

User's Guide

Tofino Central Management Platform

Version 1.7.0



TOFINO™

Copyright Information

© Byres Security Inc

While this information is presented in good faith and believed to be accurate, Byres Security Inc. disclaims the implied warranties of merchantability and fitness for a particular purpose and makes no express warranties except as may be stated in its written agreement with and for its customers. In no event is Byres Security Inc. liable to anyone for any indirect, special or consequential damages. The information and specifications in this document are subject to change without notice.

Tofino™, Tofino™ Industrial Security Solution and Tofino™ Intrinsically Secure are trademarks of Byres Security Inc. Other brand or product names are trademarks of their respective owners.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Table of Contents

Part I	15 Steps to a Secure Control System	2
Part II	Introducing the Tofino CMP	6
2.1	Tofino CMP Basics	6
2.2	Tofino CMP Menus	7
2.2.1	File Menu	8
2.2.2	Edit Menu	8
2.2.3	Tools Menu	12
2.2.3.1	Tools Database Admin Menu	16
2.2.4	Window Menu	22
2.2.5	Help Menu	24
2.3	Tofino CMP Windows	25
2.3.1	Network Editor	27
2.3.1.1	Network Editor Right Click Menus	28
2.3.1.1.1	General Editing Menu	29
2.3.1.1.2	Tofino SA Specific Menu	34
2.3.1.1.3	Network Node Menu	40
2.3.2	Network View	41
2.3.3	Tofino View	42
2.3.4	LSM License View	46
2.3.5	Nodes	47
2.3.5.1	Editing a Node's Properties	52
2.3.5.2	New Node Wizard	58
2.3.6	Modules	73

2.3.7	Protocols	74
2.3.7.1	Protocol Wizard	79
2.3.8	Special Rules	82
2.3.9	Event View	84
2.3.9.1	Event Capture	91
2.3.10	Progress	92
2.3.11	Tofino Discovery	92
2.3.12	Asset Discovery	93
2.3.13	Go Into Go Back Go Home	94
 Part III Using the Tofino CMP		97
3.1	Setting Up Your Tofino CMP	97
3.1.1	Tofino CMP Licensing	98
3.1.2	Tofino CMP Preferences	101
3.1.3	User Administration	111
3.2	Creating Your Network Diagram	112
3.2.1	Creating and Editing a Network	113
3.2.2	Network ReBuild Wizard	114
3.2.3	Using Tofino Discovery	116
3.3	Events, Alarms, and Heartbeats	126
3.4	Backing up and Restoring Databases	127
3.5	Saving Changes	128
 Part IV Working with Your Tofino SA		130
4.1	Tofino SA (100 and 220 Series) Modes	130

4.2	Editing the Properties of a Tofino 100 or 220 SA	135
4.3	Tofino SA Contact Devices	138
4.4	Configuring Tofino CMP Connections	142
4.5	Syncing Your Tofino SA's Configuration	143
4.6	Replacing Tofino SA	144
4.7	Updating Your Tofino SA Firmware	147
	Part V Tofino CMP Tab Management	152
	Part VI LSMs	167
6.1	Managing LSMs	167
6.1.1	Adding LSMs to Tofino SAs	168
6.1.1.1	How LSM Tabs Work	170
6.1.2	LSM Licensing: Upgrading or Adding	172
6.2	Firewall LSM Management	174
6.2.1	Basic Firewall Concepts	174
6.2.2	Firewall Log Settings	177
6.2.3	Firewall Rule Configuration for a Node	178
6.2.3.1	Setting Global Rules	179
6.2.3.2	Setting Talker Rules	182
6.2.4	Firewall Rule Configuration of a Tofino SA	191
6.2.4.1	Setting Global Rules	192
6.2.4.2	Setting Broadcast Rules	195
6.2.4.3	Setting Multicast Rules	198
6.3	Secure Asset Management LSM	202

6.3.1	About Asset Discovery	202
6.3.2	Using Asset Discovery	203
6.3.3	About Assisted Rule Generation	214
6.3.3.1	Using Assisted Rule Generation	214
6.3.3.2	ARG New Node Wizard	224
6.4	Modbus TCP Enforcer LSM Management	228
6.4.1	About Modbus TCP Enforcer LSM	228
6.4.2	Using the Modbus TCP Enforcer LSM	230
6.5	OPC Classic Enforcer LSM Management	238
6.5.1	About OPC Classic Enforcer LSM	238
6.5.2	Using the OPC Classic Enforcer LSM	240
6.6	VPN LSM Management	245
6.6.1	About VPN LSM	245
6.6.2	Using the VPN LSMs	247
6.6.2.1	3rd Party Servers	259
6.6.2.2	VPN Server and Client Tabs	262
6.6.2.3	Installing the VPN PC Client	265
6.6.2.4	VPN PC Client Licensing	267
6.6.3	Locating the Tofino CMP when Using the VPN	268
6.7	Event Logger LSM Management	270
6.7.1	About Event Logger LSM	270
6.7.2	Using Event Logger LSM	272
Part VII	Troubleshooting	279
7.1	Tofino Argon 100 or 220 Diagnostics	279

7.2	Asset Discovery Shows Removed Devices	284
7.3	Asset Discovery is Not Discovering Assets	285
7.4	Expired Licenses	286
7.5	Firewall Not Blocking Traffic	288
7.6	Licensing	289
7.7	Missing Tofino SA	290
7.8	Serial Tofino SAs	291
7.9	Tofino Discovery is Not Discovering Tofino SAs	293
7.10	USB Key Problems	294
7.11	Why Can't I Enter the %\$@#! Character?	295
7.12	VPN Troubleshooting	296
7.12.1	My VPN Client will not connect to my VPN Server	296
7.12.2	The Client Certificates Have Time Expired	296
7.12.3	PC Client Can't Connect to my VPN Client's Devices	296
7.12.4	PC Client Can't Connect to my Tofino VPN Server	296
7.13	Event Logger Troubleshooting	298
7.13.1	Syslog Over UDP	298
7.13.2	Syslog Over TCP	298
7.13.3	Syslog Over TLS	298
Part VIII	Glossary	301
Part IX	Technical Support	307
Part X	Appendix A: Finding Your MAC Address	309

Section 1

15 Steps to a Secure Control System

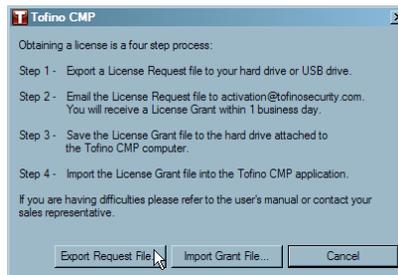
1 15 Steps to a Secure Control System

Follow the steps below to set up the Tofino Industrial Security Solution.

- Install your Tofino SA in-line on the network, between the device(s) to be trusted and the rest of the network. Please make note of the IP address of one of the devices on the opposite side of the Tofino SA from the Tofino CMP computer.



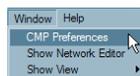
- Activate your Tofino Central Management Platform (CMP) and Loadable Security Module (LSM) licenses. [See How](#)



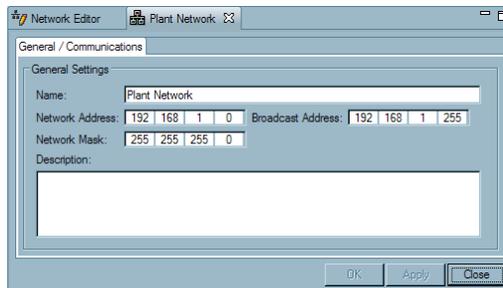
- Log into the Tofino CMP using the default user name: "admin" and password: "password". You will be prompted to change the password before you log in. [See How](#)



- Set up your preferences and user administration for your Tofino CMP. [See How](#)

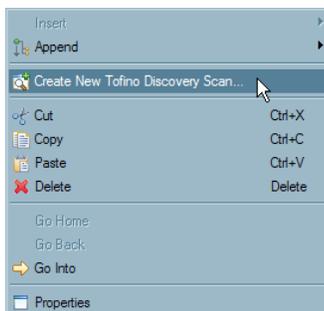


- Create a new network icon or configure the network icon present in the Network Editor to represent the address range of your control network. [See How](#)



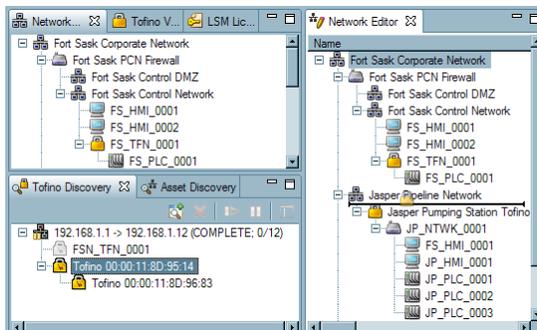
- Right click on the network icon and start a Tofino Discovery Scan ensuring that the discovery scan includes the IP address that was noted in the first step.

[See How](#)



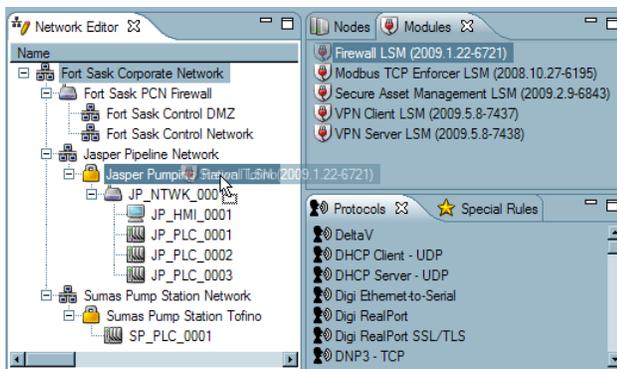
- Drag discovered Tofino SA from the Tofino Discovery view into the Network Editor, renaming as appropriate.

[See How](#)



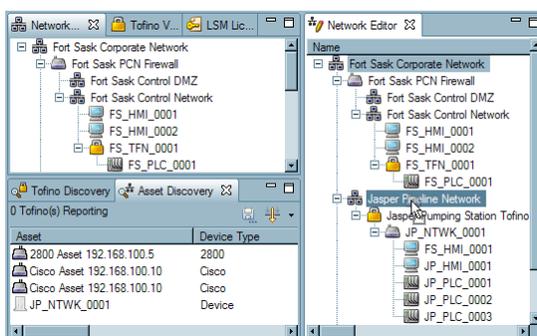
- Select the LSMs you wish to activate from the Modules tab, and drag and drop them onto the desired Tofino SAs in the Network Editor.

[See How](#)



- Build the rest of your network diagram using drag and drop from either Asset Discovery view (if the Secure Asset Management LSM is installed and activated) and/or from the Nodes view.

[See How](#)

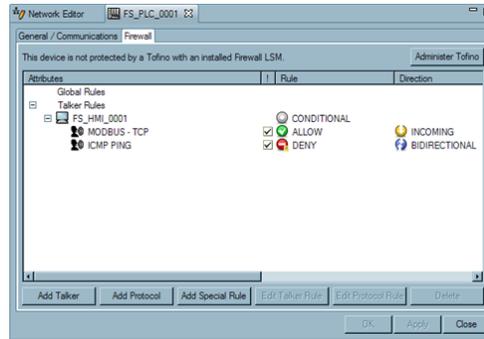


- Set the primary and backup contacts for each Tofino SA.

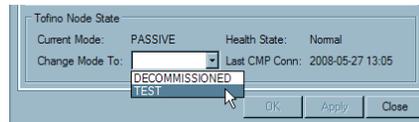
[See How](#)



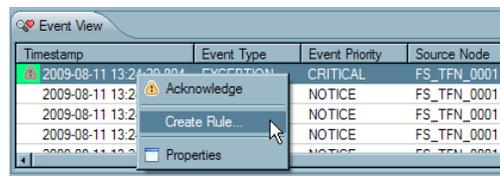
- Set up firewall rules for each protected device. (**Note:** The Firewall LSM must be installed and activated as in step 8) [See How](#)



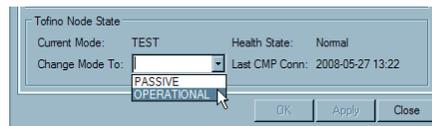
- Put the Tofino SA into TEST mode. [See How](#)



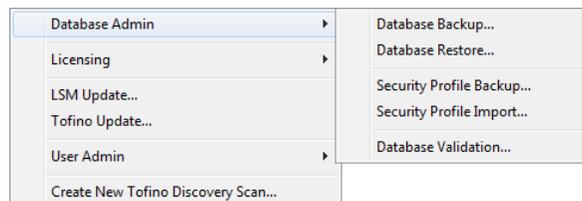
- Make sure there are no denied packets. If there are packets you think should be either allowed or blocked but not reported, use Assisted Rule Generation to help you build a new rule (Assisted Rule Generation requires that the SAM LSM be installed and activated). [See How](#)



- Once there are no unwanted alarms, put the Tofino SA into OPERATIONAL mode. [See How](#)



- Back up your Tofino CMP database to a secure location. [See How](#)



Congratulations you are done! You have successfully installed the Tofino Industrial Security Solution and significantly improved the security of your process network.



Section 2

Introducing the Tofino CMP

2 Introducing the Tofino CMP

2.1 Tofino CMP Basics

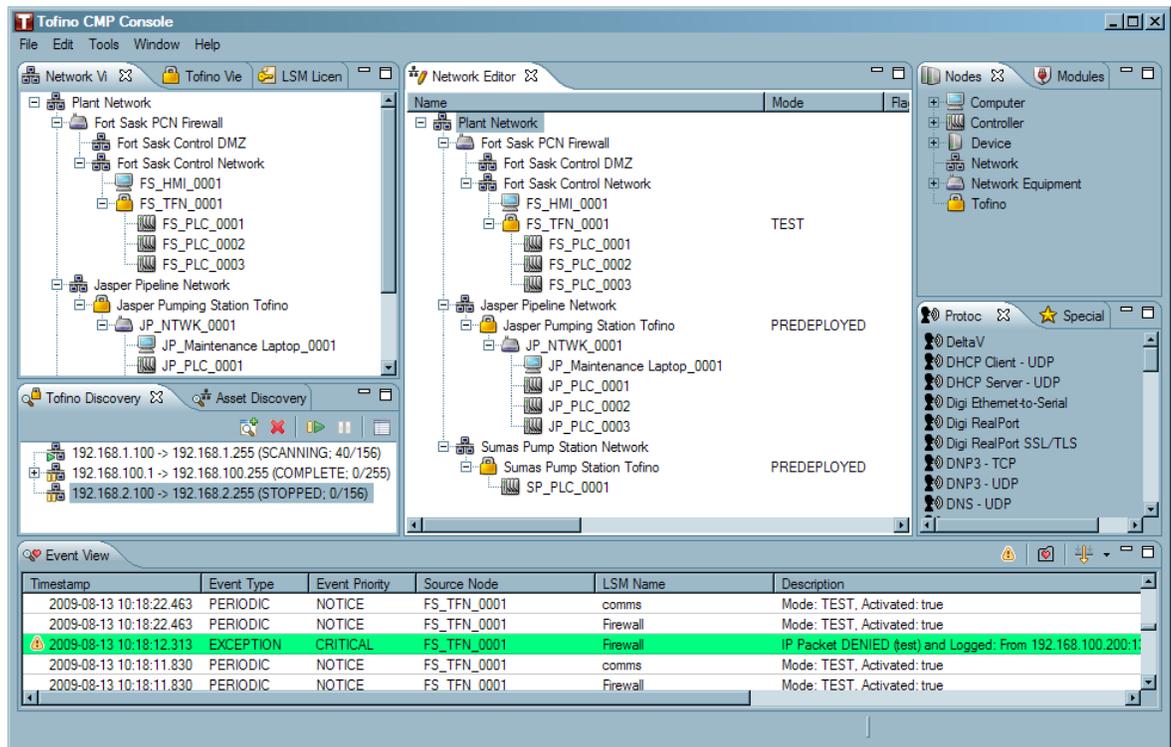
The complete Tofino Industrial Security Solution consists of three core components:

- ▶ Tofino SA – these industrially hardened appliances are installed in front of individual and/or clusters of HMI, DCS, PLC or RTU control devices that require protection.
- ▶ Tofino Loadable Security Modules (LSM) – a variety of software plug-ins providing security services such as firewall, secure asset management, intrusion detection system (IDS) and VPN encryption. Each LSM is downloaded into the security appliances to allow them to offer customizable security functions, depending on the requirements of the control system.
- ▶ Tofino Central Management Platform (CMP) – a Windows-based centralized management system and database for monitoring, supervision and configuration of each security appliance, regardless of its physical location.

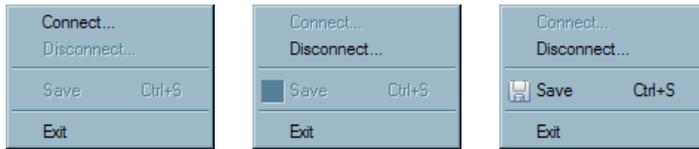
2.2 Tofino CMP Menus

The Tofino CMP has five top level menus. These are:

- ▶ **File:** Allows you to log into the Tofino CMP, save changes to the Tofino CMP database and exit the application.
- ▶ **Edit:** Used to edit a network diagram within the Network Editor window.
- ▶ **Tools:** Used to manage databases, licensing and user accounts and to activate Tofino Discovery.
- ▶ **Window:** Allows you to make changes to the Tofino CMP Preferences and open different windows on the Tofino CMP.
- ▶ **Help:** Shows Help Contents as well as Tofino CMP version and copyright information.



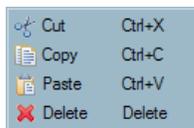
2.2.1 File Menu



The File menu allows the user to:

- ▶ Connect (login) to the Tofino CMP.
- ▶ Disconnect (logout) from the Tofino CMP.
- ▶ Save changes to the Tofino CMP Database.
- ▶ Exit and shutdown the Tofino CMP application.

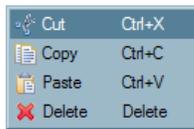
2.2.2 Edit Menu



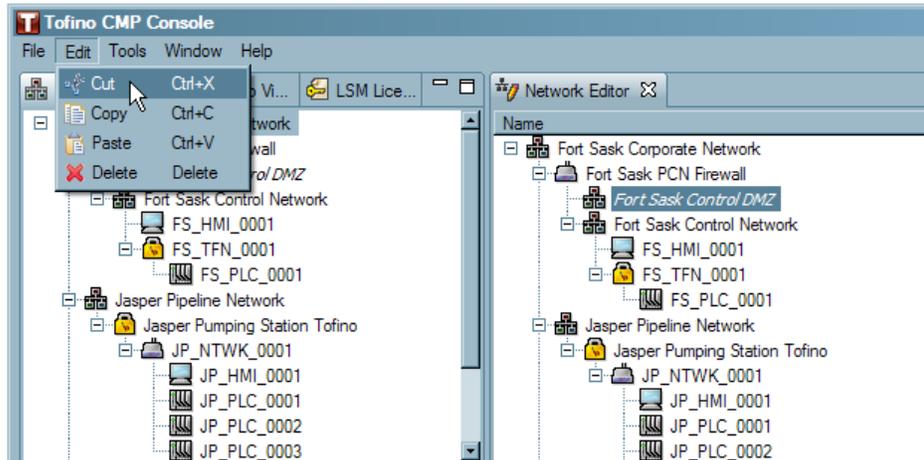
The Edit Menu can be used to create or edit a network diagram within the Network Editor window. This menu allows the user to:

- ▶ [Cut](#) nodes from one location in the network diagram for pasting to another location.
- ▶ [Copy](#) nodes from one location in the network diagram for pasting to another location.
- ▶ [Paste](#) nodes that have been cut or copied from an existing network tree to a new location.
- ▶ [Delete](#) nodes from the network diagram.

Edit ► Cut



Used to cut existing nodes from a network diagram in order to paste them elsewhere in the tree. To cut a node, click on a node and then select "Cut" or "Ctrl+X".

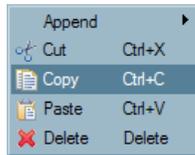


Once the node has been cut, it will appear italicized until it has been pasted to its new location. (If a node has been selected to be cut (i.e. it is italicized) and then you decide you do not wish to cut it, hit the "escape" (Esc) key on your keyboard).

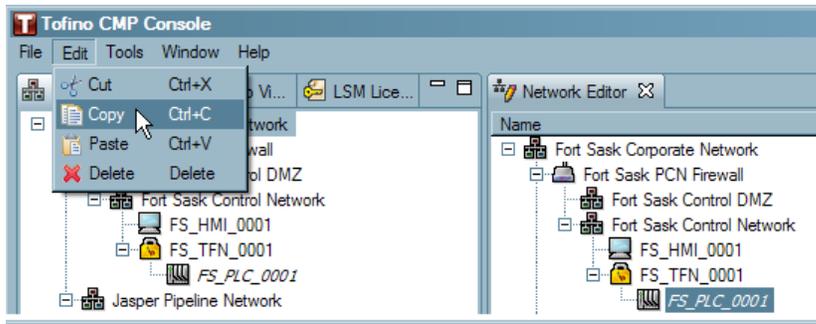
Once Paste has been selected, a Paste Node window will appear.

Note: When cutting a node, the nodes below the cut item in the network tree will also be moved.

Edit ► Copy

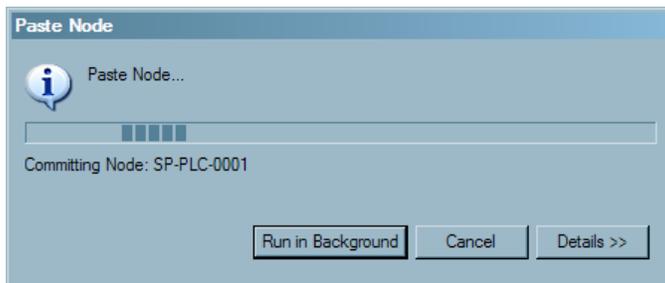


Used to copy existing nodes in order to paste them elsewhere. To copy a node, click on a node and then select "Copy" or "Ctrl+C".

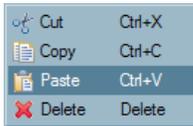


Once the node has been selected to be copied, it will appear italicized until it has been pasted to its new location. If a node has been selected to be copied (i.e. it is italicized) and then you decide you do not wish to copy it, hit the "escape" (esc) key on your keyboard).

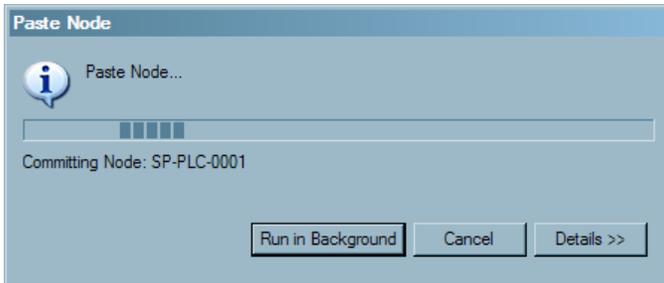
Once Paste has been selected, a Paste Node window will appear. Once the configurations have been completed, click "OK".



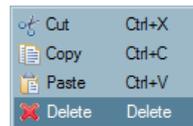
Edit ► Paste



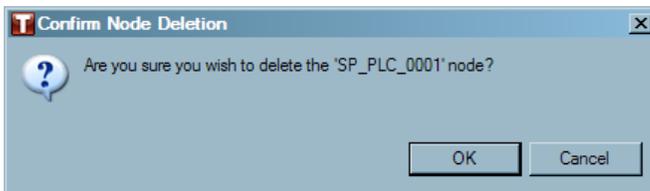
Used to paste nodes that have been cut or copied from an existing network tree to a new location. Once Paste has been selected, a Paste Node window will appear.



Edit ► Delete



Used to remove nodes from the network diagram and database that are not wanted. To delete a node, select the node to be deleted, and select "Delete" on the Edit menu or press "Delete" on the keyboard. A window will pop up confirming the deletion. Select "OK" to complete the deletion.



Note: When deleting a node, the nodes below the deleted item in the network tree will remain in the tree, but will be attached to the tree at the network level the deleted item was at.

2.2.3 Tools Menu



The tools menu allows for database, licensing and user administration functions including:

- ▶ [Database Admin](#)
- ▶ [Licensing](#) ▶ [Export Request File](#)
- ▶ [Licensing](#) ▶ [Import Request File](#)
- ▶ [LSM Update](#)
- ▶ [Tofino Update](#)
- ▶ [User Admin](#)
- ▶ [Create New Tofino Discovery Scan...](#)

Tools ▶ Database Admin

This menu allows the various databases to be backed up, restored, or validated.

See: [Tools](#) ▶ [Database Admin Menu](#)

Tools ▶ Licensing ▶ Export Request File

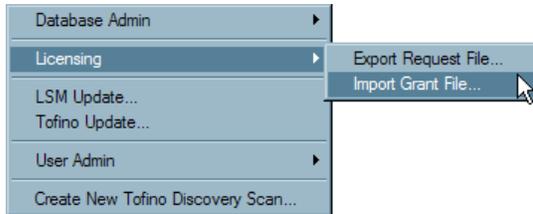
With this menu option, the user can generate an encrypted request file for additional Tofino SA licenses. This file must then be sent to activation@tofinosecurity.com.



See: [LSM Licensing](#)

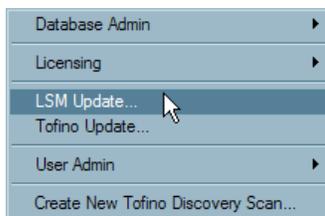
Tools ► Licensing ► Import Request File

This menu option allows the user to import licenses for Tofino SAs.



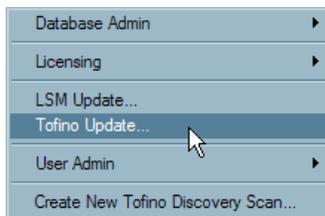
See: [LSM Licensing](#)

Tools ► LSM Update...



The **Tools ► LSM Update...** menu option allows the user to check for LSM updates.

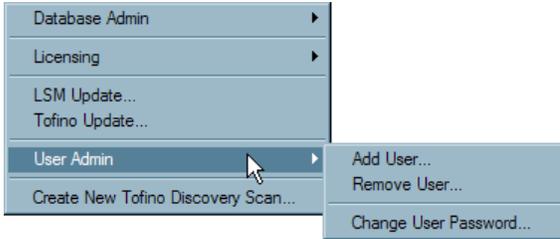
Tools ► Tofino Update...



By choosing the Tofino Update... menu item, selected software updates can be pushed out to selected Tofino SAs in the field. An Update Wizard will prompt the user through the update process.

Tools ► User Admin

By selecting **User Admin**, user accounts can be added or deleted.



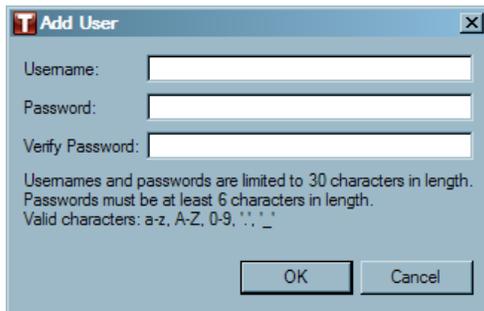
Tools ► User Admin ► Add User



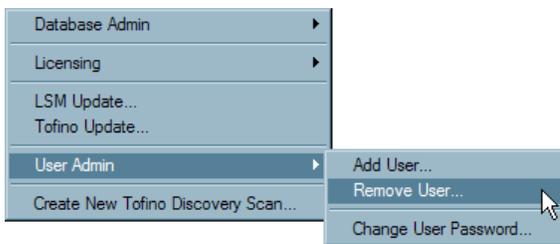
The **User Admin ► Add User** menu item allows new Tofino CMP user accounts to be added. Once “Add User...” is selected, a window will appear asking for a username and password. Complete both fields, and click “OK” to create the account.

Note: Usernames and passwords are limited to 30 characters. Passwords must be at least 6 characters long.

Valid characters are a-z, A-Z, 0-9, periods, and underscores.

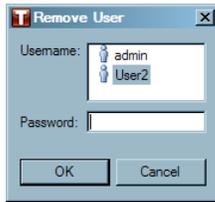
A screenshot of a dialog box titled 'Add User'. It has a close button (X) in the top right corner. The dialog contains three text input fields: 'Username:', 'Password:', and 'Verify Password:'. Below the fields, there is a block of text: 'Usernames and passwords are limited to 30 characters in length. Passwords must be at least 6 characters in length. Valid characters: a-z, A-Z, 0-9, ., _'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

Tools ► User Admin ► Remove User



This menu allows existing Tofino CMP user accounts to be deleted. Once “Remove User...” is selected, a window will open with a list of usernames. Select the username and enter the password and then click “OK”

to delete the account.

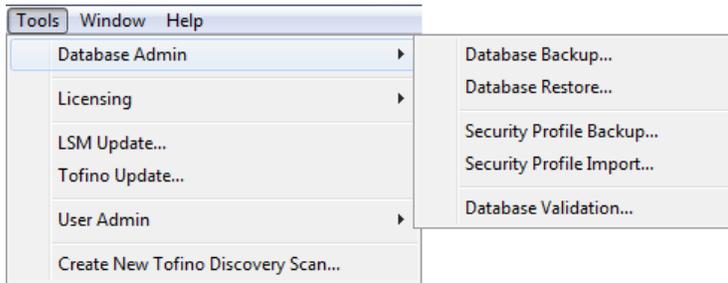


Tools ► Create New Tofino Discovery Scan...



Tofino Discovery allows the user to scan a specified portion of the network to find Tofino SAs. Newly "discovered" Tofino SAs can then be dragged and dropped in the Network Editor window in order to configure them and build your network diagram.

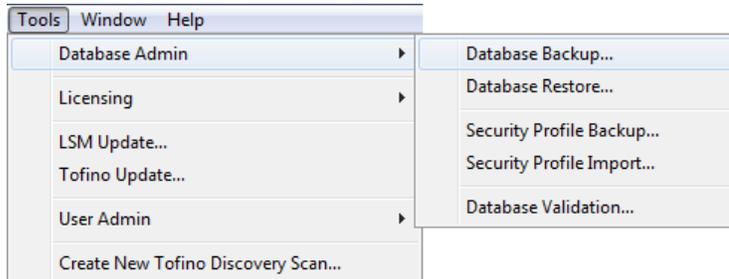
2.2.3.1 Tools Database Admin Menu



The **Tools ► Database Admin Menu** allows:

- ▶ [The network configuration Database to be backed up.](#)
- ▶ [The network configuration Database to be restored.](#)
- ▶ [The Security Profile to be backed up.](#)
- ▶ [The Security Profile to be imported.](#)
- ▶ [The checking of the Tofino CMP database for possible errors.](#)

Tools ► Database Admin ► Database Backup



By selecting **Tools ► Database Admin ► Database Backup**, a backup file is made of current network diagram and node configurations.

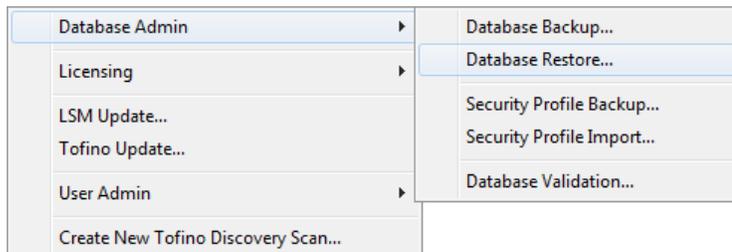
Note: If this is the first time you are backing up the database, an archive folder must be defined in the **Windows ► Preferences** menu. See: [Tofino CMP Preferences](#)

If the back up was successful, a window will appear indicating that the database was successfully backed up, while also indicating where the files were stored. Database back up files are automatically named with the following format:

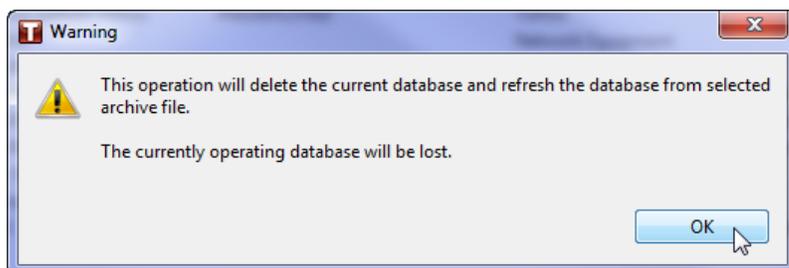
Database-backup-<Time Stamp>.tcd

The time stamp is in the format YYYY-MM-DD-HH-MM-SS and is the date and time when the back up file is created.

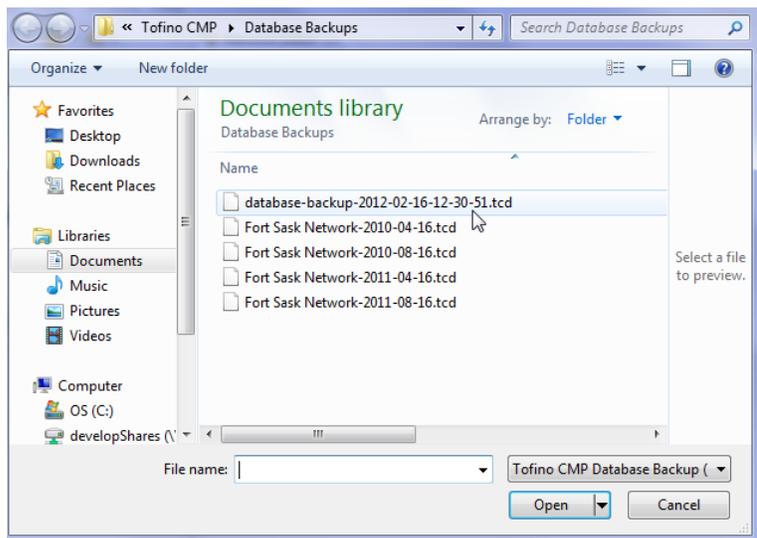
Tools ► Database Admin ► Database Restore



By selecting **Tools ► Database Admin ► Database Restore**, the current database will be deleted and replaced with a previously saved database. A warning window will indicate the consequences of restoring the database. (To prevent the unwanted loss of the current database, backup it up first). Click "OK".
Note: If this is the first time you are restoring or backing up the database, an archive folder must be defined in the **Windows ► Preferences** menu. See: [Tofino CMP Preferences](#)

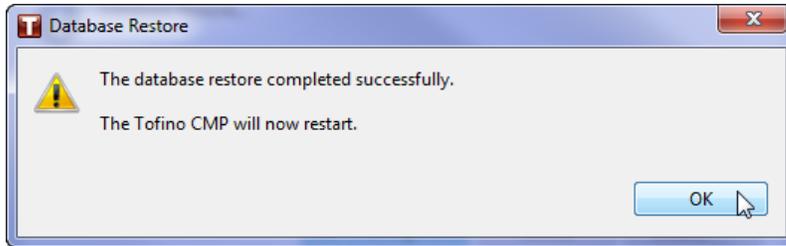


This will take you to a view of the Database archives folder. Select the database to be restored (remember the current database will be deleted when you perform a restore) and click "Open" or double click on the chosen database.

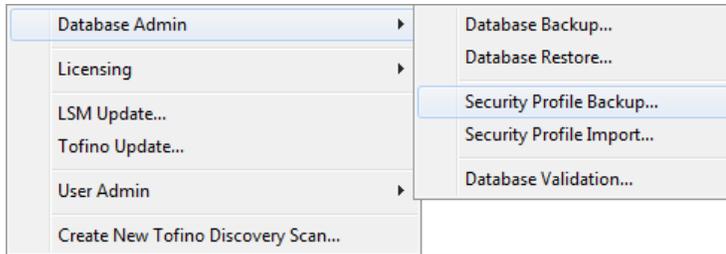


A Database Restore Monitor will appear.

Once the configurations have been completed, another window will open, warning that the Tofino CMP will now restart. Click "OK" or close the window; either will restart the Tofino CMP.



Tools ► Database Admin ► Security Profile Backup



The Security Profile contains all the node types that can be used to create a network diagram, as well as protocols and special rules.

By selecting **Tool ► Database Admin ► Security Profile Backup**, the device, protocol and special rule database will be saved. This is useful when new node types have been created that are unique to your company.

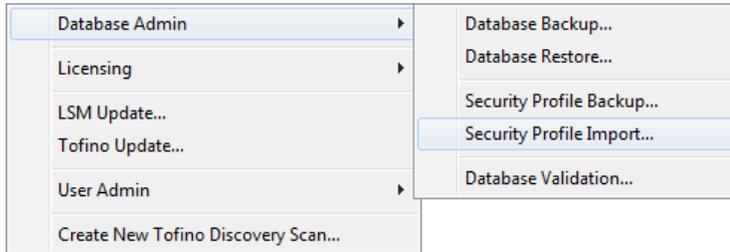
Once the selection has been made, a Security Profile Backup window will open.

A window will open indicating that the backup was successful. Database back up files are automatically named with the following format:

securityprofile-backup-<Time Stamp>.tsp

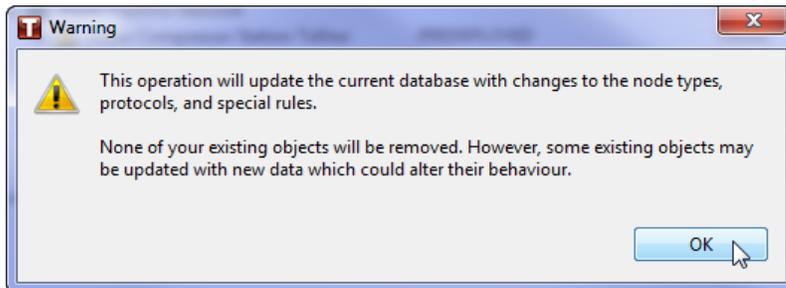
The time stamp is in the format YYYY-MM-DD-HH-MM-SS and is the date and time when the back up file is created.

Tools ► Database Admin ► Security Profile Import

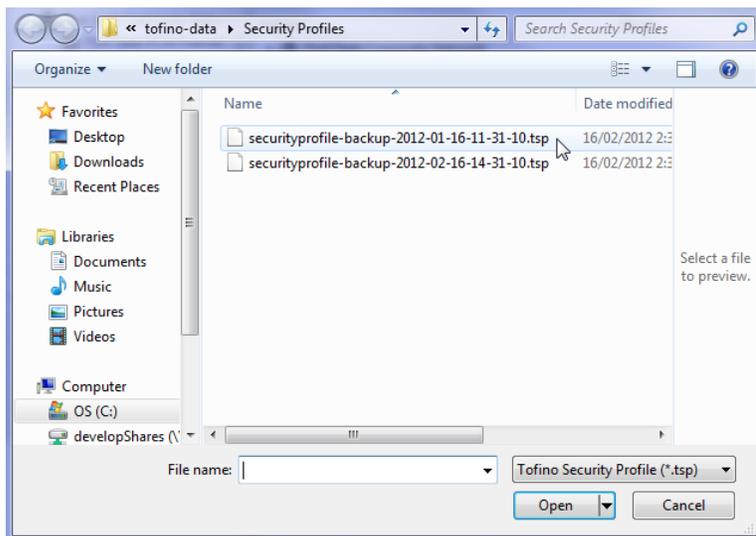


The **Tool ► Database Admin ► Security Profile Import** menu selection allows the user to restore previously saved Security Profiles. This operation will update the current database with changes to the node types, protocols, and special rules. None of your existing objects will be removed. However, some existing objects may be updated with new data which could alter their behaviour.

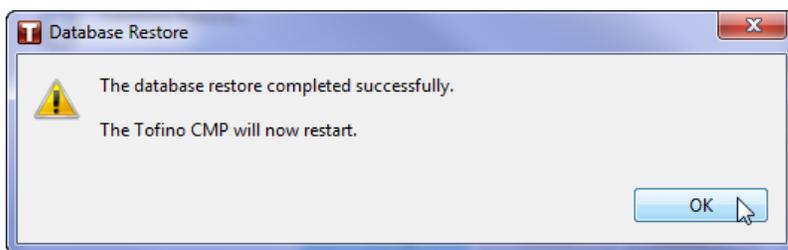
Once the selection has been made, a warning window will appear.



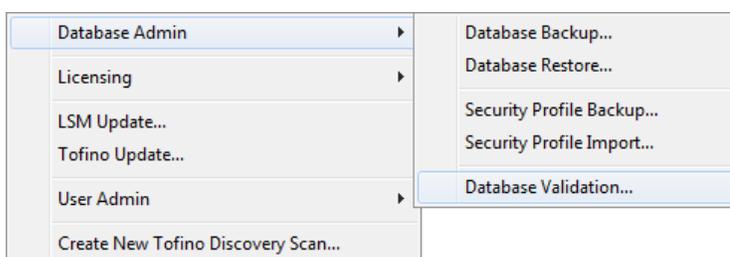
An archive window will open. Select the Security Profile you wish to restore.



A window will open indicating that the Security Profile is being imported. Another window will open once the restoration has been completed. Once "OK" has been clicked the Tofino CMP will restart.

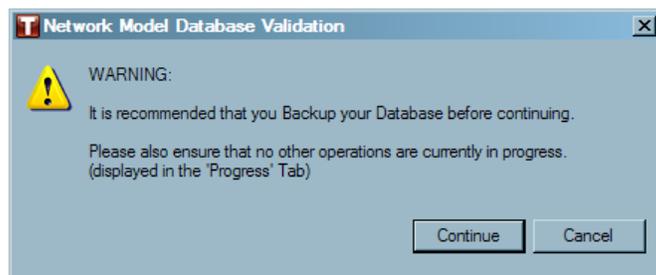


Tools ► Database Admin ► Database Validation

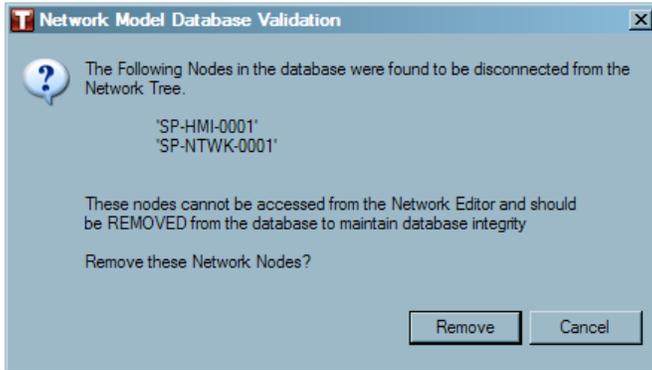


The **Tools ► Database Admin ► Database Validation** menu item checks the Tofino CMP database for possible errors.

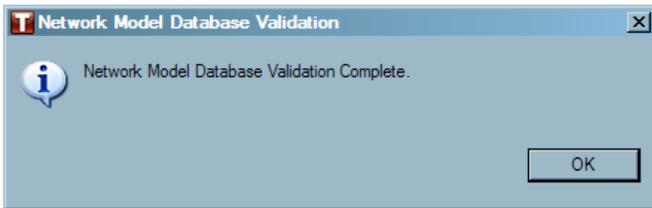
Once the selection has been made, a warning window will appear warning that the current device data base should be backed up before continuing the validation. Click "Continue" to proceed with the validation.



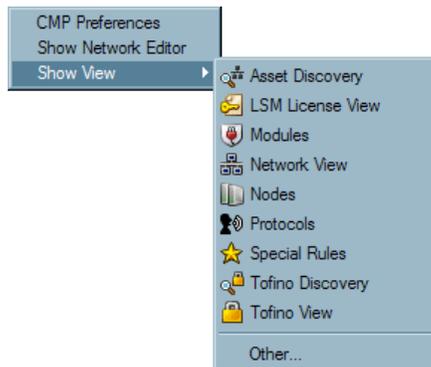
If the validation process detects nodes in the database that are no longer part of the network diagram these will be listed and you will be given the opportunity to remove them from the database. Click "Remove" to proceed with the removal of disconnected nodes.



Click "OK".



2.2.4 Window Menu



The Window menu allows:

- ▶ Changes to be made to the Tofino CMP Preferences.
- ▶ The opening of windows on the Tofino CMP.

See: [CMP Preferences](#)

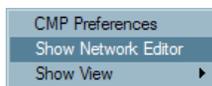
See: [Show Network Editor](#)

See: [Show View](#)

Window ▶ CMP Preferences

The CMP Preferences sets or changes settings for the Tofino CMP, including: Asset Discovery, CMP General Settings, CMP Log Settings, Database, Heartbeat, and Heartbeat syslog. See: [CMP Preferences](#)

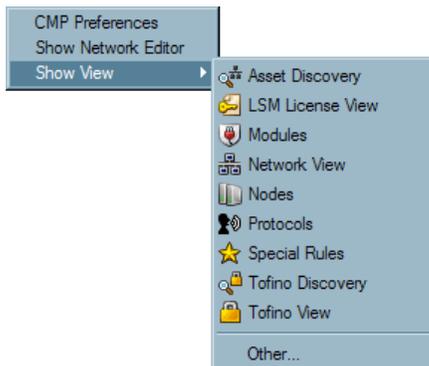
Window ▶ Show Network Editor



The Show Network Editor selection is a quick way to display the Network Editor window.

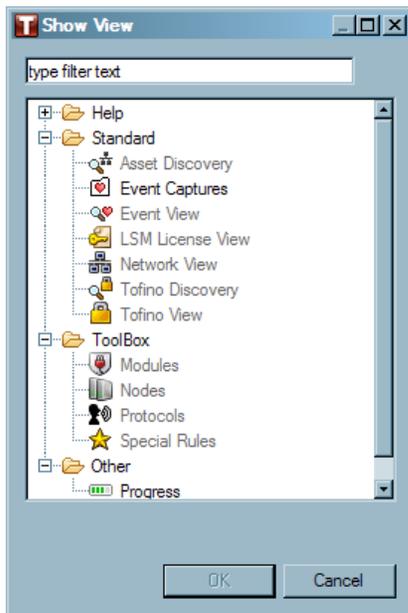
See: [Network Editor](#)

Window ► Show View



There are thirteen possible viewing windows on the Tofino CMP console. This menu option allows the user to easily open a desired window. To see a particular window, click on the list to make a selection.

Clicking on "Other...", opens a Show View window that displays the possible windows on the Tofino CMP, similar to the Show View menu.



To open the window, simply double click on the appropriate icon. To search for a specific window by name, type the name into the text box at the top of the window.

2.2.5 Help Menu



The Help menu includes:

- ▶ Help Contents.
- ▶ Configuration.
- ▶ Version and copyright information.

Help ▶ Help Contents

Helps the user operate the Tofino CMP.

Help ▶ Configuration

Provides software license information and diagnostics that may be helpful for technical support personnel. Use this feature as directed by technical support.

