Sedona Framework Sox Tunneling

This document explains Sox tunneling to a Sedona Framework device and includes these sections:

Overview of Sox tunneling

Sox tunneling provides a way to make a Workbench client Sox connection through a Niagara station to a Sedona Framework device that is networked under it. The intermediate station must have the required "SoxTunnel" configuration, and its host platform must be licensed for Sox tunnel access.

Importance change for Sox tunneling (Sedona TXS 1.2)

Starting in Sedona TXS-1.2 (with AX-3.7 and later), usage of Sox tunneling is typically bypassed in favor of "Sox Gateway" and "Sedona Tools" access to networked Sedona devices. Workbench is not the Sox client in this case—instead, the hosting JACE/station acts as Sox client, using "Sedona environment files" on that host platform. This provides the same benefits as Sox tunneling, as well as other advantages.

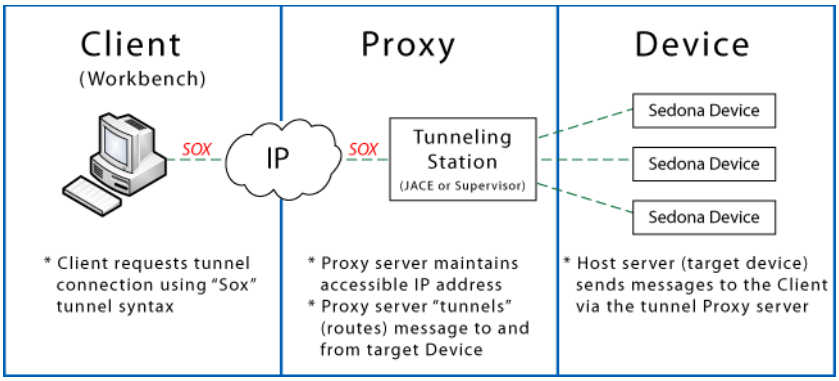
For related details, see the *Sedona Framework TXS 1.2 Networks Guide* sections "Sox Gateway" and "Sedona device 'tools' views", as well as the "Sedona environment management" appendix that explains the necessary platform configuration to support such access.

Regardless if Sedona TXS 1.2 or TXS 1.1, Sox tunneling is not required if you have direct access to a Sox device's network. In that case you can make a direct (Workbench client) Sox connection to the device.

Benefit and operation of Sox tunneling

A key benefit provided by Sox tunneling is the ability to establish a Workbench client session with one or more devices that are hidden from public access. This is done by allowing the requesting Workbench platform (client) to communicate (or "tunnel") through an intermediate station (JACE or a Supervisor) with networked Sedona Framework devices. The station acts as a proxy server to those targeted devices.

Figure 1 *Example of Sox tunneling communications*



An example use of this feature would be where IP connected Sedona Framework devices are networked under JACEs in a building. You may want to have the ability to "tunnel" the Sox connection so that when you are outside the facility you can access the devices for programming changes without having to expose the IP address of each Sedona Framework device. If you network many devices "under" a JACE, your IT department may not allow exposure of dozens or more control devices to the Internet.

Note: *If a Sedona Framework device is networked to the JACE via the secondary IP/LAN port on the JACE, the ability to tunnel Sedona (Sox) may be the only solution to make a Workbench client connection.*

Sedona Framework stations and devices serve in the following roles to comprise the typical points of reference in a tunneling scenario:

- **Client**
  This is the initiating party (for example, Workbench) that sends a communication request using "Sox tunneling" syntax to open a connection with the proxy server.
- **Proxy**
  This is the tunneling proxy server station, running on a JACE or Supervisor, that recognizes the Sox tunnel syntax and routes the message on to the tunneled host.
- **Device**
  This is the target device (or node) that is typically on a protected network that is not directly accessible to the client.

