

Information and/or specifications published here are current as of the date of publication of this document. Tridium, Inc. reserves the right to change or modify specifications without prior notice. The latest product specifications can be found by contacting our corporate headquarters, Richmond, Virginia. Products or features contained herein are covered by one or more U.S. or foreign patents. This document may be copied by parties who are authorized to distribute Tridium products in connection with distribution of those products, subject to the contracts that authorize such distribution. It may not otherwise, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written consent from Tridium, Inc. Complete Confidentiality, Trademark, Copyright and Patent notifications can be found at: <http://www.tridium.com/galleries/SignUp/Confidentiality.pdf>. © 2013 Tridium, Inc.

JACE, Niagara Framework, Niagara AX Framework and the Sedona Framework are trademarks of Tridium, Inc.

Fox Tunneling and HTTP Tunneling

This document describes Fox Tunneling and HTTP Tunneling in the following main sections:

- [About 2013 Security updates](#)
- [About Fox Tunneling](#)
- [About HTTP Tunneling](#)
- [Document change log](#)

Using NiagaraAX-3.3, or later version, a *client* can establish a workbench connection to one or more JACE *hosts* using a "tunnel" connection that is established using a NiagaraAX Web Supervisor *proxy* station. Two methods are provided. Both methods employ addressing schemes that require the following:

- specific ("fox" and "http") additional licensing on a Web Supervisor proxy station
- an appropriate network connection
- NiagaraAX-3.3, or later, on all platforms

Note: *Starting in NiagaraAX-3.5, platform tunneling is available as described in Appendix C, NiagaraAX-3.5 Platform Guide. In versions prior to NiagaraAX-3.5, tunneling is a Station-to-Station communication only; Platform tunneling is not available.*

Fox tunneling and HTTP tunneling use the Fox and HTTP communication protocols, respectively, to communicate with NiagaraAX stations. The key benefit that the tunneling feature provides is the ability to establish a workbench session with one or more JACEs that would normally be hidden from public access. This is done by allowing the requesting station (client) to communicate (or "tunnel") *through* a Supervisor station that has a connection to the targeted JACEs and acts as a proxy server for those targeted hosts.

Starting in NiagaraAX-3.4, the following properties are available to increase tunneling security options:

- **Only Tunnel Known Stations**
This property (located under the NiagaraNetwork > Fox Services component) affects the functioning and required syntax of both Fox and HTTP tunneling. It is an option to restrict both types of tunneling to only stations that are visible under the proxy station's NiagaraNetwork.
- **Proxy Authentication When Tunneling**
This property (enabled under the "Services > Web Services" component) forces authentication before allowing HTTP traffic to be tunneled to the target station. This can lead to multiple logins (one login at the proxy level and one login at the target level) unless login credentials are consistent on both the proxy and target. If credentials are identical, the login credentials at the proxy level are "shared" (for cookie", not "cookie-digest") and used for the login to the target, thus giving the effect of single sign on.

Note: See ["About 2013 Security updates"](#) on page 3-2 for information related to this property and 2013 Security Updates. This property must be set to true for tunneling to a cookie-digest station if:

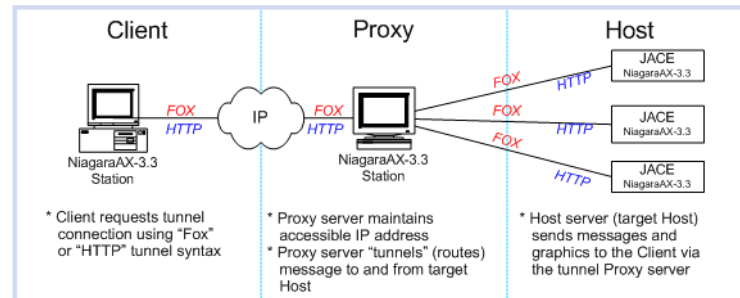
- the supervisor (proxy) station fox port is not the default port, OR
- the target station's NiagaraAX version is earlier than AX-3.5u4, 3.6u4, or 3.7u1

NiagaraAX stations serve in the following roles to comprise the typical points of reference in a tunneling scenario:

- **Client**
This is the initiating party that sends a communication request using the "Fox Tunneling" or "HTTP Tunneling" syntax to open a special session with the proxy server.