Help ▶ About

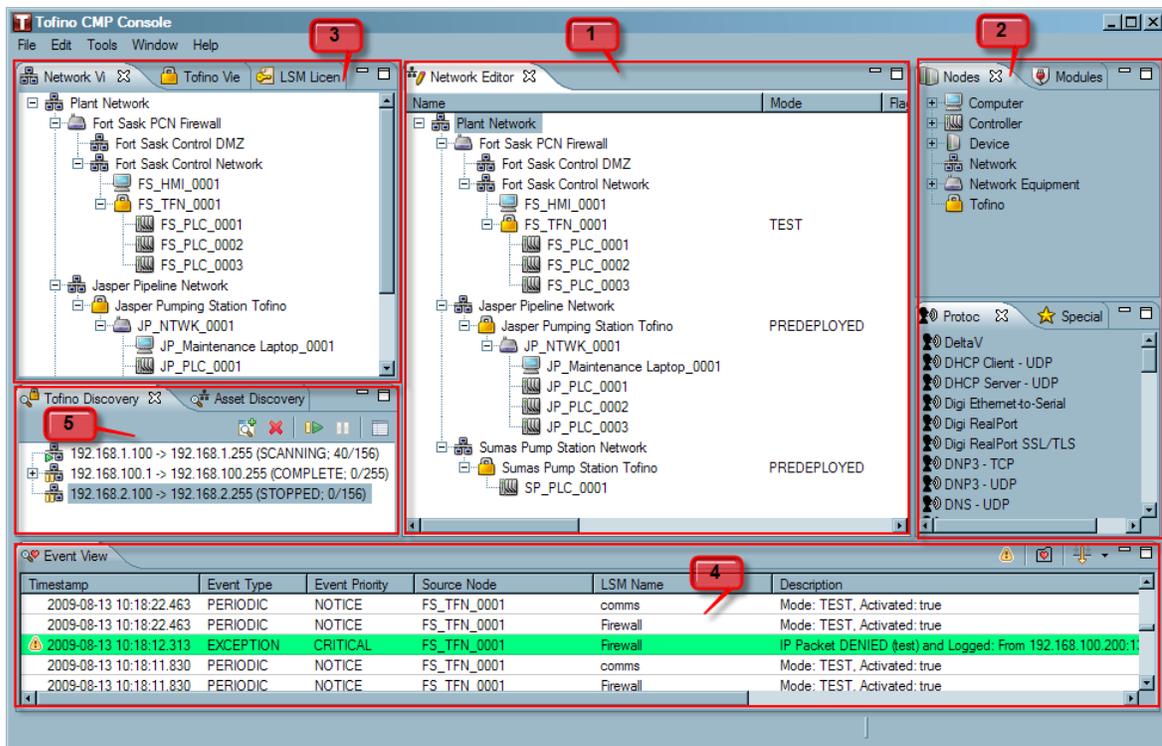
Shows version and copyright information. When calling for technical support or reporting a problem you will need the version number.



2.3 Tofino CMP Windows

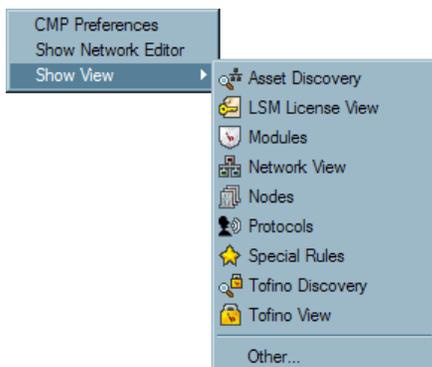
The Tofino CMP can be broken down into five main regions:

- ▶ The central window for building your network diagram, viewing and editing the properties of all the nodes in your network and managing your Tofino SAs ([Network Editor](#)).
- ▶ Four windows that contain the building blocks to create and configure your network diagram and Tofino SAs ([Nodes](#), [Modules](#), [Protocols](#) and [Special Rules](#)). These are usually located on the right hand side of the Tofino CMP screen.
- ▶ Three windows to view the components of your network diagram ([Network View](#), [Tofino View](#) and [LSM License View](#)). These are usually located on the left hand side of the Tofino CMP screen.
- ▶ Area to view events ([Event View](#), [Event Capture](#) and [Progress](#)). These are usually located on the bottom of the Tofino CMP screen.
- ▶ Two windows that aid the user in discovering assets on their network ([Tofino Discovery](#) and [Asset Discovery](#)). Usually found on the middle left hand side of the Tofino CMP screen.

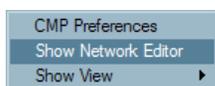


All views can be accessed in two ways:

- ▶ Clicking on the tab at the top of a specific window.
- ▶ Selecting **Window** ▶ **Show View** and choosing the view of choice.



In addition, selecting **Window** ▶ **Network Editor** is a short-cut to the **Network Editor** window.

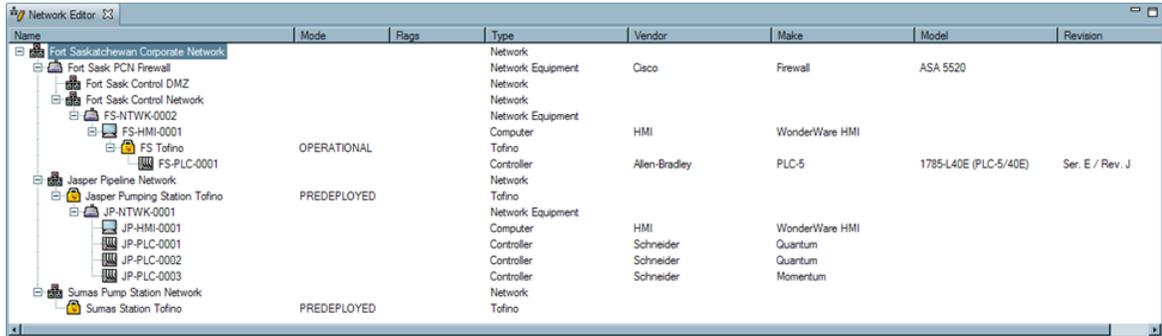


See also: [Tofino CMP Tab Management](#)

2.3.1 Network Editor

The Network Editor accesses the main editing and status window. Here, the user can view the status of the Tofino SAs in the network and create, configure and rearrange the various devices in the network diagram.

Similar to Network View, Network Editor illustrates network diagrams, including all network nodes and their connections, and also allows the user to create and edit networks.



Name	Mode	Flags	Type	Vendor	Make	Model	Revision
Fort Saskatchewan Corporate Network			Network				
Fort Sask PCN Firewall			Network Equipment	Cisco	Firewall	ASA 5520	
Fort Sask Control DMZ			Network				
Fort Sask Control Network			Network				
FS-NTWK-0002			Network Equipment				
FS-HMI-0001			Computer	HMI	WonderWare HMI		
FS Tofino	OPERATIONAL		Tofino				
FS-PLC-0001			Controller	Allen-Bradley	PLC-5	1785-L40E (PLC-5/40E)	Ser. E / Rev. J
Jasper Pipeline Network			Network				
Jasper Pumping Station Tofino	PREDEPLOYED		Tofino				
JP-NTWK-0001			Network Equipment				
JP-HMI-0001			Computer	HMI	WonderWare HMI		
JP-PLC-0001			Controller	Schneider	Quantum		
JP-PLC-0002			Controller	Schneider	Quantum		
JP-PLC-0003			Controller	Schneider	Momentum		
Sumas Pump Station Network			Network				
Sumas Station Tofino	PREDEPLOYED		Tofino				

The Network Editor tab displays eight column headings giving the user information about the network nodes.

- ▶ **Name:** The Name of each of the nodes in the network diagram. For example, Fort Saskatchewan Corporate Network might start the tree. The branches of the network can also be seen and can be opened and closed by clicking "+".
- ▶ **Mode:** The operating mode of any Tofino SA's in the diagram. Examples include Predeployed, Passive, Test, Operational, Decommissioned.
- ▶ **Flags:** Indicates if a Tofino SA is Missing. See: [Missing Tofino SA](#)
- ▶ **Type:** Displays the type of network node. Examples include Network, Network Equipment, Computer, Controller, Device and Tofino SA.
- ▶ **Vendor, Make, Model, Revision:** Provides additional details on the particular node. These will be displayed if the node has been created from a type listed in the Node database. For example, if a PLC-5 Controller was selected from the Node window to create a node on the network diagram, the Vendor would be displayed as Rockwell and the Make would be displayed as PLC-5, the Model might be 1785-L40E.

2.3.1.1 Network Editor Right Click Menus

There are three Right Click menus found in the Network Editor window depending on whether you right click on a Tofino SA, on a network node, or on any other type of node.

The menu that opens when the user right clicks is dependant on the type of node selected at that time. If a device, computer, controller, or network equipment node is selected when right clicking, the general node editing menu will appear. If a network node is selected a slightly different right click menu will open. However if a Tofino SA is selected when right clicking, a Tofino SA-specific menu will appear.

These three menus allow the user to:

- ▶ Create and edit a network.
- ▶ Synchronize Tofino SAs in the field with the Tofino CMP database.
- ▶ Create an encrypted USB key for configuring a Tofino SA in the field.
- ▶ Collect diagnostic information from a Tofino SA then transmit this encrypted file to technical support for further analysis.
- ▶ Zoom into specific areas of the network tree.
- ▶ Edit the properties of a node.
- ▶ Create a Tofino Discovery Scan

See: [General Editing Menu for all Nodes \(except Network Nodes\)](#)

See: [Network Node Right Click Menu](#)

2.3.1.1.1 General Editing Menu

The General Editing right click menu appears when any node, other than a Tofino SA or a Network node is selected in the Network Editor window.

See: [Insert](#)

See: [Append](#)

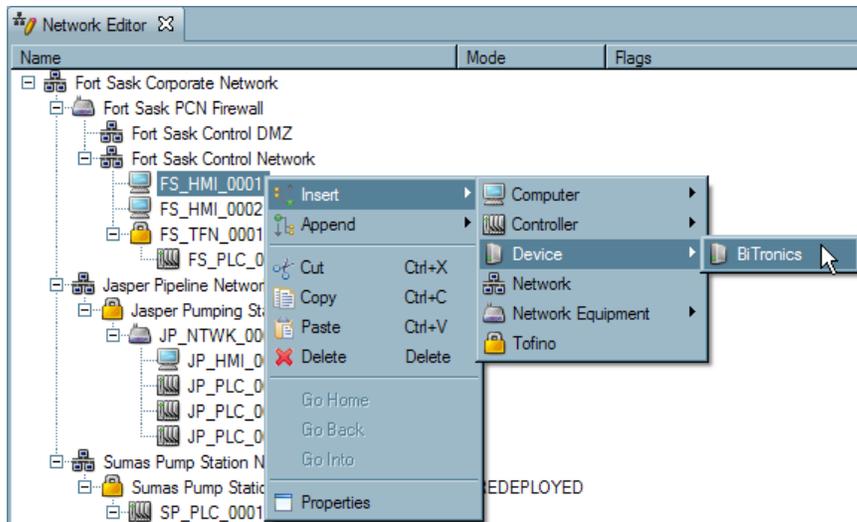
See: [Cut, Copy, Paste, Delete](#)

See: [Go Into](#)

See: [Properties](#)

Inserting Network Nodes

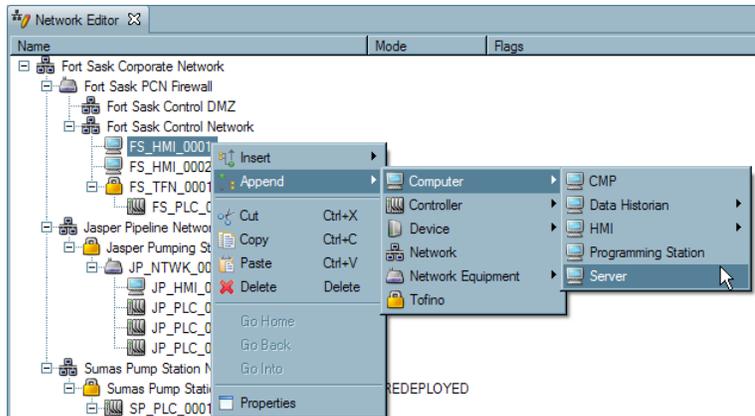
The Insert menu item allows you to add new nodes to your network diagram. These nodes appear above the currently selected node.



- Right click on a node in the Network Editor window.
- Select Insert. **Note:** Inserting a new node will place the new node above the node currently selected in the Network Editor window. This function is designed to be used to add parents to a network.
- Select the type of node to be added to the network.
- A node specific wizard will pop up to guide the set up of the node.

Appending Network Nodes

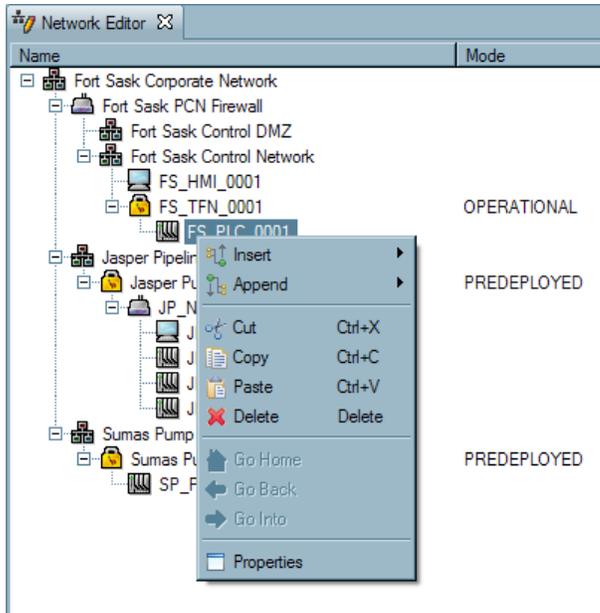
The Append menu item allows you to add new nodes to your network diagram. These nodes appear below the currently selected node.



- Right click on a node in the Network Editor window.
- Select Append. **Note:** Appending a new node will place the new node *below* the node currently selected in the Network Editor window. This function is designed to be used to add children to a network.
- Select the type of node to be added to the network.
- A node specific wizard will pop up to guide the set up of the node.

Editing a Network (Cut, Copy, Paste, Delete)

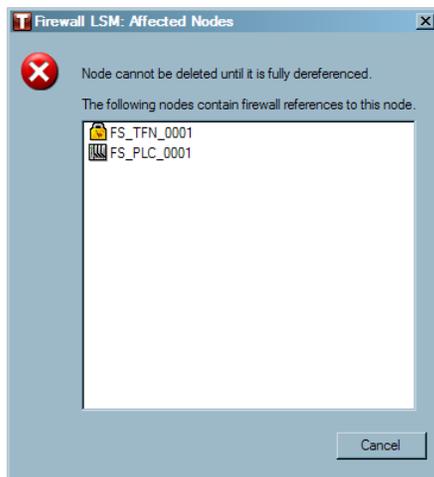
These menu items allow you to duplicate or move network nodes in your diagram.



This menu item allows nodes in the Network Editor window to be cut, copied, pasted, or deleted. Simply click on the node you choose to edit, then right click and select the chosen action.

Note: Keyboard shortcuts can also be used instead of the right click.

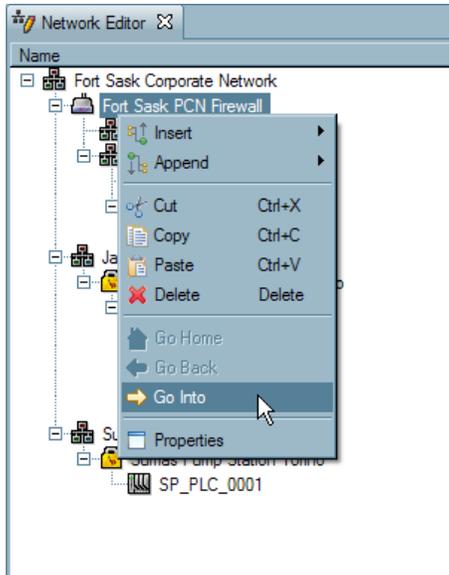
Note: A node that is in use in another location in the database cannot be deleted from the Network Editor window until all references to it have been removed from the Tofino CMP database. A window will appear warning you if there are references to the node type you are trying to delete.



Go Into/Go Back/Go Home

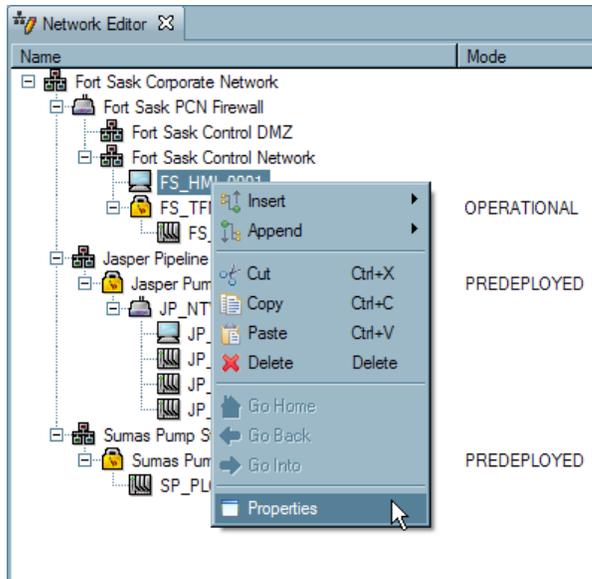
Allows a closer view of branches on the network diagram.

See: [Go Into/Go Back/Go Home](#)



Editing Network Nodes' Properties

This menu item opens a node's properties page.

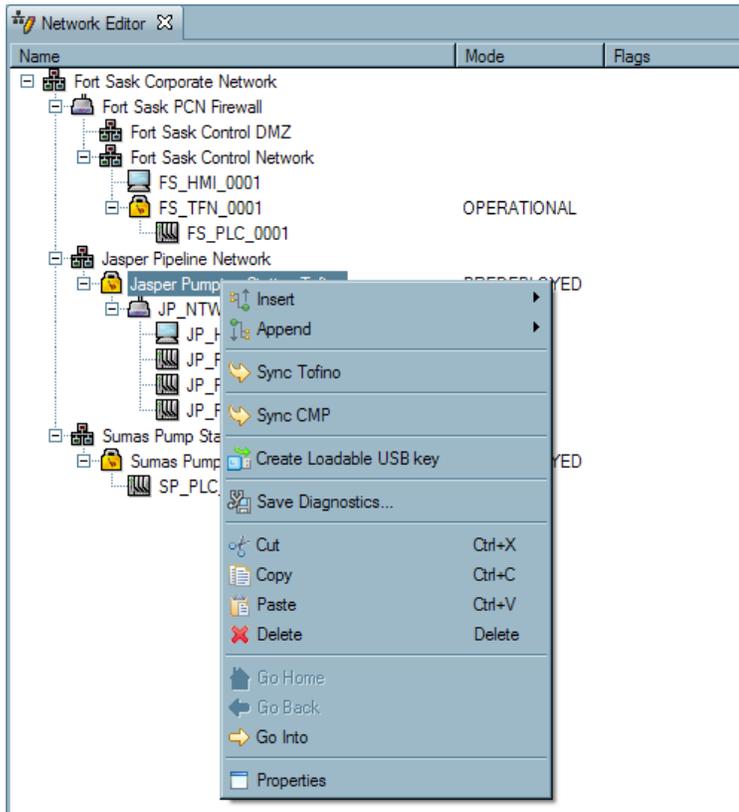


To edit the properties of a node, right click and select "Properties". A properties screen will open in the Network Editor window specific to the type of node that is being edited. See: [Editing a Node's Properties](#)

2.3.1.1.2 Tofino SA Specific Menu

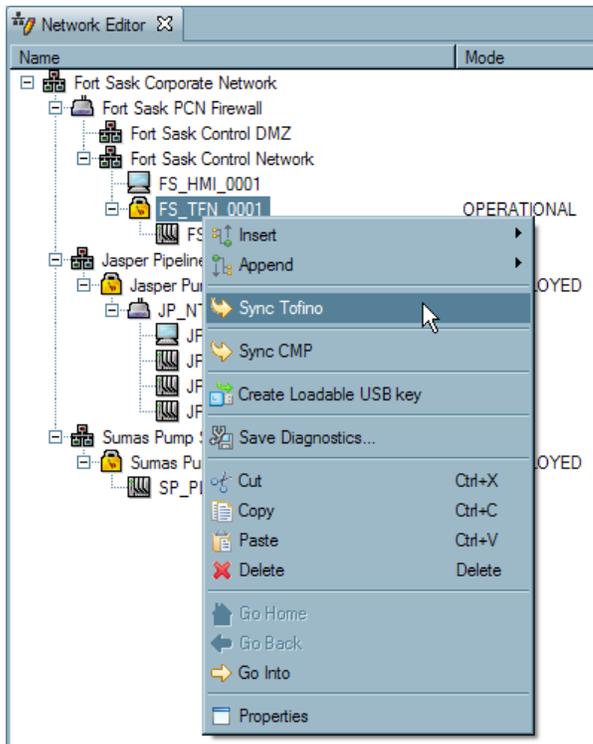
The Tofino SA Specific right click menu appears when a Tofino SA is selected in the Network Editor window.

- See: [Insert](#)
- See: [Append](#)
- See: [Sync Tofino](#)
- See: [Sync CMP](#)
- See: [Create Loadable USB Key](#)
- See: [Save Diagnostics...](#)
- See: [Cut, Copy, Paste, Delete](#)
- See: [Go Into](#)
- See: [Properties](#)



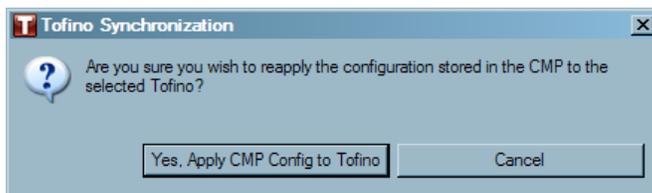
Sync Tofino

This option allows a Tofino SA in the field to have its configuration synchronized to match the configurations stored in the Tofino CMP database. In other words, the configuration in the Tofino SA will be over-written by the configuration in the Tofino CMP database.



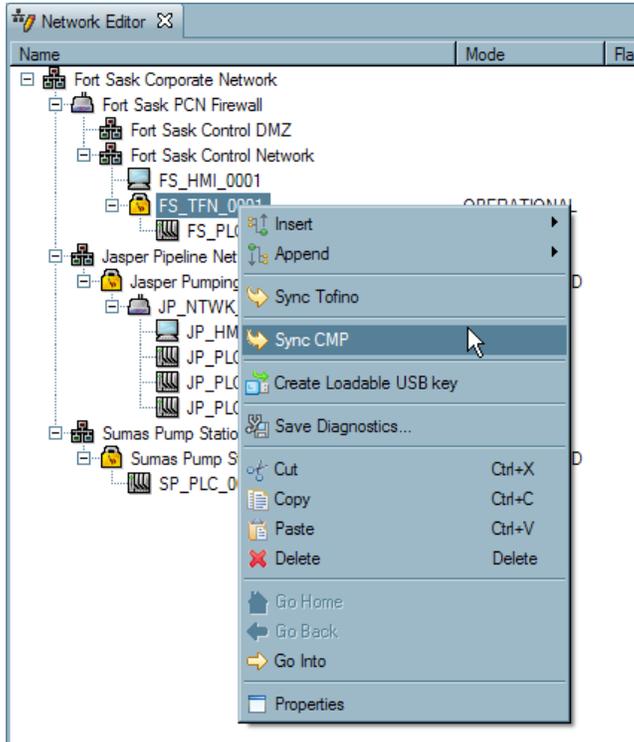
To perform this synchronization:

- Right click on the appropriate Tofino SA icon, select the "Sync Tofino" menu item.
- Then click "Yes, Apply CMP Config to Tofino" to start the synchronization.



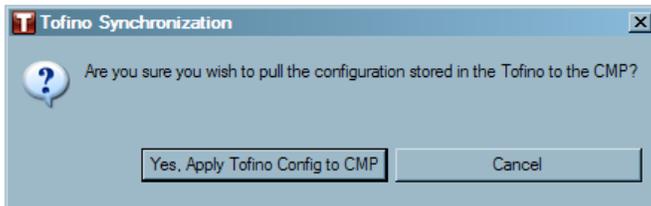
Sync CMP

This option allows Tofino SA in the field to load its configuration to the Tofino CMP database. In other words, the configuration in the Tofino CMP database will be over-written by the configuration in the Tofino SA.



To perform this synchronization:

- Right click on the appropriate Tofino SA, select the "Sync CMP" menu item.
- Next, click "Yes, Apply Tofino Config to CMP" to start the synchronization.

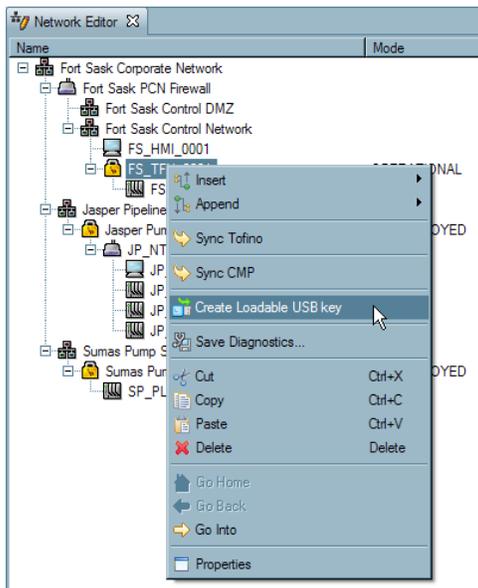


- A window will open while the configurations are completed.
- If the Tofino SA contains references to nodes that are not in the Tofino CMP database the Tofino CMP will prompt you to create these nodes in your diagram. This is known as a network re-build. For example, if a Tofino SA contains a Firewall rule that references an IP address that is missing from the current network diagram then the network re-build feature will be activated. See: [Network Re-Build Wizard](#)

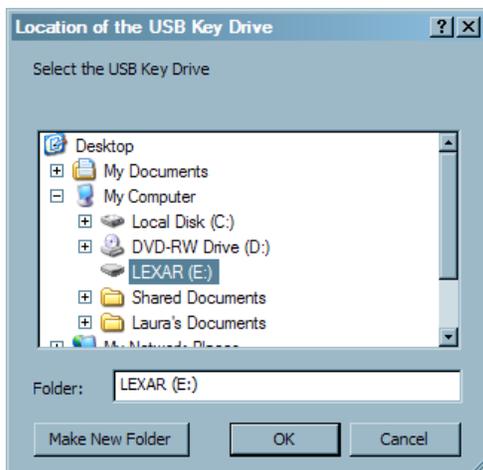
Create Loadable USB Key

This option takes the information that is contained in the Tofino CMP database for the selected Tofino SA and stores it on the USB key in encrypted form. This key can then be used to configure a Tofino SA in the field that the Tofino CMP cannot directly communicate to. For example, the Tofino SA may be located at a site that does not have network communications back to the Tofino CMP. **Remember to scan the USB key for viruses before connecting to the Tofino CMP!**

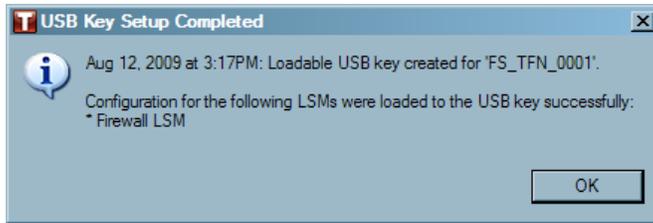
- Select the icon of the Tofino SA you wish to have a USB key created for.
- Right click on that icon and select the menu item "Create Loadable USB Key".



- Locate and select the USB key being used to save the information and click "OK".



- Once the information has been saved to the USB key, a dialog will open saying that is was successful.

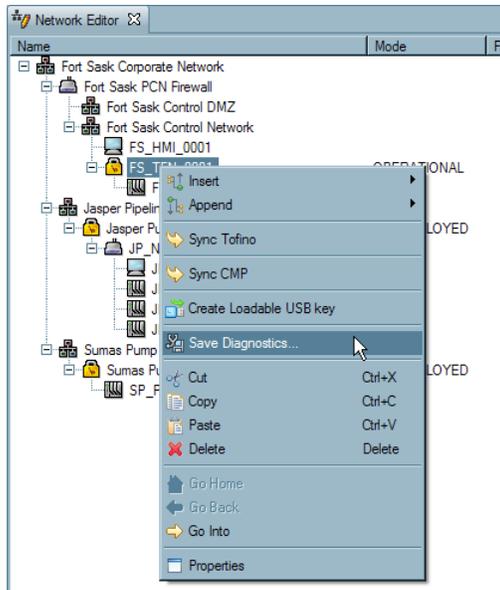


- The USB key can now be used for loading the configuration into a Tofino SA in the field.

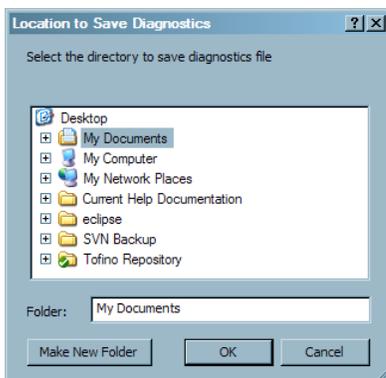
Save Diagnostics

This option allows the user to have the Tofino CMP collect diagnostic information from a Tofino SA saved to the disk file specified by the user. The user may then transmit this encrypted file to support@tofinosecurity.com for further analysis.

- Select the icon of the Tofino SA you wish to save the diagnostics for.
- Right click on that icon.
- Select the menu item "Save Diagnostics".



- Select the directory where the diagnostics file should be saved and click "OK".



- After the file location is selected, the Tofino CMP initiates an connection to the selected Tofino SA and collects diagnostic information.

Once the diagnostic information is stored in the location you specified, you can use send this file to technical support for analysis. Email support@tofinosecurity.com.

2.3.1.1.3 Network Node Menu

The Network node right click menu appears when a Network node is right clicked in the Network Editor window.

See: [Insert](#)

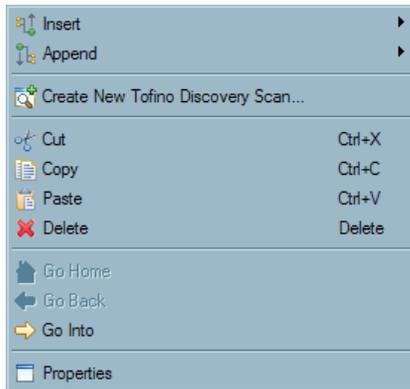
See: [Append](#)

See: [Create New Tofino Discovery Scan...](#)

See: [Cut, Copy, Paste, Delete](#)

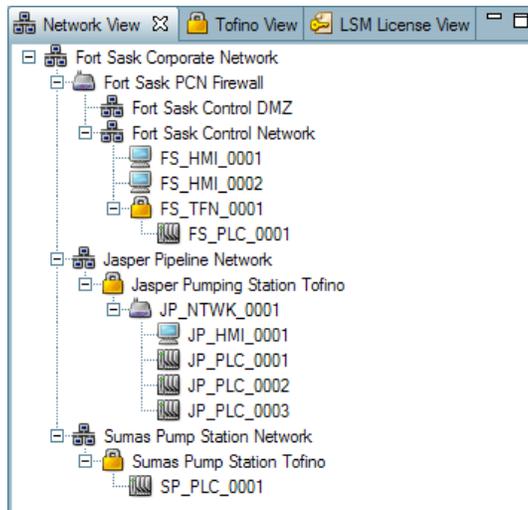
See: [Go Into](#)

See: [Properties](#)



2.3.2 Network View

The Network View window shows a schematic of the control network and is a replication of what is displayed in the Network Editor. It is intended as an easy way to select objects for dragging into other views or opening a node's properties screen (by double clicking on the node). However, unlike the Network Editor, you can not edit the network layout with this view.



The Network View window allows the user to:

- ▶ Drag and drop new icons from the Nodes window to this window in order to add to your network diagram.
- ▶ Drag and drop icons from the Modules window onto Tofino SA icons in this window in order to load LSMs into the appropriate Tofino SA in the field.
- ▶ Drag and drop icons from this window and drop them in the Network Editor window.
- ▶ Expand and collapse branches on the network diagram.
- ▶ Double click icons on the tree to view or edit a node's properties. See: [Editing a Nodes Properties](#)
- ▶ View a specific branch on the network tree by right clicking a node in the Network View window. See: [Go Into/Go Back/Go Home](#)

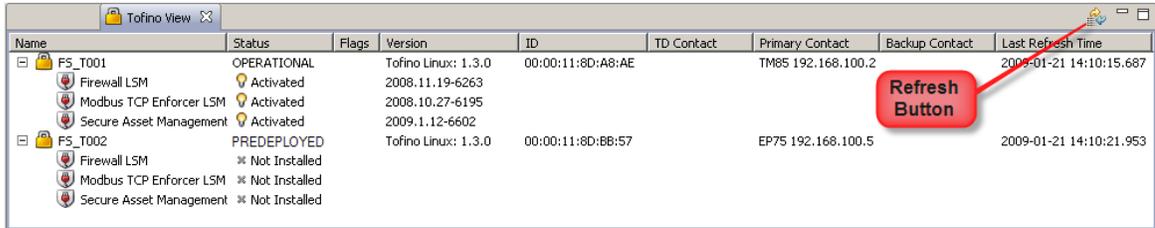
2.3.3 Tofino View

The Tofino View gives the user a snapshot of all Tofino SAs in the network diagram. Here, the user can view the status of the Tofino SAs in the network as well as view and manage LSMs.

See: [Tofino View Column Information](#)

See: [Tofino View Right Click Menu](#)

See: [Warnings in the Tofino View](#)



Name	Status	Flags	Version	ID	TD Contact	Primary Contact	Backup Contact	Last Refresh Time
FS_T001	OPERATIONAL		Tofino Linux: 1.3.0	00:00:11:8D:A8:AE		TM85 192.168.100.2		2009-01-21 14:10:15.687
Firewall LSM	Activated		2008.11.19-6263					
Modbus TCP Enforcer LSM	Activated		2008.10.27-6195					
Secure Asset Management	Activated		2009.1.12-6602					
FS_T002	PREDEPLOYED		Tofino Linux: 1.3.0	00:00:11:8D:BB:57		EP75 192.168.100.5		2009-01-21 14:10:21.953
Firewall LSM	Not Installed	✖						
Modbus TCP Enforcer LSM	Not Installed	✖						
Secure Asset Management	Not Installed	✖						

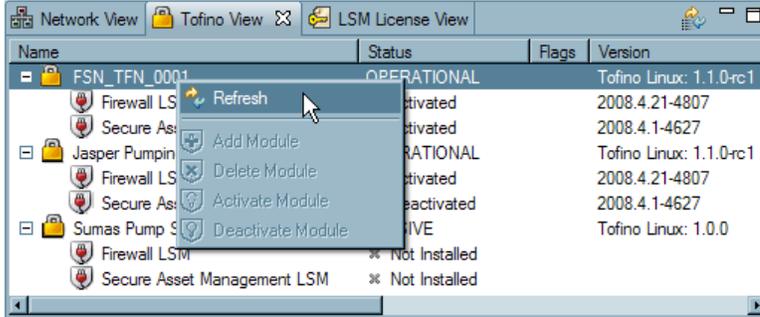
Tofino View Column Information

The Tofino View displays ten column headings giving the user information about the Tofino SAs and LSMs.

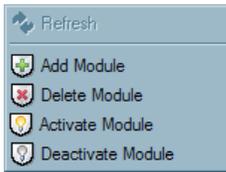
- ▶ Name: Provides the user specified name of each of the Tofino SAs in the network diagram (for example, FS_TFN_0001), as well as the LSMs available.
- ▶ Status: Indicates the operating mode of any Tofino SA's in the diagram (i.e. Predeployed, Passive, Test, Operational, Decommissioned). For LSMs it shows the status of the module (i.e. Not Installed, Deactivated, and Activated).
- ▶ Type: The hardware model.
- ▶ Flags: Indicates if a Tofino SA is Missing. See: [Missing Tofino SAs](#)
- ▶ Version: Provides the version for both the Tofino SA and for each LSM on the Tofino SA.
- ▶ ID: Provides the unique hardware ID for each Tofino SA.
- ▶ TD Contact: (Tofino Discovery Contact) Indicates the IP Address that was used to initially discover and contact the Tofino SA.
- ▶ Primary Contact: Shows the primary contact node of the Tofino SA.
- ▶ Backup Contact: Shows the backup contact node of the Tofino SA.
- ▶ Last Refresh Time: Shows a date and time the Tofino SA was last successfully contacted when doing a refresh. **Note:** The user can use the Refresh button to refresh the entire view manually or right click on specific Tofino SA icon and select "Refresh", to refresh that particular Tofino SA.

Tofino View Right Click Menu

By right clicking on a Tofino SA icon and selecting "Refresh", that particular Tofino SA's information will be refreshed.

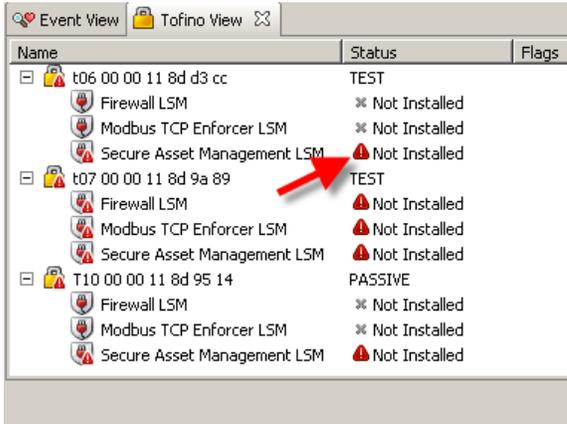


By right clicking on an LSM in the Tofino View the user will be able to manipulate LSMs by selecting "Add Module", "Delete Module", "Activate Module" or "Deactivate Module" depending on what state the particular LSM is in.



See: [Adding an LSM to a Tofino SA](#)

Warnings in the Tofino View

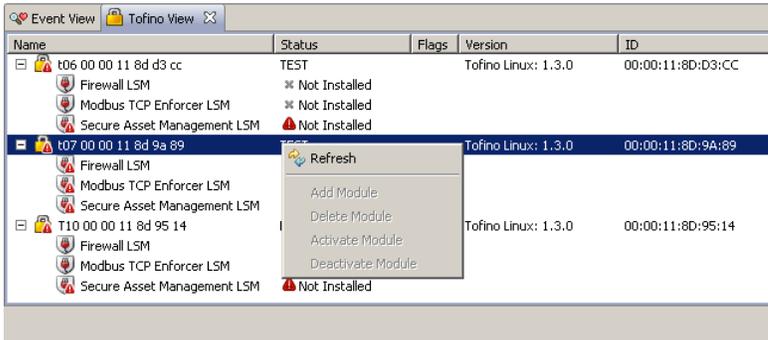


The alert symbol  in the Tofino View indicates that the information the Tofino View is receiving from the Tofino SA does not match the information in the Tofino CMP.

If the information is out of sync, the user can not perform LSM management from the Tofino View.

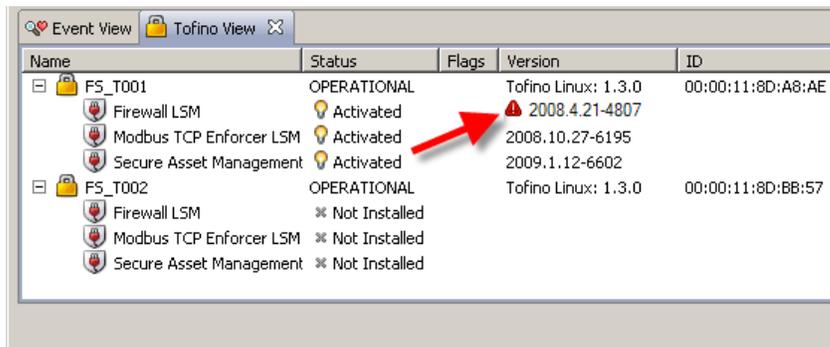
To address this issue, follow these steps:

- Right Click on the Tofino SA icon with the alert symbol and select "Refresh".



- If the alert icons are still present, the Tofino SA and the Tofino CMP need to be synced. This is done in the [Network Editor](#). Selecting "Sync Tofino" will synchronize the Tofino SA's configuration to match the Tofino CMP's current configuration
- Alternatively, selecting "Sync CMP" will synchronize the Tofino CMP's configuration to match the Tofino SA's current configuration

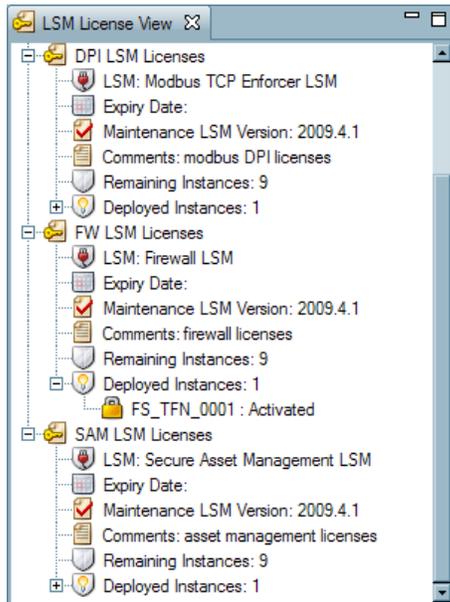
If there is an alert icon next to the Version of the LSM, this means that there is a newer version of the LSM to install.



Name	Status	Flags	Version	ID
FS_T001	OPERATIONAL		Tofino Linux: 1.3.0	00:00:11:8D:A8:AE
Firewall LSM	Activated	⚠	2008.4.21-4807	
Modbus TCP Enforcer LSM	Activated		2008.10.27-6195	
Secure Asset Management	Activated		2009.1.12-6602	
FS_T002	OPERATIONAL		Tofino Linux: 1.3.0	00:00:11:8D:BB:57
Firewall LSM	⌘ Not Installed			
Modbus TCP Enforcer LSM	⌘ Not Installed			
Secure Asset Management	⌘ Not Installed			

To update an LSM to a newer version, select **Tools ▶ LSM Update**.

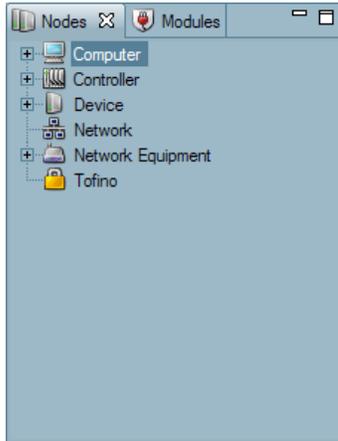
2.3.4 LSM License View



The LSM License View allows the user to view details of the LSMs licensed to the Tofino CMP. The view gives the user the following information:

- ▶ **LSM License:** The display name for a particular LSM, such as Firewall LSM or Secure Asset Management LSM.
- ▶ **LSM ID:** A unique identifier for the LSM, mostly for internal use.
- ▶ **Expiry Date:** Date the LSM license will expire. The date will be displayed in red when the license is expired. Contact support@tofinosecurity.com
- ▶ **Maintenance LSM Version:** This indicates the maintenance contract expiry date, if a newer version of this LSM is released after this date, the license does not cover the new release.
- ▶ **Comments:** General text information about the license.
- ▶ **Remaining Instances:** This indicates the number of licenses remaining to be used.
- ▶ **Deployed Instances:** This indicates the number of licenses in use.
- ▶ **Licensed Tofino:** This shows the name of the Tofino SAs that are using license instances under this LSM License and the status of the LSM.

2.3.5 Nodes



The Nodes window displays the different types of nodes that can be used to build a network diagram. The nodes are broken down into six categories:

- ▶ Computers: Devices that are based on standard computer hardware such as Human Machine Interfaces (HMIs), programming workstations and servers.
- ▶ Controllers: Devices that provide industrial control functionality such as PLCs, DCS and RTUs.
- ▶ Devices: Miscellaneous industrial devices such as Scales or Bar Code Readers.
- ▶ Networks: Collections of devices that belong on a single network or subnet.
- ▶ Network Equipment: Communications hardware such as firewalls, routers, switches, gateways and wireless access points.
- ▶ Tofino SA.

This right click menu allows the user to create and delete node types, as well as edit a node type's properties.



See: [Creating a Node](#)

See: [Importing a Node](#)

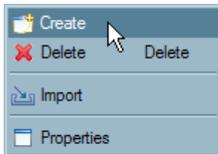
See: [Deleting a Node](#)

See: [Editing a Node's Properties](#)

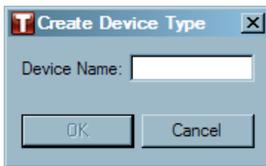
Creating a Node

This menu is found by right clicking one of four node types: Computer, Controller, Device, and Network Equipment. Here the user can create a new node that may not already be found in the node type database. To do this, right click on the node type needing to be created and select "Create".

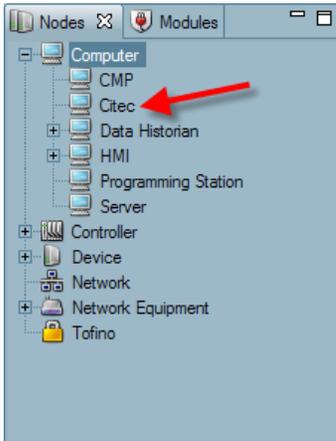
Note: Once a node type has been created the node type name cannot be modified. For example, if you create a node type called "Programming Station" and then later want to call it "Programming Terminal" you must delete the node type and re-create it.



- A window will appear. Type in a name for the device and click "OK".

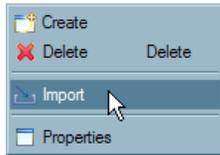


- The new node type will appear in the tree of node types of the same class.

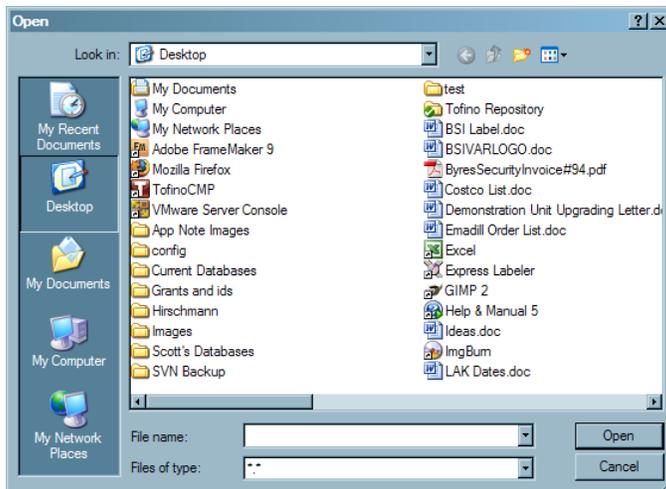


Importing a Node

This menu is found by right clicking in the node view. This menu selection will allow the user to import a Node database sent by Byres Security to update the Node view. This will not overwrite any additions you have made, but simply update the database with new entries. **WARNING:** It is important to note that when importing multiple files from Byres Security there is an order in which they should be imported: Special Rules, Protocols and then Devices (Nodes).



