CA Store files (with the *.nhicas* extension) to store and transport all certificates created by the certificate authority.

Creation of a NHI CA Store is triggered by the *Create* operation on the Trusted Certificates tab of the SIPvault Configuration Utility. The new certificate authority will be automatically imported into the Root store of the local computer, and a new NHI CA Store *(.nhicas)* file will be created. The NHI CA Store file can be used to assign trust to the certificate authority on other computers using the Trusted Certificates *Import* mechanism in the SIPvault Configuration Utility.

SIPvault host certificates may be created from a NHI CA Store by triggering the *Create* operation on the Host Certificates tab of the SIPvault Configuration Utility. The new host certificates will be automatically imported into the certificate store of the SIPvault service, and both the certificate and the associated private key will be archived in the NHI CA Store file. All host certificates generated from an NHI CA Store can be retrieved from the NHI CA Store file at a later date using the Host Certificates *Import* mechanism in the SIPvault Configuration Utility.

Follow these guidelines to ensure trouble-free usage of the NHI CA Store mechanism:

- Always use the most recent copy of the NHI CA Store. Generating host certificates with separate copies of the store will result in namespace collisions.
- Use a strong passphrase to protect the NHI CA Store. The passphrase is used to encrypt the private keys of all certificates issued from the store.
- Keep the NHI CA Store in a secure location, and always backup the most recent copy of the NHI CA Store file.

Appendix A – X.509 Certificate Signing Requests for SIP

This appendix is dedicated to explaining the format and extensions recognized by SIPvault and other SIP endpoints, and provide recommendations for certificate signing requests sent to third party certificate authorities.

Host Certificates for SIPvault Server

SIPvault and other SIP servers that use TLS and the *sips:* scheme are required to provide an X.509 certificate for authentication to other SIP entities. These servers handle data for their own domain and should declare an appropriate domain identity (e.g. *sip:example.com*). To declare this identity, the *Subject Alternative Name* extension should be used with *URI* and *DNS* extensions. In addition, it is recommended that the hostname of the SIPvault server (e.g. sip:sipvault1.example.com) also be included in the list of identities.

> *Note:*
>
> *Subject Alternative SIP identities must use the 'sip:' URI scheme. Do not encode the 'sips:' scheme in X.509 certificates.*

Also, the host certificate public key should be marked for usage in a SIP domain. To declare this usage, the *Key Usage* extension should be used with the *Digital Signature and Non-Repudiation key usage* OIDs, and the *Extended Key Usage* extension should be used with the *SIP Domain* extended key usage OID. For reverse compatibility, NHI also recommends that the *Server Authentication* and *Client Authentication* extended key usage OIDs be used.

An example OpenSSL CSR configuration file is specified below for the *example.com* SIP domain hosted on a computer with the *sipvault1.example.com* DNS host name.

```
[ req ]
prompt                  = no
distinguished_name      = server_distinguished_name
req_extensions          = v3_req

[ server_distinguished_name ]
commonName              = sipvault1.example.com
organizationName        = Example Company Name
organizationalUnitName  = Example IT Division

[ v3_req ]
basicConstraints        = CA:FALSE
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid,issuer
keyUsage                = digitalSignature,nonRepudiation
extendedKeyUsage        = serverAuth,clientAuth,1.3.6.1.5.5.7.3.20
subjectAltName          = @alt_names

[alt_names]
URI.1                   = sip:example.com
URI.2                   = sip:sipvault1.example.com
DNS.1                   = example.com
DNS.2                   = sipvault1.example.com
```

Host Certificates for SIPvault Endpoints

In addition to passphrase authentication, SIP Endpoints which connect to SIPvault may optionally use X.509 Certificates for authentication. The format of these certificates is similar to a SIPvault server certificate; the notable differences are the use of a SIP User Identity instead of a SIP Domain Identity, and the omission of the Server/Client Authentication OIDs.

> *Note:*
>
> *The recommendations for X.509 extensions found in this Appendix are derived from IETF RFC 5922 and IETF RFC 5924.*

An example OpenSSL CSR configuration file is specified below for the sip:5000@*example.com* SIP endpoint.

```
[ req ]
prompt                  = no
distinguished_name      = server_distinguished_name
req_extensions          = v3_req

[ server_distinguished_name ]
commonName              = 5000@example.com
organizationName        = Example Company Name
organizationalUnitName  = Example IT Division

[ v3_req ]
basicConstraints        = CA:FALSE
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid,issuer
keyUsage                = digitalSignature,nonRepudiation
extendedKeyUsage        = 1.3.6.1.5.5.7.3.20
subjectAltName          = @alt_names

[alt_names]
URI.1                   = sip:5000@example.com
```

Administration Certificate for SIPvault Client

Similar to SIP endpoints, SIPvault Client has the capability to connect to SIPvault Server using an X.509 Certificate. This certificate is identical to the certificate of a SIP Endpoint with a single exception; the SIPvault client must declare the 'admin' user name in the SIP Identity.

An example OpenSSL CSR configuration file is specified below for a SIPvault Client certificate that connects to a SIPvault Server running on the *sipvault1.example.com* host.

```
[ req ]
prompt                  = no
distinguished_name      = server_distinguished_name
req_extensions          = v3_req

[ server_distinguished_name ]
commonName              = admin@sipvault1.example.com
organizationName        = Example Company Name
organizationalUnitName  = Example IT Division

[ v3_req ]
basicConstraints        = CA:FALSE
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid,issuer
keyUsage                = digitalSignature,nonRepudiation
extendedKeyUsage        = 1.3.6.1.5.5.7.3.20
subjectAltName          = @alt_names

[alt_names]
URI.1                   = sip:admin@sipvault1.example.com
```

Appendix B – NAT Traversal for SIP Endpoints

This appendix provides guidance for SIPvault installations which include SIP endpoints that reside behind a Network Address Translation (NAT) routing device.

SIPvault provides support for SIP endpoints by application of Symmetric Response Routing as described in RFC 3581. Upon receipt of a REGISTER request, the SIPvault Server will record the contents of the host field and received parameter of each Via header. This data is subsequently used to route outgoing SIP requests and RTP packets to the publicly visible address of the NAT routing device.

The following guidelines should be followed when deploying SIP Endpoints behind a NAT routing device:

- Each SIP Endpoint that resides behind a NAT should use a unique extension.
- NAT-resident endpoints should implement the mechanisms described in RFC 3581.
- NAT-resident endpoints should use TCP or TLS for SIP signaling.