- **Proxy**
This is the tunneling proxy server station that recognizes the tunnel syntax and routes the message on to the tunneled host.
- **Host**
This is the target host that is typically on a protected network that is not directly accessible to the client.

Figure 3-1 Example of Fox tunneling communications



The following sections describe the unique characteristics of each type of tunneling:

- [About Fox Tunneling](#)
- [About HTTP Tunneling](#)

About 2013 Security updates

Enhanced security features were introduced in 2013 NiagaraAX releases. These updates are discussed in the document *NiagaraAX 2013 Security Updates*. Some of the updates affect the way tunneling works when using Fox and HTTP tunneling and some new properties are added to Fox and HTTP services.

Problems with client authorization can result when trying to tunnel from upgraded stations to non-upgraded stations.

Note: The "Cookie Digest" setting does not allow authentication between security-upgraded and non-upgraded stations.

Possible workarounds for these situations include:

- **Upgrade stations**
The best workaround is to upgrade all stations to the 2013 Security Update release.
- **Set "Proxy Authentication When Tunneling" to "true" on the upgraded station.**
This setting requires the client to manually enter credentials again but allows tunneling.

About Fox Tunneling

The following topics are specific to Fox tunneling:

- [Fox Tunneling Requirements](#)
- [Enabling Fox Tunneling](#)
- [Fox Tunneling Syntax](#)
- [Establishing a Fox Tunneling Session](#)
- [Fox Tunneling Examples](#)

Fox Tunneling Requirements

Proxy and Host should have same level of security upgrades, or tunneling may not work or require workarounds, see ["About 2013 Security updates"](#) on page 3-2. In addition, requirements for Fox tunneling include the following:

- **Client Requirements**
The client station must be running NiagaraAX-3.3 or later and have network access to a "Proxy" station.
- **Proxy Requirements**
The Proxy station must be licensed for Fox tunneling and be running NiagaraAX-3.3 or later on a network with an IP address that is available to the Client. Also, the Proxy station must have Tunneling enabled (see "Enabling a Tunneling Server", below).


- **Host Requirements**

The host station (or targeted station) needs to be able to provide an accessible network IP address to the Proxy server. The targeted host must be running a NiagaraAX-3.3 or later station.

Enabling Fox Tunneling

In order to perform as a "tunnel" for NiagaraAX workbench clients, allowing them to communicate with otherwise "unreachable" hosts, a NiagaraAX-3.3 or later station must be running with the *Tunneling Enabled* property set to "True". The following procedure describes how to enable tunneling.

To enable a proxy server station for tunneling, do the following:

1. In a NiagaraAX-3.3 workbench view, connect to the NiagaraAX-3.3 or later station that you want to enable for tunneling.
2. In the nav tree pane, under the Station node, expand the Config>Drivers> nodes to display the NiagaraNetwork node in the nav tree.
3. In the nav tree, right-click on the NiagaraNetwork node and select the Property Sheet from the popup menu. The property sheet view displays.
4. In the property sheet view, click to display the Fox Service properties  and set the following properties:

- **Tunneling Enabled**

Select **True** from the Tunneling Enabled property option list.

- **Only Tunnel Known Stations**

(AX-3.4 and later only) This is an added security option that affects both Fox and HTTP tunneling (introduced in AX-3.3). This property applies only if the station is configured as a tunnel (proxy server). Prior to this feature (in AX-3.3) a tunnel connection would be attempted to *any* target IP address given in the tunnel ORD.

- If left at the default (false) value, this behavior is unchanged.

- If set to true, Fox and HTTP tunneling is attempted *only* to a station that exists in the proxy server's NiagaraNetwork, where tunnel ORD (Fox) or URL (HTTP) syntax uses the target station's *name* instead of IP address.

For example, going through 10.10.8.9 to reach target station "demoStation" at 10.10.5.4

- *instead of* (Fox) tunnel at ip:10.10.8.9|fox:/10.10.5.4

- *now* (Fox) tunnel at ip:10.10.8.9|fox:/demoStation

or

- *instead of* (HTTP) tunnel at http://10.10.8.9/tunnel/10.10.5.4

- *now* (HTTP) tunnel at http://10.10.8.9/tunnel/demoStation

Again, note that if this property is set to true, that the target NiagaraStation *name* must be used in the Fox tunnel ORD or the HTTP URL—and not IP address.