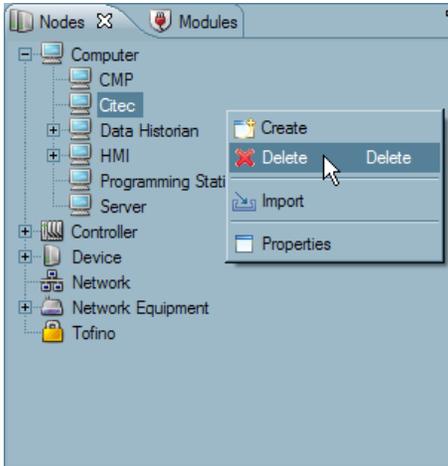
- Right click in the Node window and select "Import".
- Navigate to the file sent by Byres Security, select it and click "Open".



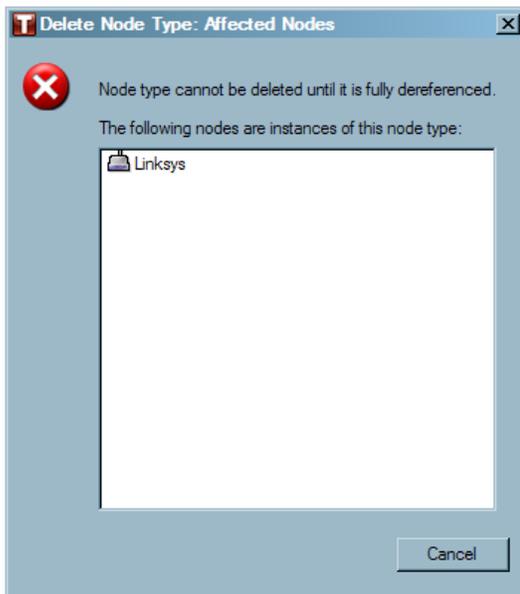
- The new nodes will now be available in the Nodes window.

Deleting a Node Type

- Select the node type to delete, right click and select "Delete".

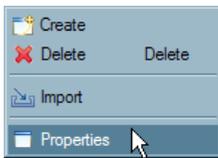


Note: A node type that is in use in the database cannot be deleted from the Nodes window until all references to it have been removed from the Tofino CMP database. A window will appear warning you if there are references to the node type you are trying to delete.

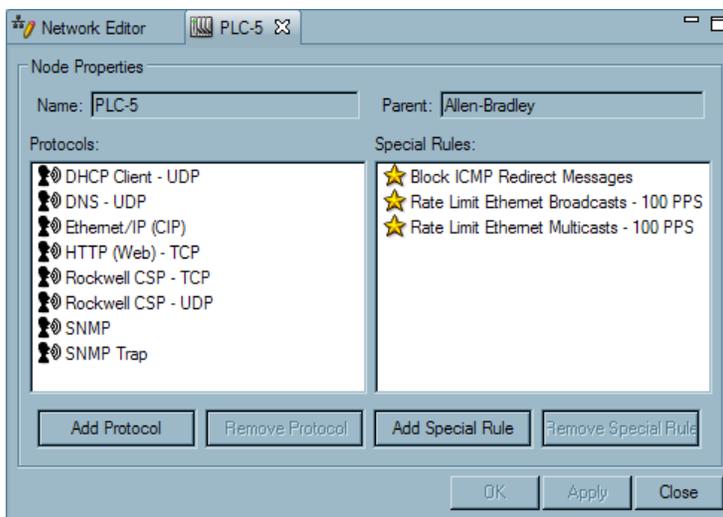


Editing a Node Type's Properties

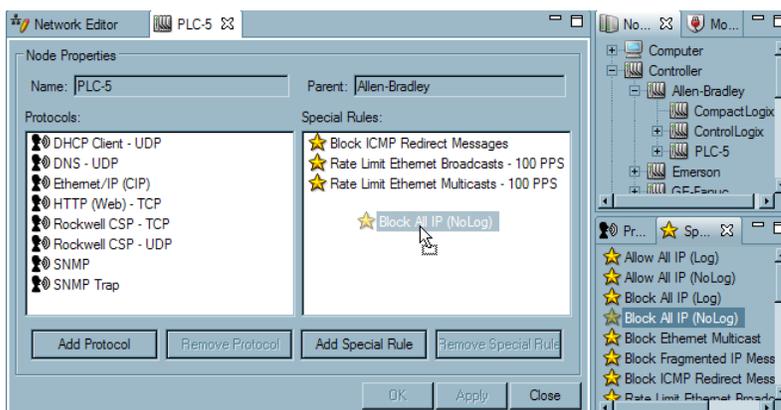
- Select a node type, right click and select "Properties", or double click a node's icon to open the Node Type Properties page.



- The Properties page of the particular node type will open. Here the user can add protocols and special rules that this node type will automatically use when it is added to a network diagram. The user can also delete protocols on the page as well. **Note:** Changing a node type's properties will **not** affect nodes already in the network diagram.



- Protocols and Special Rules can be added to a node type by dragging and dropping them from the Protocols and Special Rules windows.



2.3.5.1 Editing a Node's Properties

There are three ways to edit a node type's properties:

- ▶ Double clicking on the node's icon in the Network Editor window.
- ▶ Double clicking on the node's icon in Network View window.
- ▶ Select the node to edit in the Network Editor window, right click and select "Properties".

Note: There are different Properties pages for different nodes.

[Computer Properties](#)

[Controller Properties](#)

[Device Properties](#)

[Network Properties](#)

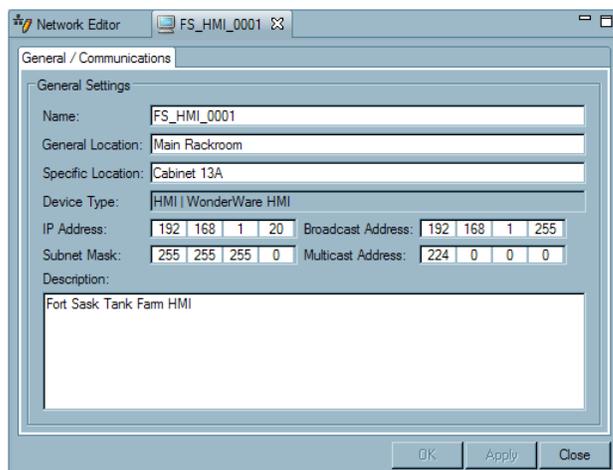
[Network Equipment Properties](#)

Computer Properties

- ▶ Object Name: Insert a name or identifier that uniquely identifies the computer. (i.e.FS-HMI-001). It is important that it is meaningful to the staff in your facility.
- ▶ Description: This will describe the function of the device.
- ▶ General Location: For reference only.
- ▶ Specific Location: For reference only
- ▶ IP Address: This is the IP address of the node. It is important that this address is correct or firewall LSM rules you create may not operate properly.
- ▶ Broadcast Address: This is the address that the node listens for IP broadcasts on. For example, if the node address is 192.168.1.1 the broadcast address might be 192.168.1.255, depending on the subnet of the node. This is required if you wish to provide broadcast filtering rules in the Firewall LSM.
- ▶ Subnet Mask: The subnet mask is used in conjunction with the IP address to identify the computers or devices that are part of a “local” or subnetwork. A subnet mask is 32-bit number that is notated by using four numbers from 0 to 255, separated by periods. Typically subnet masks use either 255 or 0 for each number (such as 255.255.255.0), but other numbers can appear in special cases.
- ▶ Multicast Address: This is the address that the node listens for IP multicasts on. Typically these are IP addresses in the range between 224.0.0.0 through 239.255.255.255 and depend on the manufacturer of controller hardware, the protocols in use and the network configuration. For example, 239.192.22.121 is often used in Ethernet/IP networks, while 234.5.6.7 is often used with Fault Tolerant Ethernet Systems. This is required if you wish to provide multicast filtering rules in the Firewall LSM.

Note: If the node is downstream from a Tofino SA with a firewall LSM, a Firewall tab will be present. If the node was at once but is no longer downstream from a Tofino SA and had firewall rules set, the firewall tab will now be italicized to indicate that the rules are no longer active.

See: [Firewall Rule Configuration for a Node](#)



Controller Properties

- ▶ Object Name: Insert a name or identifier that uniquely identifies the controller. (i.e. Controller Pump station or FS-PLC-0001). It is important that it is meaningful to the staff in your facility.
- ▶ Description: This will describe the function of the device.
- ▶ General Location: For reference only.
- ▶ Specific Location: For reference only.
- ▶ IP Address: This is the IP address of the node. It is important that this address is correct or firewall LSM rules you create may not operate properly.
- ▶ Broadcast Address: This is the address that the node listens for IP broadcasts on. For example, if the node address is 192.168.1.1 the broadcast address might be 192.168.1.255, depending on the subnet of the node. This is required if you wish to provide broadcast filtering rules in the Firewall LSM.
- ▶ Subnet Mask: The subnet mask is used in conjunction with the IP address to identify the computers or devices that are part of a “local” or subnetwork. A subnet mask is 32-bit number that is notated by using four numbers from 0 to 255, separated by periods. Typically subnet masks use either 255 or 0 for each number (such as 255.255.255.0), but other numbers can appear in special cases.
- ▶ Multicast Address: This is the address that the node listens for IP multicasts on. Typically these are IP addresses in the range between 224.0.0.0 through 239.255.255.255 and depend on the manufacturer of controller hardware, the protocols in use and the network configuration. For example, 239.192.22.121 is often used in Ethernet/IP networks, while 234.5.6.7 is often used with Fault Tolerant Ethernet Systems. This is required if you wish to provide multicast filtering rules in the Firewall LSM.

Note: If the node is downstream from a Tofino SA with a firewall LSM, a Firewall tab will be present. If the node was at once but is no longer downstream from a Tofino SA and had firewall rules set, the firewall tab will now be italicized to indicate that the rules are no longer active.

See: [Firewall Rule Configuration for a Node](#)

The screenshot shows a window titled "Network Editor" with a tab for "FS_PLC_0001". The "General Settings" section is active, displaying the following configuration:

Name:	FS_PLC_0001								
General Location:	Main Rackroom								
Specific Location:	Cabinet 16A								
Device Type:	Wago 750-842 PLC								
IP Address:	192	168	1	1	Broadcast Address:	192	168	1	255
Subnet Mask:	255	255	255	0	Multicast Address:	127	0	0	1
Description:	Fort Sask: Tank Farm PLC								

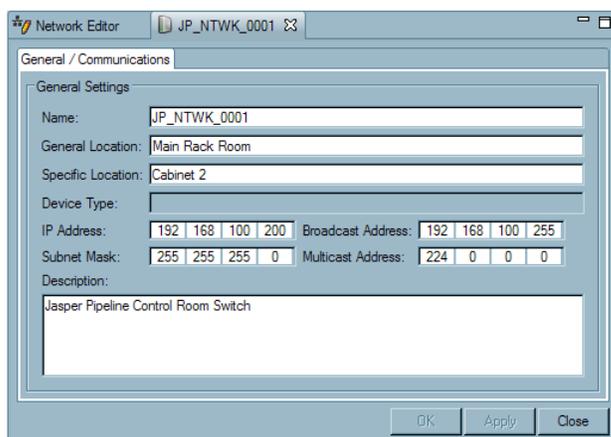
Buttons for "OK", "Apply", and "Close" are visible at the bottom of the dialog.

Device Properties

- ▶ **Object Name:** Insert a name or identifier that uniquely identifies the particular device. (i.e. Pump Station Bar Code Reader or FS-BCR-0001). It is important that it is meaningful to the staff in your facility.
- ▶ **Description:** This will describe the function of the device.
- ▶ **General Location:** For reference only.
- ▶ **Specific Location:** For reference only.
- ▶ **IP Address:** This is the IP address of the node. It is important that this address is correct or firewall LSM rules you create may not operate properly.
- ▶ **Broadcast Address:** This is the address that the node listens for IP broadcasts on. For example, if the node address is 192.168.1.1 the broadcast address might be 192.168.1.255, depending on the subnet of the node. This is required if you wish to provide broadcast filtering rules in the Firewall LSM.
- ▶ **Subnet Mask:** The subnet mask is used in conjunction with the IP address to identify the computers or devices that are part of a “local” or subnetwork. A subnet mask is 32-bit number that is notated by using four numbers from 0 to 255, separated by periods. Typically subnet masks use either 255 or 0 for each number (such as 255.255.255.0), but other numbers can appear in special cases.
- ▶ **Multicast Address:** This is the address that the node listens for IP multicasts on. Typically these are IP addresses in the range between 224.0.0.0 through 239.255.255.255 and depend on the manufacturer of controller hardware, the protocols in use and the network configuration. For example, 239.192.22.121 is often used in Ethernet/IP networks, while 234.5.6.7 is often used with Fault Tolerant Ethernet Systems. This is required if you wish to provide multicast filtering rules in the Firewall LSM.

Note: If the node is downstream from a Tofino SA with a firewall LSM, a Firewall tab will be present. If the node was at once but is no longer downstream from a Tofino SA and had firewall rules set, the firewall tab will now be italicized to indicate that the rules are no longer active.

See: [Firewall Rule Configuration for a Node](#)

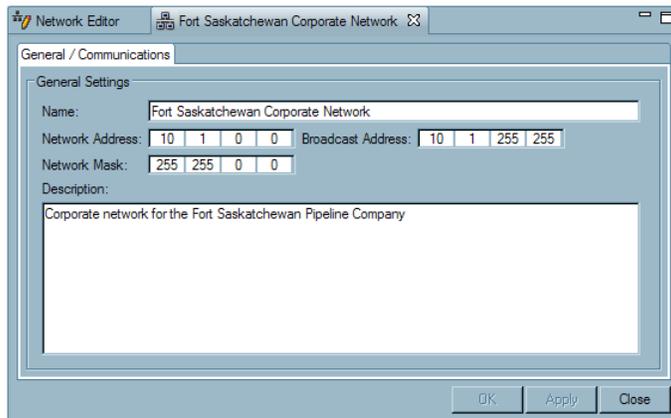


Network Properties

- ▶ **Object Name:** Insert a name or identifier that uniquely identifies the network. (i.e. Fort Sask Control Network). It is important that it is meaningful to the staff in your facility.
- ▶ **Network Address:** This is the general address of the network. For example, if the network has an address range of 192.168.1.1 to 192.168.1.254 then the address of the network is 192.168.1.0.
- ▶ **Network Mask:** This is the subnet mask for the devices on the network. For example, if the network has an address range of 192.168.1.1 to 192.168.1.254 then the network mask is 255.255.255.0.
- ▶ **Broadcast Address:** This is the address that the nodes on this network listens for IP broadcasts on. For example, if the network address is 192.168.1.0 the broadcast address is 192.168.1.255. This is required if you wish to provide broadcast filtering rules in the Firewall LSM.

Note: If the node is downstream from a Tofino SA with a firewall LSM, a Firewall tab will be present. If the node was at once but is no longer downstream from a Tofino SA and had firewall rules set, the firewall tab will now be italicized to indicate that the rules are no longer active.

See: [Firewall Rule Configuration for a Node](#)

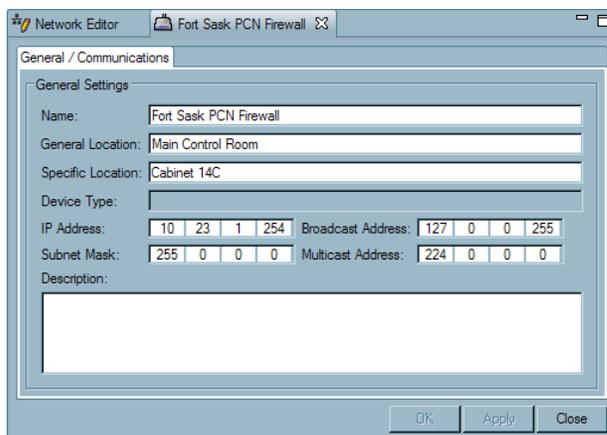


Network Equipment Properties

- ▶ Object Name: Insert a name or identifier that uniquely identifies the network equipment. (i.e. Fort Sask PCN Switch or FS-NTWK-0001). It is important that it is meaningful to the staff in your facility.
- ▶ General Location: For reference only.
- ▶ Specific Location: For reference only.
- ▶ IP Address: If your network device has an IP address, enter it here. If it does not enter in the address 127.0.0.0 as this is a loop back address and will have no impact on the system.
- ▶ Broadcast Address: This is the address that the node listens for IP broadcasts on. For example, if the node address is 192.168.1.1 the broadcast address might be 192.168.1.255, depending on the subnet of the node. This is required if you wish to provide broadcast filtering rules in the Firewall LSM.
- ▶ Subnet Mask: The subnet mask is used in conjunction with the IP address to identify the computers or devices that are part of a “local” or subnetwork. A subnet mask is 32-bit number that is notated by using four numbers from 0 to 255, separated by periods. Typically subnet masks use either 255 or 0 for each number (such as 255.255.255.0), but other numbers can appear in special cases.
- ▶ Multicast Address: This is the address that the node listens for IP multicasts on. Typically these are IP addresses in the range between 224.0.0.0 through 239.255.255.255 and depend on the manufacturer of controller hardware, the protocols in use and the network configuration. For example, 239.192.22.121 is often used in Ethernet/IP networks, while 234.5.6.7 is often used with Fault Tolerant Ethernet Systems. This is required if you wish to provide multicast filtering rules in the Firewall LSM.

Note: If the node is downstream from a Tofino SA with a firewall LSM, a Firewall tab will be present. If the node was at once but is no longer downstream from a Tofino SA and had firewall rules set, the firewall tab will now be italicized to indicate that the rules are no longer active.

See: [Firewall Rule Configuration for a Node](#)



The screenshot shows a window titled "Network Editor" with a sub-tab "Fort Sask PCN Firewall". The window is divided into "General / Communications" and "General Settings". The "General Settings" section contains the following fields:

Name:	Fort Sask PCN Firewall								
General Location:	Main Control Room								
Specific Location:	Cabinet 14C								
Device Type:									
IP Address:	10	23	1	254	Broadcast Address:	127	0	0	255
Subnet Mask:	255	0	0	0	Multicast Address:	224	0	0	0
Description:	 								

At the bottom of the window are three buttons: "OK", "Apply", and "Close".

2.3.5.2 New Node Wizard

When a node is added to a network tree, a node wizard will guide the set-up of the particular node type.

When adding a new Node to your network (with the exception of a Network Node) using drag and drop or using a Network Editor [right click menu](#), the New Node Wizard will pre-fill the Subnet Mask and the Broadcast Address once an IP address has been entered. Both the Subnet Mask and the Broadcast Address can be modified as desired. When adding a Network Node to to your network, once a Network Address has been entered, the Network Mask and the Broadcast Address will automatically pre-fill.

When adding a new Node to your network (with the exception of a Network Node) using [Asset Discovery](#) or through [Assisted Rule Generation](#), the New Node Wizard will automatically pre-fill the IP Address, the Subnet Mask and the Broadcast Address. When adding a Network Node to your network through Assisted Rule Generation, the Network Address, the Network Mask and the Broadcast address will all be automatically pre-filled; all three can be modified as desired.

There are six possible node types used to create a network diagram:

- ▶ [Computer Wizard](#)
- ▶ [Controller Wizard](#)
- ▶ [Device Wizard](#)
- ▶ [Network Wizard](#)
- ▶ [Network Equipment Wizard](#)
- ▶ [Tofino SA \(100 and 220 Series\) Wizard](#)

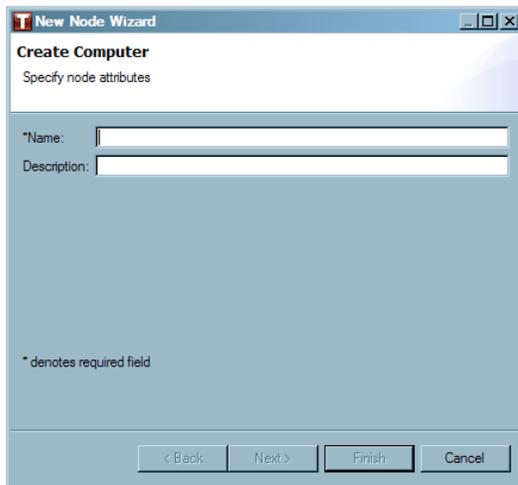
To learn how to build a network diagram see: [Creating Your Network Diagram](#)

Computer Wizard

The Computer Wizard will guide you through configuring the properties for a new Computer node on your network diagram. It will prompt you for the following information:

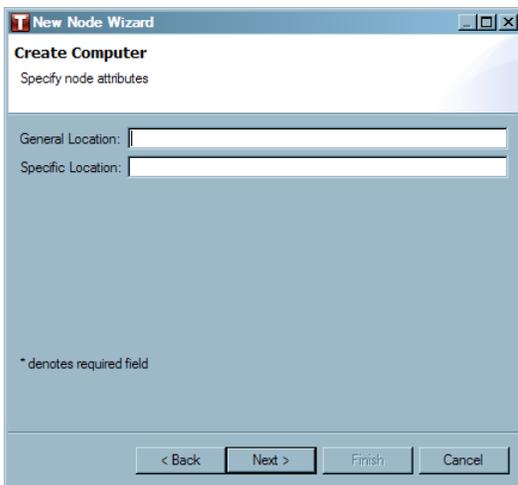
(Note: “ * ” denotes a required field)

- ▶ *Object Name: Insert a name or identifier that uniquely identifies the computer. (i.e.FS-HMI-001). It is important that it is meaningful to the staff in your facility.
- ▶ Description: This will describe the function of the device.
- Once these fields have been completed, click "Next".



The screenshot shows a window titled "New Node Wizard" with a sub-header "Create Computer" and the instruction "Specify node attributes". There are two text input fields: "Name:" and "Description:". The "Name:" field has an asterisk next to it, indicating it is a required field. Below the fields, there is a note: "* denotes required field". At the bottom of the window, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- ▶ General Location: For reference only.
- ▶ Specific Location: For reference only.
- Click "Next" to move on with the set-up.



The screenshot shows a window titled "New Node Wizard" with a sub-header "Create Computer" and the instruction "Specify node attributes". There are two text input fields: "General Location:" and "Specific Location:". The "General Location:" field has an asterisk next to it, indicating it is a required field. Below the fields, there is a note: "* denotes required field". At the bottom of the window, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- ▶ ***IP Address:** This is the IP address of the node. It is important that this address is correct or firewall LSM rules you create may not operate properly.
 - ▶ **Broadcast Address:** This is the address that the node listens for IP broadcasts on. For example, if the node address is 192.168.1.1 the broadcast address might be 192.168.1.255, depending on the subnet of the node. This is required if you wish to provide broadcast filtering rules in the Firewall LSM.
 - ▶ **Multicast Address:** This is the address that the node listens for IP multicasts on. Typically these are IP addresses in the range between 224.0.0.0 through 239.255.255.255 and depend on the manufacturer of controller hardware, the protocols in use and the network configuration. For example, 239.192.22.121 is often used in Ethernet/IP networks, while 234.5.6.7 is often used with Fault Tolerant Ethernet Systems. This is required if you wish to provide multicast filtering rules in the Firewall LSM.
- Click "Finish" to complete the set-up.

The screenshot shows a Windows-style dialog box titled "New Node Wizard" with a sub-header "Create Computer". Below the sub-header is the instruction "Specify node attributes". There are four input fields, each with a small asterisk to its left, indicating they are required: "IP Address:", "Subnet Mask:", "Broadcast Address:", and "Multicast Address:". Each field is represented by a grid of small boxes for digit entry. At the bottom left, there is a note: "* denotes required field". At the bottom of the dialog, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Controller Wizard

The Controller Wizard will guide you through configuring the properties for a new Controller node on your network diagram. It will prompt you for the following information:

(Note: “ * ” denotes a required field)

- ▶ *Object Name: Insert a name or identifier that uniquely identifies the controller. (i.e. Controller Pump station or FS-PLC-0001). It is important that it is meaningful to the staff in your facility.
- ▶ Description: This will describe the function of the device.
- Once these fields have been completed, click "Next".

New Node Wizard

Create Controller

Specify node attributes

*Name:

Description:

* denotes required field

< Back Next > Finish Cancel

- ▶ General Location: For reference only.
- ▶ Specific Location: For reference only
- Click "Next" to move on with the set-up.

New Node Wizard

Create Controller

Specify node attributes

General Location:

Specific Location:

* denotes required field

< Back Next > Finish Cancel

- ▶ ***IP Address:** This is the IP address of the node. It is important that this address is correct or firewall LSM rules you create may not operate properly.
 - ▶ **Broadcast Address:** This is the address that the node listens for IP broadcasts on. For example, if the node address is 192.168.1.1 the broadcast address might be 192.168.1.255, depending on the subnet of the node. This is required if you wish to provide broadcast filtering rules in the Firewall LSM.
 - ▶ **Multicast Address:** This is the address that the node listens for IP multicasts on. Typically these are IP addresses in the range between 224.0.0.0 through 239.255.255.255 and depend on the manufacturer of controller hardware, the protocols in use and the network configuration. For example, 239.192.22.121 is often used in Ethernet/IP networks, while 234.5.6.7 is often used with Fault Tolerant Ethernet Systems. This is required if you wish to provide multicast filtering rules in the Firewall LSM.
- Click "Finish" to complete the set-up.

The screenshot shows a Windows-style dialog box titled "New Node Wizard" with a sub-header "Create Controller". Below the sub-header is the instruction "Specify node attributes". There are four input fields, each with a small asterisk to its left, indicating they are required: "IP Address:", "Subnet Mask:", "Broadcast Address:", and "Multicast Address:". Each field is represented by a grid of four small boxes. At the bottom left, there is a note: "* denotes required field". At the bottom right, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Device Wizard

The Device Wizard will guide you through configuring the properties for a new Device on your network diagram. It will prompt you for the following information:

(Note: “ * ” denotes a required field)

- ▶ *Object Name: Insert a name or identifier that uniquely identifies the particular device. (i.e. Pump Station Bar Code Reader or FS-BCR-0001). It is important that it is meaningful to the staff in your facility.
- ▶ Description: This will describe the function of the device.
- Once these fields have been completed, click "Next".

The screenshot shows a window titled "New Node Wizard" with a sub-header "Create Device" and the instruction "Specify node attributes". There are two text input fields: the first is labeled "*Name:" and the second is labeled "Description:". Below the fields, a note states "* denotes required field". At the bottom, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- ▶ General Location: For reference only.
- ▶ Specific Location: For reference only.
- Click "Next" to move on with the set-up.

The screenshot shows the same "New Node Wizard" window, but now it prompts for location information. The "Name" and "Description" fields are no longer visible. Instead, there are two text input fields: "General Location:" and "Specific Location:". The note "* denotes required field" is still present. The buttons at the bottom are "< Back", "Next >", "Finish", and "Cancel".

- ▶ ***IP Address:** This is the IP address of the node. It is important that this address is correct or firewall LSM rules you create may not operate properly.
 - ▶ **Broadcast Address:** This is the address that the node listens for IP broadcasts on. For example, if the node address is 192.168.1.1 the broadcast address might be 192.168.1.255, depending on the subnet of the node. This is required if you wish to provide broadcast filtering rules in the Firewall LSM.
 - ▶ **Multicast Address:** This is the address that the node listens for IP multicasts on. Typically these are IP addresses in the range between 224.0.0.0 through 239.255.255.255 and depend on the manufacturer of controller hardware, the protocols in use and the network configuration. For example, 239.192.22.121 is often used in Ethernet/IP networks, while 234.5.6.7 is often used with Fault Tolerant Ethernet Systems. This is required if you wish to provide multicast filtering rules in the Firewall LSM.
- Click "Finish" to complete the set-up.

The screenshot shows a Windows-style dialog box titled "New Node Wizard" with a sub-header "Create Device". Below the sub-header is the instruction "Specify node attributes". There are four input fields, each with a red asterisk indicating it is required: "IP Address:", "Subnet Mask:", "Broadcast Address:", and "Multicast Address:". Each field is represented by a grid of four small boxes. At the bottom left, there is a note: "* denotes required field". At the bottom right, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Network Wizard

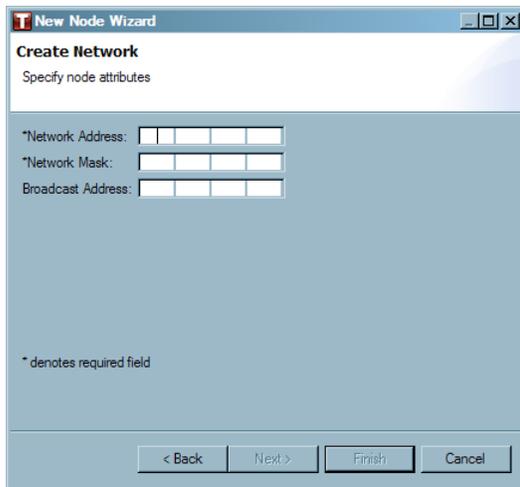
The Network Wizard will guide you through configuring the properties for a new Network on your network diagram. It will prompt you for the following information:

(Note: “ * ” denotes a required field)

- ▶ *Object Name: Insert a name or identifier that uniquely identifies the network. (i.e. Fort Sask Control Network). It is important that it is meaningful to the staff in your facility.
- ▶ Description: This will describe the function of the network.
- Once these fields have been completed, click "Next".

The screenshot shows a Windows-style dialog box titled "New Node Wizard". The main content area is titled "Create Network" and has the subtitle "Specify node attributes". There are two text input fields: one labeled "*Name:" and another labeled "Description:". Below these fields, there is a note that says "* denotes required field". At the bottom of the dialog, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- ▶ *Network Address: This is the general address of the network. For example, if the network has an address range of 192.168.1.1 to 192.168.1.254 then the address of the network is 192.168.1.0.
 - ▶ *Network Mask: This is the subnet mask for the devices on the network. For example, if the network has an address range of 192.168.1.1 to 192.168.1.254 then the network mask is 255.255.255.0.
 - ▶ Broadcast Address: This is the address that the nodes on this network listens for IP broadcasts on. For example, if the network address is 192.168.1.0 the broadcast address is 192.168.1.255. This is required if you wish to provide broadcast filtering rules in the Firewall LSM.
- Click "Finish" to complete the set-up.



The screenshot shows a window titled "New Node Wizard" with a sub-header "Create Network". Below the sub-header is the instruction "Specify node attributes". There are three input fields, each with an asterisk indicating it is required: "*Network Address:", "*Network Mask:", and "Broadcast Address:". Each field is a four-part grid for entering IP address octets. At the bottom left, there is a note: "* denotes required field". At the bottom right, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Network Equipment Wizard

The Network Equipment Wizard will guide you through configuring the properties for a new Network Equipment node on your network diagram. It will prompt you for the following information:

(Note: “ * ” denotes a required field)

- ▶ *Object Name: Insert a name or identifier that uniquely identifies the network equipment. (i.e. Fort Sask PCN Switch or FS-NTWK-0001). It is important that it is meaningful to the staff in your facility.
- ▶ Description: This will describe the function of the device.
- Once these fields have been completed, click "Next".

New Node Wizard

Create Network Equipment

Specify node attributes

*Name:

Description:

* denotes required field

< Back Next > Finish Cancel

- ▶ General Location: For reference only.
- ▶ Specific Location: For reference only.
- Click "Next" to move on with the set-up.

New Node Wizard

Create Network Equipment

Specify node attributes

General Location:

Specific Location:

* denotes required field

< Back Next > Finish Cancel

- ▶ ***IP Address:** If your network device has an IP address, enter it here. If it does not, enter in the address 127.0.0.0 as this is a loop back address and will have no impact on the system.
 - ▶ **Broadcast Address:** This is the address that the node listens for IP broadcasts on. For example, if the node address is 192.168.1.1 the broadcast address might be 192.168.1.255, depending on the subnet of the node. This is required if you wish to provide broadcast filtering rules in the Firewall LSM.
 - ▶ **Multicast Address:** This is the address that the node listens for IP multicasts on. Typically these are IP addresses in the range between 224.0.0.0 through 239.255.255.255 and depend on the manufacturer of controller hardware, the protocols in use and the network configuration. For example, 239.192.22.121 is often used in Ethernet/IP networks, while 234.5.6.7 is often used with Fault Tolerant Ethernet Systems. This is required if you wish to provide multicast filtering rules in the Firewall LSM.
- Click "Finish" to complete the set-up.

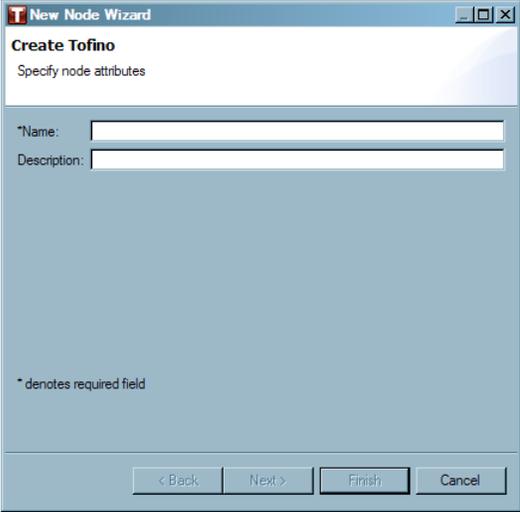
The screenshot shows a window titled "New Node Wizard" with a sub-header "Create Network Equipment". Below the sub-header is the instruction "Specify node attributes". There are four input fields, each with an asterisk indicating it is required: "IP Address:", "Subnet Mask:", "Broadcast Address:", and "Multicast Address:". Each field is represented by a grid of small boxes for entering digits. At the bottom of the window, there is a note "* denotes required field" and four buttons: "< Back", "Next >", "Finish", and "Cancel".

Tofino SA (100 and 220 Series)

The Tofino SA Wizard will guide you through configuring the properties for a new Tofino SA node on your network diagram. It will prompt you for the following information:

(Note: “ * ” denotes a required field)

- ▶ *Name: Insert a name or identifier that uniquely identifies the Tofino SA. (i.e. Jasper Pump Station Tofino or JP-TFN-001). It is important that it is meaningful to the staff in your facility. **Remember that each Tofino SA needs to have a unique name to avoid confusion.**
- ▶ Description: This will describe the function of the device.
- Once these fields have been completed, click "Next".



The screenshot shows a window titled "New Node Wizard" with a sub-header "Create Tofino" and the instruction "Specify node attributes". It contains two text input fields: "*Name:" and "Description:". Below the fields is a note: "* denotes required field". At the bottom, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- ▶ General Location: For reference only.
- ▶ Specific Location: For reference only.
- Click "Next" to move on with the set-up.

The screenshot shows a window titled "New Node Wizard" with a sub-header "Create Tofino" and the instruction "Specify node attributes". Below this, there are two text input fields: "General Location:" and "Specific Location:". A legend at the bottom left states "* denotes required field". At the bottom of the window, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- ▶ *Tofino ID: Enter the ID number from the lower front of the Tofino 100 SA's face or on the right side of the Tofino 220 SA's face.
 - ▶ *Heartbeat Interval: This number indicates the number of seconds between periodic heartbeats coming from this Tofino SA. These heartbeats give regular status updates of the Tofino SAs listed in the network. Setting the heartbeat value to a low number provides more rapid updates of the Tofino CMP but generates more network traffic. Note: If heartbeats are set to 0, this shuts the periodic heartbeats off. The default setting is 10 seconds.
 - ▶ *Untrusted Media Type: This sets the interface settings on the upper or Untrusted Ethernet port. The Tofino SA supports auto-negotiation of both Ethernet ports. Auto-negotiation means the Tofino SA's connection and transmission parameters are negotiated automatically with the switch or device it is attached to. The Ethernet ports can also be manually set to:
 - 100base TX-HD
 - 100base TX-FD
 - 10base T-HD
 - 10base T-FD
 - ▶ *Protected Media Type: This sets the interface settings on the lower or trusted Ethernet port. The Tofino SA supports auto-negotiation of both Ethernet ports. Auto-negotiation means the Tofino SA's connection and transmission parameters are negotiated automatically with the switch or device it is attached to. The Ethernet ports can also be manually set to:
 - 100base TX-HD
 - 100base TX-FD
 - 10base T-HD
 - 10base T-FD
 - ▶ *USB Load Config: If this option is set to Enabled, configurations can be loaded from a USB storage device to the Tofino SA and Tofino SA log files can be saved to the flash drive. If this is option is set to Disabled, the USB ports cannot be used.
 - ▶ Mode Button Behaviour: Allows the user to set the behaviour of the Mode button on the Tofino SA, there are 3 possible functions: Toggle, Disabled, and Timed. (Only available with the Tofino 100 SA)
 - ▶ Mode Button Timeout (m): This field will remain grayed out unless the Mode Button Behaviour is set to Timed. If the behaviour is set to Timed, this field will allow the user to enter an amount of time, in minutes, that the Tofino SA will remain in TEST-FIELD-FORCE before reverting back to OPERATIONAL mode once the technician in the field presses the Mode button. (Only available with the Tofino 100 SA)
- Click "Finish" to complete the set-up.

New Node Wizard

Create Tofino
Specify node attributes

*Tofino ID:

*Heartbeat Interval (s):

Unprotected Media Type:

Protected Media Type:

*USB Load Config:

*Mode Button Behavior:

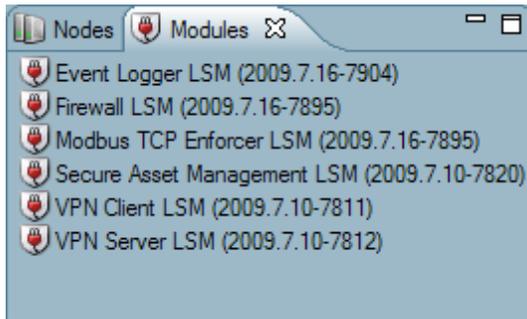
*Mode Button Timeout (m):

* denotes required field

Note: Contact Devices must be configured for proper operation.

< Back Next > Finish Cancel

2.3.6 Modules



The Modules window displays the Loadable Security Modules (LSM) available to add to Tofino SA.

LSMs can be added to a Tofino SA in three ways:

- ▶ Dragged and dropped from the Modules window on to the Tofino SAs icon in the Network Editor window.
- ▶ Through the Tofino SA's Properties window by double clicking the Tofino SA icon in the Network Editor window and then selecting the Modules tab.
- ▶ By right clicking an LSM in the Tofino View.

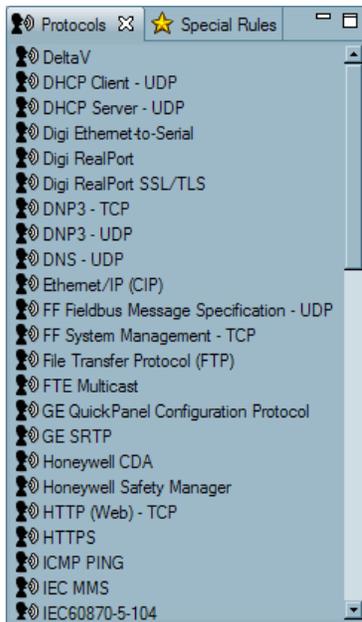
See: [Editing a Node's Properties](#)

See: [LSM Licensing](#)

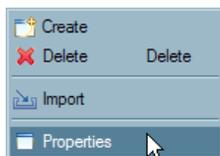
See: [Tofino View](#)

2.3.7 Protocols

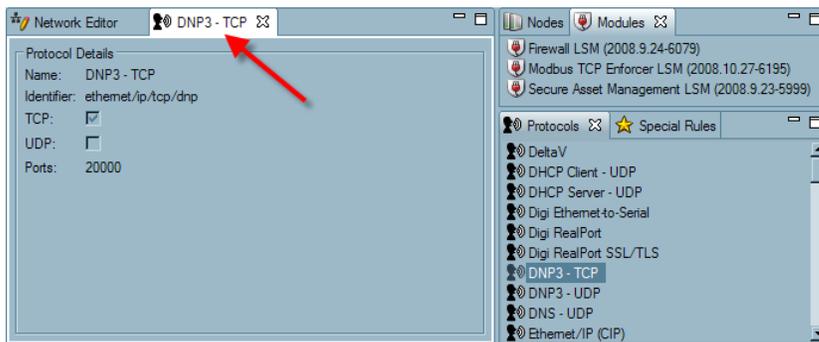
The Protocols window shows all protocols in the Tofino CMP database that are available for various LSM configurations such as rule building using the Firewall LSM. This view also allows the viewing of protocol properties, the creation of new protocols and the importing of predefined protocols created by Byres Security Inc.



To view information about a protocol, double click on the icon and an information window will open. A protocol's properties can also be viewed using the right click menu.



This is a view only window.



Protocols can also be created, deleted, and imported using the right click menu. See: [Protocols View Right Click Menu](#).

Protocol Right Click Menu

The protocol right click menu allows protocols to be created and deleted. The user is also able to import new protocols provided by Byres Security Inc., as well as view Protocols' properties.



See: [Create](#)

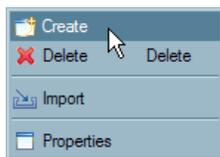
See: [Delete](#)

See: [Import](#)

See: [Properties](#)

Create

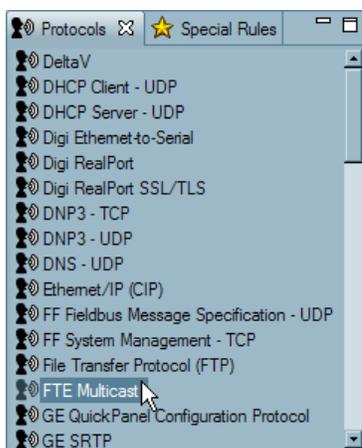
- Right click and select "Create".



- The Protocol Wizard will open. See: [Protocol Wizard](#)

Delete Protocol

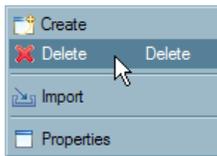
- To delete a protocol, select the protocol in the protocol window to be deleted.



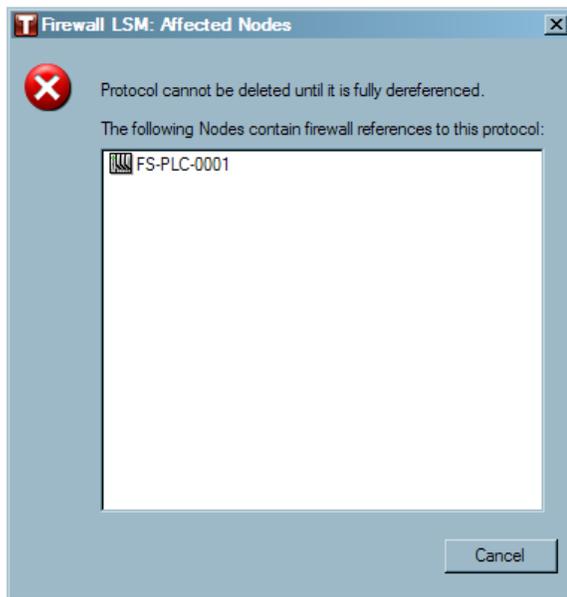
- Open the Edit Menu and select "Delete".



- Right click to open the right click menu and select "Delete".



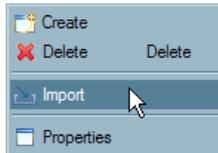
Note: A protocol that is in use in the network diagram or the device database cannot be deleted from the Protocols window until all references to it have been removed. A window will appear warning you if there are references to the protocol you are trying to delete.



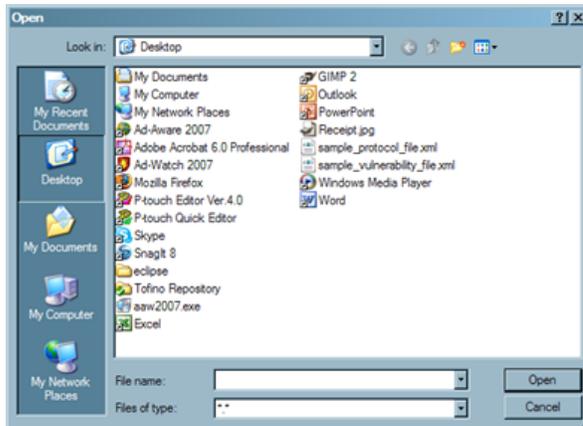
Import

WARNING: It is important to note that when importing multiple files from Byres Security there is an order in which they should be imported: Special Rules, Protocols and then Devices (Nodes).

- To import a protocol, select "Import".



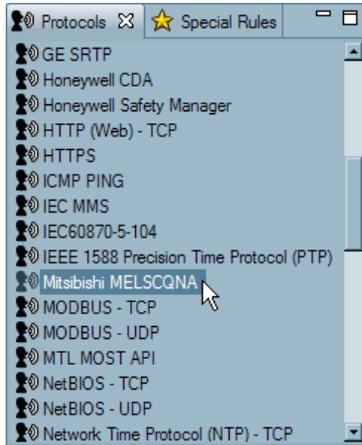
- Locate and select the protocol file and click "OK".



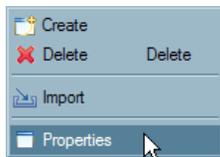
- The protocol will now be in the list in the Protocol view.

Properties

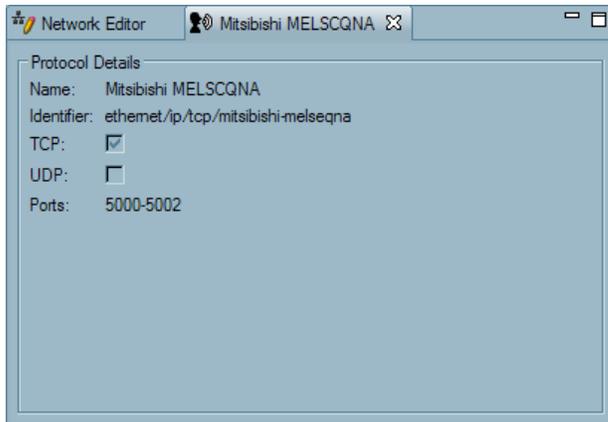
- To see the properties of a protocol select the desired protocol in the Protocol View.



- Right click and select "Properties".

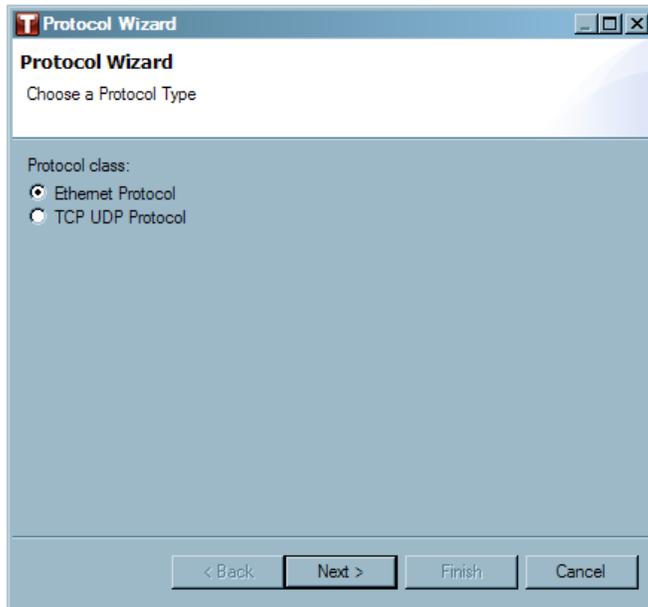


- A screen will open in the Network Editor window showing the properties of the selected protocol.



2.3.7.1 Protocol Wizard

A Protocol Wizard will open and prompt the user through the set-up.