Sox Tunneling requirements

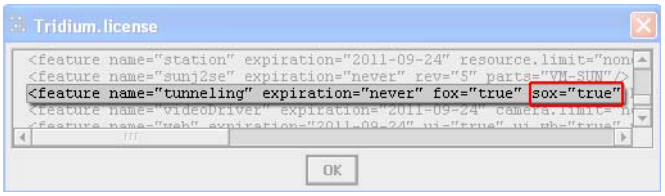
Requirements for Sox tunneling include the following:

- **Client requirements**
  The client Workbench platform must have Sedona TXS 1.1 or later installed and licensed with network access to the tunneling "Proxy" station.
- **Proxy requirements**
  The Proxy platform must have the nsedona module nsedona, be licensed for Sox tunneling and have an IP address that is accessible to the client platform. SoxTunnel service must be installed and enabled (available from the nsedona palette). A Sedona network must be configured, enabled and communicating with the target Sedona device nodes.
- **Device requirements**
  Sedona Framework devices must be communicating on the Sedona network in the Proxy station.

Licensing SoxTunnel service

This feature is relevant for JACE or Supervisor installations that serve as a Sedona tunneling proxy platform. Sox tunneling requires a `sox="true"` entry in the `feature name="tunneling"` line of the license file, as shown below.

Figure 2 *SoxTunnel service license feature*



The SoxTunnel service is an enhancement to the existing tunneling feature, so you must have the standard tunneling feature in your license. Without this license feature the SoxTunneling service displays a "fault" status when installed.

Installing the SoxTunnel service

In order to function as a "tunnel" for Sedona Framework clients a Niagara station must be running with the SoxTunnel service installed, licensed, and enabled. You can install the service by dragging the SoxTunnel service from the `nsedona` palette in Workbench onto the services node in the Workbench nav tree pane. The following steps provide detailed instructions for installing, enabling, and configuring the SoxTunnel service.

Install the SoxTunnel service

Prerequisites for installing the SoxTunnel service, include:

- The station with target networked Sedona devices (hosts) must be running and accessible from the Workbench platform that you are using.
- The `nsedona` module (containing the SoxTunnel service component) must be licensed and installed on the proxy station.

To install and enable the SoxTunnel service, do the following:

Step 1 In NiagaraAX Workbench, make a standard Fox connection to the station that you want to enable tunneling on.

Step 2 In the nav tree pane, under the Station node, expand the Config node and double-click on the Services node. The Service Manager view displays.

Step 3 From the Workbench main menu, select **`Window > Side Bars > Palette`**.

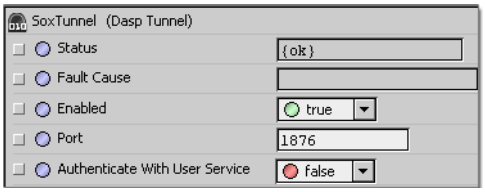
Step 4 In the Palette side bar, open the **`nsedona`** palette. It displays the **`SoxTunnel`** component.

Step 5 From the **`nsedona`** palette, drag and drop the **`SoxTunnel`** component onto the Service Manager view. The **`Name`** dialog box displays, so you can edit the name, if desired, and then click the **`OK`** button.

The **`SoxTunnel`** service displays in both the Service Manager view and under the **`Services`** node.

Step 6 Double-click the **`SoxTunnel`** node in the Service Manager view or in the nav tree for its property sheet.

Step 7 In the **`SoxTunnel`** service property sheet view edit the following properties, as necessary.



- **Status**
  Standard Niagara read-only status field indicating the current service state. Possible values include:
  - **ok**
    Normal communications, no other status flags.
  - **disabled**
    Enabled property is set to false. While status is disabled, Sox tunneling communications are suspended.

- **fault**
  Typically this is caused by a configuration error, such as a duplicate or invalid Port number.
- **down**
  Typically caused by a communications error.