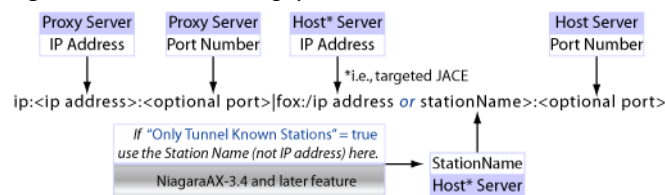
5. Click the **Save** button to complete the setup. Tunneling is now enabled on the station.

Fox Tunneling Syntax

The key to fox tunneling is the ORD syntax that is used to initiate tunneling from the Client station.

[Figure 3-2](#) illustrates the basic fox tunneling syntax (in the top of the graphic) and shows an example of the required syntax (station name instead of IP address) for target stations when the "Only Tunnel Known Stations" option is set to true.

Figure 3-2 Fox tunneling syntax



In this graphic:

- **Proxy Server**

This is the NiagaraAX-3.3 Supervisor station with an IP address that is available to the client station that you are currently using. The Proxy Server port number defaults to port 1911 (the standard default Fox port) unless otherwise specified.

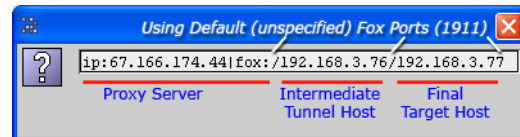
- **Host Server**
This is the station that you are trying to tunnel to. The Host Server address (like the Proxy Server address) may be followed by an optional port number. If not specified, the port number defaults to port 1911. You can complete the ORD by including the "space" and address of the desired view, if known.
- **Host, Session, Space**
These are identified in the graphic above to indicate the standard segments of a typical ORD.

Syntax Examples

The following examples illustrate Fox tunneling syntax using NiagaraAX-3.3 or later:

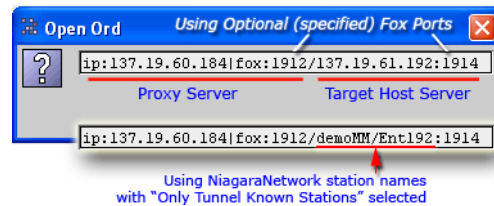
- **Example 1**
The following graphic shows an example of tunneling through a Proxy server (67.166.174.44) and then through an intermediate NiagaraAX-3.3 Supervisor tunnel host (192.168.3.76) and on to a final target host (192.168.3.77). In this example, no ports are specified so the default Fox port 1911 is used for all Fox connections.

Figure 3-3 Tunneling through an additional host



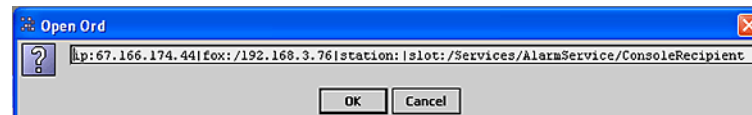
- **Example 2**
The following graphic shows an example of tunneling through a Proxy server (137.19.60.184) using a specified Fox port (1912) and also specifying a Fox port (1914) for the targeted Host server (137.19.61.192). Figure 3-4 also shows an additional example ORD that uses "station name" instead of "IP address". Available starting in NiagaraAX-3.4, the "Only Tunnel Known Stations" option requires you to use station name, not the host IP address and restricts tunneling to stations that are under the proxy server's NiagaraNetwork.

Figure 3-4 Specifying Fox ports on Proxy server and targeted Host server (and using a station name)



- **Example 3**
The following graphic shows an example of tunneling through a Proxy server (67.166.174.44) to a target host (192.168.3.76) and specifying a particular view in the station (station:|slot:/Services/AlarmService/ConsoleRecipient). All stations are using the default fox port 1911, since no port is specified.

Figure 3-5 Tunneling to a specified view in the targeted host

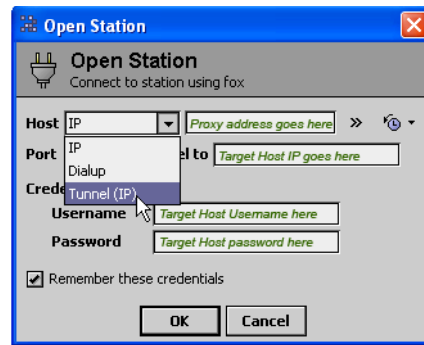


Establishing a Fox Tunneling Session

You can establish a fox tunneling session using NiagaraAX-3.3 workbench in any one of the following ways:

- **Open Station dialog box**
This dialog box displays when you select "Open Station" from the workbench *File* menu.