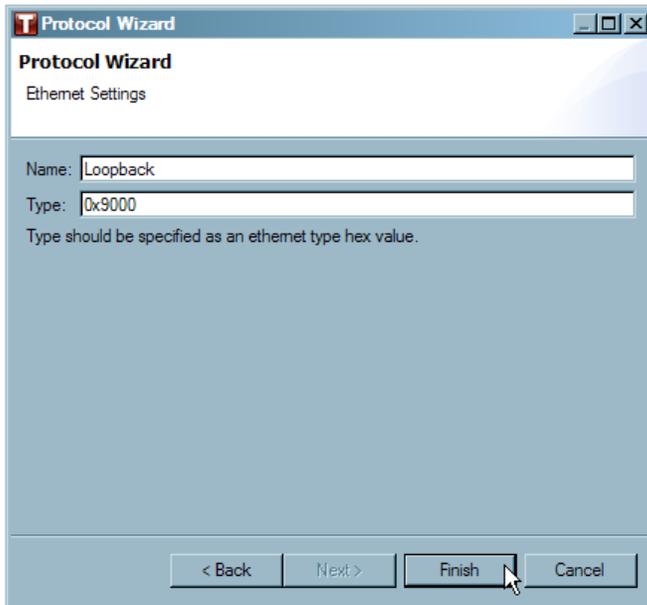
- First, choose the protocol type and click "Next". **Note:** If this wizard was invoked from the Assisted Rule Generation feature, Ethernet protocols can be created but will not be visible within ARG as this protocol type is only supported in manual rule creation.

See: [Ethernet](#)

See: [TCP/UDP Protocol](#)

Ethernet

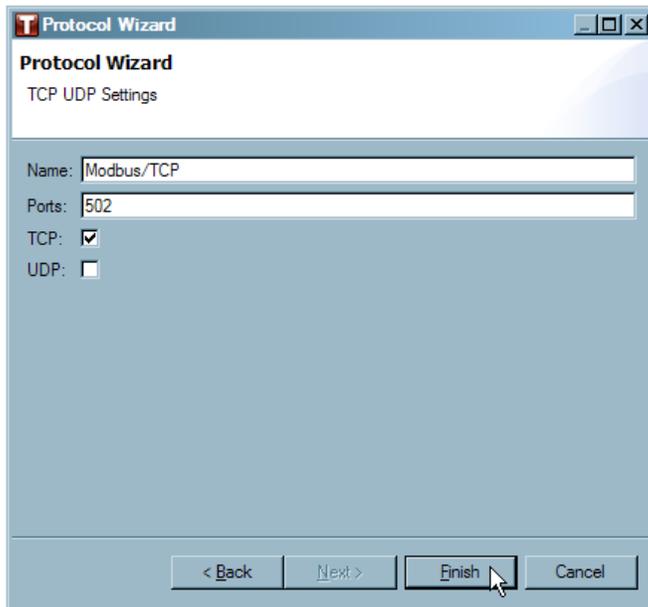
- Give the protocol a name.
- Enter the type number (in hexadecimal format). For more information see: <http://www.iana.org/assignments/ethernet-numbers>
- Click "Finish" when all necessary fields are completed. The created protocol will be available in the protocols window, listed in alphabetical order.



The screenshot shows a window titled "Protocol Wizard" with a sub-header "Ethernet Settings". It contains two text input fields: "Name:" with the value "Loopback" and "Type:" with the value "0x9000". Below the "Type:" field, there is a note: "Type should be specified as an ethernet type hex value." At the bottom of the window, there are four buttons: "< Back", "Next >", "Finish", and "Cancel". A mouse cursor is pointing at the "Finish" button.

TCP/ UDP Protocol

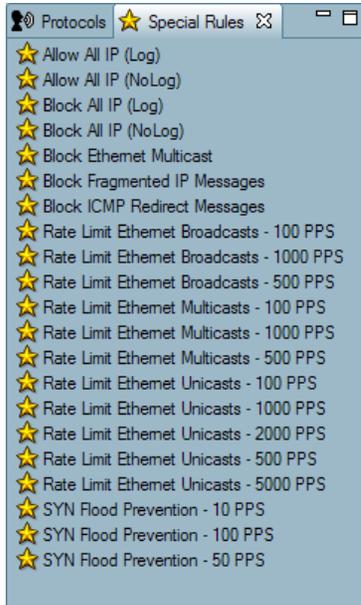
- Give the protocol a name.
- Identify the ports using commas to separate individual port numbers or dashes to separate a range of port numbers. For example if the protocol uses the TCP ports 5000 through 5004, they can be entered as either 5000, 5001, 5002, 5003, 5004 or 5000-5004. Do not use any characters other than the numbers 0 through 9 and commas and dashes.
- Select the TCP box, the UDP box or both boxes.
- Click "Finish" when all necessary fields are completed. The created protocol will be available in the protocols window, listed in alphabetical order or in the Assisted Rule Generation list.



The screenshot shows a window titled "Protocol Wizard" with a sub-header "TCP UDP Settings". It contains two text input fields: "Name:" with the value "Modbus/TCP" and "Ports:" with the value "502". Below these are two checkboxes: "TCP:" which is checked, and "UDP:" which is unchecked. At the bottom of the window are four buttons: "< Back", "Next >", "Finish", and "Cancel". A mouse cursor is positioned over the "Finish" button.

2.3.8 Special Rules

The Special Rules window shows special rules that can be added to Tofino SA firewall configurations. These special rules generally have specific permission, protocol, and direction attributes embedded within them. This window also allows the user to import special rules created by Byres Security Inc.



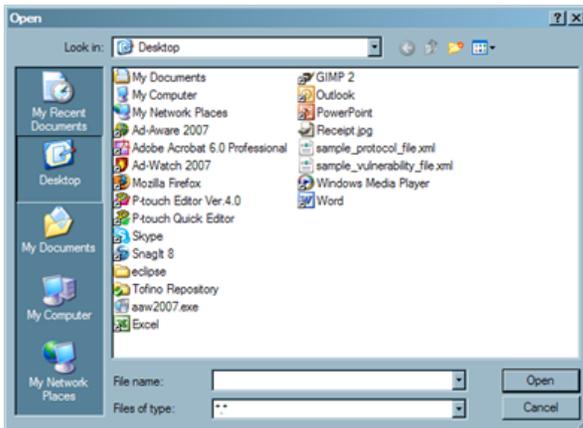
Importing Special Rules

The Special Rules right click menu allows the user to import Special Rules created by Byres Security Inc. **WARNING:** It is important to note that when importing multiple files from Byres Security there is an order in which they should be imported: Special Rules, Protocols and then Devices (Nodes).

- Right click in the Special Rules window and select "Import".



- Locate and select the Special Rules file and click "Open".

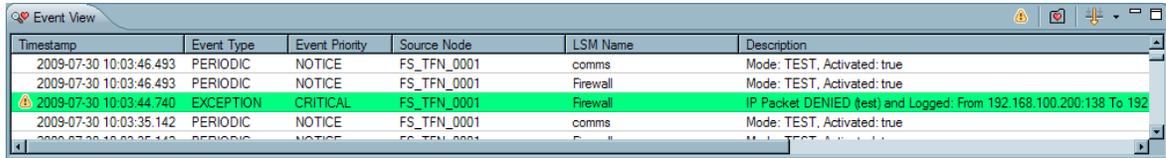


- The Special Rule will now be available on the list in the Special Rules view.

Note: If you import updated Special Rules they are not automatically updated on the Tofino SA. For safety reasons only the Special Rules View on the Tofino CMP is updated. If you want to update Special Rules on the Tofino SA, you must re-apply the new version of the rule.

2.3.9 Event View

The Event View displays all alarm and event information generated by the Tofino SAs or Tofino CMP. This is in the form of Tofino “Heartbeats” which are the messages sent back to the Tofino CMP from each Tofino SA, as well as locally generated events such as a Tofino SA being reported as missing by the Tofino CMP.



Timestamp	Event Type	Event Priority	Source Node	LSM Name	Description
2009-07-30 10:03:46.493	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:03:46.493	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true
2009-07-30 10:03:44.740	EXCEPTION	CRITICAL	FS_TFN_0001	Firewall	IP Packet DENIED (test) and Logged: From 192.168.100.200:138 To 192
2009-07-30 10:03:35.142	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:03:35.142	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true

The Event View tab organizes alarm and event information under six headings: Also note, that the heartbeats are colour coded as per the set up of Tofino CMP Heartbeat Preferences. See: [CMP Preferences](#)

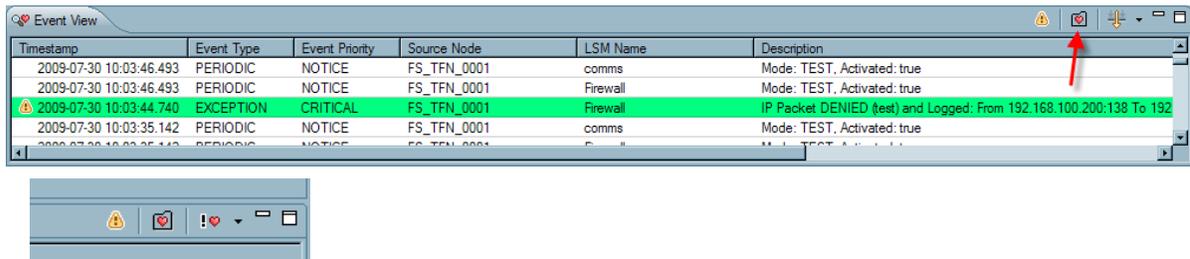
- Timestamp: When the event occurred.
- Event Type:
 - ▶ Periodic: regular reporting messages (heartbeats) from each Tofino SA. The reporting interval is set in the Tofino SAs properties page.
 - ▶ Exception: messages that have been generated because a specific event has occurred such as a packet being blocked by the firewall LSM.
- Event Priority: Shows the priority of the event or alarm. There are seven levels of priority. See: [CMP Preferences](#)
- Source Node: Shows which Tofino SA generated the event (if applicable).
- LSM Name: Shows which Tofino LSM generated the event (if applicable).
- Description: Provides details on the event (such as the IP addresses of blocked network packet).

Event View Buttons

There are three Event View Buttons located on the top right corner of the Event View window. These control the display of events in the window and include:

- ▶ [Acknowledge Event Button](#)
- ▶ [Event Capture Button](#)
- ▶ [Filter Heartbeats Button](#)

There is also a [Right Click](#) menu available that allows you to acknowledge heartbeats and view heartbeat properties.



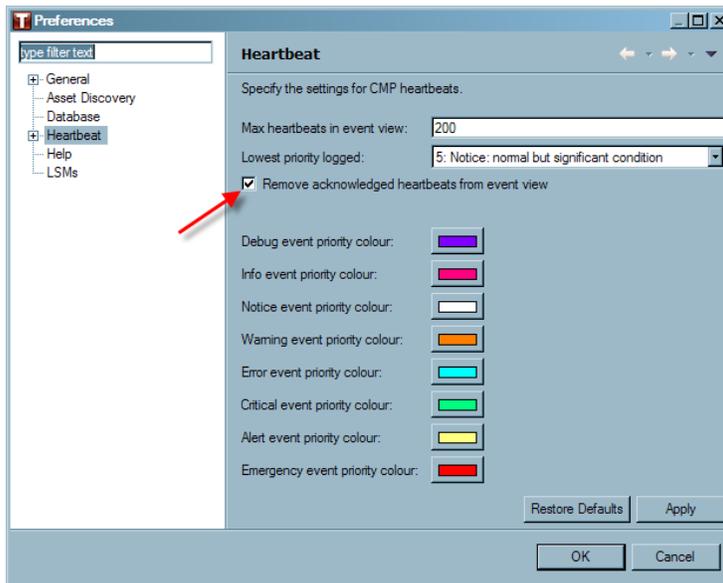
Acknowledge Event Button



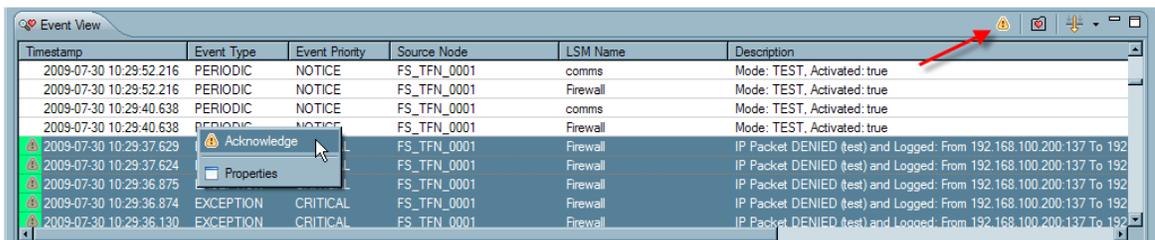
The Acknowledge Item button allows an event or alarm to be acknowledged by the Tofino CMP user. This feature is a memory aid for the user; it helps the user to keep track of which events they have already reviewed and identifies new events that have not yet been dealt with.

Events that have not yet been acknowledged will have the  symbol beside them. This symbol will remain beside the event until the user has acknowledged it. To acknowledge an event select it and click on the  button on the top, right hand side of the screen, or by selecting the particular event and right clicking and selecting "Acknowledge".

The user can also set Heartbeat preferences so that acknowledged events are automatically removed from the Event View, keeping the event view tidy. To activate this feature, select the "Remove acknowledged heartbeats" from event view box under **Window ► CMP Preferences ► Heartbeat**.



To acknowledge multiple Exception heartbeats, hold down the "Shift" or "Ctrl" button on your key board to select multiple heartbeats.

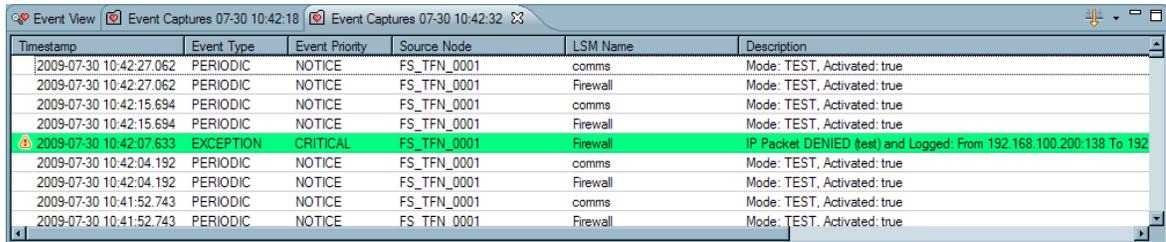


Next, right click and select "Acknowledge" or click the acknowledge button on the right hand side of the screen.

Event Capture Button



The Event Capture button takes a snapshot of current Event View and displays it in a new view window. This is useful during times when events are scrolling rapidly on the screen and a critical event may become obscured by incoming new events.

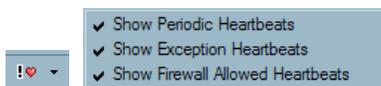


The screenshot shows a window titled 'Event View' with three tabs: 'Event Captures 07-30 10:42:18', 'Event Captures 07-30 10:42:32', and 'Event Captures 07-30 10:42:32'. The main content is a table with the following columns: Timestamp, Event Type, Event Priority, Source Node, LSM Name, and Description. The table contains several rows of event data, with one row highlighted in green.

Timestamp	Event Type	Event Priority	Source Node	LSM Name	Description
2009-07-30 10:42:27.062	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:42:27.062	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true
2009-07-30 10:42:15.694	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:42:15.694	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true
2009-07-30 10:42:07.633	EXCEPTION	CRITICAL	FS_TFN_0001	Firewall	IP Packet DENIED (test) and Logged: From 192.168.100.200:138 To 192
2009-07-30 10:42:04.192	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:42:04.192	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true
2009-07-30 10:41:52.743	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:41:52.743	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true

See: [Event Capture](#)

Filter Heartbeats Button



The Filter Heartbeats button allows users to either display or hide periodic or exception heartbeat events using the Show Periodic Heartbeats or the Show Exception Heartbeats filters. Generally only exception heartbeats should be displayed, as viewing periodic heartbeats can result in excessive screen clutter.

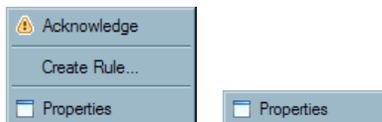
As well, the Show Firewall Allowed Heartbeats filter allows the user to either display or hide traffic from established connections.

Established Connections: The default behaviour of the Tofino SA firewall is to block any traffic that does not have a firewall rule to permit it. However, if a network connection is already in place ('established') when the Tofino SA Firewall begins operation, the Tofino SA will not block that connection even if no firewall rule exists to permit it.

If an established connection is present when the Tofino SA is in TEST mode, the Tofino SA will generate a special form of Firewall Exception Heartbeat to alert the user to the presence of the established connection. These Firewall Exception Heartbeats include the text 'ALLOWED' in their description to differentiate them from other Firewall Exception Heartbeats that are used to report blocked traffic. When a Firewall Heartbeat reports a connection as 'ALLOWED', the user should check the IP addresses and port numbers in this connection to see if it should be permitted, and if so the firewall rules should also be checked on the Tofino SA to ensure that a rule has been created to allow this traffic.

Heartbeat Right Click Menu

The Heartbeat Right Click menu allows the user to acknowledge events and alarms (also known as heartbeats), view the properties of an event or alarm, and create firewall rules using the Assisted Rule Generation feature.



Note: The Acknowledge selection is only available when there is an event or alarm that needs to be acknowledged. The "Create Rule..." selection will only be available when right clicking on an exception heartbeat and if the Secure Asset Management LSM is installed on the Tofino SA. See: [Using Assisted Rule Generation](#)

Acknowledge



When an alarm (heartbeat) needs to be acknowledged, the  symbol will appear beside the alarm record. Events or alarms that need acknowledgment include: Warning, Alert, and Critical. To acknowledge the alarms select the specific record, right click and select "Acknowledge". Or click on the  button on the right side of the Event View window.

Properties

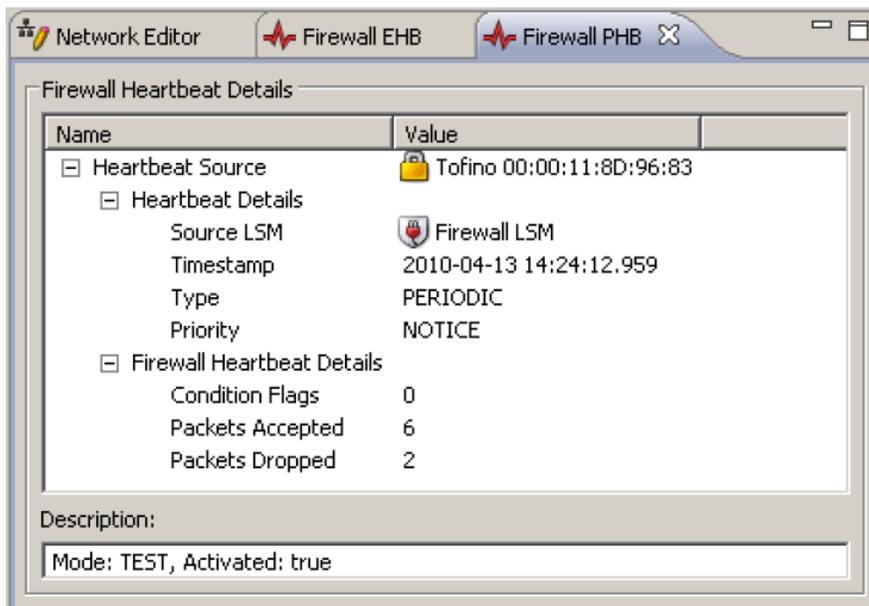
Every heartbeat event or alarm has additional information included in its record. To view the details of a Heartbeat event or alarm:

- Select the heartbeat in the Event View window, right click and select "Properties" or simply double click on the heartbeat.



- The properties of that particular heartbeat will be displayed. Below are examples of both Periodic Heartbeats and Exception Heartbeats.

Periodic Heartbeat Properties Page



Exception Heartbeat Properties Page

Name	Value
Heartbeat Source	Tofino 00:00:11:8D:96:83
Heartbeat Details	
Source LSM	Firewall LSM
Timestamp	2010-04-13 14:14:02.278
Type	EXCEPTION
Priority	CRITICAL
Firewall Heartbeat Details	
Logged Packet Details	
Node (Untrusted Network)	HMI System F025
MAC Address	00:19:D2:69:30:FF
IP Address	192.168.1.106
TCP Port	1252
Direction	INCOMING
Node (Trusted Network)	Trusted Controller C0947
MAC Address	00:19:5B:0D:2C:C7
IP Address	192.168.1.104
TCP Port	80
Protocol	HTTP (Web) - TCP
Advanced	
Capture Length	54 bytes
Ethernet Type	0x800
IP Version	4
IP Protocol	6

Description:
IP Packet DENIED (test) and Logged: From 192.168.1.106:1252 To 192.168.1.104:80; Mode: TEST, Activated: true

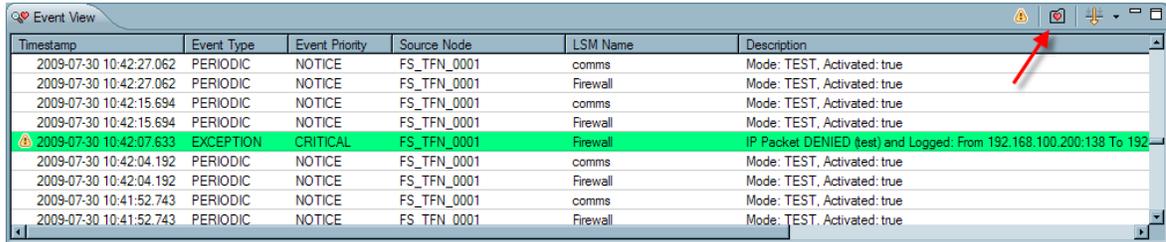
Create Rule

- The Assisted Rule Generation feature can be accessed on the properties page, by click on the "Create Rule" button. See: [Using Assisted Rule Generation](#)

2.3.9.1 Event Capture

The Event Capture window provides a snapshot of the current Event View. It is used to capture an interesting set of events for more in-depth analysis before they scroll off the screen.

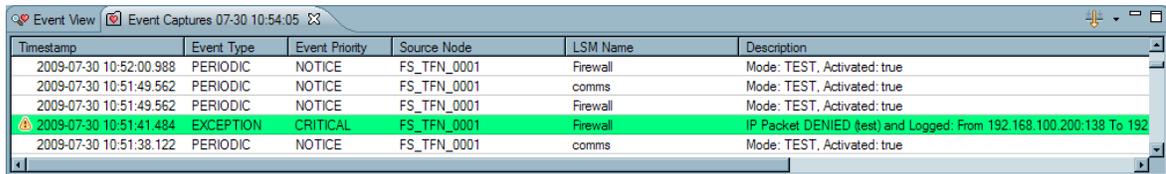
See: [Event View](#)



Timestamp	Event Type	Event Priority	Source Node	LSM Name	Description
2009-07-30 10:42:27.062	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:42:27.062	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true
2009-07-30 10:42:15.694	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:42:15.694	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true
2009-07-30 10:42:07.633	EXCEPTION	CRITICAL	FS_TFN_0001	Firewall	IP Packet DENIED (test) and Logged: From 192.168.100.200.138 To 192
2009-07-30 10:42:04.192	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:42:04.192	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true
2009-07-30 10:41:52.743	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:41:52.743	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true

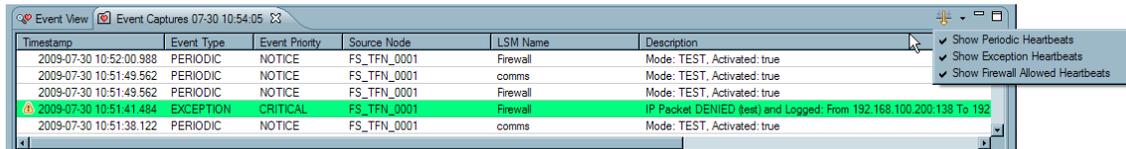


To capture a snapshot from the Events View window, click on the "Event Capture" button on the top right corner of the Event View window, and the current alarms and events in the Event View will be captured in a new screen.



Timestamp	Event Type	Event Priority	Source Node	LSM Name	Description
2009-07-30 10:52:00.988	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true
2009-07-30 10:51:49.562	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:51:49.562	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true
2009-07-30 10:51:41.484	EXCEPTION	CRITICAL	FS_TFN_0001	Firewall	IP Packet DENIED (test) and Logged: From 192.168.100.200.138 To 192
2009-07-30 10:51:38.122	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true

Note: When capturing a view, once the capture has been completed, the user is able to filter that Event Capture using the menu on the top right hand side of the Event View.



Timestamp	Event Type	Event Priority	Source Node	LSM Name	Description
2009-07-30 10:52:00.988	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true
2009-07-30 10:51:49.562	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:51:49.562	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true
2009-07-30 10:51:41.484	EXCEPTION	CRITICAL	FS_TFN_0001	Firewall	IP Packet DENIED (test) and Logged: From 192.168.100.200.138 To 192
2009-07-30 10:51:38.122	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true

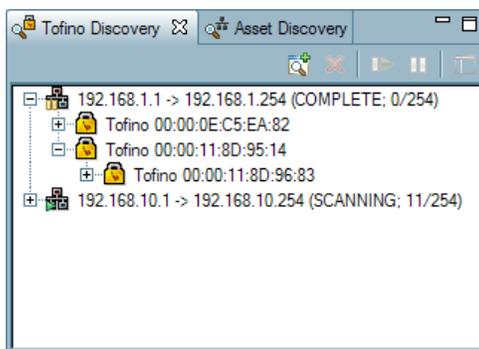
- Show Periodic Heartbeats
- Show Exception Heartbeats
- Show Firewall Allowed Heartbeats

2.3.10 Progress



The Progress window allows the user to see the status of tasks that have been cued on the Tofino CMP. Examples of tasks include updating the Tofino CMP database with new information, generating configurations and updating Tofino SAs in the field.

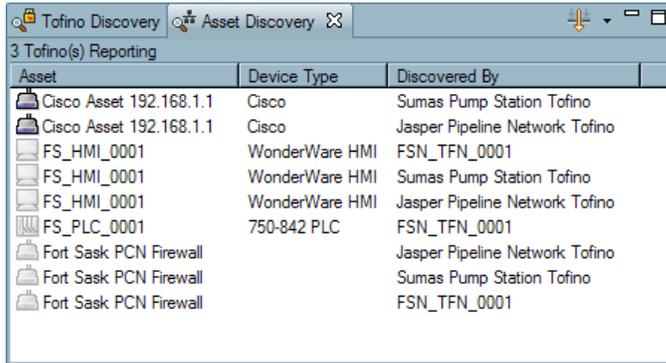
2.3.11 Tofino Discovery



The Tofino Discovery View allows the user to search for new and existing Tofino SAs on their network. By scanning specific IP address ranges, Tofino SAs are discovered and shown in the Tofino Discovery View. These discovered Tofino SAs can then be dragged and dropped into the network diagram in the Network Editor.

See: [Using Tofino Discovery](#)

2.3.12 Asset Discovery



The screenshot shows a window titled 'Tofino Discovery' with a sub-tab 'Asset Discovery'. Below the title bar, it says '3 Tofino(s) Reporting'. The main content is a table with three columns: 'Asset', 'Device Type', and 'Discovered By'. The table lists several discovered assets, including Cisco routers, WonderWare HMI devices, a 750-842 PLC, and Fort Sask PCN Firewalls, each associated with a specific Tofino SA.

Asset	Device Type	Discovered By
Cisco Asset 192.168.1.1	Cisco	Sumas Pump Station Tofino
Cisco Asset 192.168.1.1	Cisco	Jasper Pipeline Network Tofino
FS_HMI_0001	WonderWare HMI	FSN_TFN_0001
FS_HMI_0001	WonderWare HMI	Sumas Pump Station Tofino
FS_HMI_0001	WonderWare HMI	Jasper Pipeline Network Tofino
FS_PLC_0001	750-842 PLC	FSN_TFN_0001
Fort Sask PCN Firewall		Jasper Pipeline Network Tofino
Fort Sask PCN Firewall		Sumas Pump Station Tofino
Fort Sask PCN Firewall		FSN_TFN_0001

The Asset Discovery view shows the assets (nodes) discovered by Tofino SAs on your network. Tofino SAs will only populate the Asset Discovery view if the Secure Asset Management LSM is installed and activated. See: [Adding an LSM to a Tofino SA](#)

Once the Secure Asset Management LSM is activated on a Tofino SA, it will continue to discover new nodes until it is either deactivated or until the Tofino SA it is installed on is put into decommissioned mode. See: [Using Asset Discovery](#)

2.3.13 Go Into Go Back Go Home

These right clicking menu options allow the user to maneuver different views of the network.

[Go Into](#)

[Go Back](#)

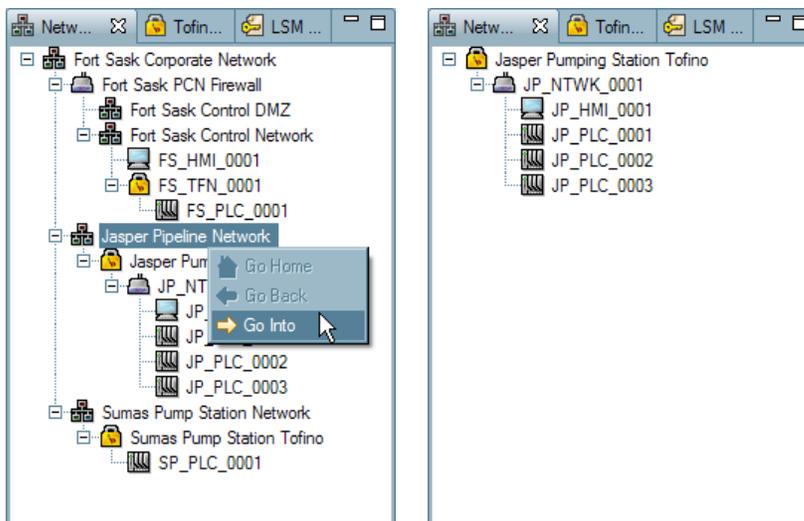
[Go Home](#)

Go Into

This function allows for a more precise view of a branch on a network.

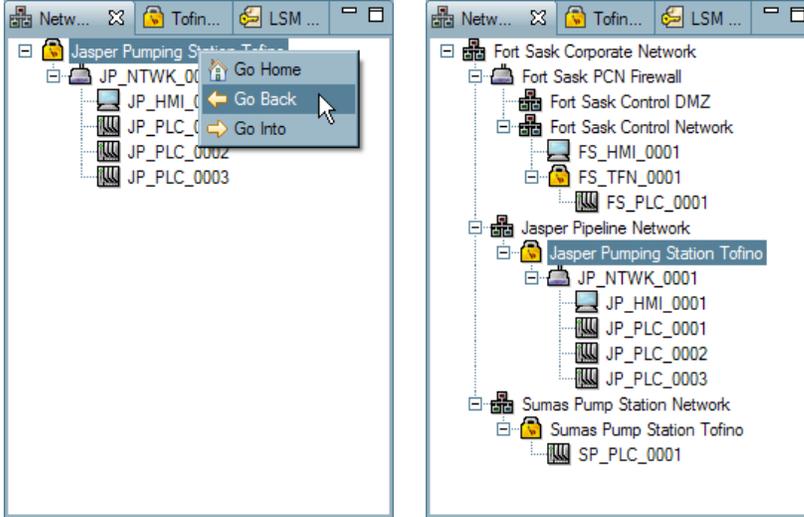
This is done by: right clicking a specific branch in the Network View and selecting "Go Into".

Note: Continue clicking "Go Into", in order to view more specific areas of a network.



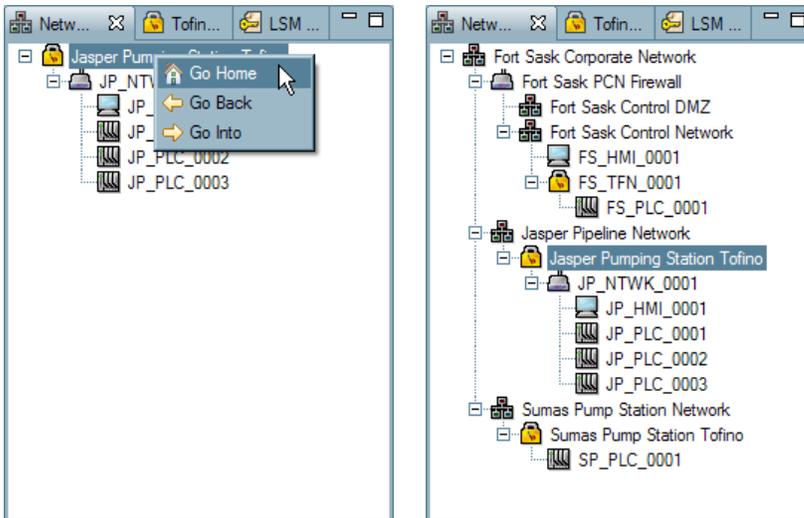
Go Back

Clicking "Go Back" will change the view to the previous view. This is done by: right clicking and selecting "Go Back".



Go Home

Clicking "Go Home" will change the view to show the entire network diagram.



Section 3

Using the Tofino CMP

3 Using the Tofino CMP

3.1 Setting Up Your Tofino CMP

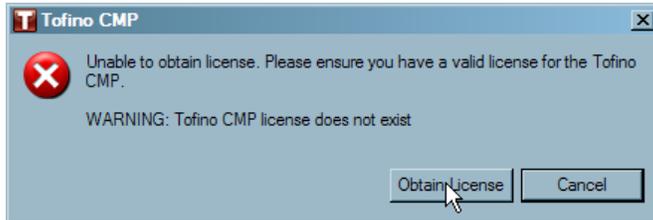
To set up your Tofino CMP for use you must:

- Set up the Tofino CMP license as well as the licenses for the required LSMs. See: [Tofino CMP Licensing](#)
- Define the Database, Heartbeats, Log Settings, and File Locations settings. See: [Tofino CMP Preferences](#)
- Set up the user accounts. See: [User Administration](#)

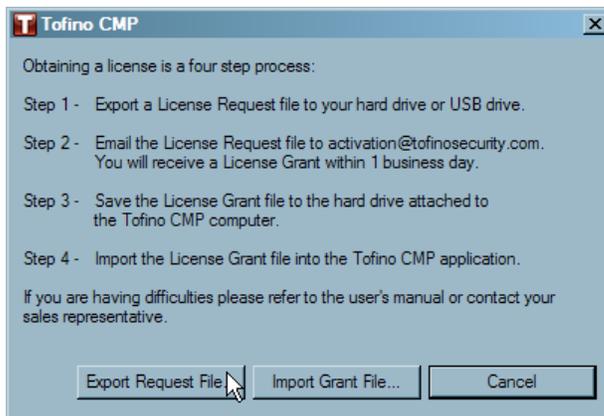
3.1.1 Tofino CMP Licensing

Once the Tofino CMP has been installed on the desired computer, start the program.

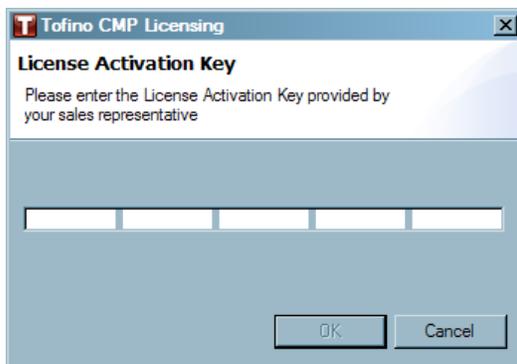
- An error message will appear indicating that the licensing needs to be set-up. Click "Obtain License" in order to proceed (this will allow you to obtain both the Tofino CMP license and LSM licenses you require).



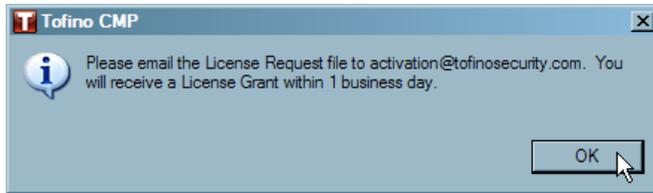
- The next window will list the steps required to obtain licenses. Click "Export Request File"; this will create the License Request file you will send to activation@tofinosecurity.com in order to request and activate your Tofino CMP and LSM licenses. Activation will take 1 business day.



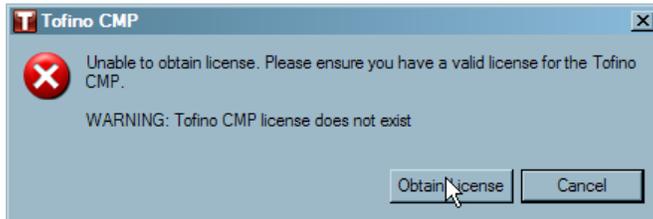
- Next, you will be asked to enter the License Activation Key that is provided to you by your sales representative, then click "OK".



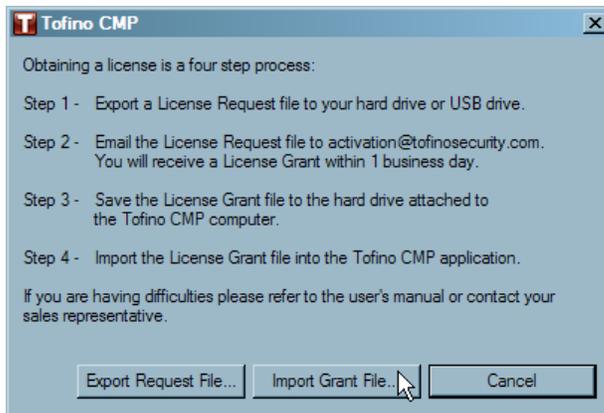
- A "Save As" window will open. Type in a name for the License Request file and then click "Save". Remember that you will need to email this file, so you may want to save it to a USB drive or a server with email access.
- Click "OK" and then shut down the Tofino CMP.



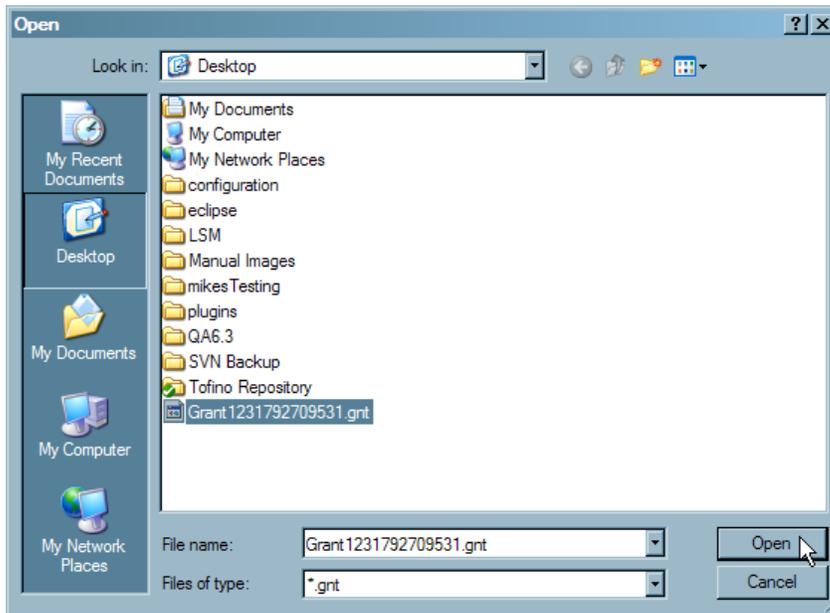
- Now you will need to email the License Request file that you have created to activation@tofinosecurity.com, and the License Grant file will be sent back to you within 1 business days. If you have any questions or concerns, please contact your local sales representative or email activation@tofinosecurity.com.
- Once the License Grant file has been returned to you, save it to a location you will remember and then re-start the Tofino CMP, and click "Obtain License".



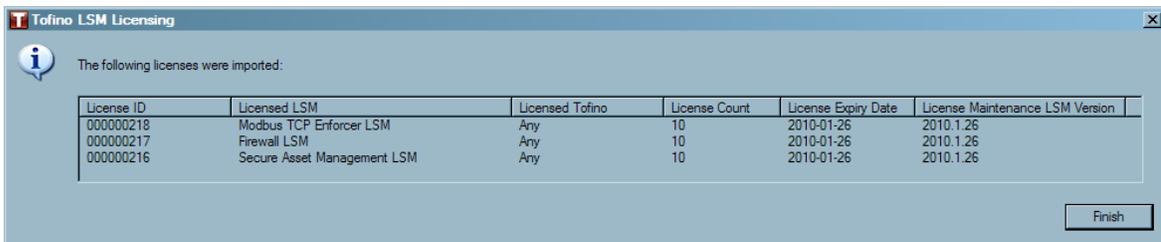
- Next, click "Import Grant File..."



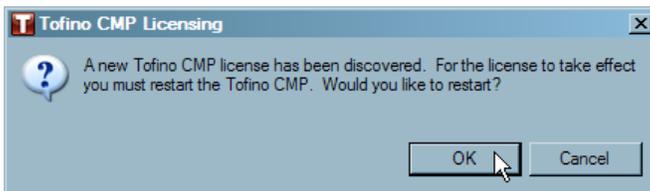
- A window will open. Navigate to where you have saved the License Grant file, click on it, and then click "Open".



- Next you will be shown a window that summarizes the LSM licenses you have been granted. Click "Finish". See also: [LSM Licensing](#)



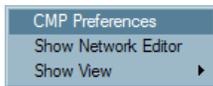
- A window will open explaining that a Tofino CMP license has been discovered and the Tofino CMP needs to be restarted. Click "OK".



- The Tofino CMP will restart, and you will be able to log in. See: [User Administration](#)

3.1.2 Tofino CMP Preferences

Window ► CMP Preferences



The CMP Preferences menus allow you to set or change settings for the Tofino CMP, including the Asset Discovery, CMP General Settings, CMP Log Settings, Database, and Heartbeats.

See: [General](#)

See: [Logs](#)

See: [Asset Discovery](#)

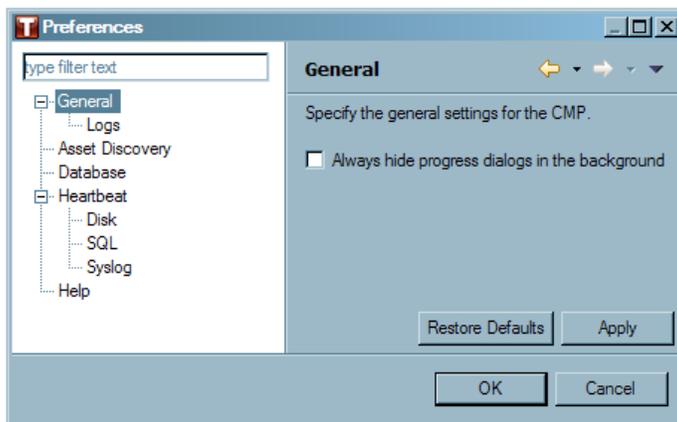
See: [Database](#)

See: [Heartbeat](#)

See: [Disk](#)

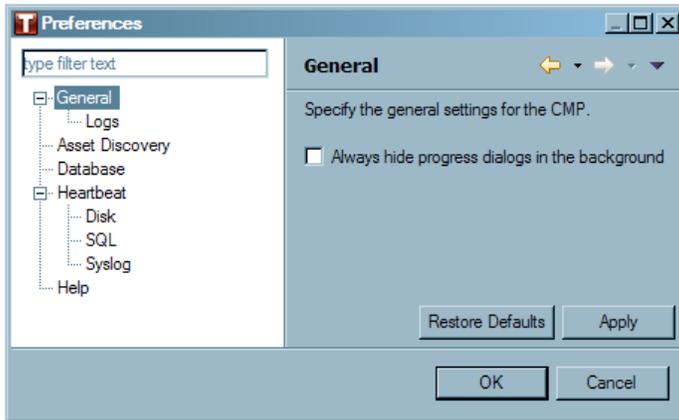
See: [SQL](#)

See: [Syslog](#)

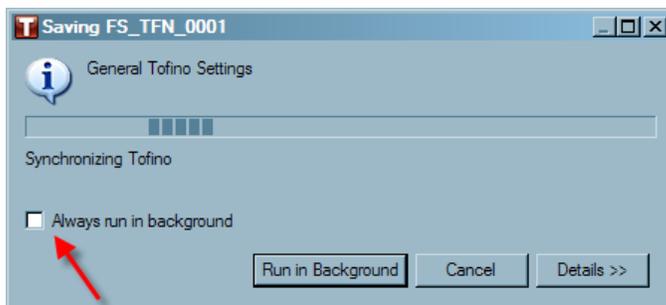


General

This setting allows the user to show or hide the progress dialogs that appear on the Tofino CMP when a change has been made.



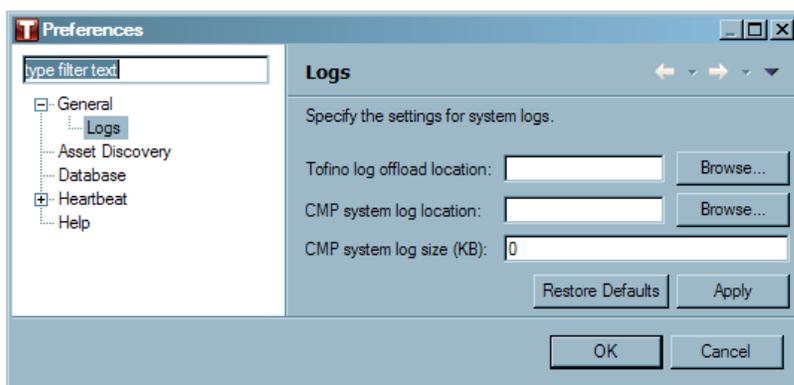
When a change has been made the user can choose to always run dialogs in the background by checking the box "Always run in background".



Logs

Log files are automatically created by the Tofino CMP and each Tofino SA each time important event occurs. There are several types of log files:

- ▶ Tofino SA System and Event Logger Logs: Logs created when either system events (such as a power supply fault) occur or the Event Logger LSM is active.
- ▶ CMP Logs: Logs created when events such as failed login attempts are noted by the Tofino CMP.