- **Fault Cause**
  When there is a status fault, this read-only field displays text that indicates the reason for the fault.
- **Enabled**
  This property lets you enable (default setting) or disable the SoxTunnel service. When `true`, the Sox tunnel is "open". To prevent the Sox tunnel from processing Sox messages, set this `false`.
- **Port**
  This property value is the port that the SoxTunnel service communicates (listens on) for tunneling. The default value is 1876 but you can change it, if desired. If other than 1876 is set, the port must be specified in the path of any tunnelling request using this station. See "Sox tunneling syntax" on page 4 for details.
  Note: *Do not confuse this SoxTunnel Service port (default 1876) with the SedonaNetwork or Device port (also 1876 by default).*
- **Authenticate With User Service**
  Note: *Typically you change this (from default `true`) to `false` to prevent failed tunnel connections. As one example, failure can occur if Sedona device credentials use a "blank" password (something no longer permitted in station user credentials, since recent NiagaraAX releases and security patches).*
  If `true` (the default), when a Sox tunnel session is attempted, authentication requires the entered username/password combination to also exist for a *station User* in the tunnel station. To disable this behavior, set the property to `false`.

Step 8 Click **`Save`** to complete the task.

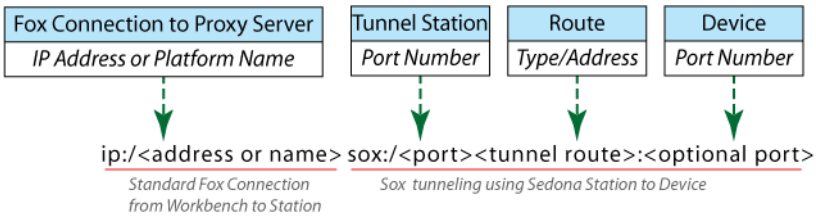
Sox tunneling syntax

For tunneling, the basic Sox scheme is comprised of the following segments that define the communications from the tunneled station (proxy) to the Sedona Framework device:

```
sox:<port> <tunnel route>
```

- **sox**
  This term specifies the "Sox scheme".
- **port**
  This is the optional declaration of which port to use on the tunneling station. If no port is declared here, then port 1876 is used.
- **tunnel route**
  Tunnel route includes a "/" followed by the route type and route address
  - **route type**
    This is a declaration of the type of communication protocol to use for tunneling. Route types may be "ip" or "bacnet", for example. If no route type is stated, then "ip" is used by default.
  - **route address**
    Route address is the address of the targeted device.

Figure 3 *Sox tunnel syntax*



Sox tunneling syntax examples

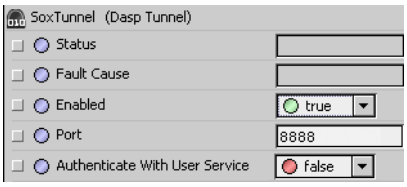
The following examples illustrate Sox tunneling in Sedona TXS.

- **Example 1**
  `ip:10.10.6.66|sox:/192.168.1.99`
  This example shows a connection to a Sox tunnel on port 1876 on a station running at 10.10.6.66. The tunnel uses an "ip" route since "route type" is *not* explicitly specified and sends messages to a

Sedona device at address 192.168.1.99. Note that in this example, the port for the Sedona Framework device is also assumed to be the default 1876, so it is not specified on the end of the address.

- **Example 2**
  `ip:10.10.6.66|sox:8888/ip=192.168.1.99`
  This example is the same as Example 1 except that port 8888 is specified for the "tunnel station". This port number must match the station's SoxTunnel Port property value (Figure 4).

Figure 4 *SoxTunnel Port property set to 8888*

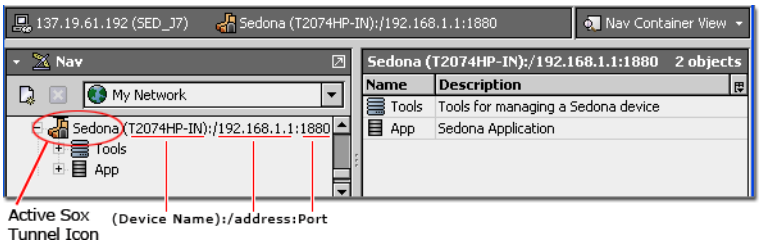


- **Example 3**
  `ip:136.19.60.54|sox:/bacnet=7`
  This example specifies a tunnel connection on port 1876 of the station at 136.19.60.54. The tunnel looks for a "bacnet" route with a route address of "7".

Opening a Sox tunneling session

The following illustration shows an example of a successful Sox tunneling session.