Figure 3-6 Selecting Tunnel (IP) in the Open Station dialog box

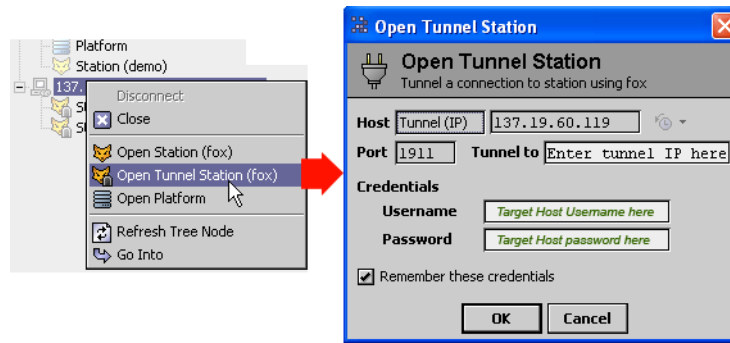


Note: In the Open Station dialog box the Host field label **Host** Tunnel (IP) refers to the Proxy Server and its associated IP address. This is because the Proxy Server is in a host relationship to your current workbench view. Do not confuse this Proxy server "Host" with the targeted host that you are tunneling to.

- **Open Tunnel Station dialog box**

This dialog box displays when you right-click on a Proxy Server in your workbench nav tree and select "Open Tunnel Station" from the popup menu.

Figure 3-7 Displaying the Open Tunnel Station from the popup menu



Once you have opened a fox tunneling workbench session on a target host (typically a JACE), the Proxy Server and the target host display in the workbench nav tree. If you disconnect from the station, you can always reconnect to the station by right-clicking on the station and selecting "Connect" from the popup menu.

Fox Tunneling Examples

The following list includes syntax examples to illustrate different ways to use fox tunneling:

Note: Starting in NiagaraAX-3.4, you can use the "Only Tunnel Known Stations" property to restrict tunneling to only stations that are under the proxy server's NiagaraNetwork. When this option is used, the required syntax for the targeted host includes "station name" instead of IP address.

Example 1 - Simple tunnel

- `ip:137.19.60.184 | fox: /137.19.61.192`

This example ORD specifies the following network actions:

- Establish a connection to the tunneling *Proxy server* at the IP address 137.19.60.184 using default fox port 1911 (since no port specified).
- Establish a fox connection to the targeted *host* at 137.19.61.192 using default port 1911 (since no port is specified).
- Using the "Only Tunnel Known Stations" option, the syntax is as follows for this example:
`ip:137.19.60.184 | fox: /myStation`

Example 2 - Tunnel specifying fox port and target view

`ip:137.19.60.184 | fox:1912/137.19.61.192 | station: | slot:/AirHandler`

This example ORD specifies the following network actions:

- Establish a connection to the tunneling *Proxy server* at IP address 137.19.60.184 using the proxy serv-

- er fox port 1912.
- The proxy server establishes a fox connection to the tunneled *host* at 137.19.61.192 using the targeted host default fox port 1911.
- Display the view defined by the rest of the ORD (station:|slot:/AirHandler)

Example 3 - Multiple tunnelling specifying target view

```
ip:137.19.60.184|fox:/137.19.61.242/137.19.60.119|station:|slot:/Services/Alarm-Service/ConsoleRecipient
```

This example ORD specifies the following network actions:

- Establish a connection to the tunneling *Proxy server* at the IP address 137.19.60.184 using default fox port 1911.
- Proxy server establishes a fox connection to the *host* at 137.19.61.242 again using default fox port 1911.
- Tunnel through the intermediate *host* at 137.19.61.242 and connect to the *host* at 137.19.60.119 using default fox port 1911.
- Display the view (alarm console) defined by the rest of the ORD (station:|slot:/Services/AlarmService/ConsoleRecipient)

Note: *Note the following additional information about the examples described, above.*

- When doing multiple tunnels, as in the example above, each "parent" tunnel must be a NiagaraAX-3.3 Supervisor station running with tunneling enabled. The final targeted host requires NiagaraAX-3.3 but does not need to be an AXSupervisor station.
- Instead of typing a long ORD, as in Examples 2 and 3, it may be easier to simply establish a connection at the station level and then use the nav tree to open the view you want.