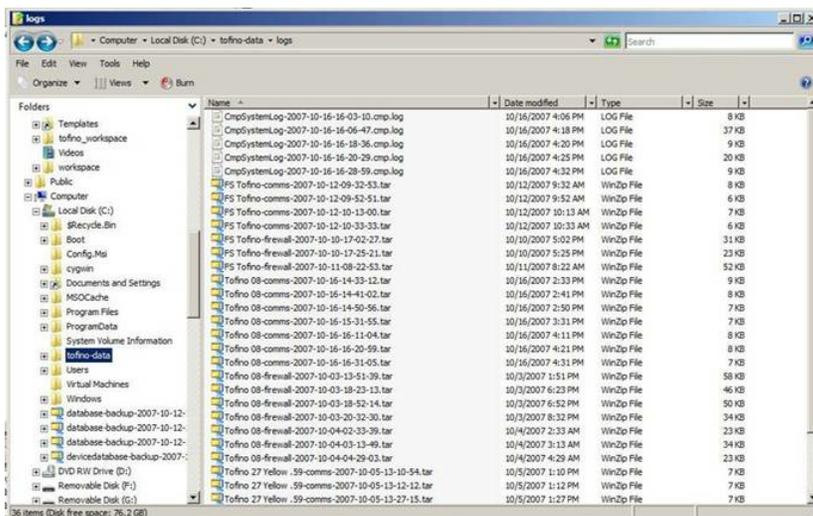
The CMP Log Settings screen allows you to define where the Tofino CMP and Tofino SA Log Files are saved and how big each Tofino CMP log file can be in Kbytes. **Note:** All Tofino SA System and LSM logs are automatically compressed before being sent to the Tofino CMP and thus will not match the Log Size setting. All Tofino CMP generated log files have the following format:

CmpSystemLog-<Time Stamp>.cmp.log

All Tofino SA generated log files have the following format:

<TofinoName>-<LSM Name>-<Time Stamp>.tar

The time stamp is in the format YYYY-MM-DD-HH-MM-SS and is the date and time when the file was first created. Do not rely on this time stamp as an accurate indication of event times. Much more reliable times are included as part of each event record in the file.



To set the log file preferences:

- Select the location where log files will be saved to by clicking "Browse..." The Browse for Folder window will open.
- Navigate to the folder where logs should be stored.
- Double click on the folder or click "OK" to accept.
- Set the maximum CMP Log file size (in Kbytes). **Note:** A value of 0 Kbytes will result in empty log files.
- Click "Apply" or "OK" to save the log file preferences.

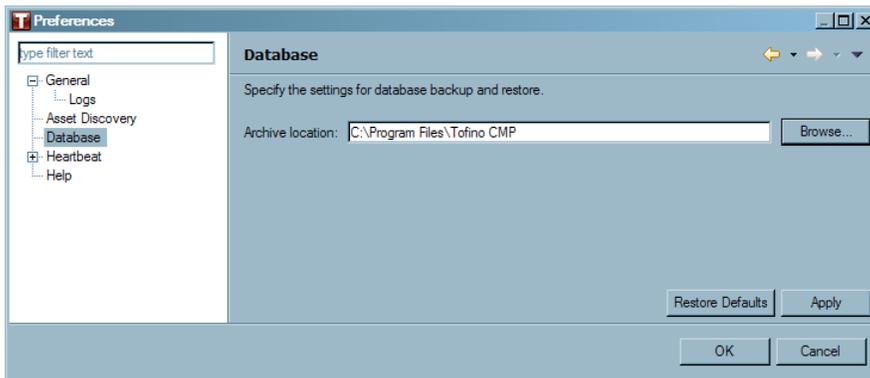
Asset Discovery

By checking this box, an Exception Heartbeat (EHB) will be sent when a new asset is discovered in the Asset Discovery view. If the box is left unchecked, no exception heartbeat will be sent when a new asset is discovered.



Database

The Database preferences window determines the folder for backing up or restoring the Tofino CMP databases. See: [Backing Up and Restoring Databases](#)

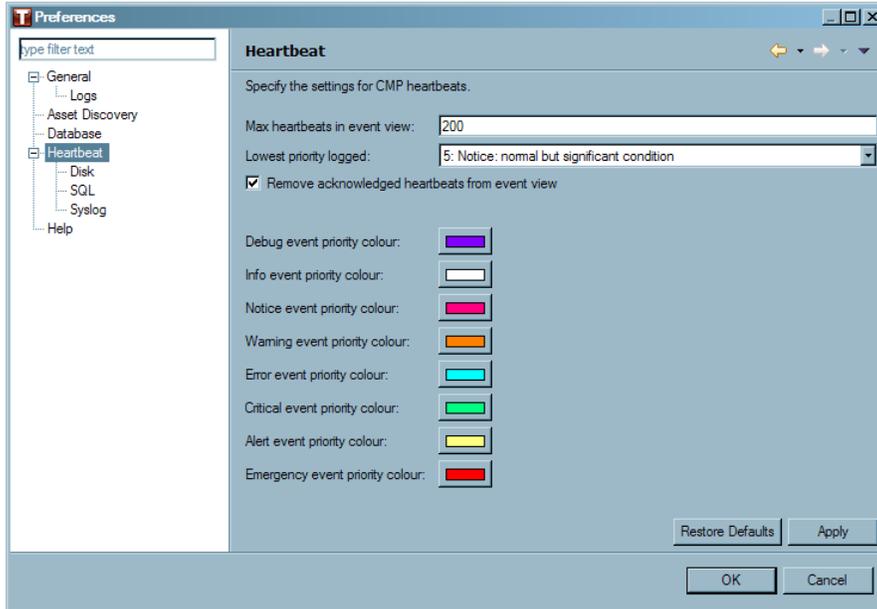


To set the location for storing the archives of the database backups:

- Click the "Browse..." button beside Archive Location field.
- Navigate to the folder where Tofino CMP database backup files should be stored.
- Once an Archive Location folder has been chosen, click "Apply" or "OK" to save the settings.

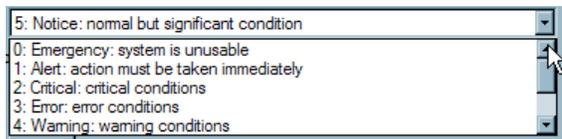
Heartbeat

The Heartbeat preferences window determines the maximum number of heartbeats to be displayed in the Event View. See: [Events, Alarms and Heartbeats](#)

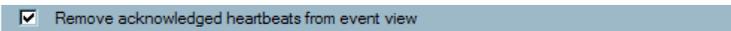


Setting Priority

Set the priority log as needed. This sets which heartbeats will be displayed in the Event View and logged. There are seven levels of priority in order from most important to least important: Emergency, Alert, Critical, Error, Warning, Notice, Informational, and Debug.

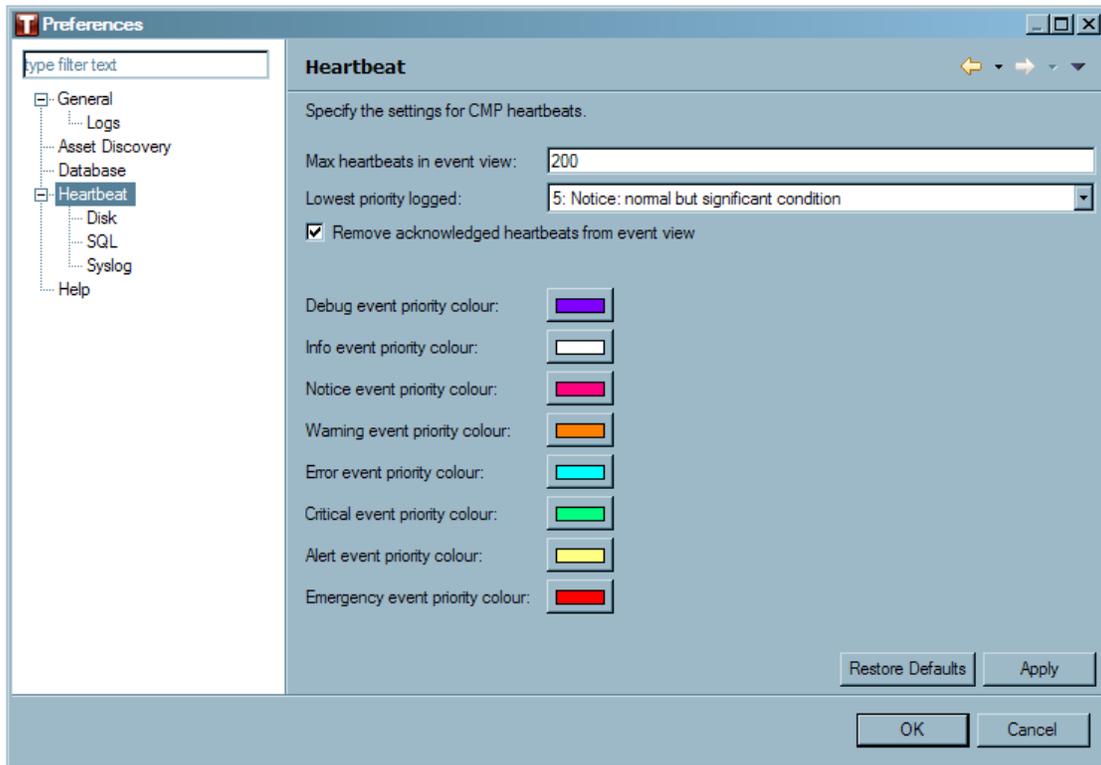


Decide whether acknowledged heartbeats should be removed from the Event View. If yes, tick the box.



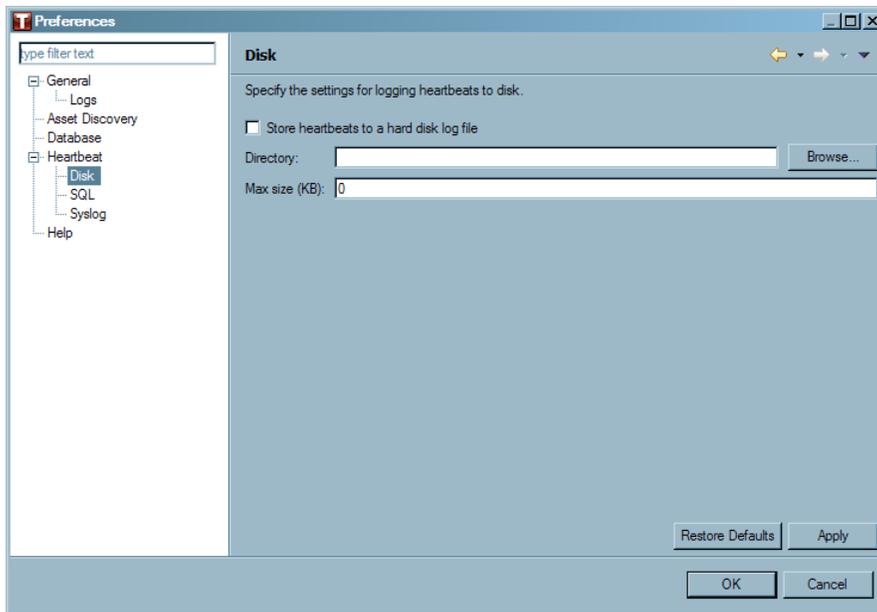
Priority Colours

Each priority can be assigned a colour to help differentiate between the priorities.



Disk

The Disk preferences window determines if the heartbeats will be stored to a hard disk log file.



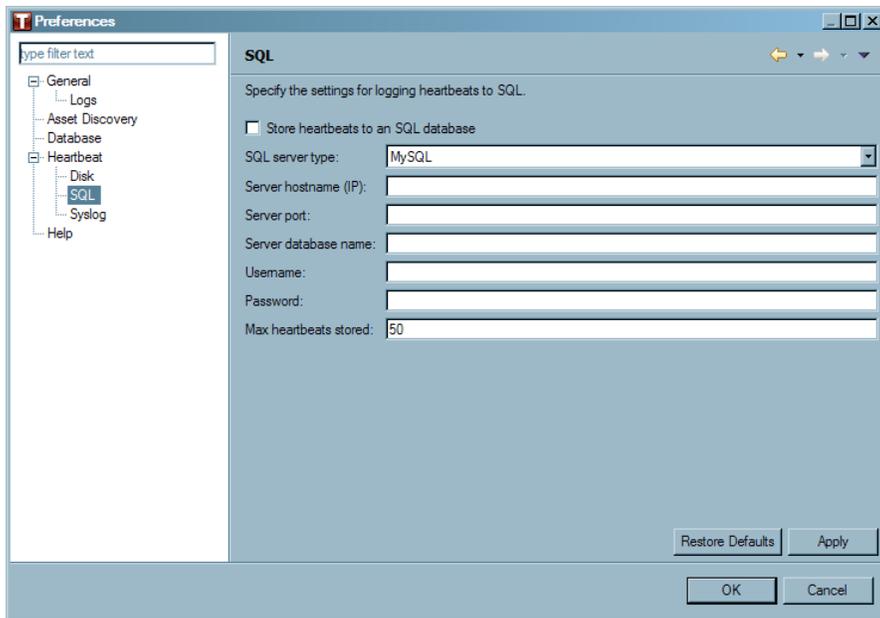
Heartbeat Log (Text) File

If heartbeats should be stored as a text file:

- Check the box beside Store heartbeats to a hard disk log file.
- Select the folder where the Heartbeat log files are to be stored by clicking "Browse..." button. The Browse for Folder window will open.
- Navigate to the folder where the Heartbeat log files are to be stored.
- Double click on the folder or click "OK".
- Set the maximum Heartbeat Log file size (in Kbytes). A value of 0 Kbytes will result in empty log files.
- Click "Apply" or "OK" to save the log file preferences.

SQL

The SQL preferences window determines if the heartbeats will be stored to an SQL database.



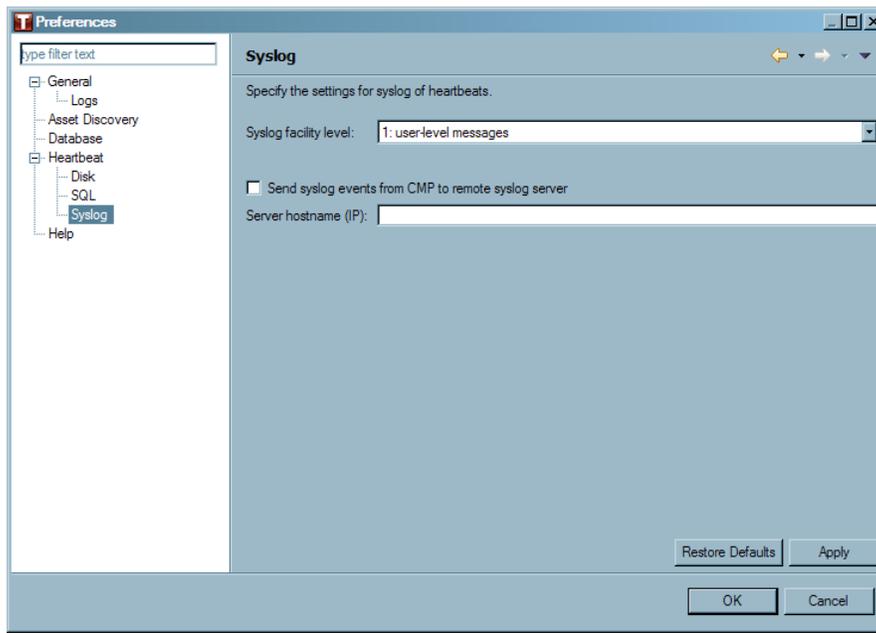
SQL Database

If heartbeats should be stored in an SQL database follow the steps below. The database needs to already exist on your SQL server, but the tables do not need to be defined as the Tofino CMP will automatically create them the first time the connection is made.

- Check the box beside Store heartbeats to an SQL database.
- Select the SQL Server Type. Supported SQL server applications are MySQL and Microsoft SQL
- Enter the IP Address of the SQL server.
- Enter the TCP port number used by the SQL server. For MySQL this is usually 3306 and for Microsoft SQL this is usually 1433.
- Enter the Name of the SQL database that the heartbeats will be stored in.
- Enter the Username of the account needed to log into the SQL server. Make sure that this account has the correct permissions to be able to create the tables needed.
- Enter the Password needed to log into the SQL server.
- Set the maximum number of heartbeats to be stored to the database and the maximum number of heartbeats to be displayed in the **Event View**. See: [Event View](#).

Syslog

The syslog preferences determines whether or not Tofino CMP exception heartbeats will be sent to a remote syslog server. These preference settings also allow you to determine the facility levels of the heartbeat syslog events.



- Set the syslog facility level.
- To enable remote syslogging check the box: "Send syslog events from CMP to remote syslog server".
- Enter the IP address of the remote server.
- Click "Apply" or "OK" to save the log file preferences.

For more information see: <http://en.wikipedia.org/wiki/Syslog>

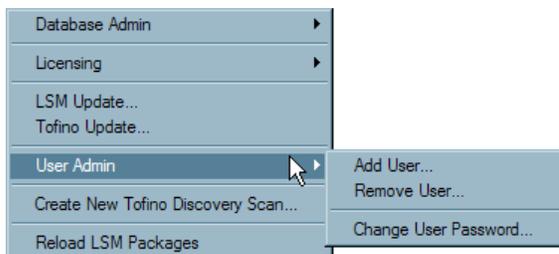
3.1.3 User Administration

The User Administration feature allows you to control who has access to the Tofino CMP. It allows you to create or delete user accounts. All accounts have the same access rights.

When first setting up a Tofino CMP the default username is “admin” and the default password is “password”. The user will be prompted to change the password right away in the opening window.



It is highly recommended that once the user signs into the Tofino CMP for the first time that a new user name and password be created. To do this select **Tools ► UserAdmin ► Add User** See: [Tools Menu](#)



Usenames and passwords are limited to 30 characters. Passwords must be at least 6 characters long. Valid characters are a-z, A-Z, 0-9, “.” (Periods), “_”(Underscores), and “-“ (Dashes).

User administration is accessed through the **Tools ► User Admin** menu. See: [Tools Menu](#)

3.2 Creating Your Network Diagram

The Network Diagram is the heart of your Tofino CMP configuration. It represents the devices and networks in your system, how they are interconnected and where Tofino SAs are located.

There are six types of nodes to consider when creating a network diagram:

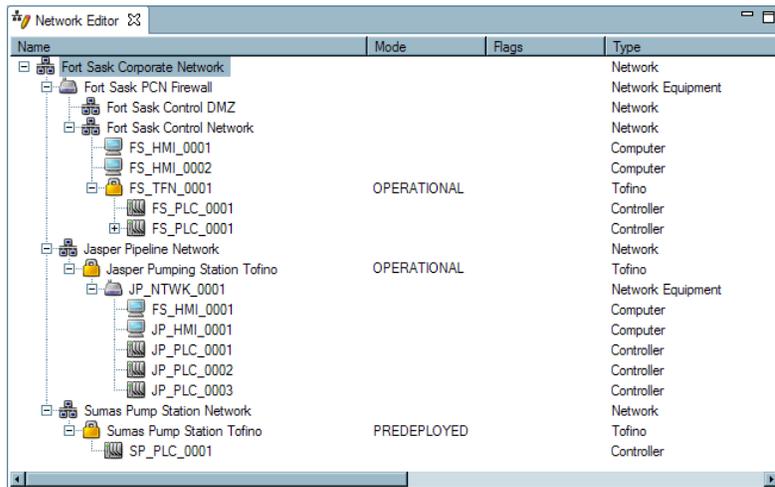
- ▶ Computers: Devices that are based on standard computer hardware such as Human Machine Interfaces (HMIs), programming workstations and servers.
- ▶ Controllers: Devices that provide industrial control functionality such as PLCs, DCS and RTUs.
- ▶ Devices: Miscellaneous industrial devices such as Scales or Bar Code Readers.
- ▶ Networks: Collections of devices that belong on a single network or subnet.
- ▶ Networking Equipment: Communications hardware such as firewalls, routers, switches , gateways and wireless access points.
- ▶ Tofino SAs: Security Appliances that are installed in front of individual and/or clusters of HMI, DCS, PLC or RTU control devices that require protection.

All the node types available for you to work with are displayed in the Nodes window. See: [Nodes](#)

With each node there are a number of attributes that are stored in the Tofino CMP database, such as IP address, node name, and physical location. When a node is added to the network diagram, a wizard will appear that will guide you through entering these attributes.

See: [Creating and Editing a Network](#)

3.2.1 Creating and Editing a Network



There are three ways to create or edit a network.

► Tofino Discovery and Asset Discovery

Tofino Discovery is a feature of the Tofino CMP that discovers configured Tofino SAs on a network and lists them in the Tofino Discovery view, these discovered Tofino SAs can then be dragged and dropped into the Network Editor window.

Asset Discovery uses the Secure Asset Management LSM to discover what "assets" (nodes) are on the network and display them in the Asset Discovery view. The user can then drag these "discovered" nodes into the network diagram in the Network Editor window.

See: [Tofino Discovery](#)

See: [About Asset Discovery](#)

► Drag and Drop Nodes

Allows the user to drag and drop icons from various windows to other windows on the Tofino CMP.

► Right Click Menu

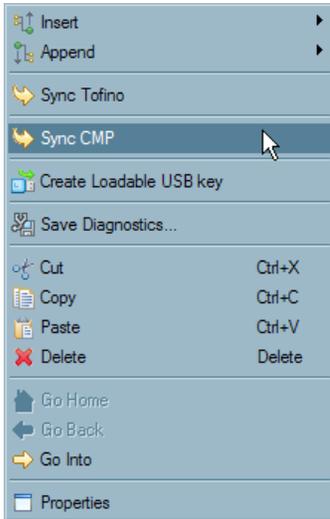
The right click menu allows network nodes to be appended, inserted, cut, copied, pasted, deleted, and edited.

See: [Network Editor Right Click Menus](#)

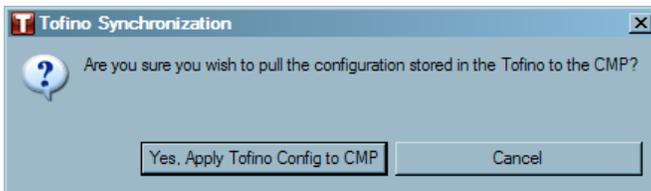
3.2.2 Network ReBuild Wizard

When you use the Sync CMP function, the Tofino SA in the field may have rules in it that reference nodes and devices that are not in the Tofino CMP database. Since it is important that the Tofino CMP database can cross reference all rules to actual devices, the Network Rebuild Wizard may appear to guide you through adding the new nodes to your Tofino CMP database.

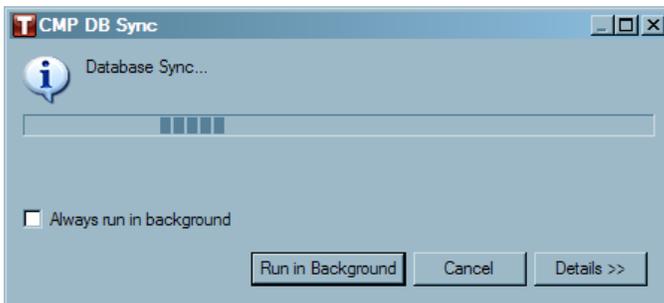
- Right click on the Tofino SA to open the right click menu.
- Select "Sync CMP".



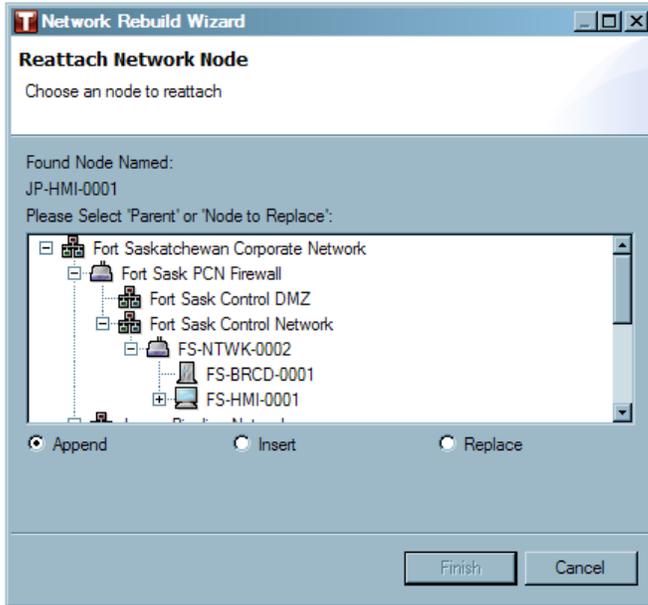
- Select, "Yes, Apply Tofino Config to CMP."



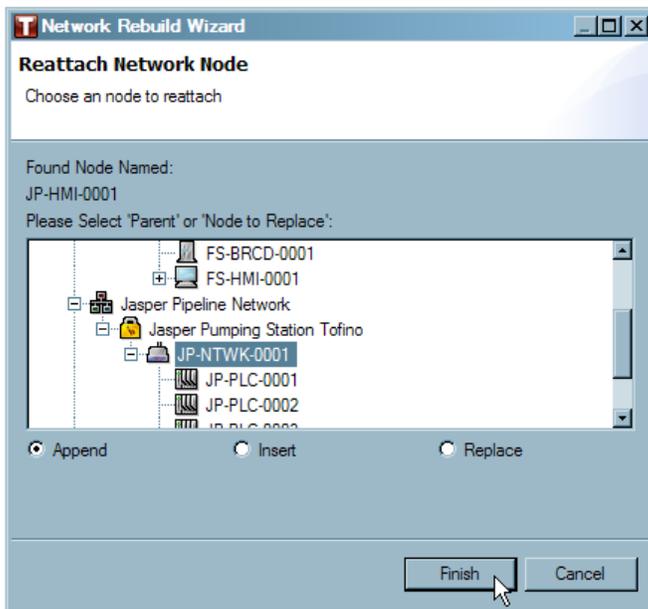
- A window will open while the configurations are completed.



- The Network Rebuild Wizard will appear if node references are found in the Tofino SA that are not in the Tofino CMP database. It will ask you where you wish to place the found node on the network diagram and whether the node should be inserted above the selected node or append below. You can also replace an existing node.



Select the location where you want to place the found node, and click "Finish".



3.2.3 Using Tofino Discovery

Tofino Discovery allows the user to scan a specified portion of a network to find new or existing Tofino SAs. These "discovered" nodes can then be dragged and dropped in the Network Editor window in order to help build a network diagram. The user can create and hold a list of created scans called scan objects in the Tofino Discovery view. These scan objects can be run once or can be set to run continuously, searching for newly added Tofino SAs to the network.

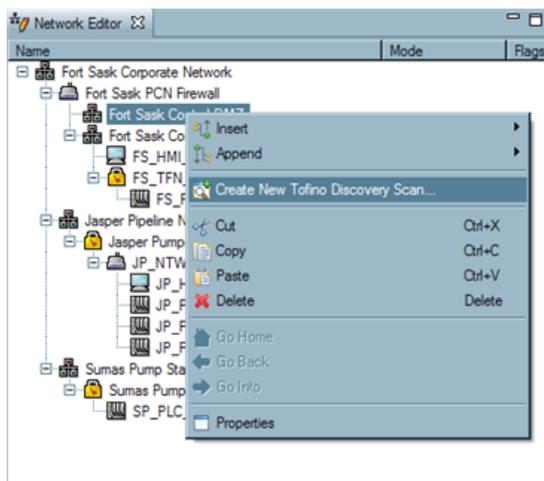
See: [Beginning a Scan](#)

See: [Working With "Scan Objects"](#)

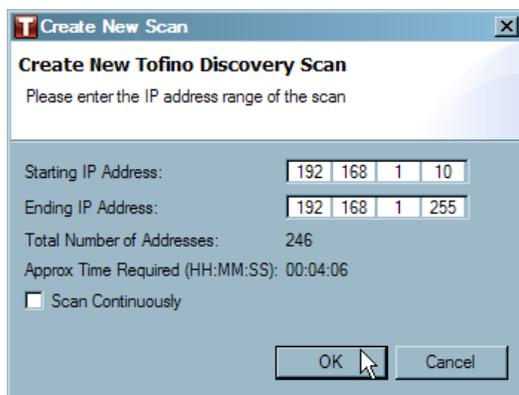
See: [Building Your Network Using Discovered Tofino SAs](#)

Beginning a Scan

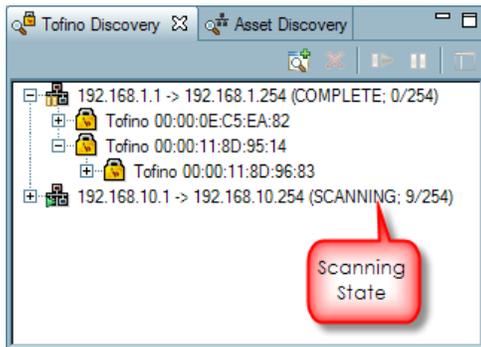
To create a new scan object select **Tools ► Create New Tofino Discovery Scan...** or right click on a network icon in the Network Editor window and select "Create New Tofino Discovery Scan..." With this option the start and end IP addresses will be pre filled in the "Create New Scan" window in the next step.



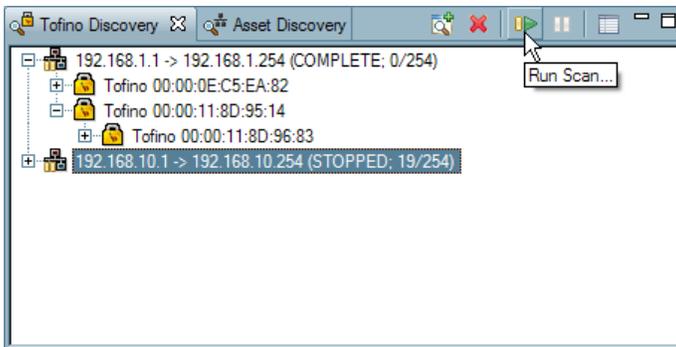
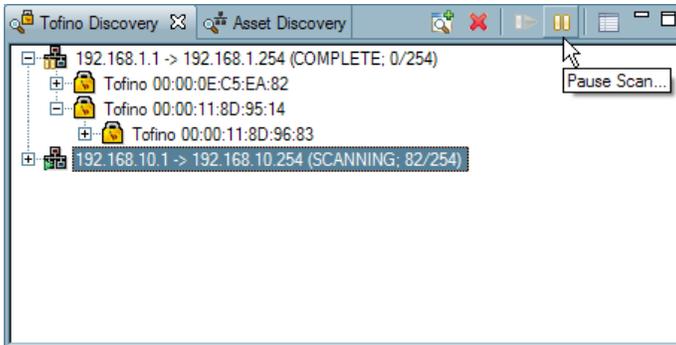
- Fill in the Create New Scan window. **Note:** When setting scan ranges it is helpful to keep them as small as possible as scanning is deliberately slow in order to ensure that the scanning does not impact the process network in any way. Only one scan message is sent each second, so scanning large ranges (i.e. greater than 5000 addresses) may take several hours.
- Enter the starting IP address for the scan (if required).
- Enter the ending IP address for the scan (if required).
- Check the box if you want this scan object to scan continuously.
- Click "OK".



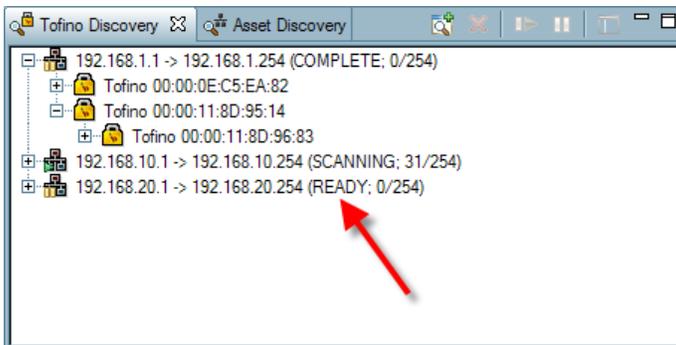
- In the Tofino Discovery view, you will see the scan object you just created displayed with the address range, scan state and number of addresses scanned, out of the total addresses (e. g. 192.168.1.10-> 192.168.1.255 (READY); 0/255). There are five possible scan states:
- ▶ Stopped: the user has disabled this scan from running by clicking the pause button.
 - ▶ Ready: the scan is enabled, but has not yet started as it is waiting for another scan(s) to be completed.
 - ▶ Scanning: the first scan of this address range is in progress.
 - ▶ Complete: the entire address range has been scanned.
 - ▶ Rescanning: the entire address range has been scanned at least once and is being scanned again (the scan continuously box may have been checked).



- If there are no other scan objects in the list currently scanning, your new scan object will begin the scan automatically. This scanning process can be paused and re-started at any time by clicking on the scan object and using the "Pause Scan" and "Run Scan" buttons at the top of the page.



- If there are other scan objects already in progress, the new scan object will be added to the list and will be in the Ready state. The scanning will begin as soon as other scan objects in the list have completed their scans.



Working with "Scan Objects"

See: [Deleting Scan Objects](#)

See: [Continuous Scanning](#)

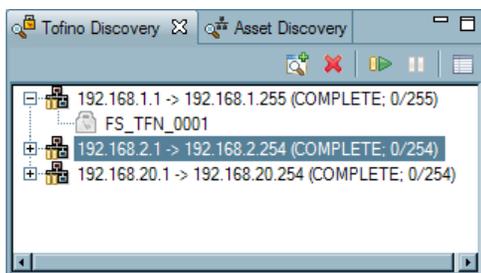
See: [Scan Object Information](#)

Deleting Scan Objects

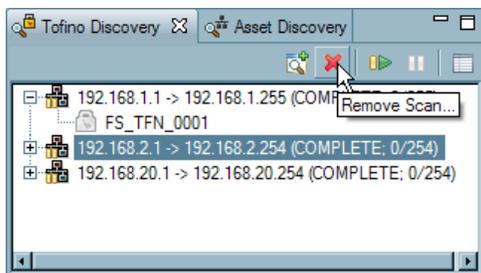
Once a scan object has been entered and is present in the Tofino Discovery view, it will remain there until it is deleted from this view. Also note that Tofino SAs icons can not be individually deleted from the list. The only way to delete Tofino SA icons from the Tofino Discovery view is to delete the scan object they are associated with.

There are three ways to delete a scan object:

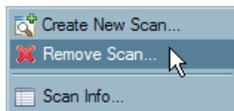
- ▶ Select the scan object to highlight it and then press "Delete" on the keyboard.



- ▶ Select the scan object to highlight it and then click the "Remove Scan" button in the Tofino Discovery view.



- ▶ Right click on the scan object and select "Remove Scan..." from the right click menu.

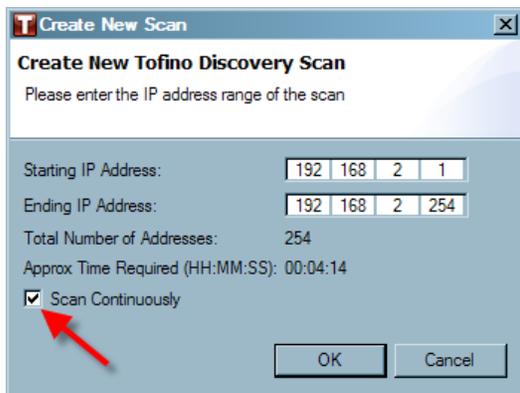


Continuous Scanning

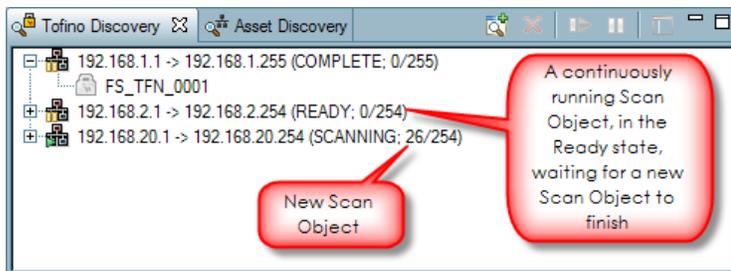
If the Continuous Scanning check box was checked when the scan object was created, the scan object will keep scanning until it is paused or deleted. This is useful for situations when you know a new Tofino SA is being installed on the network but you are uncertain as to the exact time of the installation.

Note: At any time a scan object can be set to scan continuously by checking the "Scan Continuously" box in the Scan Information window and pressing the "Start" button.

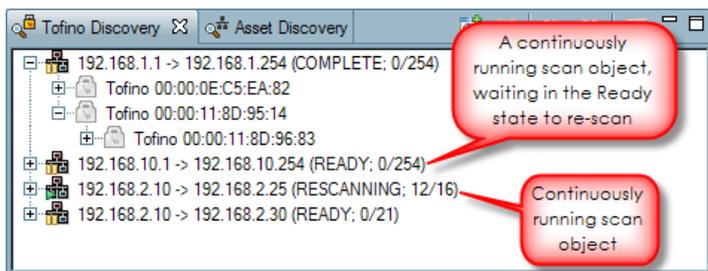
See: [Scan Object Information](#)



Note that a continuously running scan object, at the end of a scan, will pause and wait in a Ready state if a new scan object is created. Once the new scan object has completed a scan, the continuously running scan object will resume scanning.

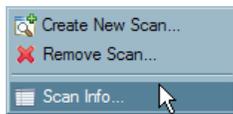


If there are multiple continuously running scan objects they will take turns scanning continuously in the order they were created. If a new scan object is created while multiple scan objects are taking turn running continuously, the continuously running scan objects will pause and sit in the Ready state waiting for the new scan object to complete its scan.

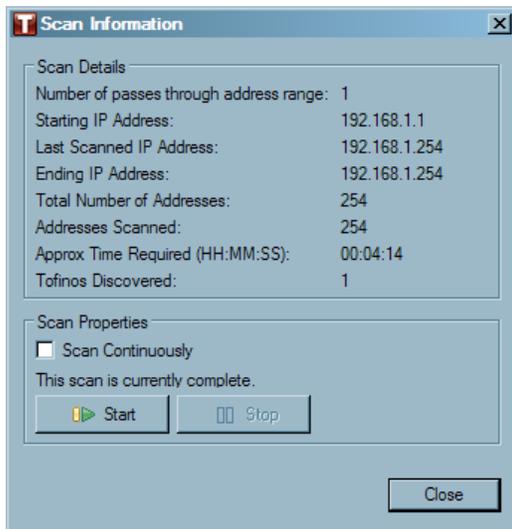


Scan Object Information

To view a scan object's properties, right click on a scan object and select "Scan Info..."



The Scan Info window includes:



Scan Details

- ▶ Number of scans that have been completed
- ▶ Starting IP address of the scan
- ▶ Last scanned IP address
- ▶ Ending IP address of the scan
- ▶ Number of addresses in the scan object
- ▶ Number of addresses scanned
- ▶ The time required to complete this scan (approx)
- ▶ The number of Tofino SAs discovered

Scan Properties

- ▶ 1. A check box that allows the user to make the scan object continuously running. (To start a continuous scan from the Scan Information window, check the Scan Continuously box and then click the "Start" (Run Scan) button on the Scan Information window or in the Tofino Discovery view).
- ▶ 2. The state the scan is currently in: Ready, Stopped, Rescanning, Scanning, or Complete.
- ▶ 3. Buttons that allow the scan object to be started or stopped

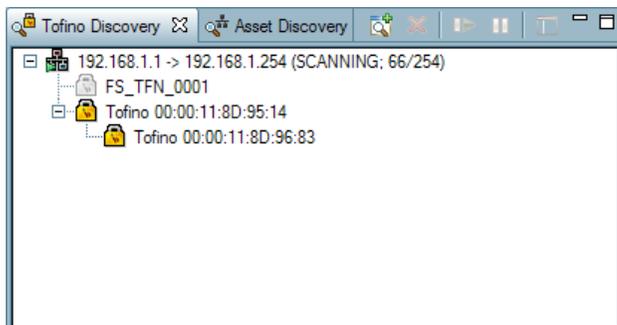
Building Your Network Using Discovered Tofino SAs

See: [Discovered Tofino SAs](#)

See: [Deploying Discovered Tofino SA](#)

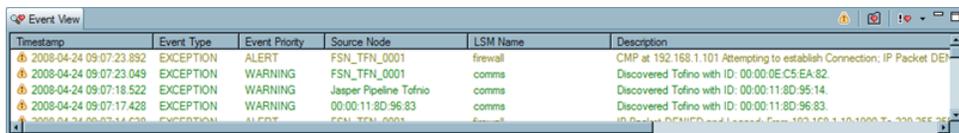
Discovered Tofino SAs

Once a scan object has discovered Tofino SAs, they will be represented in the Tofino Discovery view in a tree format, in the hierarchy of how they were discovered.



When a Tofino SA is discovered on the network, a green exception heartbeat will appear in the Event View.

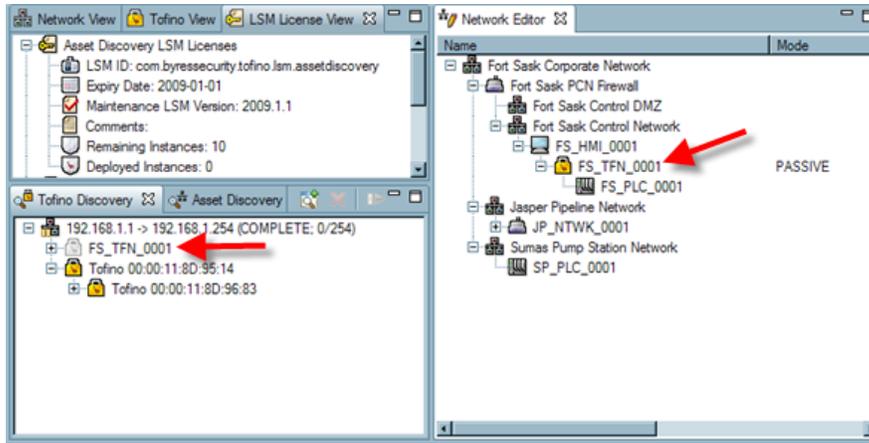
The Source Node indicates the Tofino SA that found the discovered Tofino SAs. The Description of the heartbeat will include the Tofino ID(s) of the discovered Tofino SA(s).



Timestamp	Event Type	Event Priority	Source Node	LSM Name	Description
2008-04-24 09:07:23.892	EXCEPTION	ALERT	FSN_TFN_0001	firewall	CMP at 192.168.1.101 Attempting to establish Connection: IP Packet DE
2008-04-24 09:07:23.049	EXCEPTION	WARNING	FSN_TFN_0001	comms	Discovered Tofino with ID: 00:00:0E:C5:EA:82.
2008-04-24 09:07:18.522	EXCEPTION	WARNING	Jasper Pipeline Tofino	comms	Discovered Tofino with ID: 00:00:11:8D:95:14.
2008-04-24 09:07:17.428	EXCEPTION	WARNING	00:00:11:8D:96:83	comms	Discovered Tofino with ID: 00:00:11:8D:96:83.
2008-04-24 09:07:14.638	EXCEPTION	ALERT	FSN_TFN_0001	firewall	IP Packet ICMP and Layer 4 from 192.168.1.101 to 192.168.1.101

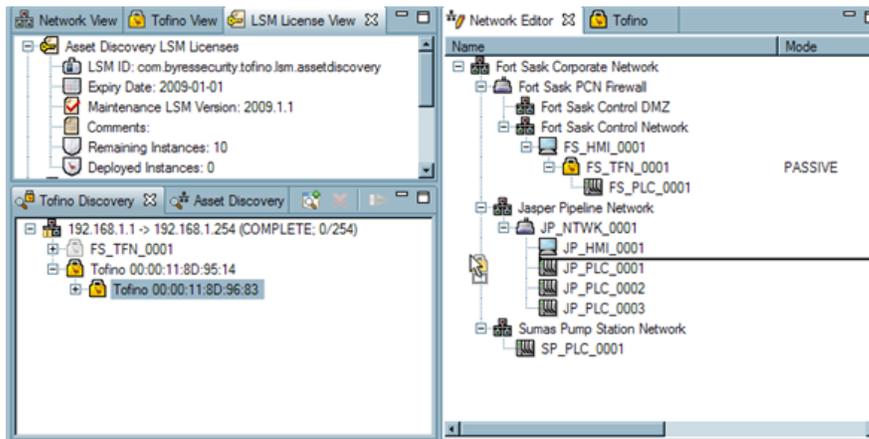
Deploying Discovered Tofino SAs

If a Tofino SA icon in the Tofino Discovery view is already present in the network diagram in the Network Editor, the icon will show up greyed out in the Tofino Discovery view.

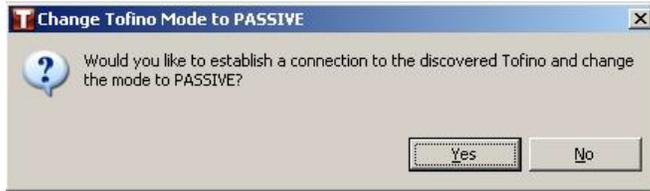


□ If the Tofino SA icon is not in the network diagram, the icon in the Tofino Discovery view will be in colour and will be able to be dragged and dropped into the network diagram in the Network Editor.

Note: If a Tofino SA icon is deleted from the network diagram in the Network Editor the icon will no longer be greyed out in the Tofino Discovery view. It will now be in colour and will be able to be dragged and dropped back into the network diagram.



- Once a Tofino SA icon is dragged from the Tofino Discovery view into the network diagram, a Tofino SA wizard will open to guide the user through the setting the Tofino SA's properties.



- Once the Tofino SA wizard has finished, the user can choose to set the mode of the Tofino SA to PASSIVE immediately by clicking "OK".
- Now the user can start adding LSMs to the Tofino SA. By using the Secure Asset Management LSM the user can discover assets on the network to help build their network diagram. Also, by deploying the Firewall LSM the user would be able to use the Assisted Rule Generation tool to help establish firewall rules for the network.

See: [Adding an LSM to a Tofino SA](#)

See: [About Asset Discovery](#)

See: [Assisted Rule Generation](#)

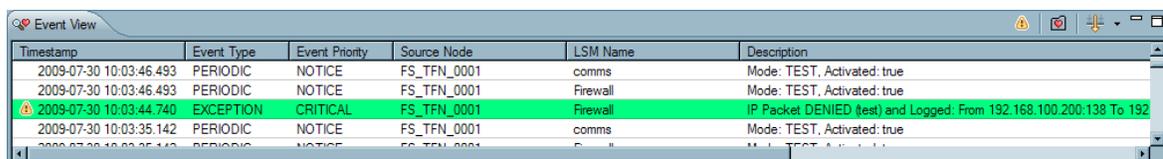
3.3 Events, Alarms, and Heartbeats

Events and alarms generated by the Tofino SAs in the field are known as heartbeats. There are two main types of heartbeats sent to the Tofino CMP:

- ▶ Periodic Heartbeats (PHBs): these are regular reporting messages (heartbeats) from each Tofino SA. The reporting interval is set in the Tofino SA's Properties page.
- ▶ Exception Heartbeats (EHBs): these are messages that have been generated because a specific event has occurred such as a packet being blocked by the Firewall LSM. If the Secure Asset Management LSM and the Firewall LSM are activated, then exception heartbeats can be used to create firewall rules using the [Assisted Rule Generation feature](#).

Events and alarms can also be generated locally by the Tofino CMP itself for occurrences such as a Tofino SA going missing or a failed log in attempt.

Alarms and Events are viewed through the [Event View](#) window. They also can be stored to either an SQL database or as a text log file based on the settings in the Tofino [CMP Preferences](#)



Timestamp	Event Type	Event Priority	Source Node	LSM Name	Description
2009-07-30 10:03:46.493	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:03:46.493	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true
2009-07-30 10:03:44.740	EXCEPTION	CRITICAL	FS_TFN_0001	Firewall	IP Packet DENIED (test) and Logged: From 192.168.100.200:138 To 192
2009-07-30 10:03:35.142	PERIODIC	NOTICE	FS_TFN_0001	comms	Mode: TEST, Activated: true
2009-07-30 10:03:35.142	PERIODIC	NOTICE	FS_TFN_0001	Firewall	Mode: TEST, Activated: true

Settings for controlling heartbeat generation, display and storage are found in two locations:

[Tofino CMP Preferences](#): Contains settings for where heartbeat records are stored and the priority level for storing a heartbeat.