Figure 5 *Sox tunneling session established*



There are several ways to establish a Sox tunneling session from Workbench. You can use the main menu and related dialog boxes or you can use one of the context-sensitive popup (right-click) menus in the nav tree. In addition, if you have previously established a Fox connection that is disconnected, the connection node in the nav tree only dims when you disconnect. You can right-click on the dimmed node and quickly reconnect by selecting the "Connect" menu item.

These methods are described in the following procedures.

- "Open a Sox tunnel session from the Workbench main menu" on page 5
- "Open a Sox tunnel session from a device node in Workbench nav tree" on page 6
- "Open a Sox tunnel session from a station node in the nav tree" on page 7
- "Open a Sox tunnel session from a "disconnected" node in the nav tree" on page 7

Before establishing a Sox tunnel session you must have network access to a NiagaraAX station with the following features or conditions:

- Sox tunneling licensed (see "Licensing SoxTunnel service" on page 3)
- Sedona network connection between station and Sedona Framework device nodes
- SoxTunnel service installed and configured (see "Installing the SoxTunnel service" on page 3)

Open a Sox tunnel session from the Workbench main menu

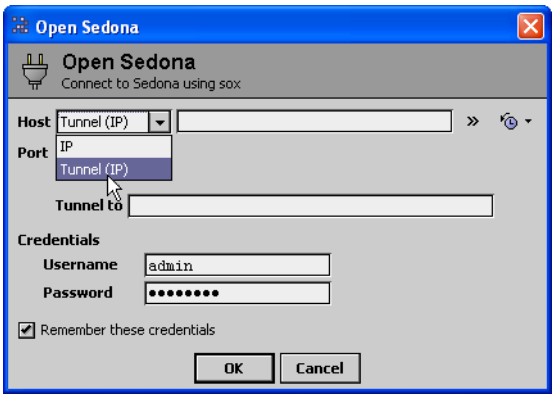
To establish a Sox tunneling session from Niagara Workbench, do the following:

Step 1 From the Workbench AX-3.7 or later main menu, select **`File > Open >`** **`Open Device`**

or

from the Workbench AX-3.6 or later main menu, select **`File > Open >`** **`Open Sedona (sox)`**

The **Open Sedona** dialog box displays.



Step 2 In the **Open Sedona** dialog, select the Tunnel (IP) option from the Host option box.

The **Open Sedona** dialog box now displays a Tunnel to field.

Step 3 In the **Open Sedona** dialog box, complete the following fields and click **OK**:

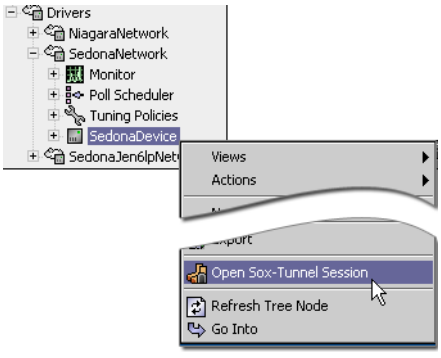
- **Host (IP)**
  Enter the IP address or name of the station platform that you are trying to use for tunneling.
- **Port**
  By default, this is port 1876. Change this if you know that the SoxTunnel service on the tunneling platform is set to a different port.
- **Tunnel to**
  Enter the IP address of the Sedona device that you are trying to reach.
- **Credentials**
  Type in the Username and Password for the *Sedona Framework device* that you are trying to reach.
  Note: *If the Authenticate with User Service is set to* `true` *in the SoxTunneling service on the tunnelling station, then the users Credentials in the station and in the device app must match.*

If the connection is successful, the session is established, the device Nav Container view displays and an active "tunneled session" node appears in the nav tree.

Open a Sox tunnel session from a device node in Workbench nav tree

In Workbench, if you have a station open with networked Sedona Framework devices (SedonaNetwork or SedonaJen6lpNetwork), you can quickly establish a Sox tunnel connection to one using the popup menu, as described below:

Step 1 In the Workbench nav tree, right-click on the device under the desired Sedona network node and select **Open Sox-Tunnel Session** from the popup menu.