About HTTP Tunneling

HTTP tunneling provides the ability to establish a workbench connection in the browser using only HTTP communications. However, using only HTTP tunneling restricts you to the Hx workbench interface. If you enable both Fox and HTTP tunneling, you can use both tunneling protocols for the richer media interface that is provided by the workbench applet in the browser.

The following topics are specific to HTTP tunneling:

- [HTTP Tunneling Requirements](#)
- [Enabling HTTP Tunneling \(Proxy Server and Host Server\)](#)
- [Establishing an HTTP Tunneling Connection](#)
- [HTTP Tunneling Syntax](#)
- [HTTP Tunneling URL Examples](#)

HTTP Tunneling Requirements

Proxy and Host should have same level of security upgrades, or tunneling may not work or require workarounds, see "[About 2013 Security updates](#)" on page 3-2. Requirements for HTTP tunneling include the following:




Note: *Https tunneling is not supported.*

- **Client Requirements**
The client station must have a standard browser and network access to a "Proxy" station.
- **Proxy Requirements**
The Proxy station must be licensed for HTTP tunneling and be running NiagaraAX-3.3 on a network with an IP address that is available to the Client. Also, the Proxy station must have Tunneling enabled (see Enabling a Tunneling Web Server, below).
- **Host Requirements**
The host station (or targeted station) needs to provide an accessible network IP address to the Proxy server and must be running NiagaraAX-3.3.

Enabling HTTP Tunneling (Proxy Server and Host Server)

In order to perform as a "tunnel" for NiagaraAX workbench clients, allowing them to communicate with otherwise "unreachable" hosts, a NiagaraAX-3.3 station must be running with the Web Services *Tunneling Enabled* property set to "True". This is true for any targeted (or intermediate) Host that is specified in the tunnel URL. The following procedure describes how to enable HTTP tunneling on a NiagaraAX-3.3, or later version station.

To enable HTTP tunneling, do the following for each station that you are enabling:

1. In a NiagaraAX-3.3, or later, workbench view, connect to the station that you want to use as an HTTP server (this could be a Proxy or Host server station).
2. In the nav tree pane, under the Station node , expand the Config>Services nodes to display the WebService node  in the nav tree.
3. In the nav tree, right-click on the WebService node  and select Property Sheet from the popup menu. The property sheet view displays.
4. In the property sheet view, set the following properties, as desired:
 - **Tunneling Enabled**
Select `true` from the property option list to enable HTTP tunneling. Select `false` (default) to leave tunneling disabled. See [“Enabling Fox Tunneling”](#) for information about how to limit allowable tunneling destinations (Fox and HTTP) using the Only Tunnel Known Stations property.
 - **Proxy Authentication When Tunneling (available in NiagaraAX-3.4 and later)**
Select `true` to require authentication before rerouting any HTTP tunnel requests. This means that the user probably has to clear multiple login screens. Leave the property at `false` (default) to require authentication only at the target station.
5. Click the *Save* button to complete the setup. HTTP Tunneling is now enabled on the station.

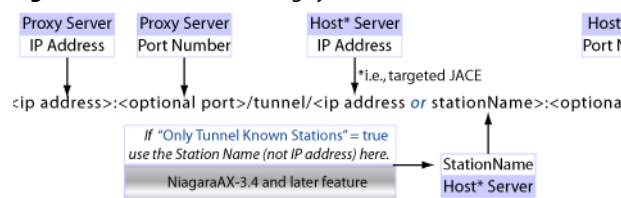
Establishing an HTTP Tunneling Connection

HTTP tunneling, unlike Fox tunneling, is performed from a browser. Instead of typing in an ORD, you type in a URL that initiates the tunnel connection in the browser. To initiate an HTTP tunnel connection, open a browser and type the proper URL into the address bar, using the syntax described in the following section.

HTTP Tunneling Syntax

The key to HTTP tunneling is the syntax that is used to initiate tunneling from the Client station. [Figure 3-8](#) illustrates the basic HTTP tunneling syntax. It also shows (lower part of the graphic) the different syntax required when the Only Tunnel Known Stations property is set to true and the station name is required instead of the host IP address.