Properties: The reporting interval for the periodic heartbeats from each Tofino SA are set on that Tofino SAs properties page.

Events can also be recorded and either saved locally on the Tofino SA or sent directly to a syslog server using the Event Logger LSM. See: [Using Event Logger LSM](#)

3.4 Backing up and Restoring Databases

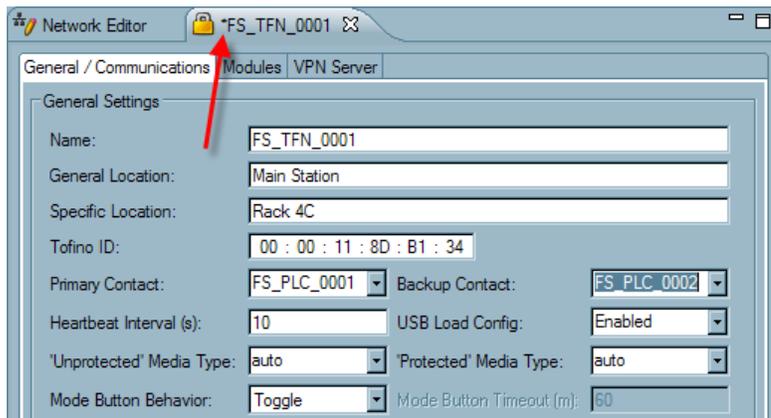
There are two main databases for every Tofino CMP installation:

- ▶ Tofino CMP Database: Information on the current network diagram and node configurations. See: [Creating Your Network Diagram](#)
- ▶ Tofino Device Database: The device database contains all the node types that can be used to create a network diagram. See: [Nodes](#)

Details on how to back up and restore these databases can be found at [Tools](#) ▶ [Database Admin Menu](#).

In addition, there are two secondary databases that are supplied by Byres Security Inc. and are not editable. These are the Protocols database and the Special Rules database. For details on how to import new Protocols or Special Rules see: [Protocols](#) or [Special Rules](#)

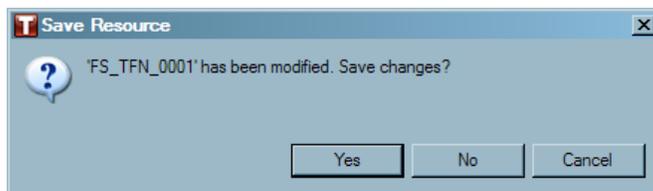
3.5 Saving Changes



When changes are made to any page open in the Network Editor, a star* will appear on the tab.

There are four ways to save changes made:

- ▶ Select **File** ▶ **Save**.
- ▶ Press "Ctrl + S".
- ▶ Click "Apply".
- ▶ Click "OK".
- ▶ Or close the tab and click "Yes" on the window that opens when the tab is closed.



Section 4

Working with Your Tofino SA

4 Working with Your Tofino SA

4.1 Tofino SA (100 and 220 Series) Modes

See: [Modes Explained](#)

See: [Changing Modes Using the Tofino CMP](#)

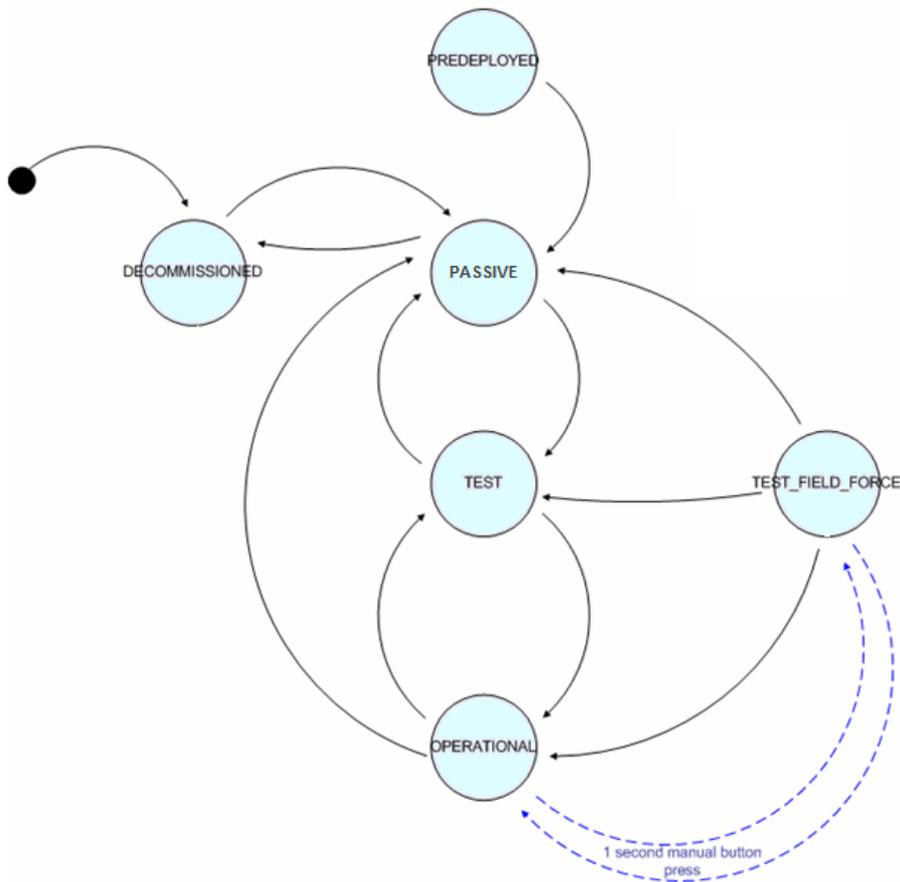
See: [Mode Button Behaviour](#)

Modes Explained

Tofino SAs can operate in one of the modes shown in the table below.

Mode	Description
PREDEPLOYED	The Tofino SA is either a virtual Tofino SA on a Tofino CMP screen (used to allow an engineer to configure the device offline, say before the plant is built) or a virgin Tofino in the field that has never been paired to by a Tofino CMP. LSMs can be virtually added, activated and configured in the Tofino CMP, but this information is not pushed out to the Tofino SA until the mode is changed to PASSIVE.
PASSIVE	A Tofino SA that has been installed and communicated to at least once by a Tofino CMP, but has not been requested to process traffic. It listens for commands so LSMs can be loaded and configured, but does not impact the network traffic in anyway.
TEST	The Tofino SA is fully operational, processes all traffic but will not drop any messages. This is used to test if a Tofino SA is correctly configured before it is used to filter control system traffic.
TEST FIELD FORCE	Same as TEST, but driven by the field. (Available only on the Tofino 100 SA)
OPERATIONAL	Provides full packet processing and protection.
DECOMMISSIONED	Has all its LSM turned off and is only listening for commands.

Note: Modes available on the pull-down menu on the Tofino CMP depend on the current mode the Tofino SA is in. Modes must be moved through progressively working towards OPERATIONAL. See the diagram below.



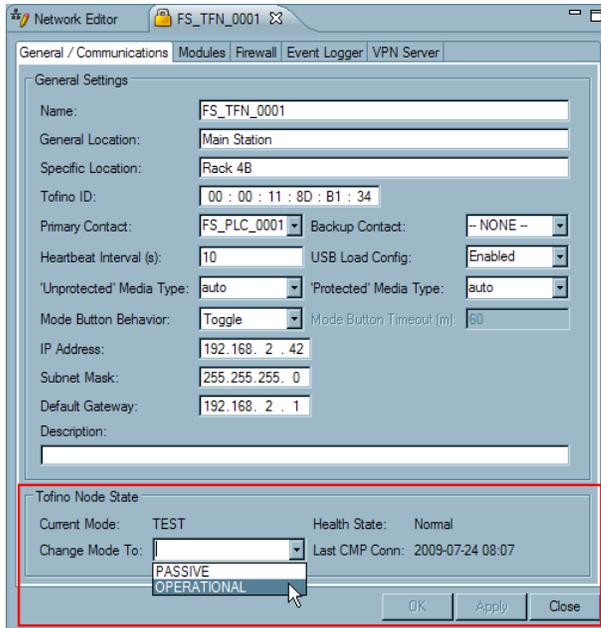
Tofino SA Mode Diagram .

Note: All mode transitions are a cause of Tofino CMP operator actions, except for the transitions highlighted in blue. Technicians can cause blue transitions by pressing the Mode button on the Tofino SA for 1 second.

Changing Modes Using the Tofino CMP

To change the mode of a Tofino SA from the Tofino CMP, double click the appropriate Tofino SA icon in the Network Editor window.

At the bottom of the General/Communications tab is a section labeled: Tofino Node State. Here the current mode and the health state can be seen.

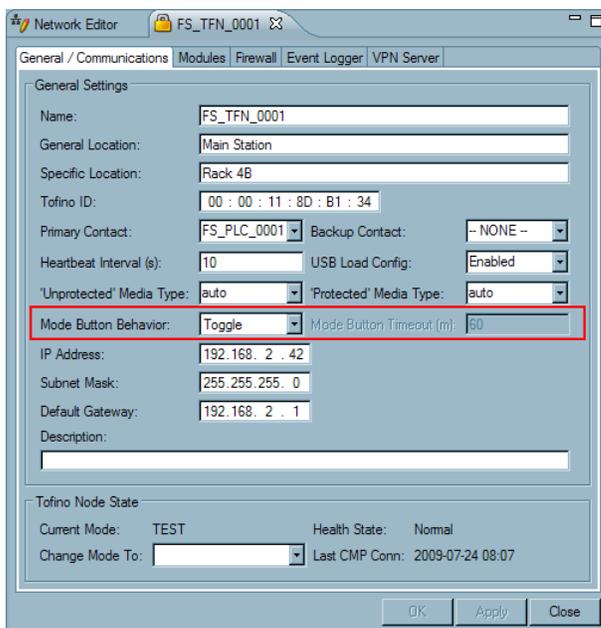


Select the mode of choice from the pull-down menu and click "Apply" to apply the changes and keep the tab open. Or click "OK" to apply the changes and close the tab.

Mode Button Behaviour

The Mode button on the Tofino 100 SA can be set to function in 3 different ways: [Toggle](#), [Disabled](#), and [Timed](#). (Available only on the Tofino 100 SA) The default setting is Toggle. The Mode button behaviour is controlled using the Tofino CMP, from the Tofino SA's General/Communications tab. **Note:** To get to the General/Communications tab, double click on a Tofino SA icon in the Network Editor.

Note: The Mode button is inactive for the first 30 seconds after a Tofino SA is powered up.



Toggle

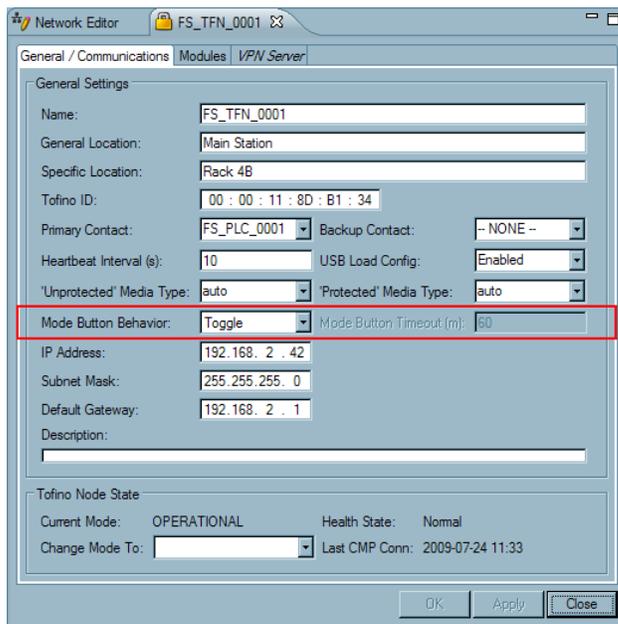
When the Mode Button Behaviour is set to Toggle, the mode button on the Tofino Security Appliance allows field technicians to toggle between OPERATIONAL mode and TEST-FIELD-FORCE mode.

TEST-FIELD-FORCE mode temporarily disables all protection features from the Tofino SA and is useful for troubleshooting firewall configurations. To switch modes using the Mode button:

- Press and hold the Mode button for 1 second while it is in OPERATIONAL mode to change the Tofino SA to TEST-FIELD-FORCE mode. The Mode LED will change to Long Flashing when you remove your finger.
- Press and hold the Mode button for 1 second while it is in TEST-FIELD-FORCE mode to change the Tofino SA to OPERATIONAL mode. The Mode LED will change to Solid ON when you remove your finger.

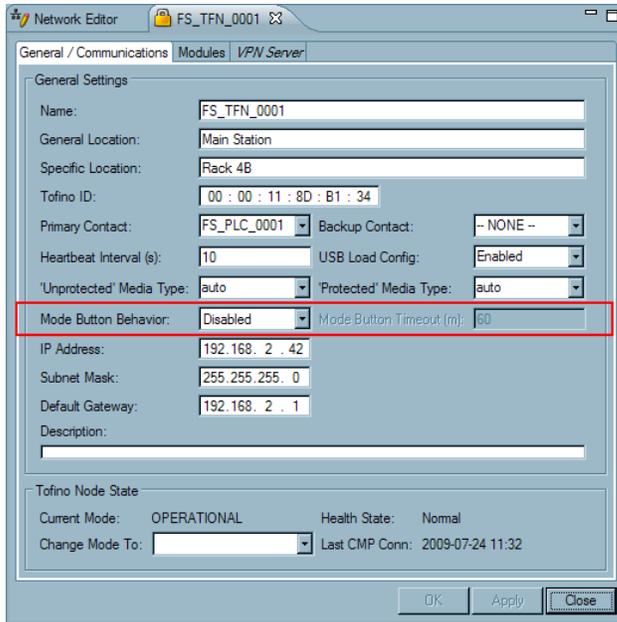
If the Tofino SA is not in either OPERATIONAL or TEST-FIELD-FORCE mode then the button has no effect.

Please also note that once a Toggle has been performed to move to either OPERATIONAL or TEST-FIELD-FORCE the field technician must wait for up to 30 seconds before toggling again to move back to another mode.



Disabled

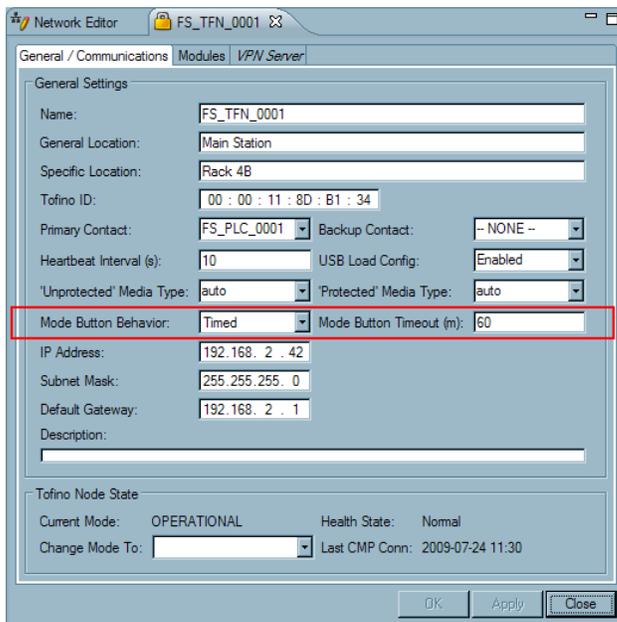
When the Mode Button Behaviour is set to Disabled, the mode button on the Tofino Security Appliance will not change modes (factory resets are still possible).



Timed

When the Mode Button Behaviour is set to Timed, field technicians can change the Tofino SA from OPERATIONAL mode to TEST-FIELD-FORCE mode with a set amount of time before the mode automatically reverts back to OPERATIONAL mode. The amount of time (in minutes) is specified in the Mode Button Timeout field; the default is 60 minutes.

To activate the Timed feature, press and hold the Mode button for 1 second while it is in OPERATIONAL mode to change the Tofino SA to FIELD-FORCE TEST mode. The Mode LED will change to Long Flashing when you remove your finger. Once the set amount of time is up, the Tofino SA will automatically revert to OPERATIONAL mode; the Mode LED will change back to Solid ON.



4.2 Editing the Properties of a Tofino 100 or 220 SA

There are two tabs on the Tofino SA's properties page:

[General/Communication Modules](#)

As well, any LSMs that are installed on the Tofino SA will also have tabs. For details on these tabs see the specific LSM section. See: [How LSM Tabs Work](#)

General/Communications Tab

The screenshot shows a 'Network Editor' window with the 'General / Communications' tab selected. The 'General Settings' section contains the following fields and values:

- Name: Jasper Pumping Station Tofino
- General Location: Main Station
- Specific Location: Rack 4C
- Tofino ID: 00 : 80 : 63 : 78 : 2C : C6
- Primary Contact: JP_PLC_0002
- Backup Contact: JP_PLC_0003
- Heartbeat Interval (s): 10
- USB Load Config: Enabled
- 'Unprotected' Media Type: auto
- 'Protected' Media Type: auto
- Mode Button Behavior: Toggle
- IP Address: 192.168.2.42
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.167.2.1
- Description: (empty text box)

The 'Tofino Node State' section shows:

- Current Mode: TEST
- Health State: Normal
- Change Mode To: (dropdown menu)
- Last CMP Conn: (empty text box)

Buttons for 'OK', 'Apply', and 'Close' are located at the bottom of the window.

- ▶ Name: Insert a name or identifier that uniquely identifies the Tofino SA. (i.e. Jasper Pump Station Tofino or JP-TFN-001). It is important that it is meaningful to the staff in your facility. Remember that each Tofino SA needs to have a unique name to avoid confusion.
- ▶ General Location: For reference only.
- ▶ Specific Location: For reference only.
- ▶ Tofino ID: Enter the ID number from the lower front of the Tofino 100 SA's face or on the right side of the Tofino 220 SA's face
- ▶ Primary Contact/Backup Contact: To help the Tofino CMP locate Tofino SAs in the field and direct TCP/IP messages to them, the system uses the concept of contact devices. These are the devices that are on the other side of the Tofino SA from the Tofino CMP (typically this is the trusted interface of the Tofino SA). For every Tofino SA you may specify two contact devices, a Primary Contact and a Backup Contact. See: [Tofino SA Contact Devices](#)
- ▶ Heartbeat Interval: This number indicates the number of seconds between periodic heartbeats coming from this Tofino SA. It also sets the syslog heartbeat interval if the Event Logger LSM is installed. These heartbeats give regular status updates of the Tofino SAs listed in the network. Setting the heartbeat value to a low number provides more rapid updates of the Tofino CMP but generates more network traffic. Note: If heartbeats are set to 0, this shuts the periodic heartbeats off. The default setting is 10 seconds.

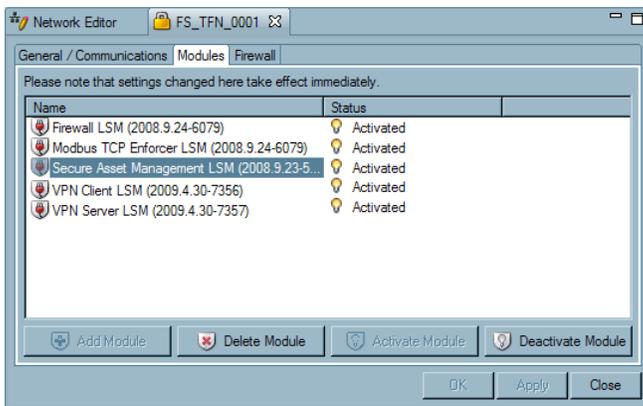
- ▶ **USB Load Config:** If this option is set to Enabled, configurations can be loaded from a USB flash drive to the Tofino SA and Tofino SA log files can be saved to the flash drive. If this option is set to Disabled, the USB ports cannot be used.
- ▶ **Unprotected Media Type:** This sets the interface settings on the upper or Untrusted Ethernet port. The Tofino SA supports auto-negotiation of both Ethernet ports. Auto-negotiation means the Tofino SA's connection and transmission parameters are negotiated automatically with the switch or device it is attached to. Depending on the media type, the Ethernet ports can also be manually set to:
 - ▶ Auto
 - ▶ 100base TX-HD
 - ▶ 100base TX-FD
 - ▶ 10base T-HD
 - ▶ 10base T-FD
 - ▶ 100baseFX-HD
 - ▶ 100baseFX-FD
- ▶ **Protected Media Type:** This sets the interface settings on the lower or trusted Ethernet port. The Tofino SA supports auto-negotiation of both Ethernet ports. Auto-negotiation means the Tofino SA's connection and transmission parameters are negotiated automatically with the switch or device it is attached to. Depending on the media type, the Ethernet ports can also be manually set to:
 - ▶ Auto
 - ▶ 100base TX-HD
 - ▶ 100base TX-FD
 - ▶ 10base T-HD
 - ▶ 10base T-FD
 - ▶ 100baseFX-HD
 - ▶ 100baseFX-FD
- ▶ **Mode Button Behaviour:** Allows the user to set the behaviour of the Mode button on the Tofino SA, there are 3 possible functions: Toggle, Disabled, and Timed. (Available only on the Tofino 100 SA)
- ▶ **Mode Button Timeout (m):** This field will remain grayed out unless the Mode Button Behaviour is set to Timed. If the behaviour is set to Timed, this field will allow the user to enter an amount of time, in minutes, that the Tofino SA will remain in TEST-FIELD-FORCE before reverting back to OPERATIONAL mode once the technician in the field presses the Mode button. (Available only on the Tofino 100 SA)
- ▶ The next three fields only need to be set when using LSMs that specifically require the Tofino SA to have a unique IP address, such as the VPN LSM and Event Logger LSM using TCP or TLS. If they are left blank the Tofino CMP will use the IP addresses of the contact devices to communicate to the Tofino SA.
 - ▶ **IP Address:** The IP address of the Tofino SA (optional except for specific LSMs).
 - ▶ **Subnet Mask:** The subnet mask for the IP address of the Tofino SA (optional except for specific LSMs)
 - ▶ **Default Gateway:** The default gateway for the Tofino SA (optional except for specific LSMs)
- ▶ **Link State Pass Through:** Allows the Tofino SA to pass the link state on one interface to the other interface for redundancy systems. For example, if Link State Pass Through is enabled, and the untrusted interface detects that the network connection is down, it will disable the trusted interface on the Tofino SA. (Available only on the Tofino 100 SA)

- ▶ Description: This information is optional, and may be used to describe the function of this Tofino SA.
- ▶ Change Mode to: This is where a Tofino SA's mode can be changed.
- ▶ Health State: Is either Normal or Missing. Normal indicates the Tofino SA is communicating normally. Missing indicates the Tofino CMP has not received two or more expected heartbeats from this Tofino SA.

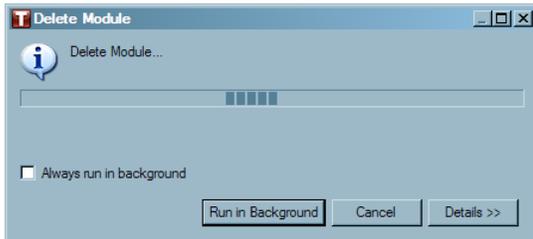
Modules Window (Adding/Deleting/Activating/Deactivating LSMs)

The Modules window displays LSMs that have been added to a Tofino SA. Here LSMs can be viewed, added, deleted, activated, or deactivated.

- Click on the LSM to be edited. Next, click on the button at the bottom of the page to add, delete, activate, or deactivate.



- When any changes are made, a progress dialog will open while the changes are completed.



4.3 Tofino SA Contact Devices

Is it true that the Tofino SA does not have an IP address?

Yes this is true. It is important to understand that a Tofino SA does not have an IP address when it is first installed. This makes it very simple to install in the field. Technicians can simply mount it on a DIN-rail, attach power and plug in the network cables.

Note: The Tofino SA can optionally be assigned an IP address, but this only needs to be done when using the VPN or Event Logger LSMs. See: [Assigning an IP Address to Your Tofino](#)

If the Tofino SA does not have an IP address, then how does it work?

The Tofino SA uses a patent-pending technology to learn the IP addresses of the devices that it will be protecting and then “borrows” those for its configuration and event messages. This does not impact the devices being protected in any way, but it makes the Tofino SA almost impossible for hackers to detect.

How does the Tofino CMP identify which Tofino SA is which?

When there are several Tofino SAs installed, the Tofino CMP determines which Tofino SA is which by taking advantage of a unique serial number that is burned into the hardware. If a Tofino SA sees a Tofino CMP message that contains a serial number it doesn't recognize, it simply forwards the message onto the next Tofino SA in line. Typically the message will get to the correct Tofino SA in one or two forwarding hops.

What are contact devices?

To help the Tofino CMP locate Tofino SAs in the field and direct TCP/IP messages to them, the system uses the concept of contact devices. These are the devices that are on the other side of the Tofino SA from the Tofino CMP (typically this is the trusted interface of the Tofino SA).

How are contact devices determined?

Contact devices are determined in two ways:

- ▶ If you use Tofino Discovery then the Tofino CMP will determine a contact device known as the Tofino Discovery (TD) Contact.
- ▶ Alternatively, you can manually specify two contact devices, a Primary Contact and a Backup Contact on the properties page of the Tofino SA icon. At least one of these three must be configured before the Tofino SA and Tofino CMP will initiate communications.

Can the Tofino CMP, the Tofino SA and Contact device be on a VLAN?

Yes, the Tofino SA will correctly process VLAN-tagged discovery and management messages from a Tofino CMP. However, remember that the Tofino CMP must be able to deliver a packet to a contact device. If the Tofino CMP and contact device are not on the same VLAN, then they may not be able to receive packets from each other. For this reason, when using VLANs a contact device such as a switch is recommended, as it will typically be on the same management VLAN as the Tofino CMP.

We highly recommend that Tofino SAs have the TD Contact device determined (using Tofino Discovery) and have both a Primary and Backup Contact device manually set. This provides redundancy in case a contact device is accidentally or deliberately removed from the network. You can determine if the contact devices are set by looking at the [Tofino View](#).

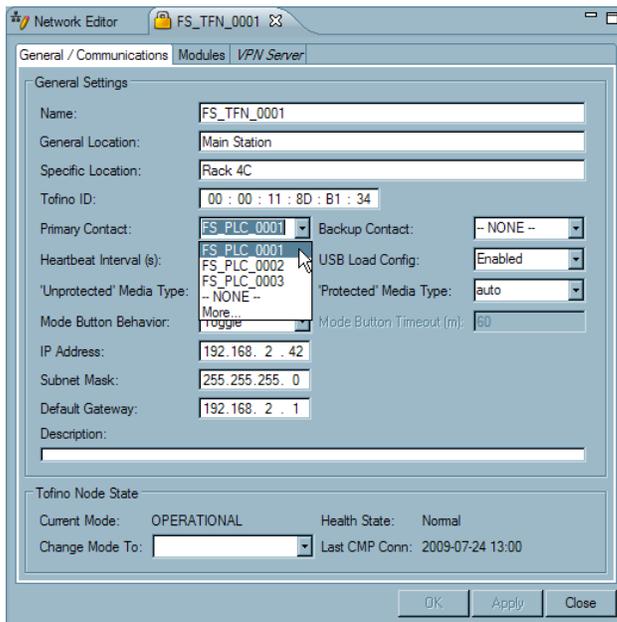
Name	Status	Flags	Version	ID	TD Contact	Primary Contact	Backup Contact
FSN_TFN_0001	OPERATIONAL	⊗ Not Installed	Tofino Linux: 1.1.0-rc2	00:00:0E:C5:EA:82	192.168.1.12	FS_PLC_0001	
Firewall LSM							
Secure Asset Management LSM	⚡ Activated		2008.4.1-4627				
Jasper Pipeline Network Tofino	OPERATIONAL	⊗ Not Installed	Tofino Linux: 1.1.0-rc2	00:00:11:8D:95:14	192.168.1.1	JP_PLC_0003	JP_PLC_0002
Firewall LSM							
Secure Asset Management LSM	⚡ Activated		2008.4.1-4627				
Sumas Pump Station Tofino	OPERATIONAL	⊗ Not Installed	Tofino Linux: 1.1.0-rc2	00:00:11:8D:96:83	192.168.1.1	SP_PLC_0001	
Firewall LSM							
Secure Asset Management LSM	⚡ Activated		2008.4.1-4627				

To set the TD Contact Device see [Using Tofino Discovery](#).

Configuring Contact Devices

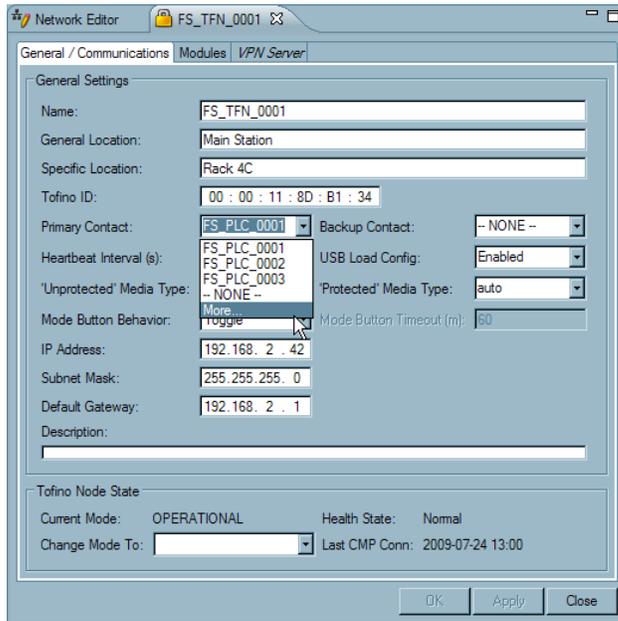
To configure the Tofino SAs Primary and Backup Contact device:

- Double click the Tofino SA icon in the Network Editor window.
- Under the General/Communications tab use the pull-down menus to identify the Primary and Backup contacts. If you would prefer to set a contact device that is not listed in the pull-down menu, select the more... option.
- Save your changes. See: [Saving Changes](#)



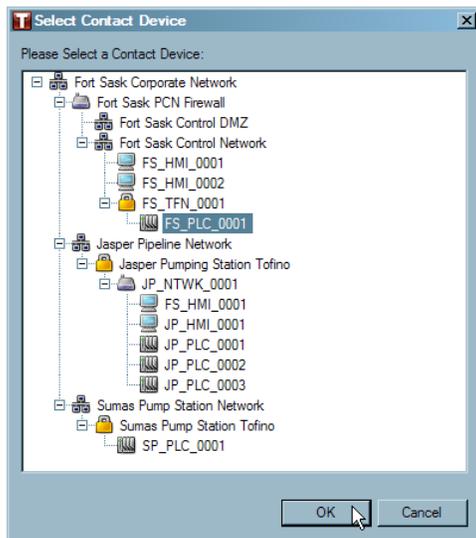
Specifying a Contact Device

- If you would prefer to set a contact device that is not on the list provided, click "More..."



- A window will open displaying your network. Select the Node you would like to set as your contact device and click "OK".

Note: The Node selected as your contact device must be on the other side of the Tofino SA from your Tofino CMP. Traffic going between your contact device and your Tofino CMP, must pass through the Tofino SA.



Assigning an IP Address to Your Tofino

It is not necessary to assign an IP address to your Tofino SA unless you are using the Client VPN LSM, the Server VPN LSM or Event Logger LSM with TCP/TSL transport on that Tofino SA. However, if an IP address is set, the Tofino CMP will first attempt to use this address to communicate to the Tofino SA. If this fails, it will fall back to using the addresses of the contact devices.

4.4 Configuring Tofino CMP Connections

Once the Tofino SA is installed in the field, it must be connected to the Tofino CMP network diagram. This involves the following steps:

- Adding a Tofino SA node icon to your network diagram. See: [Creating Your Network Diagram](#)
- Configuring your Tofino SA's properties. See: [Nodes Properties Wizard](#)
- Setting up the Tofino SA's contact devices. See: [Tofino SA Contact Devices](#)
- Confirm that the Tofino SA and Tofino CMP can communicate by checking for incoming Periodic Heartbeats. See: [Event View](#)

Each Tofino CMP has a unique public and private security key pair. The first time a Tofino CMP establishes a connection to a new Tofino SA in the field, it shares its public key with that Tofino SA. From then on, that Tofino SA only communicates to the Tofino CMP that owns the matching private key. This way, even if a potential attacker both obtains a copy of Tofino CMP software and intercepts the public key on the network, the legitimate Tofino CMP's private key will remain secret.

4.5 Syncing Your Tofino SA's Configuration

Occasionally a Tofino SA installed in the field may have a different configuration from what is stored in the Tofino CMP database. This can be caused by configuration changes when network communications between the Tofino CMP and Tofino SA is unavailable or when a replacement Tofino SA has been installed. To synchronize the Tofino SA configuration with the Tofino CMP configuration you have two choices:

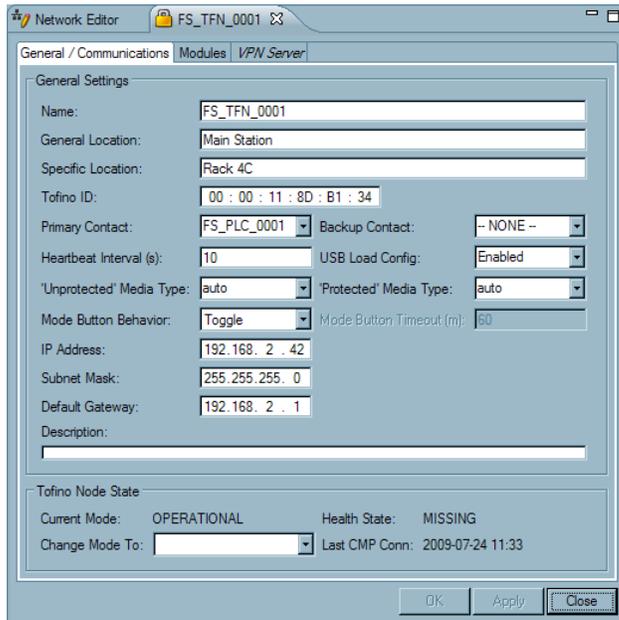
- ▶ Synchronizing the Tofino SA's configuration to match the Tofino CMP's current configuration.
- ▶ Synchronizing the Tofino CMP's configuration to match the Tofino SA's current configuration.

See: [Network Editor Right Click Menus](#)

4.6 Replacing Tofino SA

Replacing a failed Tofino SA with a new Tofino SA is simple.

- Install the new Tofino SA in the field. Make sure that you record the new Tofino SA's ID number.
- On the Tofino CMP, open the old Tofino SA's properties page by double clicking on the icon in the Network Editor window.



The screenshot shows the 'Network Editor' window with the 'General / Communications' tab selected. The 'Modules' section is set to 'VPN Server'. The 'General Settings' section contains the following fields:

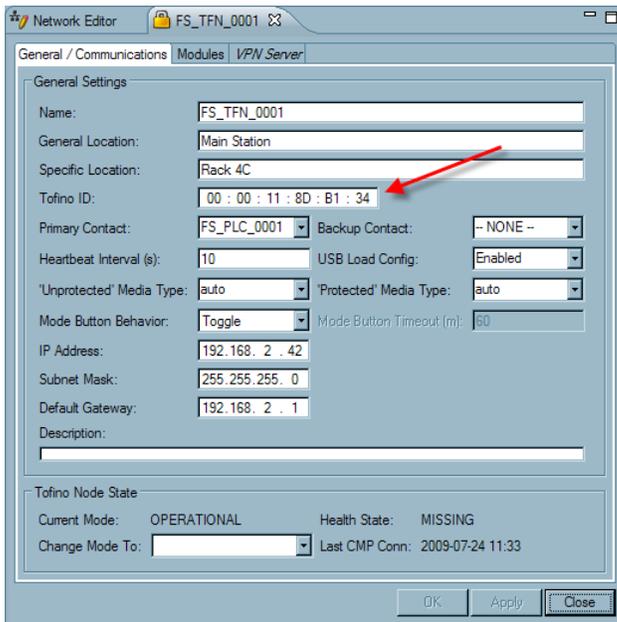
- Name: FS_TFN_0001
- General Location: Main Station
- Specific Location: Rack 4C
- Tofino ID: 00 : 00 : 11 : 8D : B1 : 34
- Primary Contact: FS_PLC_0001
- Backup Contact: -- NONE --
- Heartbeat Interval (s): 10
- USB Load Config: Enabled
- 'Unprotected' Media Type: auto
- 'Protected' Media Type: auto
- Mode Button Behavior: Toggle
- Mode Button Timeout (m): 60
- IP Address: 192.168.2.42
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.2.1
- Description: (empty)

The 'Tofino Node State' section shows:

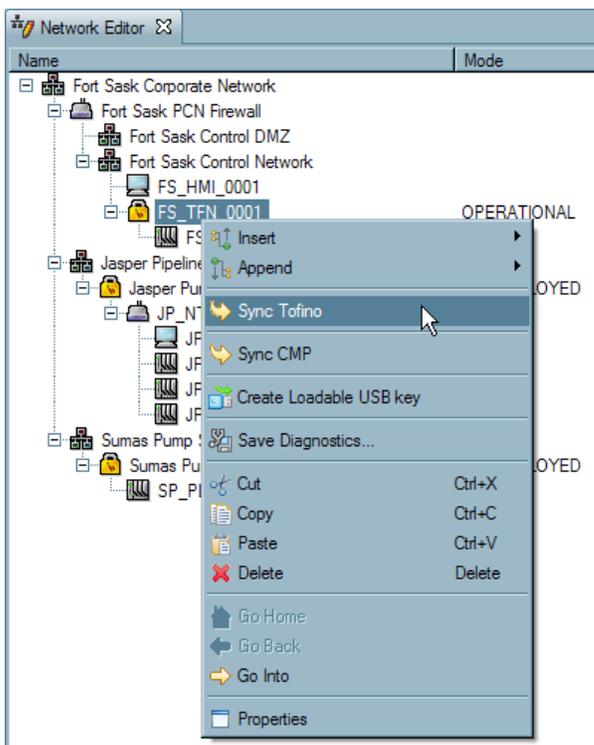
- Current Mode: OPERATIONAL
- Health State: MISSING
- Change Mode To: (dropdown menu)
- Last CMP Conn: 2009-07-24 11:33

Buttons at the bottom: OK, Apply, Close.

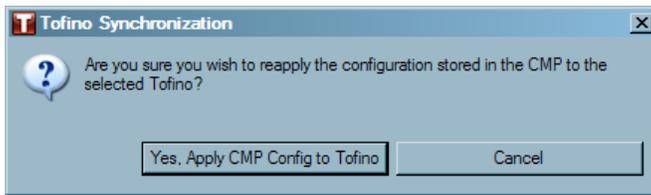
- Type in the **new** Tofino SA's ID number, replacing the old ID number and click "OK".



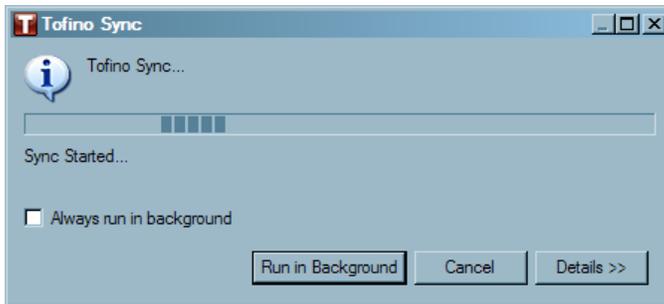
- Right click the Tofino SA icon, and select "Sync Tofino."



- Click "Yes, Apply CMP Config to Tofino".



- A Tofino Sync window will appear while configurations are completed.



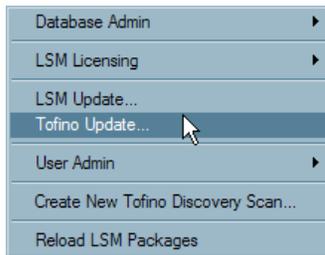
4.7 Updating Your Tofino SA Firmware

The Tofino Industrial Security Solution is designed to allow easy updating of system firmware in the Tofino SA's installed in the field. This is a three stage process:

- Obtain the new Update Packages for your Tofino SA.
- Store the packages on the Tofino CMP hard drive or on a server that the Tofino CMP can access.
- Use the **Tools ► Tofino Update...** wizard to guide you through the update process.

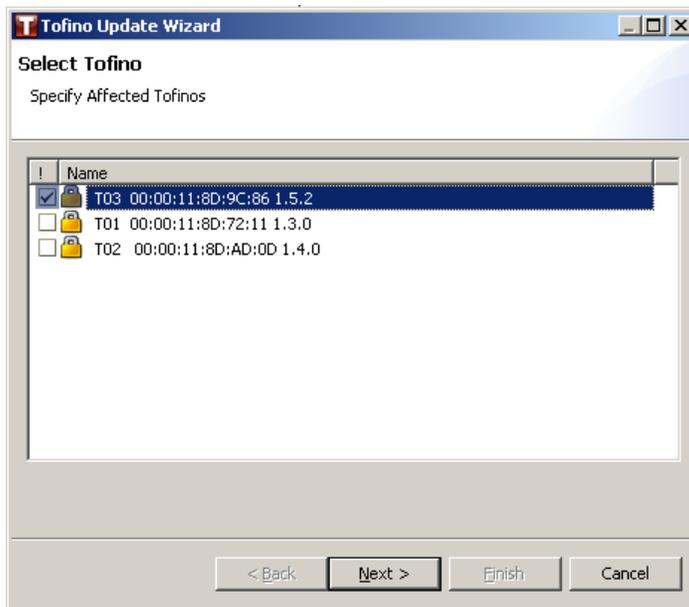
Note that this update wizard only updates Tofino SA firmware.

Tools ► Tofino Update...

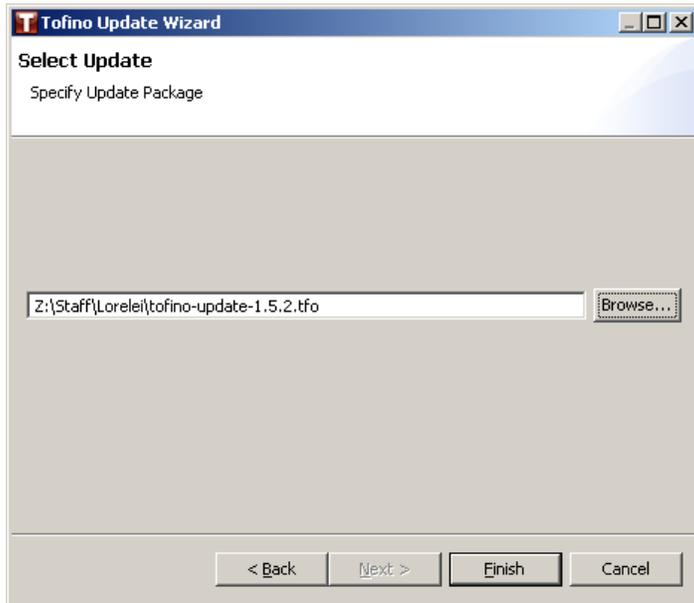


The Tofino Update wizard allows the user to add or update system firmware:

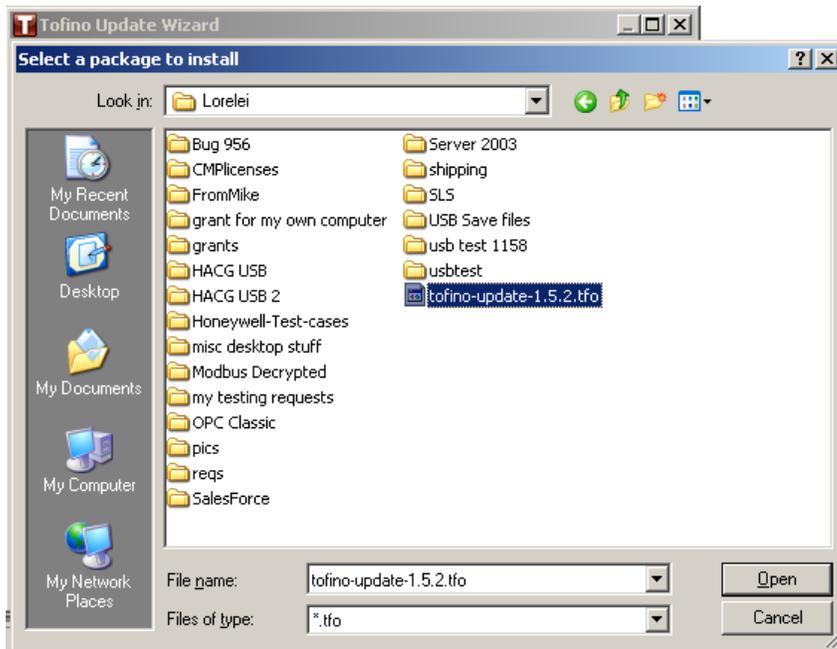
- Select "Tofino Update..." from the Tools menu.
- A window will open with a list of Tofino SAs on the network. Select the Tofino SAs needing to be updated by clicking on the box beside the name. Then click "Next".



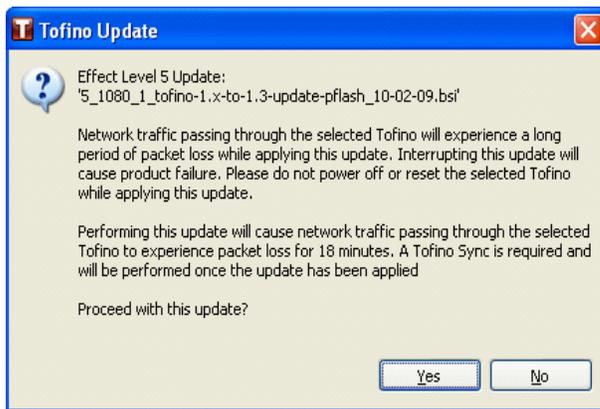
- Click on the "Browse" button to search for the .tfo file provided.



- Select the .tfo file and click "Open".



- After all firmware update packages have been selected, click the 'Finish' button in the Update Wizard, the Tofino CMP will display a dialog informing the user of the impact effect level of the update.
- If the user is satisfied that the update's impact on the control network is acceptable, the user may click the 'Yes' button to proceed with the update. If the impact is not acceptable, the user may click the 'No' button to cancel the update.



For further detail on updating your Tofino SA's firmware, see the application note titled: [Tofino™ Security Appliance Firmware Update Process](#)

Section 5

Tofino CMP Tab Management

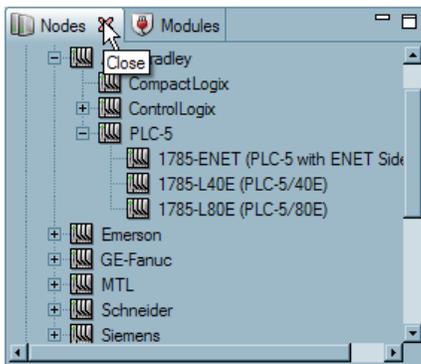
5 Tofino CMP Tab Management

The Tofino CMP has multiple tabs with viewing windows. This interface allows the user to rearrange, minimize, maximize, open, and close views as desired.