The **Authentication** dialog box displays.

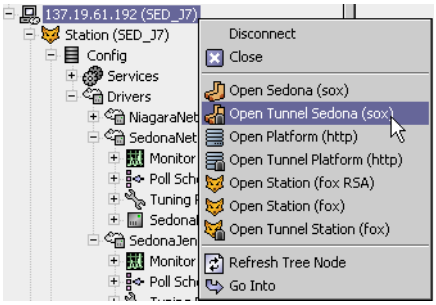
Step 2 In the **Authentication** dialog box, enter your credentials and click the **OK** button.

If the connection is successful, the session is established, the device Nav Container view displays and an active "tunneled session" node appears in the nav tree.

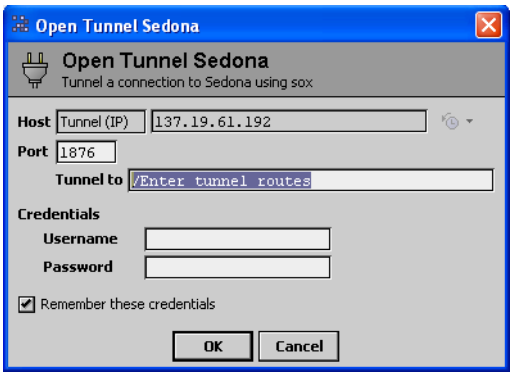
Open a Sox tunnel session from a station node in the nav tree

(AX-3.6 only) If you have a host station (JACE or supervisor) visible in the Workbench nav tree, you can open a Sox tunneling connection to a device under it using the following steps:

Step 1 In the Workbench nav tree, right-click the desired station and select the **`Open Tunnel Sedona (sox)`** menu item from the popup menu.



The **`Open Tunnel Sedona`** dialog box displays.



Step 2 In the **`Open Tunnel Sedona`** dialog box, enter values in the following fields and click the **`OK`** button.

- **Port**
  Verify the Port number or change the port number, if necessary.
- **Credentials**
  Enter Username and Password
- **Tunnel to**
  Enter the tunnel route information. See "Sox tunneling syntax" on page 4 for related details.

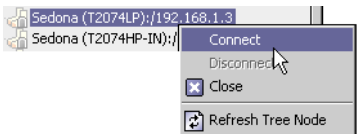
If the connection is successful, the session is established, the device Nav Container view displays and an active "tunneled session" node appears in the nav tree.

Open a Sox tunnel session from a "disconnected" node in the nav tree

In Workbench, if you "disconnected" from a Sox tunnel connection without "Closing" the node in the Workbench nav tree, then the node continues to display as dimmed in the nav tree (this is standard display behavior in the Workbench nav tree).

You can quickly re-establish a Sox tunnel connection to a Sedona device using the following steps:

Step 1 In the Workbench nav tree, right-click on the desired (dimmed) disconnected node and select **`Connect`** from the popup menu.



The **`Authentication`** dialog box displays.

Step 2 In the **`Authentication`** dialog box, enter your credentials and click the **`OK`** button.

If the connection is successful, the session is established, the device Nav Container view displays and an active "tunneled session" node appears in the nav tree.

Document change log

Updates (changes/additions) to this *Sedona Framework Sox Tunneling—Engineering Notes* document are listed below.

- Updated: January 14, 2013
  Minor changes concurrent with the release of Sedona Framework TXS 1.2, including a new "Overview" subsection "Importance change for Sox tunneling (Sedona TXS 1.2)" on page 1 that explains the *diminished importance* of Sox tunneling (in favor of "Sox Gateway" and "Sedona Tools" access for networked Sedona Framework devices). Another content change is the recommendation of changing the "Authenticate With User Service" property of the SoxTunnel service in a station from the default `true` to `false`. See "Installing the SoxTunnel service" on page 3.
  Other text changes were mostly cosmetic. Note although screen captures using AX-3.6 (with Sedona TXS-1.1) were retained, content is still applicable for an AX-3.7 system using Sedona TXS-1.2.
- Publication: November 9, 2011
  Initial document.