Figure 3-8 HTTP tunneling syntax



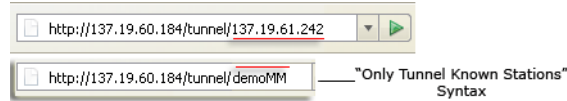
Where:

- **Proxy Server**
This is the NiagaraAX-3.3 (or later) station with an IP address that is available to the client station that you are currently using. The proxy server web service port number defaults to port 80 (the standard default HTTP port) unless otherwise specified.
- **Host Server**
This is the station that you are trying to tunnel to. After supplying the IP address of the proxy server, complete the URL by including a slash and the word "tunnel" followed by another slash and the address of the host server. If tunneling is limited to known stations, only, then the station's name is used in place of the host server IP address. The host server http port number defaults to port 80 (the standard default HTTP port) unless otherwise specified.

HTTP Syntax Examples

- Syntax example 1**
 The following graphic shows an example of a URL address for tunneling through a Proxy server (137.19.60.184) and then to the target host (137.19.61.242). If “Only Tunnel Known Stations” is enabled then the station name is used instead of the target host IP address. No port is specified for either station in this example, so HTTP port 80 is used.

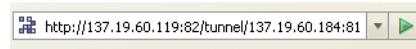
Figure 3-9 HTTP tunneling address



- **Syntax example 2**

The following graphic shows an example of a URL address for tunneling through a proxy server (137.19.60.119) using the proxy server http port 82, then tunneling and connecting to the host server (137.19.60.184) using the host server http port 81.

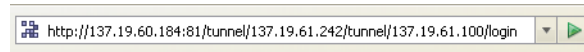
Figure 3-10 Tunneling using designated port numbers



- **Syntax example 3**

The following graphic shows an example of tunneling through a proxy server (137.19.60.184) that uses port 81, then through a second proxy server (137.19.61.242) and on to the target host and login view at (137.19.61.100/login). Note that port 81 is specified and used only on the proxy server station. The intermediate and target host server ports are not specified so they are assumed to be port 80.

Figure 3-11 Tunneling to a specified view in the targeted host



HTTP Tunneling URL Examples

Note: In all of the following examples you must substitute the station name for IP address if you are restricted to tunneling only known NiagaraNetwork stations. See [“Enabling Fox Tunneling”](#).

The following example URLs illustrate HTTP tunneling examples:

Example 1 - Simple tunnel

`http://137.19.61.242/tunnel/137.19.60.184`

This example URL specifies the following network actions:

- Establish a connection to the tunneling *Proxy server* at IP address 137.19.61.242 making the connection to proxy server port 80 (since no port is specified).
- Establish an HTTP connection to the target *host server* at 137.19.60.184 making the connection to the host server port 80 (since no port is specified).

Example 2 - Tunneling specifying station name and optional port:

`http://137.19.60.119:82/tunnel/myStation:81`

This example URL specifies the following network actions:

- Establish a connection to the tunneling *proxy server* at ip address 137.19.60.119 making the connection to proxy server port 82.
- Tunnel to the target server identified by station name (myStation) making the connection to the proxy server port 81. This example assumes that “Only Tunnel Known Stations” is active. If this is not the case, then you would use the host IP address here.

Example 3 - Multiple tunneling specifying client port and view

`http://137.19.60.184:81/tunnel/137.19.61.242/tunnel/137.19.61.100/tunnel/137.19.60.119/ord?station:|slot:/PxHome`

This example URL specifies the following network actions:

- Establish a connection to the tunneling *Proxy server* at the IP address 137.19.60.184
- Use the Proxy server port 81 to tunnel through the *hosts* at 137.19.61.242 and 137.19.61.100, and then finally connect to the station at 137.19.60.119
- Display the view defined by the trailing ORD information (ord?station:|slot:/PxHome)

Note: This example may be unusually long (and impractical) but it illustrates the ability to tunnel through multiple stations using HTTP.

Document change log

Updates (changes/additions) to this *Fox Tunneling and HTTP Tunneling* document are listed below.

- Updated: May 23, 2013
Added section [“About 2013 Security updates”](#) on page 3-2.
- Updated: January 29, 2010
Mentioned new platform tunneling feature added in AX-3.5 and added reference to *Appendix C, NiagaraAX-3.5 Platform Guide*.
- Updated: August 8, 2008
Changes were made throughout this document to reflect the “Only Tunnel Known Stations” and “Proxy Authentication When Tunneling” properties added with NiagaraAX-3.4.
Main section links were added to the first page.
- Publication: December 10, 2007
Initial publication.