- See: [Closing Tabs](#)
- See: [Opening Tabs](#)
- See: [Minimizing Viewing Window](#)
- See: [Maximizing Viewing Window](#)
- See: [Rearranging Viewing Windows](#)
- See: [Managing Multiple Open Tabs](#)
- See: [Tab Management Right Click Menu](#)

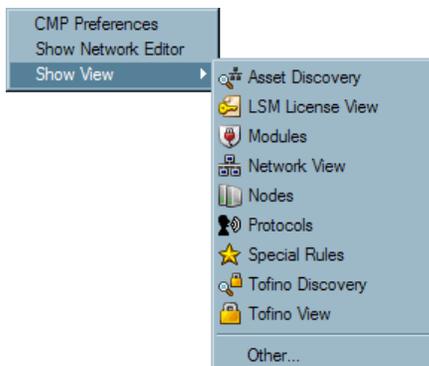
Closing Tabs

All tabs can be closed by clicking on the X in the right hand corner of the tab.



Opening Tabs

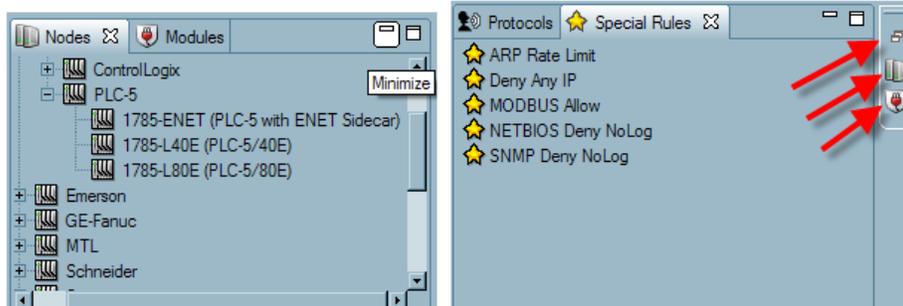
See: [Window Menu](#)



Minimizing Viewing Windows

A window can be minimized by clicking the minimizing button in the top right hand corner of each window.

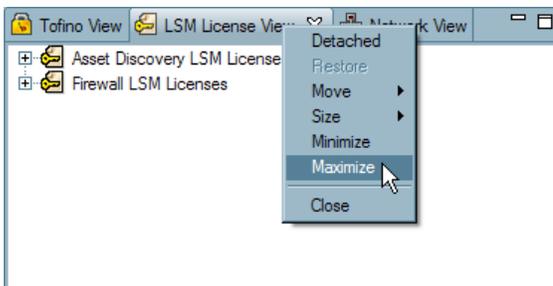
Note: A box will appear allowing the user to re-open the tabs. Click on an icon to restore the viewing window (the top icon will restore all windows to their original state).



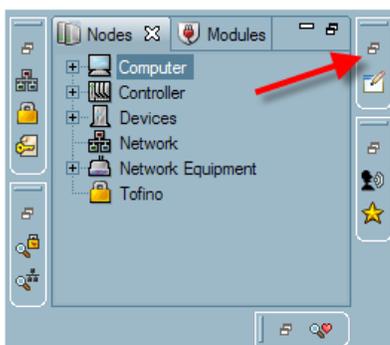
Note: At any time a viewing window can be restored by clicking the **Window ► Show View**.

Maximizing Viewing Windows

A window can be maximized by clicking on the maximize button in the top right hand corner of each window.

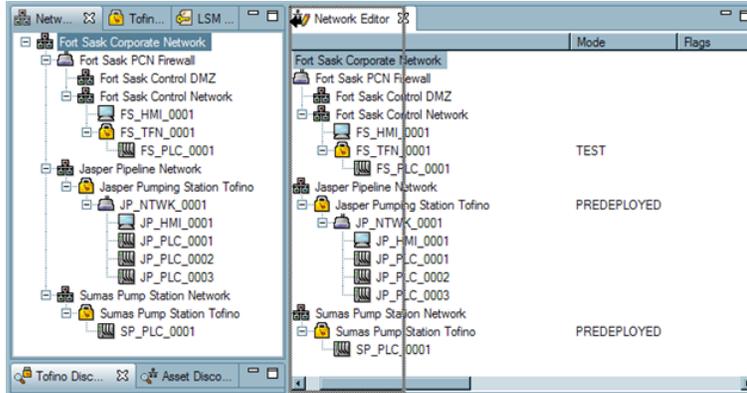


To restore the window to its previous view click the "Restore" button on the top right hand corner of the window or click on the icon of a particular view to re-open it.



Rearranging Viewing Windows

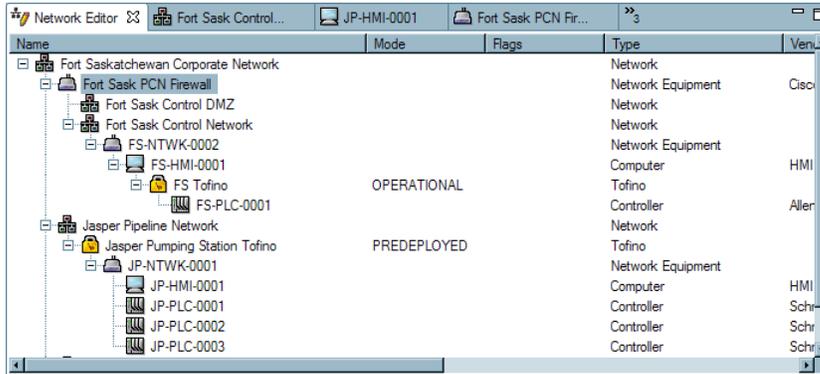
Any of the windows on the Tofino CMP can be dragged and dropped to other locations. To do this, click on the tab to be re-located and drag. Gray outlines will appear showing the user where the tab would be re-located.



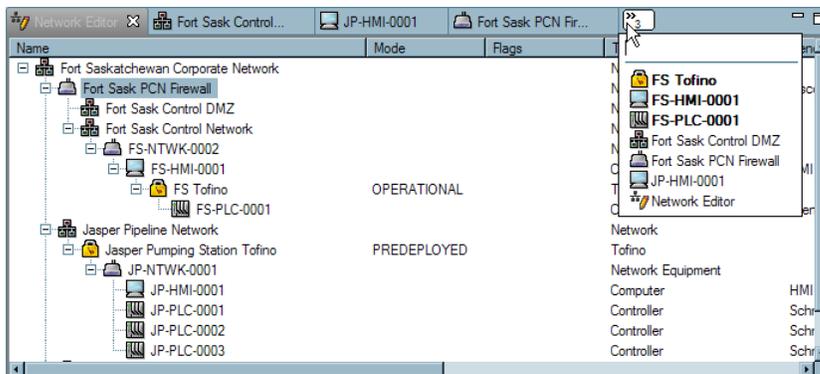
Managing Multiple Open Tabs

When editing devices in the Network Editor window and multiple tabs are open there are tools available to make managing these tabs easier.

When multiple entities tabs are open they will be displayed in the Network Editors window. If more than six tabs are open a number will appear indicating the number of additional tabs open (in this case 3).



To view a specific tab, click on the ">>" to open a menu that shows the selection of windows to view. Select a name from the menu and that window will open.



Tab Management Right Click Menu

To access the Tab Management Menu, Right Click on any tab on the Tofino CMP. A tab managing right click menu will appear. There are two tab managing right click menus: one is found when right clicking on the Network Editor tab and the other is found when right clicking any other tab on the Tofino CMP.

Tab Management Right Click Menu (Network Editor)

When right clicking on the Network Editor tab, the following menu should appear:



See: [Minimize](#)

See: [Maximize](#)

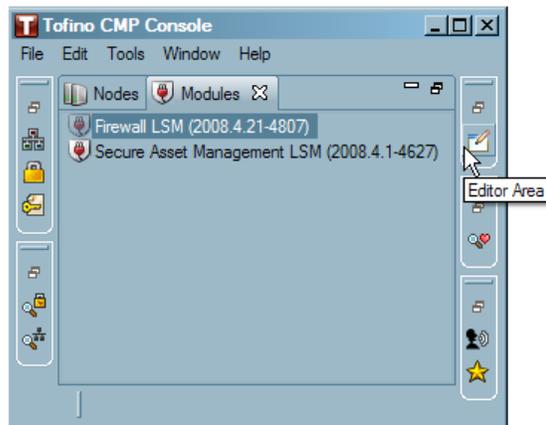
See: [Close/Close All](#)

Minimize

This selection minimizes the Network Editor window.



To re-open the Network Editor, window click on the Editor Area button on the right side of the screen.

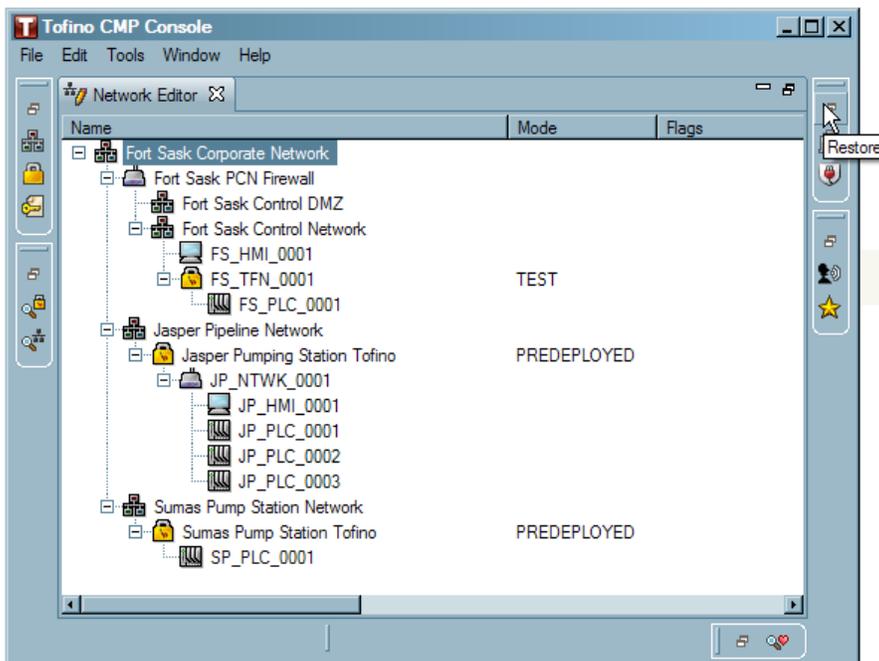


Maximize

This selection maximizes the Network Editor window.

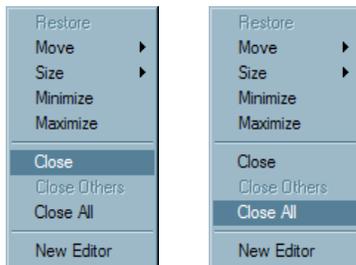


To restore the Network Editor window to its previous view click on the "Restore" button on the right side of the screen.



Close/Close All

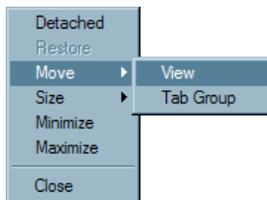
To close the Network Editor window, select "Close" or "Close All".



To restore the Network Editor window, select the Window menu option and click Show Network Editor.

Tab Management Right Click Menu (All tabs except Network Editor)

Note: To re-open a tab at any time, click **Window ▶ Show View** or **Window ▶ Show Network Editor**.



See: [Detached](#)

See: [Move ▶ View](#)

See: [Move ▶ Tab Group](#)

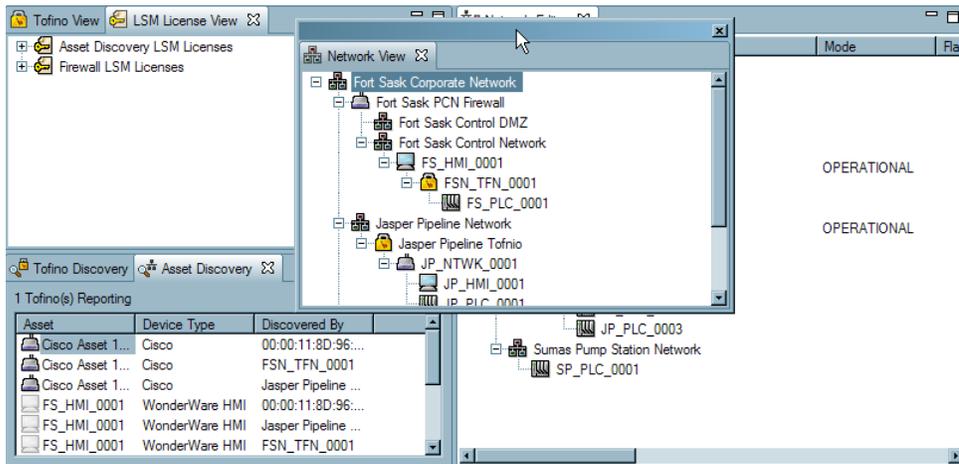
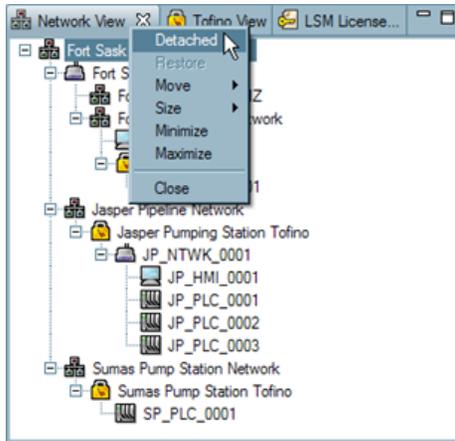
See: [Minimize](#)

See: [Maximize](#)

See: [Close](#)

Detached

By right clicking any tab (except Network Editor) and selecting Detached the selected window will detach its self and will be moveable to any location.

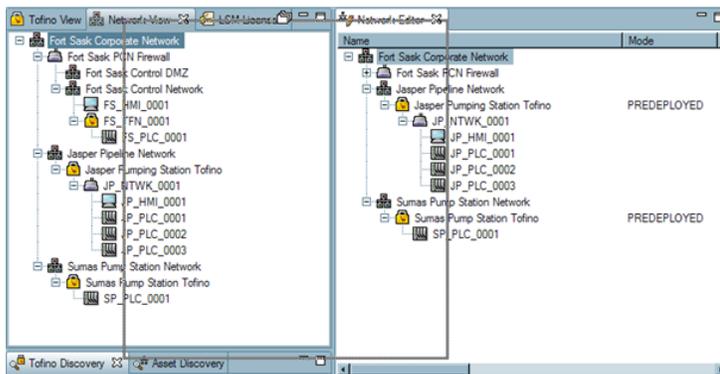
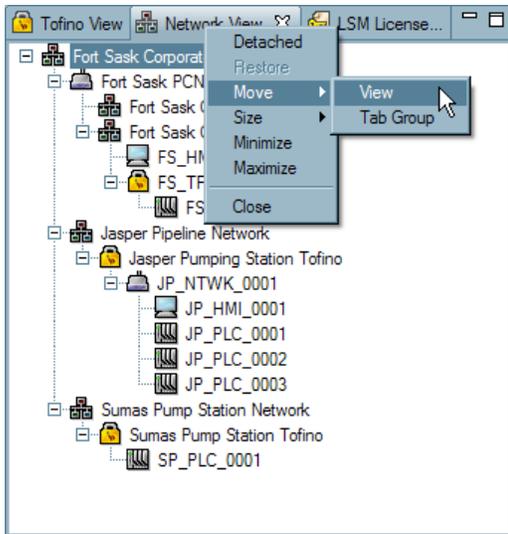


To move the detached window back to its original location (or another location) drag and drop the tab to the desired location. Gray lines will display where the window will be moved to.

Move ►View

By right clicking on a tab and selecting **Move ►View**, the window of the tab that was clicked will detach and become moveable to another location. Gray lines will display where the window will be moved to.

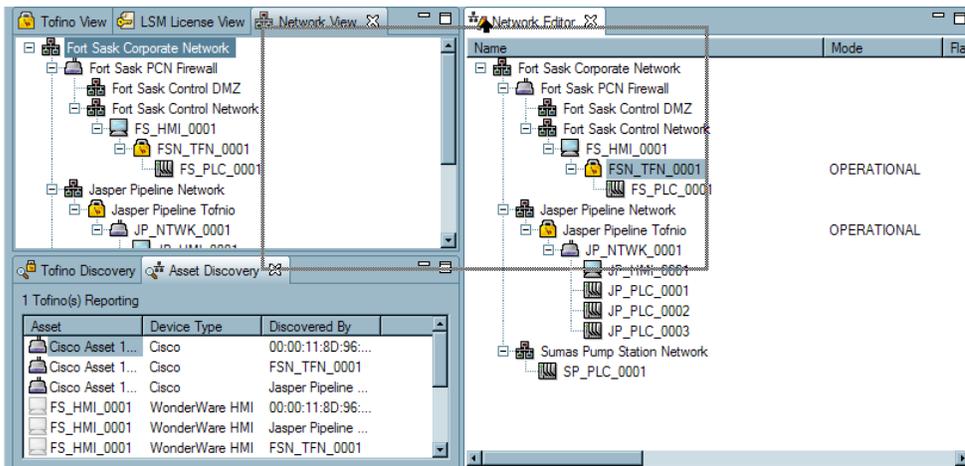
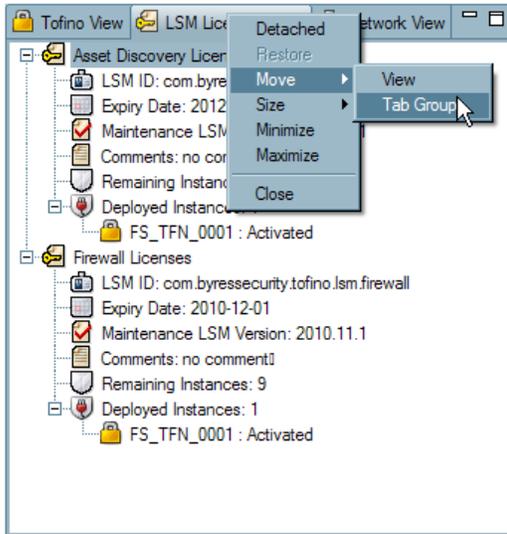
Note: By clicking escape on the keyboard, the gray lines will disappear.



Move ► Tab Group

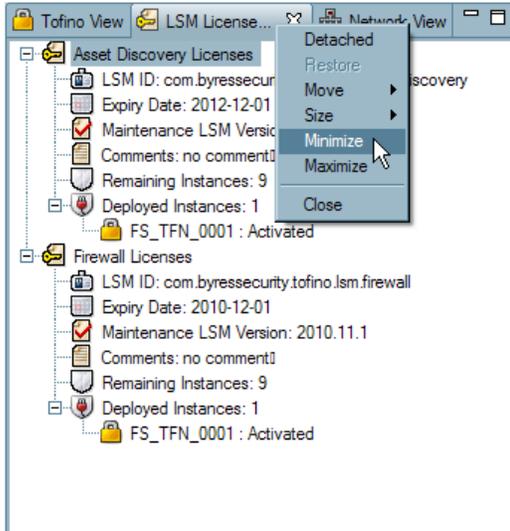
By right clicking on a tab and selecting **Move ► Tab Group**, the tab that was clicked on and other tabs in its group will be moveable as a unit. Gray lines will display where the windows will be moved to.

Note: By clicking escape the gray lines will disappear.

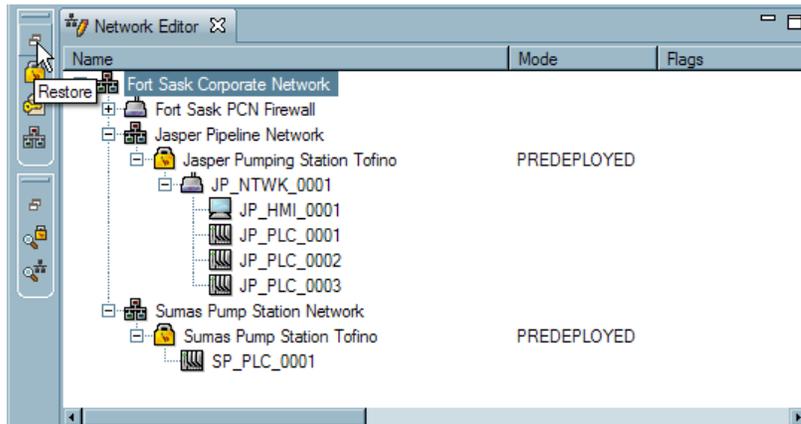


Minimize

By right clicking on a tab and selecting minimize, the windows of the tab group will be minimized. Noted: The Network Editor window is considered a group.

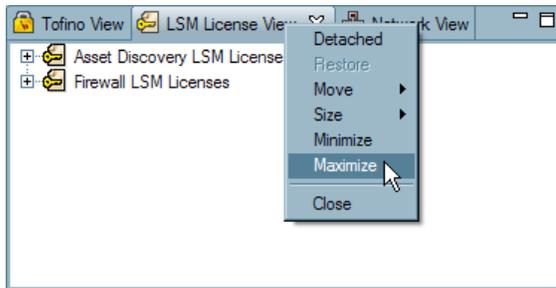


To re-open the all the windows click on the restore button. Or to restore specific window, click on that window's icon.

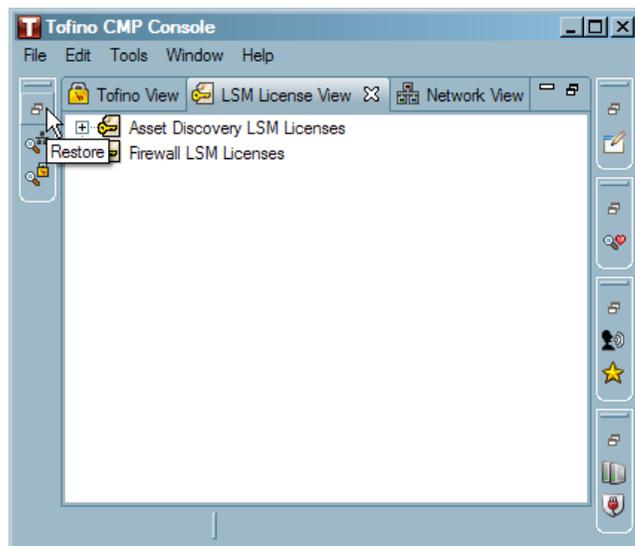


Maximize

By right clicking on a tab and selecting Maximize, the window of the tab will open over the entire Tofino CMP. This may be useful for the Event View window for viewing heartbeats.

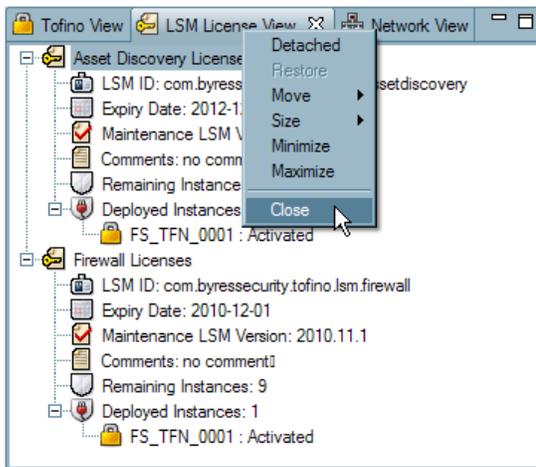


To return the Tofino CMP to the normal view click "Restore" or to restore a specific window, click on that window's icon.

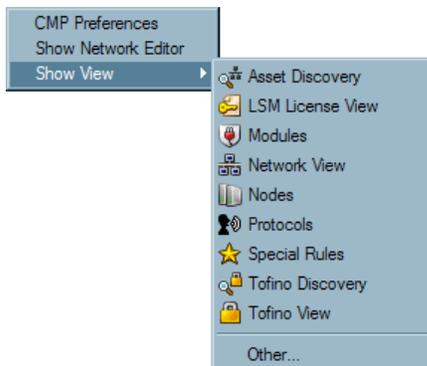


Close

By right clicking on a tab and selecting Close, the window of the tab selected will close.



To re-open the tab click **Window ► Show View** or **Window ► Show Network Editor**.



Section 6

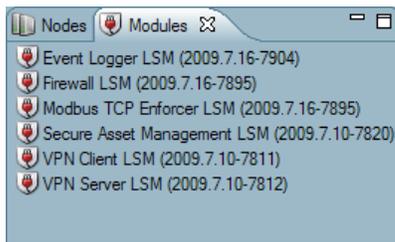
LSMs

6 LSMs

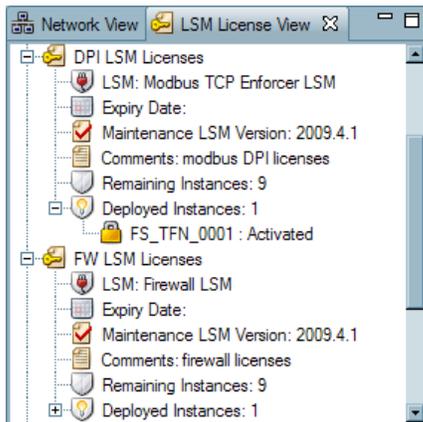
6.1 Managing LSMs

Tofino Loadable Security Modules (LSM) are software plug-ins that provide security services such as firewall, secure asset management, intrusion detection system (IDS) and VPN encryption. Each LSM is downloaded into the Tofino SA to allow it to offer customizable security functions, depending on the requirements of the control system.

The available LSMs are shown in the Modules window. The Modules window also shows the version number for each type of LSM available. For directions on how to install an LSM in a Tofino SA see: [Adding an LSM to a Tofino SA](#)



All LSMs must be licensed before they can be activated in a Tofino SA. For directions on how to license an LSM see: [LSM Licensing](#)



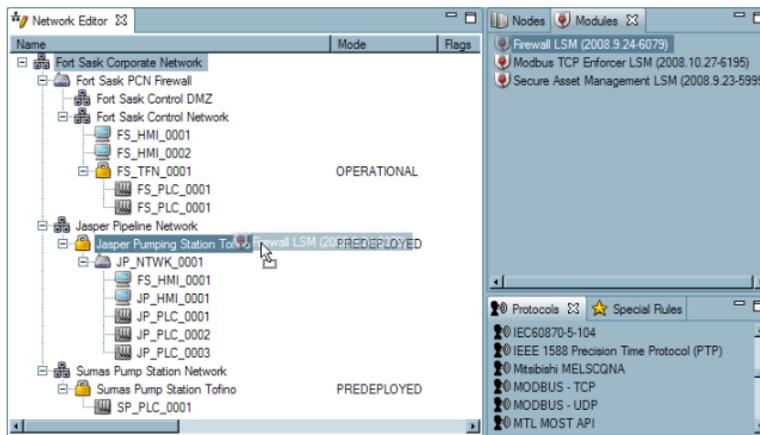
As new versions of LSMs are available, they can be updated to the Tofino SA using **Tools ► LSM Update...** menu. See: [Tools Menu](#)

6.1.1 Adding LSMs to Tofino SAs

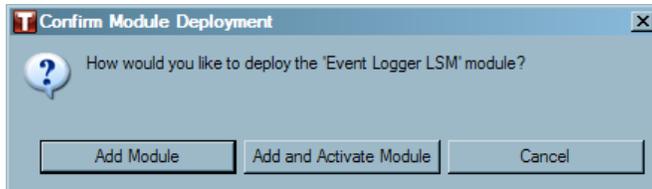
Note: Before an LSM can be activated, licenses need to be imported. See: [LSM Licensing](#)

Adding an LSM to a Tofino SA using Drag and Drop

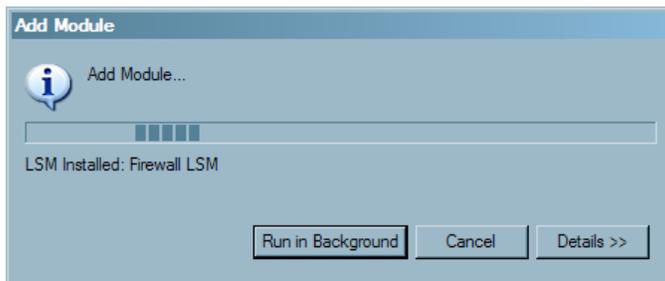
- Drag and drop an LSM, from the Modules tab, onto a Tofino SA icon in the Network Editor window. By dragging and dropping a module onto a Tofino SA icon you are adding the module to the Tofino SA.



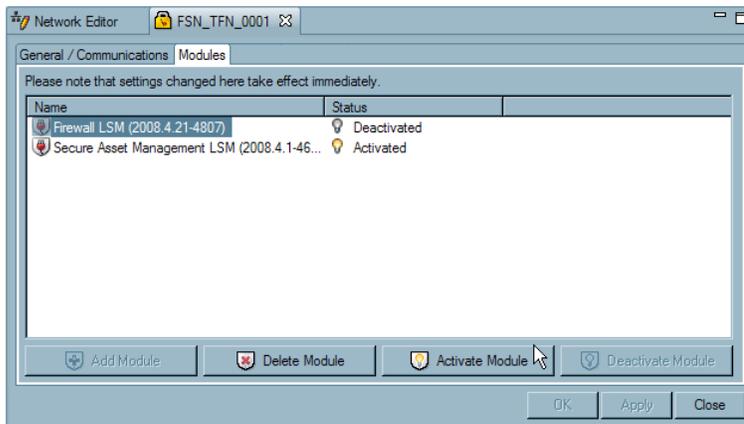
- A window will appear asking "How would you like to deploy the "XXX LSM module"? Click "Add Module" to add the module without activating it or click "Add and Activate Module" to add and activate the module.



An LSM Update Monitor will appear.



- Double click the Tofino SA icon in the Network Editor window. A Properties page will appear.
- Select the Modules tab for the Tofino SA. This will display the modules present on the Tofino SA and their activation status.



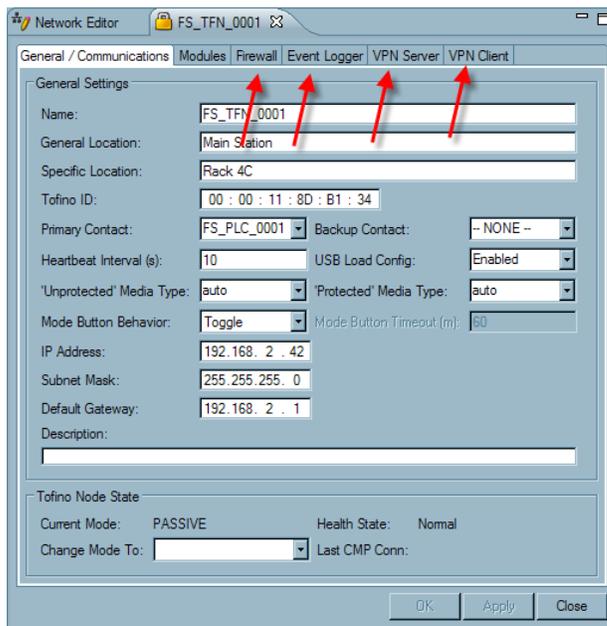
- Now click "Activate Module". The LSM will now be installed and activated. At any time any LSM can be deactivated and deleted from the Modules tab using the appropriate buttons.

Note: LSMs can also be added to Tofino SAs by going directly to the Modules tab and using the buttons at the bottom of the window. The modules tab can be located by double clicking on a Tofino SA in the Network Editor.

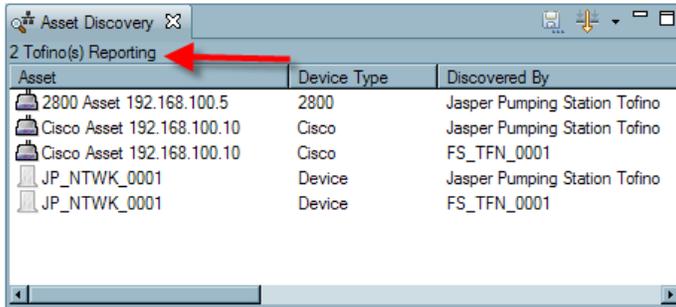
6.1.1.1 How LSM Tabs Work

Once an LSM has been added to a Tofino SA (and is either Deactivated or Activated), an LSM tab will appear either on the Tofino SA's properties page or on a downstream device (or in some cases on both the Tofino SA and the downstream device).

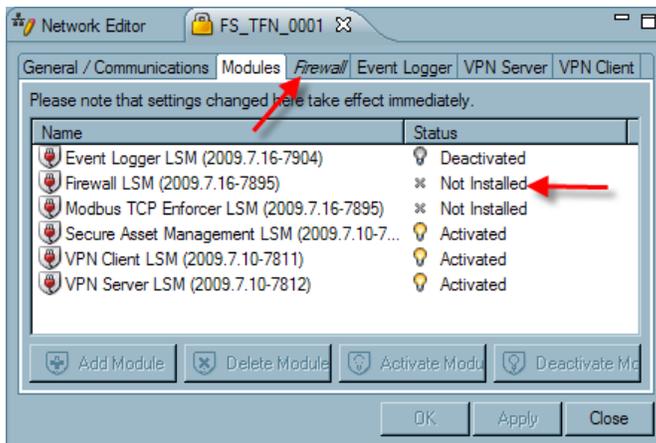
- ▶ The Firewall LSM will display a tab on the Tofino SA's on which it is installed, as well as on any downstream devices from that Tofino SA.
- ▶ The Modbus LSM will display on any downstream devices from a Tofino SA with the LSM installed.
- ▶ The VPN Server LSM will display a tab on the Tofino SA on which it is installed.
- ▶ The VPN Client LSM will display on a Tofino SA's properties page if that Tofino SA is set up to be a VPN client of another Tofino SA or a 3rd party VPN server.
- ▶ The Event Logger LSM will display a tab on the Tofino SA on which it is installed.



Note: There is one exception to this rule and that is with the Secure Asset Management LSM. A tab will not appear on the Tofino SA's properties page or on a downstream device, but devices will begin to show up as they are discovered in the Asset Discovery window. The number of Tofino SAs that have the SAM LSM installed and activated will be displayed in the top left hand corner of the Asset Discovery window.



Note: If a Tofino SA has an LSM configured and then that LSM is deleted, the tab will remain but will be italicized. This indicates that the LSM is removed but there is configuration data still remaining.



The VPN Server tab and Event Logger tab will always remain visible once they have been configured even if all configurations have been removed. The reason for this is that the certificates, keys generated and revoked certificates remain in the database. Deleting and re-adding the Tofino SA into the Tofino CMP Network Editor is the only way to remove the VPN Server tab or Event Logger tab from the properties page.

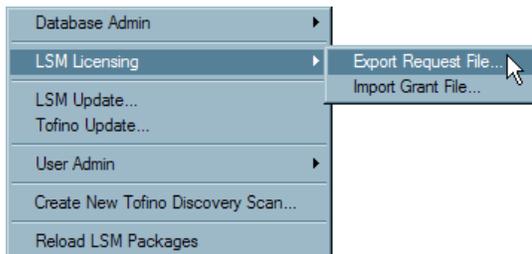
6.1.2 LSM Licensing: Upgrading or Adding

LSM Licensing will usually be set up when the Tofino CMP is initially set up (See: [Tofino CMP Licensing](#)); however, additional LSMs can be requested at any time and will take one business day to obtain.

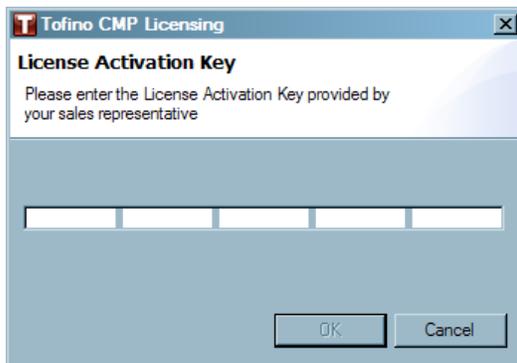
Each LSM used on each Tofino SA needs to be licensed in order for it to work. **Note:** LSMs can be installed but cannot be activated until a license is in place.

To license an LSM, follow these steps:

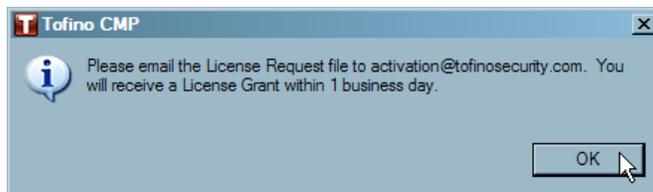
- Have your new License Activation Key ready.
- Create a license request file. To do this click **Tools ▶ LSM Licensing ▶ Export Request File...**



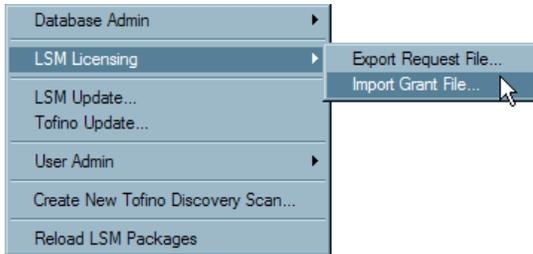
- Enter the License Activation Key that your sales representative provided and click "OK".



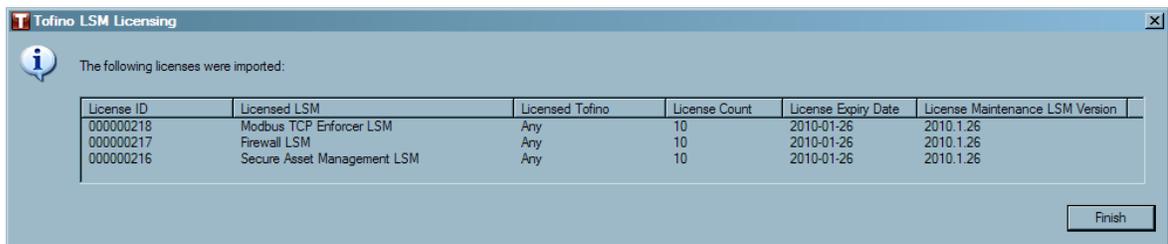
- Select a location to save the request file and give it a name that is appropriate for your organization. Click "Save" and the file will be created.
- Click "OK", and email the License Request file to activation@tofinosecurity.com



- Once the License Grant file has been returned to you, save it to a location you will remember and then re-start the Tofino CMP, and click *Obtain License* and then *Import Grant File...* If this dialog does not appear, once the Tofino CMP has opened, select **Tools ▶ LSM Licensing ▶ Import Grant File...**



- A list of the LSM licenses that you imported will appear, click "Finish".



6.2 Firewall LSM Management

6.2.1 Basic Firewall Concepts

What is a Firewall?

A firewall is a mechanism used to control and monitor traffic between two networks (or two portions of the same network) for the purpose of protecting devices on the network. It compares the traffic passing through the firewall to a predefined set of rules, discarding traffic that does not meet the rule criteria. In effect, it is a filter blocking unwanted network traffic and placing limitations on the amount and type of communication that occurs between a protected device or network and other networks (such as the corporate network, or another portion of a site's control network).

The Tofino Firewall is a LSM that is loaded into the Tofino SA to process traffic. The firewall is a highly advanced firewall known as a stateful deep-packet inspection firewall.

Where Can I Add Firewall Rules?

Firewall Rules can be added to specific nodes that need protection or to the Tofino SA itself. All rules are actually stored in the Tofino SA, but where you create them on the Tofino CMP determines how they act.

- ▶ Firewall Rules on Tofino SAs: These are generalized rules that apply to all traffic passing through the Tofino SA without regard to the final destination. There are three types of rules that can be added to a Tofino SA: [Global Rules](#), [Broadcast Rules and Multicast Rules](#).
- ▶ Firewall Rules on Nodes: These are rules specifically intended to filter traffic to a specific device or network. There are two types of rules that can be added to a Node: [Global Rules and Talker Rules](#).

Global Rules versus Talker Rules

Depending on whether or not you want the source address of a message checked by the firewall, there are two types of firewall rules:

- ▶ Global Rules: These allow the user to set the direction and permission for all traffic of a particular protocol type or special rule destined for the selected node (e.g.: FS-PLC-0001) without regard for the source of the traffic. In other words, if the user wants to allow Modbus/TCP traffic to any device upstream from the Tofino SA (i.e.: the entire plant) from the protected device, a Global Rule could be used. Because Global Rules are so liberal they should be used with extreme caution.
- ▶ Talker Rules: These allow the user to set the direction and permission for traffic from a specific upstream device or network to the selected node (e.g.: FS-PLC-0001). For example, if the user wants to allow Modbus/TCP traffic between a specific upstream device to the protected device, a Talker Rule can be used. Talker Rules can also be used for a group of devices if the talker selected is a network node.

Global Rules can be applied to both Tofino SAs and protected nodes, while Talker Rules can only be applied to protected nodes.

Broadcast and Multicast Rules

Most rules used in the Tofino SA are designed to filter what are known as Unicast messages. A Unicast message is network traffic directed from a specific device to another specific device. However, in all networks there are messages that are sent to a general address and are expected to be received by everyone on the network. These are called Broadcast and Multicast messages. The Tofino Firewall LSM has special rules designed to handle these types of messages.

- ▶ Broadcast Rules: Broadcast packets, which are a normal part of network operation, are transmitted by a device to a broadcast address that all devices listen to. For example, IP networks use

broadcasts to resolve network addresses using Address Resolution Protocol (ARP). Because they are directed to a broadcast address and not a specific device's address the Tofino SA must have specific rules that can detect the broadcast address in the message. Creating a Broadcast Rule automatically sets up the correct address detection.

- ▶ **Multicast Rules:** Multicast packets are transmitted to a multicast address that a set of devices listen to. For example, Ethernet/IP networks use multicasts to send I/O traffic to a set of interested devices known as consumers. Because they are directed to a multicast address and not a specific device's address the Tofino SA must have specific rules that can detect the multicast address in the message. Creating a Multicast Rule automatically sets up the correct address detection.

Broadcast and Multicast Rules can only be applied to Tofino SAs.

Protocol Rules versus Special Rules

The difference between Protocol Rules and Special Rules is their underlying complexity.

- ▶ **Protocol Rules:** These rules are designed to simply allow or deny specific protocols passing through the firewall. They allow the user to set the source, destination, direction and permission for all traffic of a particular protocol type. For example, if the user wants to allow Modbus/TCP traffic between two devices, a Protocol Rule can be used. Protocol Rules can be applied to both Global Rules and Talker Rules. All available Protocols can be viewed in the Protocols View. See: [Protocols](#)
- ▶ **Special Rules:** These rules are highly complex rules that go beyond simple allow or deny. For example, a Special Rule could be used to rate limit a type of traffic or to block a subset of a particular type of traffic. All available Special Rules can be viewed in the Special Rules View. See: [Special Rules](#)

Incoming versus Outgoing versus Bidirectional

Most firewall rules have a direction associated with them. This direction indicates the direction that a connection between two nodes is set up. It does not refer to packet flow. For example, if a HMI is using Modbus/TCP to request data from a PLC, the HMI will be the device initially setting up the communications connection. Once the connection is established, then packets will flow in both directions.

Another way of thinking of this is to consider a normal telephone system. The person dialing the phone number (Person 1) is who is establishing the connection. Once the other person (Person 2) answers the phone, then speech can go both ways.

The Tofino Firewall LSM allows three choices on direction of connections set up:

- ▶ **Incoming:** The connections can only be established from an external device to the protected device. For example, an HMI connecting to a PLC that is protected by a Tofino SA.
- ▶ **Outgoing:** The connections can only be established from the protected device to the external device. For example, a Work Station that is protected by a Tofino SA connecting to a web server.
- ▶ **Bidirectional:** The connections can be established by either the protected device or the external device.

Remember, once the connection is established, traffic will be able to flow in both directions regardless of the direction rule.

Note: The direction on a protected device's firewall rules always considers the device as the reference point. On rules associated only with a Tofino SA, Incoming refers to traffic coming in to the Tofino SA and Outgoing refers to traffic going out of the Tofino SA.

VLAN-tagging and Firewall Rules

Virtual Local Area Network (VLAN) is a network technology that network administrators use to make managing large networks easier. Using VLANs, a system administrator can create and then manage distinct groups of computers existing on the same physical network.

For example, a network administrator might ideally want separate networks for closed circuit video, HMI client communications and data management communications. Unfortunately, cost constraints might require that these systems all use the same local area network (LAN) backbone. To solve this (well at least partially solve it), the administrator could assign each group of devices to different “virtual LAN” or VLAN. To the system user, each group would appear to be on separate networks, while in reality the messages would all be travelling on the same physical LAN.

Most VLAN technologies follow a standard called IEEE 802.1q. This technology has VLAN-capable switches mark each Ethernet message with a special “tag” that indicates which VLAN group the message belongs to. When a switch receives a VLAN tagged message, it is configured to only forward that message to devices that belong to the same VLAN. This is particularly useful for managing broadcast traffic.

The Tofino SA firewall manages VLAN-tagged packets transparently and does not require additional rules for VLAN. For example, a single Modbus Enforcer rule can manage both tagged and untagged Modbus packets.

6.2.2 Firewall Log Settings

The firewall settings allow you to control the number of events and alarms sent by the Tofino Firewall LSM when packets are either denied and logged or allowed and logged. There are two main controls:

- ▶ **Rate Limits:** The user has the option to change the settings for rate and burst limit of exception heartbeats. These settings configure firewall exception heartbeats to be logged (sent to the Tofino CMP) at a limited rate using a token bucket filter algorithm.

To understand how token bucket filtering works, picture a 'bucket' of 'tokens'. It costs one token in order for the Firewall LSM to log one packet.

- ▶ **Rate Limit:** is the rate at which the bucket is refilled with tokens. The "rate limit" setting is calculated as "per minute", but the refilling of the bucket is done at a gradual rate over a minute (not once a minute).
- ▶ **Burst Limit:** is the initial number of tokens in the bucket, as well as the maximum number of tokens the bucket can hold.

At any point, a burst of packets equal to the number of tokens in the bucket will be logged immediately. Once the bucket is empty, the firewall can only log packets as the bucket refills over time at the rate specified by the "rate limit". If the rate of packets is faster than the "rate limit", the bucket will empty at the rate of packets, and then will be limited by the "rate limit" which refills the bucket. In other words, if your burst limit is 50 and your rate limit is 25 and a 1000 packets are denied and logged the first 50 will be sent to the Tofino CMP, followed by another 25 packets per minute.

- ▶ **Log Type:** These control whether heartbeats are generated on a per packet basis or on per connection basis.
 - ▶ **Log By Packet:** When this option is selected, exception heartbeats are sent for each packet that triggers a log rule. For example, if an attacker sends 10 MODBUS packets to the same protected device and the Tofino Firewall LSM blocks them, then 10 exception heartbeats will be sent to the Tofino CMP. With this option you will see all the packets being denied (and logged) by the firewall, but may experience an excessive number of alarms.
 - ▶ **Log By Connection:** When this option is selected, exception heartbeats are sent for each packet that triggers a log rule. For example, if an attacker sends 10 MODBUS packets to the same protected device and the Tofino Firewall LSM blocks them, then only 1 exception heartbeat will be sent to the Tofino CMP. With this option you will only see the first packet sent to that protected device being denied (and logged) by the firewall which should reduce the number of alarms. If a TCP connection is not made by the packets being logged then a "reminder" heartbeat will be sent every 30 seconds.

Note: In TEST mode you will get Log by Packet exception heartbeats for any connections that were already established when the Tofino SA was switched into TEST mode.

6.2.3 Firewall Rule Configuration for a Node

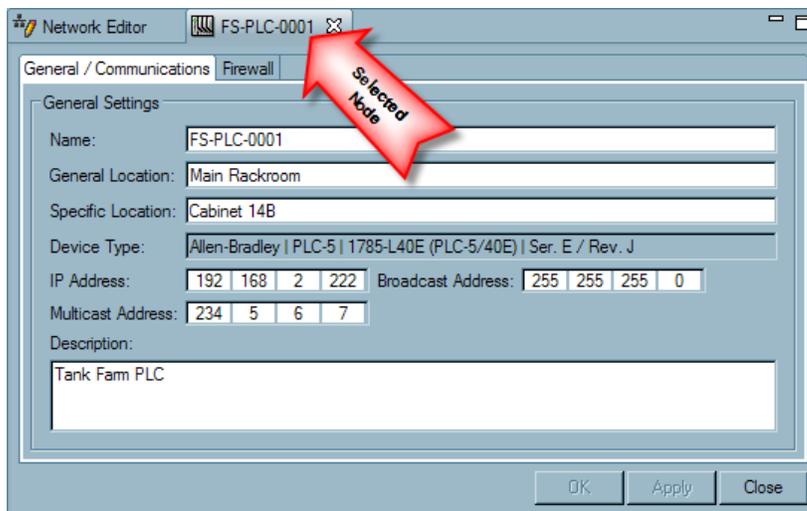
Please note that a Tofino SA must be located upstream from the node in order to be able to configure firewall rules (i.e. a Firewall tab will not appear on the Node's properties page until a Tofino SA is inserted above the node in your network diagram).

To view the properties and modules of the Tofino SA protecting a node, click the "Administer Tofino" button on the node's Firewall tab. Note however that if the node is downstream from a Tofino SA with a firewall LSM, a Firewall tab will be present.

If the node was at one time, but is no longer downstream from a Tofino SA and had firewall rules set, the firewall tab will now be italicized to indicate that the rules are no longer active.

To configure firewall rules for a specific device or network that is downstream from a Tofino SA complete the following steps:

- From the Network Editor or the Network View window, double click the icon for the node you want the firewall rules to protect. Keep in mind that in order for a node to be protected it must be downstream from a Tofino SA in the Network Editor window and this Tofino SA must have a Firewall LSM installed. See: [Adding an LSM to a Tofino SA](#).



- There are two types of firewall rules that can be added to a node: [Global Rules and Talker Rules](#). Decide which type of rule to add.
 - ▶ See: [Setting Global Rules](#)
 - ▶ See: [Setting Talker Rules](#)

6.2.3.1 Setting Global Rules

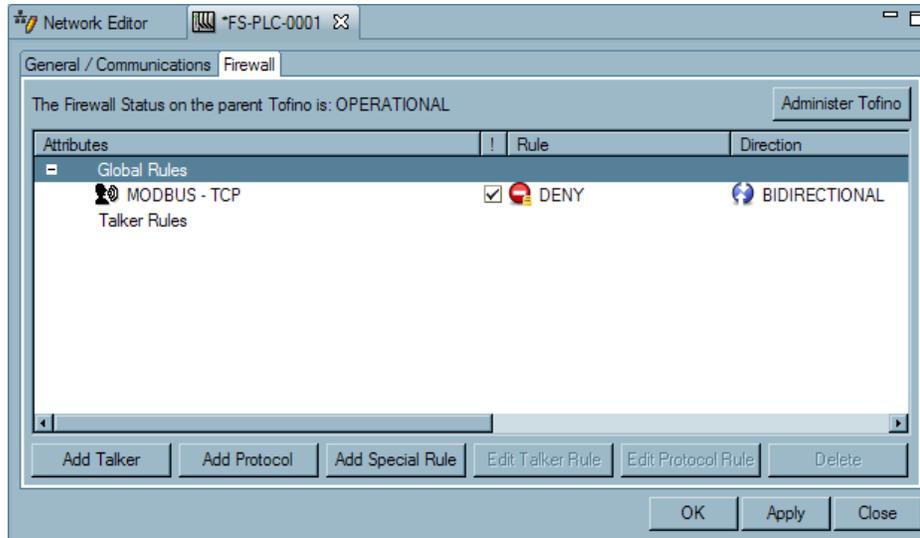
Decide if you want to add a Protocol or a Special Rule to the Global Rules list for your selected Node. See: [Basic Firewall Concepts](#)

[Drag and Drop Protocol](#)

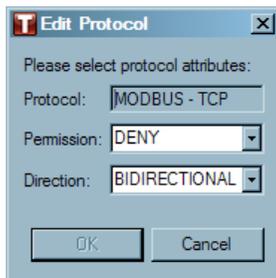
[Drag and Drop Special Rule](#)

Drag and Drop Protocol

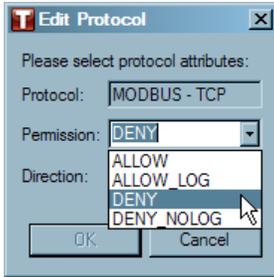
- Drag and drop a protocol from the protocol window onto the Global Rule text.



- Set the Global Policy by double clicking on the protocol text **or** clicking on the protocol and then clicking the Edit Protocol button at the bottom of the screen.

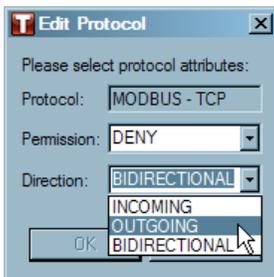


- Select the Permission for the rule. There are four types of Permissions:
 - ▶ Allow: Traffic matching the rule is allowed through the Tofino SA with no logging or alarms reported to the Tofino CMP.
 - ▶ Allow Log: Traffic matching the rule is allowed through the Tofino SA. This traffic is logged and exception heartbeats are generated.
 - ▶ Deny No Log: Traffic matching the rule is blocked by the Tofino SA with no logging or alarms reported to the Tofino CMP.
 - ▶ Deny: Traffic matching the rule is blocked by the Tofino SA. This traffic is logged and exception heartbeats are generated.

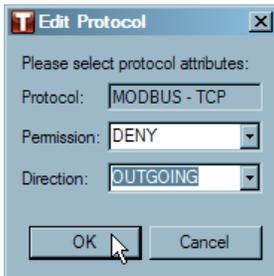


- Select the Direction that the network connection will originate from:
 - ▶ Bidirectional: Connection initiation is allowed from either side of the Tofino SA.
 - ▶ Incoming: Connection initiation is allowed only from the untrusted side of the Tofino SA.
 - ▶ Outgoing: Connection initiation is allowed only from the trusted side of the Tofino SA.

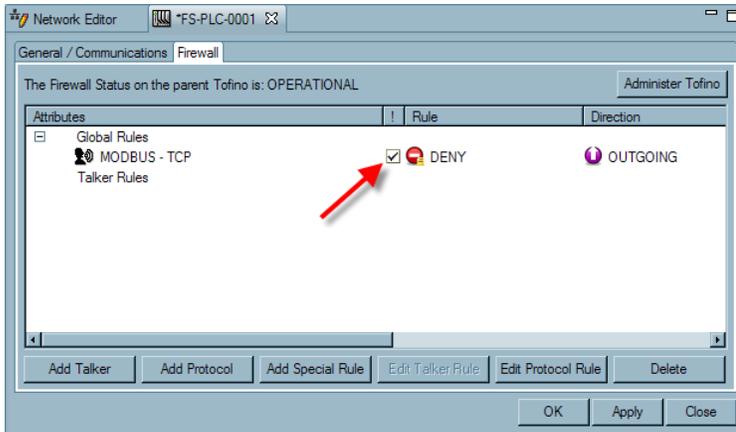
Note: Traffic can still flow in both directions with any of these three settings – only the side initiating the connection is controlled. For example, if an HMI is located on the untrusted side and it needs to communicate using Modbus/TCP to a PLC on the trusted side, incoming is sufficient as the state feature of the firewall will automatically allow Modbus/TCP reply messages out if a Modbus/TCP command message was previously seen by the Tofino SA.



- Click "OK".



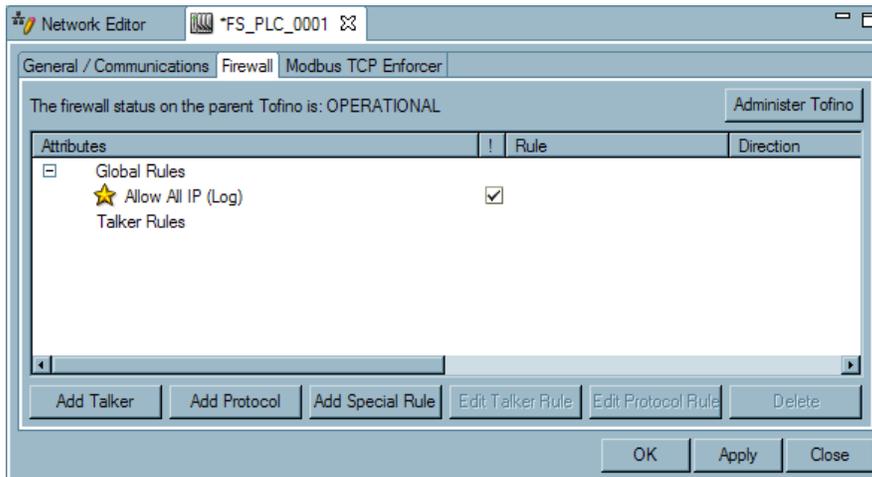
- The rule should now appear under Global Rules. The checked box is where the rule is activated or deactivated. A checked box means the rule is activated. An unchecked box indicates the rule is deactivated. A rule may be deactivated in order to test the rule or as a reminder of rules that have been in use.



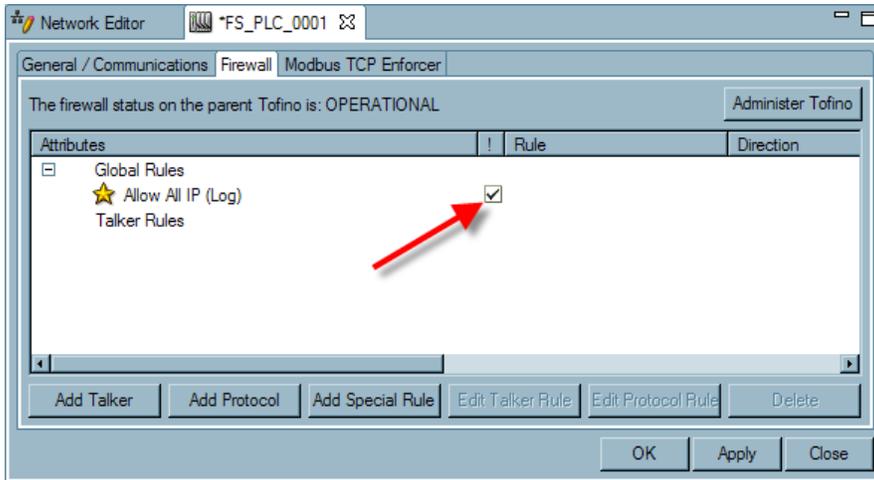
- Save your changes. See: [Saving Changes](#)

Drag and Drop Special Rule

- Drag and drop the desired Special Rule from the Special Rules window onto the Global Rule text.



- The rule should now appear under Global Rules. The checked box is where the rule is activated or deactivated. A checked box means the rule is activated. An unchecked box indicates the rule is deactivated. A rule may be deactivated in order to test the rule or as a reminder of rules that have been in use.



3. Save your changes. See: [Saving Changes](#)

6.2.3.2 Setting Talker Rules

Talker Rules allow the user to set the direction and permission for traffic from a specific upstream device (e.g.: FS-HMI-0001) or network to the selected node (e.g.: FS-PLC-0001). For example, if the user wants to allow Modbus/TCP traffic between a specific HMI to a protected PLC, a Talker Rule can be used. Talker Rules can also be used for a group of devices if the talker selected is a network node that is a parent to a number of devices.

When a Talker is added to the Talker Rules section of a protected device, the Tofino CMP automatically calculates what protocols the two devices have in common, based on the node's settings in the device database. It then automatically builds a list of allowed protocols. You can delete any protocols you don't feel are appropriate or add new protocols (see below).

To set Talker Rules:

- Decide if you want to add a Protocol or a Special Rule to the Talker Rules list for your selected Node.

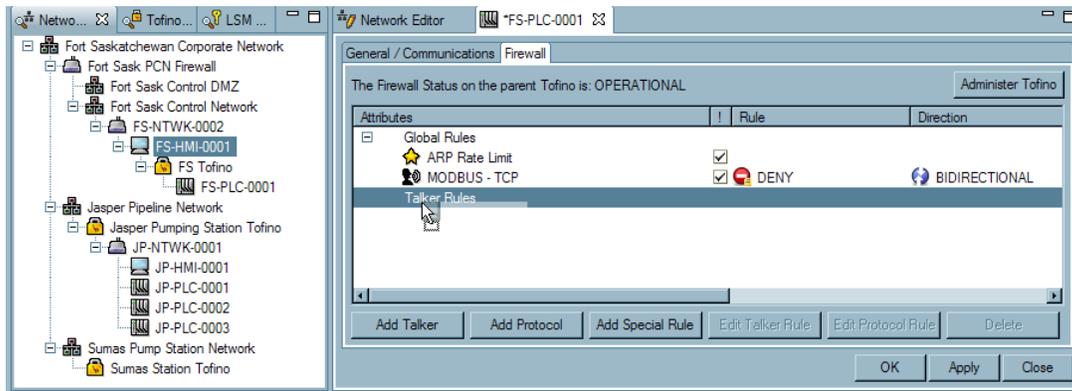
See: [Basic Firewall Concept](#)

See: [Drag and Drop Protocol](#)

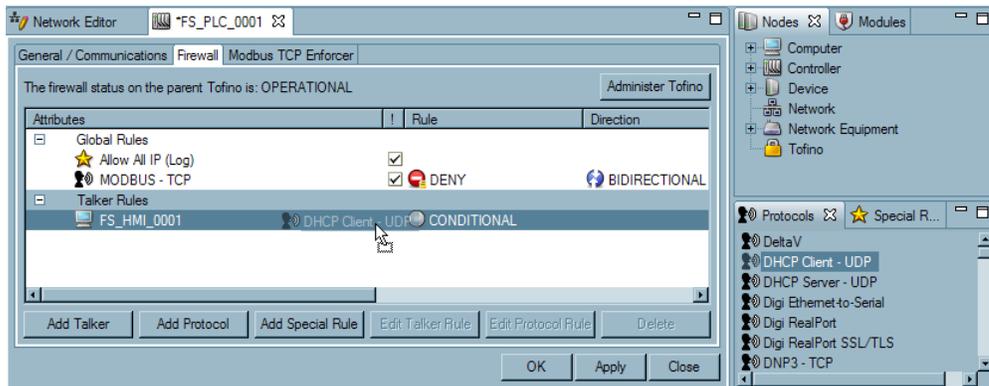
See: [Drag and Drop Special Rule](#)

Drag and Drop Protocol

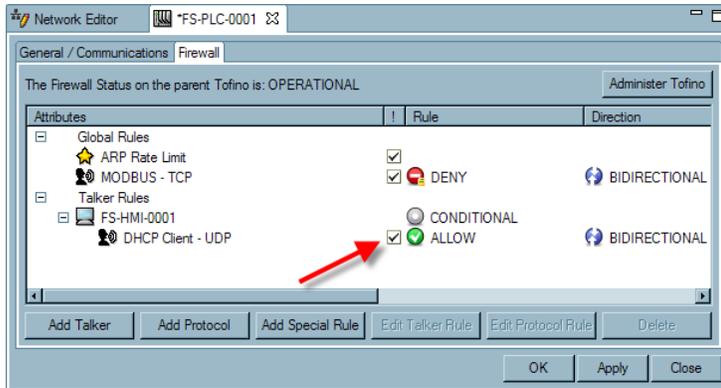
- First, drag a talker from the Network View window and drop it on the Talker Rules text.



- Now, drag a protocol from the Protocols View and drop it on the talker (i.e.: FS-HMI-0001).



- The rule should now appear under Talker Rules. The checked box is where the rule is activated or deactivated. A checked box means the rule is activated. An unchecked box indicates the rule is deactivated. A rule may be deactivated in order to test the rule or as a reminder of rules that have been in use.

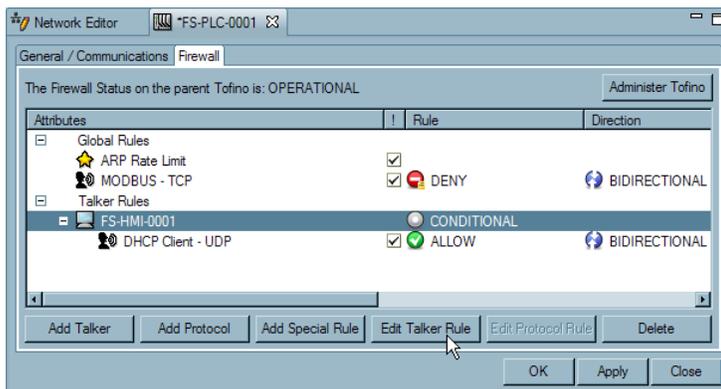


To Edit a Talker Rule see: [Editing a Talker Rule](#)

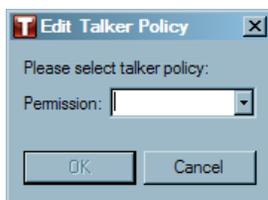
To Edit a Protocol Rule see: [Editing a Protocol Rule](#)

Editing a Talker Rule

- To edit the Talker Rule's permission, select the Talker, and click the "Edit Talker Rule" button. Or Right Click on the Talker and select Edit Talker Rule.



- An Edit Talker Policy window will open.

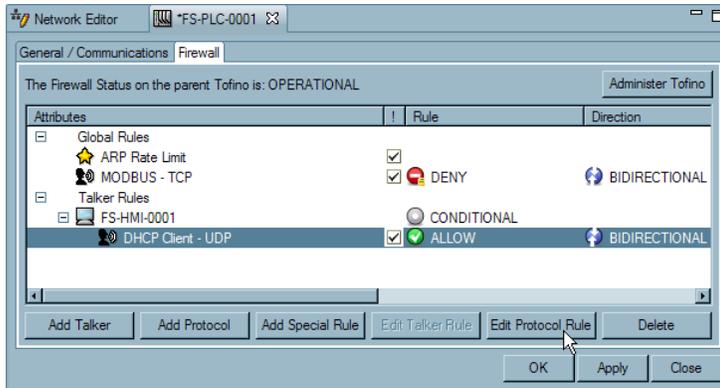


- Select the default permission for the Talker. There are five types of default permissions:
 - ▶ Allow: Traffic matching the rule is allowed through the Tofino SA with no logging or alarms reported to the Tofino CMP.
 - ▶ Allow Log: Traffic matching the rule is allowed through the Tofino SA. This traffic is logged and exception heartbeats are generated.
 - ▶ Conditional: Traffic will only be allowed if it matches a Talker firewall rule that has its permission set to Allow or Allow_Log.
 - ▶ Deny No Log: Traffic matching the rule is blocked by the Tofino SA with no logging or alarms reported to the Tofino CMP.
 - ▶ Deny: Traffic matching the rule is blocked by the Tofino SA. This traffic is logged and exception heartbeats are generated.

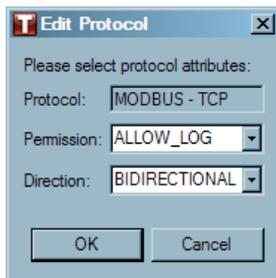


Editing a Protocol Rule

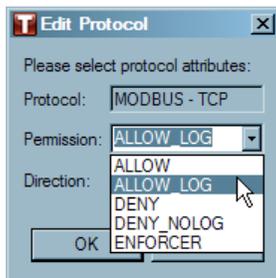
- To edit the Protocol rule, select the protocol, and click the "Edit Protocol Rule" button. Or Right Click on the Protocol and select "Edit Protocol Rule".



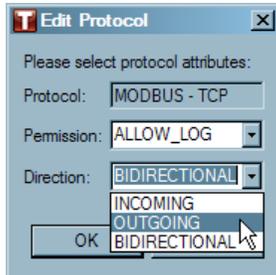
- An Edit Protocol window will open.



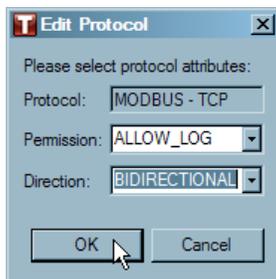
- Select the Permission for the rule. There are five types of Permissions:
 - ▶ Allow: Traffic matching the rule is allowed through the Tofino SA with no logging or alarms reported to the Tofino CMP.
 - ▶ Allow Log: Traffic matching the rule is allowed through the Tofino SA. This traffic is logged and exception heartbeats are generated.
 - ▶ Deny No Log: Traffic matching the rule is blocked by the Tofino SA with no logging or alarms reported to the Tofino CMP.
 - ▶ Deny: Traffic matching the rule is blocked by the Tofino SA. This traffic is logged and exception heartbeats are generated.
 - ▶ Enforcer: Traffic will be filtered based on Deep Packet Inspection settings. This option is only available when using Enforcer LSMs.



- Select the Direction that the network connection will originate from:
 - ▶ Bidirectional: Connection initiation is allowed from either side of the Tofino SA.
 - ▶ Incoming: Connection initiation is allowed only from the untrusted side of the Tofino SA.
 - ▶ Outgoing: Connection initiation is allowed only from the trusted side of the Tofino SA.



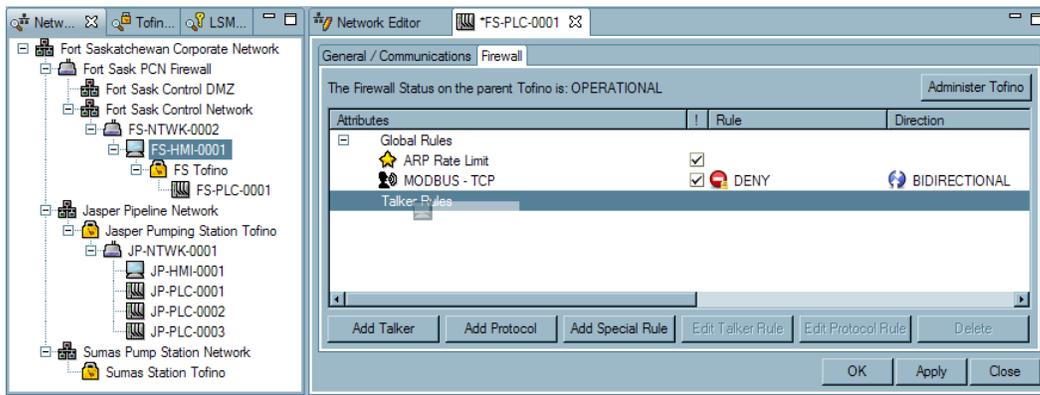
- Click "OK".



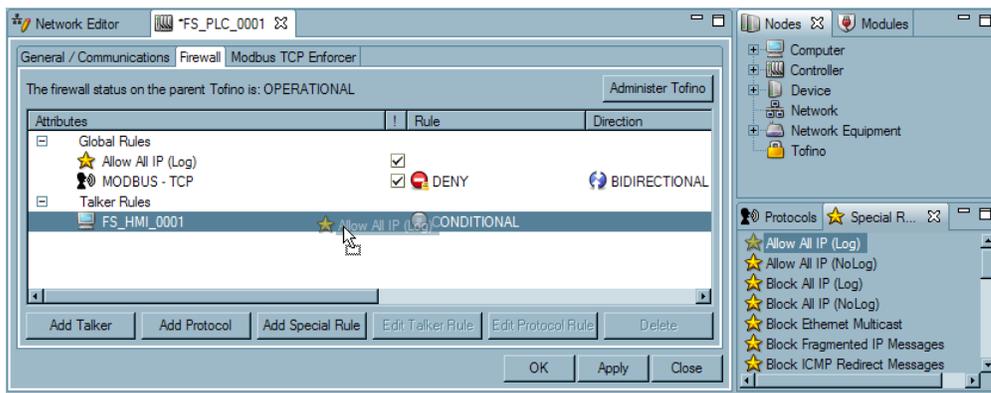
- Save your changes. See: [Saving Changes](#)

Drag and Drop Special Rule

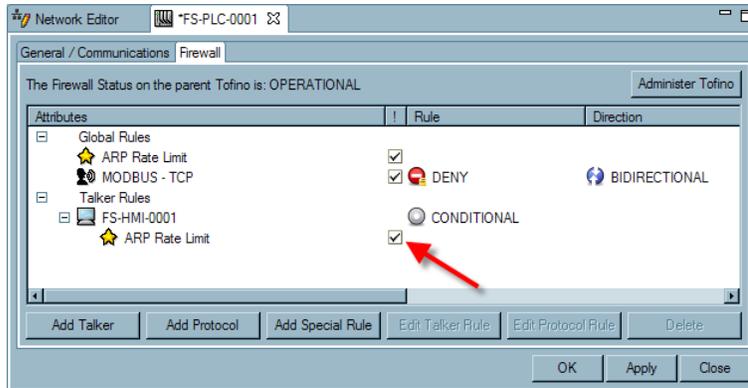
- First, drag a talker from the Network View window and drop it on the Talker Rules text.



- Now drag a Special Rule from the Special Rules window.



- The rule should now appear under Talker Rules. The checked box is where the rule is activated or deactivated. A checked box means the rule is activated. An unchecked box indicates the rule is deactivated. A rule may be deactivated in order to test the rule or as a reminder of rules that have been in use.



- The Talker Rules can now be edited. See: [Editing a Talker Rule](#)
- Save your changes. See: [Saving Changes](#)

6.2.4 Firewall Rule Configuration of a Tofino SA

Before firewall rules can be configured, there must be a Firewall LSM installed on the Tofino SA. See: [Adding an LSM to a Tofino SA](#)

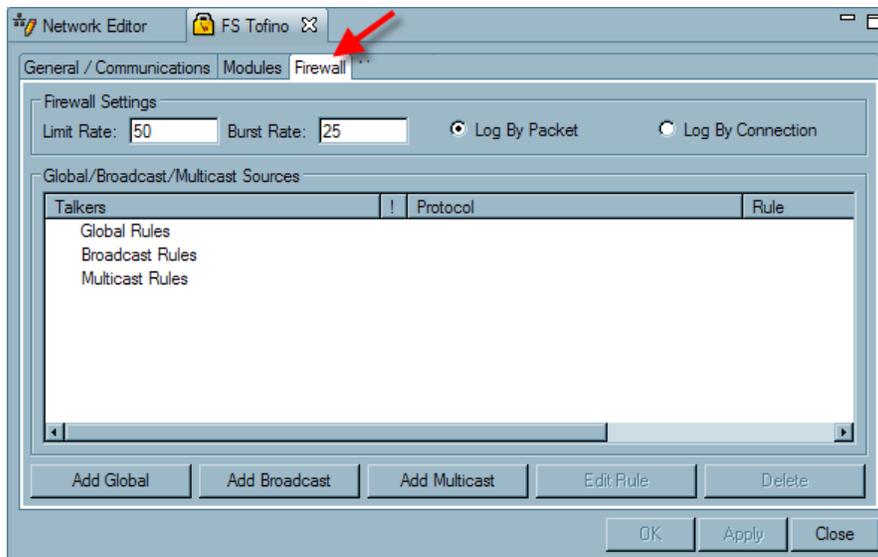
There are two sections on the Firewall tab. These are:

- ▶ Firewall Settings: Provides controls on the events and alarms sent by the Tofino Firewall LSM when packets are denied and logged or allowed and logged. See: [Firewall Log Settings](#)
- ▶ Rule Settings: Allows you to set rules on the Tofino SA that affect all devices protected by this Tofino SA. See: [Configuring Firewall Rules](#).

Configuring Firewall Rules

To configure firewall rules for a Tofino SA complete the following steps:

- From the Network Editor or the Network View window, double click the icon of the Tofino SA you want to configure, and select the Firewall tab.



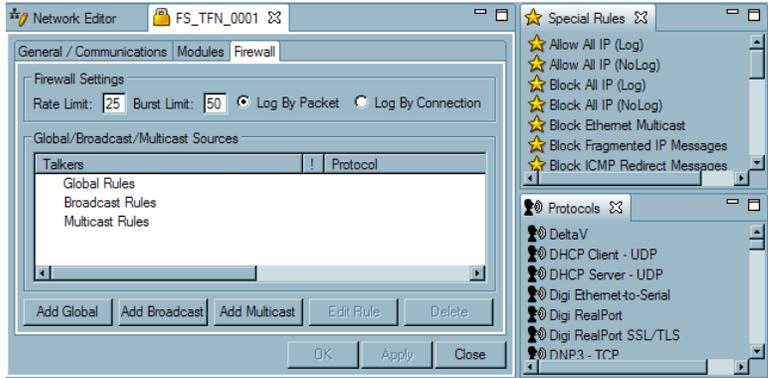
- There are three types of firewall rules that can be added to a Tofino SA: [Global Rules](#), [Broadcast Rules](#) and [Multicast Rules](#). Decide which type of rule to add.
 - ▶ See: [Setting Global Rules](#)
 - ▶ See: [Setting Broadcast Rules](#)
 - ▶ See: [Setting Multicast Rules](#)

6.2.4.1 Setting Global Rules

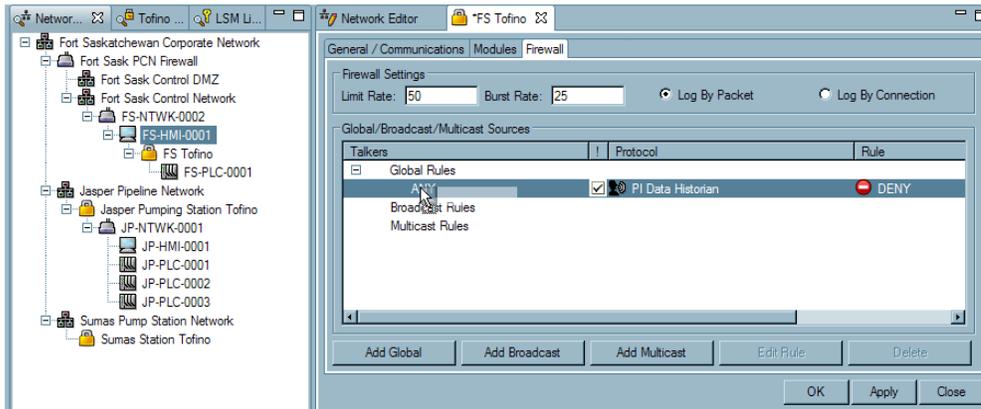
- Decide if you want to add a Protocol or a Special Rule to the Global Rules list for your selected Tofino SA. See: [Basic Firewall Concepts](#)
 - ▶ [Drag and Drop Protocol](#)
 - ▶ [Drag and Drop Special Rule](#)

Drag and Drop Protocol

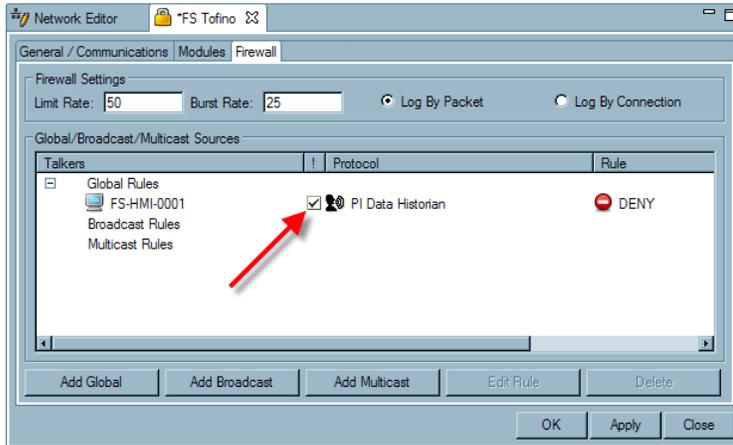
- Drag and drop a protocol from the protocol window onto the Global Rule text.



- Drag and drop a device from the Network View window onto the protocol.



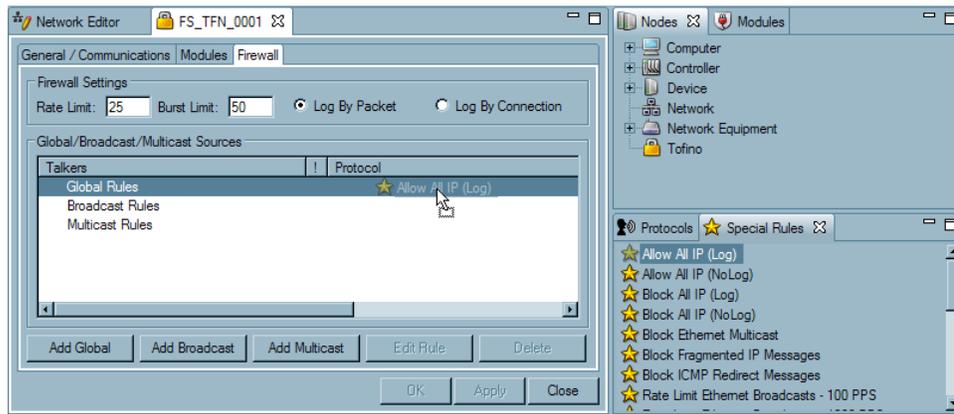
- The rule should now appear under Global Rules. The checked box is where the rule is activated or deactivated. A checked box means the rule is activated. An unchecked box indicates the rule is deactivated. A rule may be deactivated in order to test the rule or as a reminder of rules that have been in use.



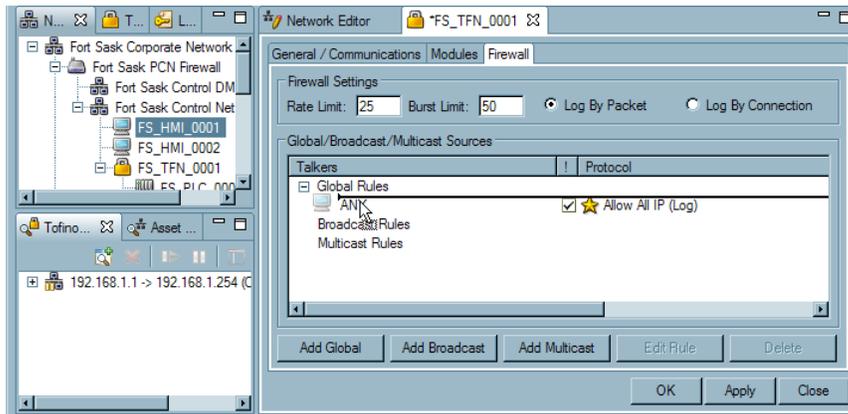
- Save your changes. See: [Saving Changes](#)

Drag and Drop Special Rule

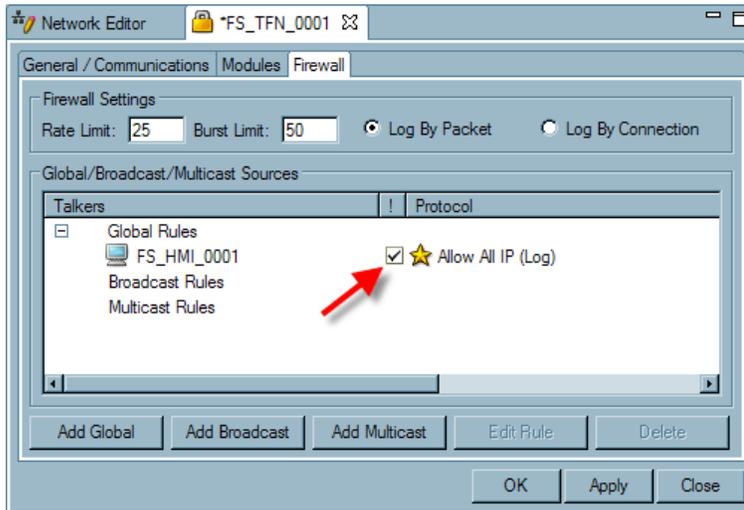
- Drag and drop a Special Rule from the Special Rule window onto the *Global Rule* text.



- Drag and drop a device from the Network View window onto the protocol.



- The rule should now appear under Global Rules. The checked box is where the rule is activated or deactivated. A checked box means the rule is activated. An unchecked box indicates the rule is deactivated. A rule may be deactivated in order to test the rule or as a reminder of rules that have been in use.



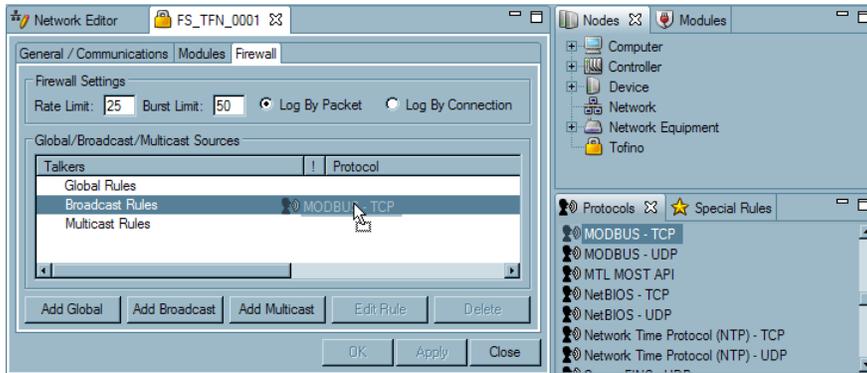
- Save your changes. See: [Saving Changes](#)

6.2.4.2 Setting Broadcast Rules

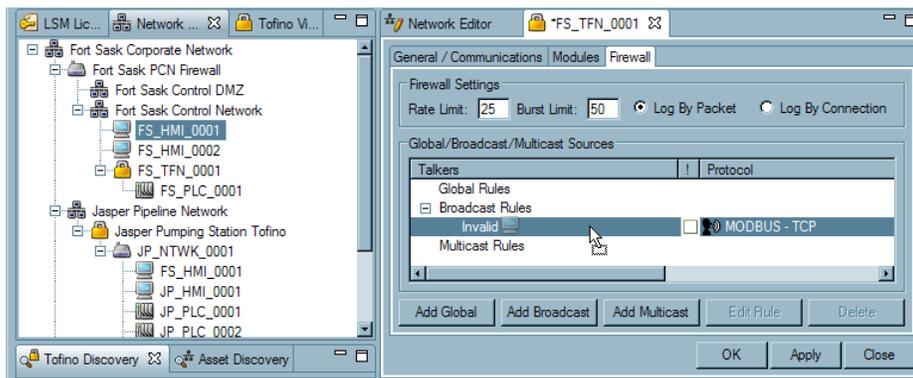
- Decide if you want to add a Protocol or a Special Rule to the Broadcast Rules list for your selected Tofino SA. See: [Basic Firewall Concepts](#)
 - ▶ [Drag and Drop Protocol](#)
 - ▶ [Drag and Drop Special Rule](#)

Drag and Drop Protocol

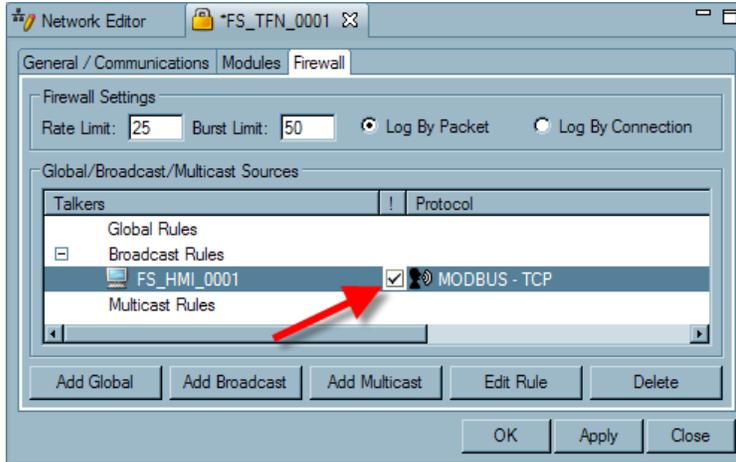
- Drag and drop a protocol from the protocol window onto the Broadcast Rule text.



- Drag and drop a device from the Network View window onto the protocol.



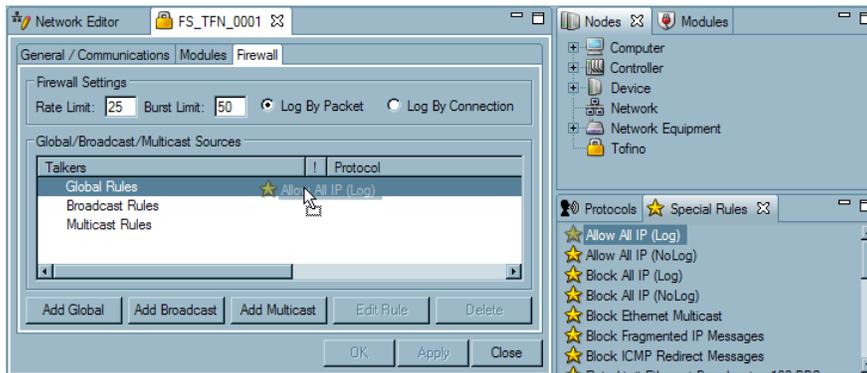
- The rule should now appear under Broadcast Rules. The checked box is where the rule is activated or deactivated. A checked box means the rule is activated. An unchecked box indicates the rule is deactivated. A rule may be deactivated in order to test the rule or as a reminder of rules that have been in use.



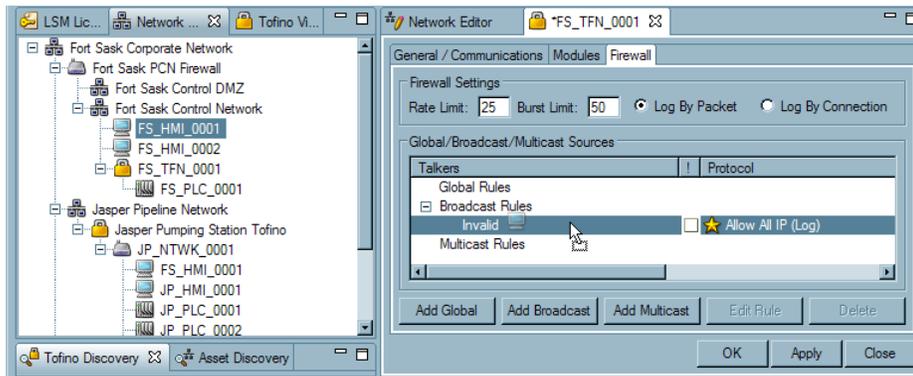
- Click "OK" or "Apply" to save your changes. See: [Saving Changes](#)

Drag and Drop Special Rule

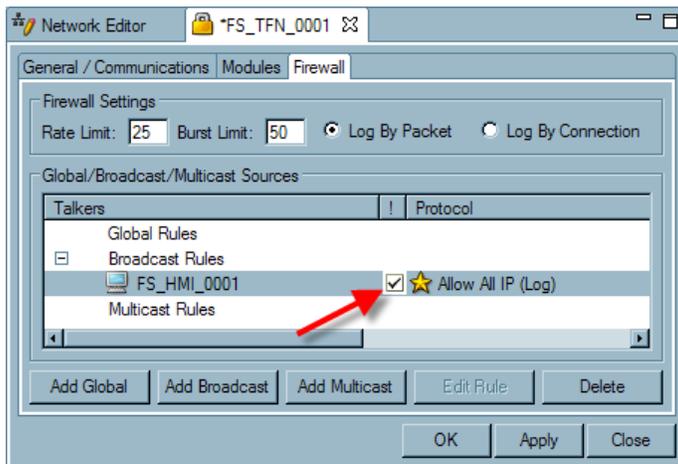
- Drag and drop a Special Rule from the Special Rule window onto the Global Rule text.



- Drag and drop a device from the Network View window onto the protocol.



- The rule should now appear under Global Rules. The checked box is where the rule is activated or deactivated. A checked box means the rule is activated. An unchecked box indicates the rule is deactivated. A rule may be deactivated in order to test the rule or as a reminder of rules that have been in use.



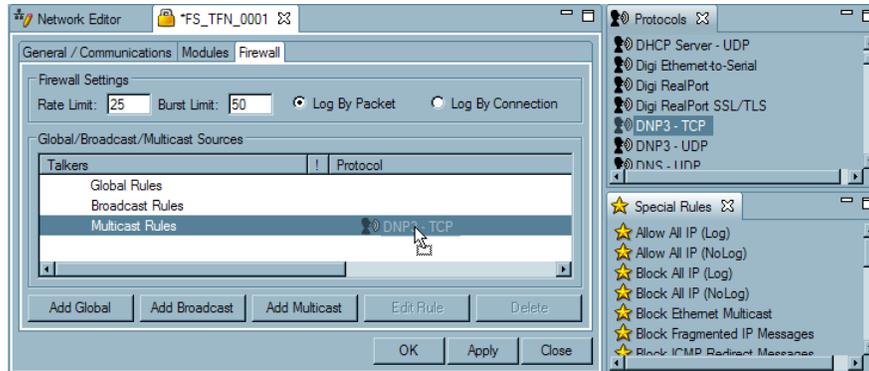
- Save your changes. See: [Saving Changes](#)

6.2.4.3 Setting Multicast Rules

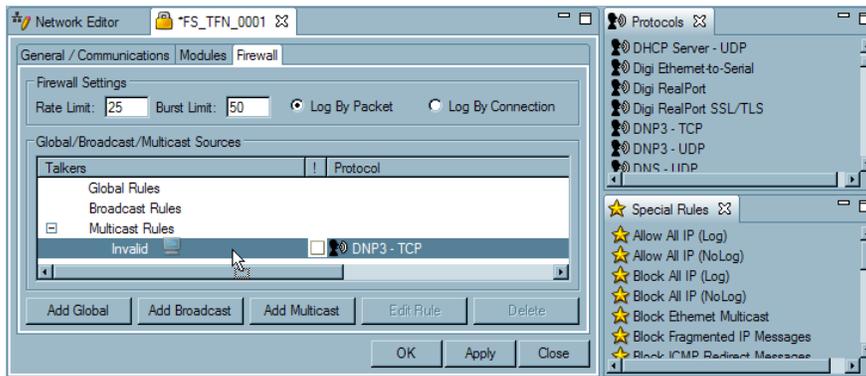
- Decide if you want to add a Protocol or a Special Rule to the Multicast Rules list for your selected Tofino SA. See: [Basic Firewall Concepts](#)
 - ▶ [Drag and Drop Protocol](#)
 - ▶ [Drag and Drop Special Rule](#)

Drag and Drop Protocol

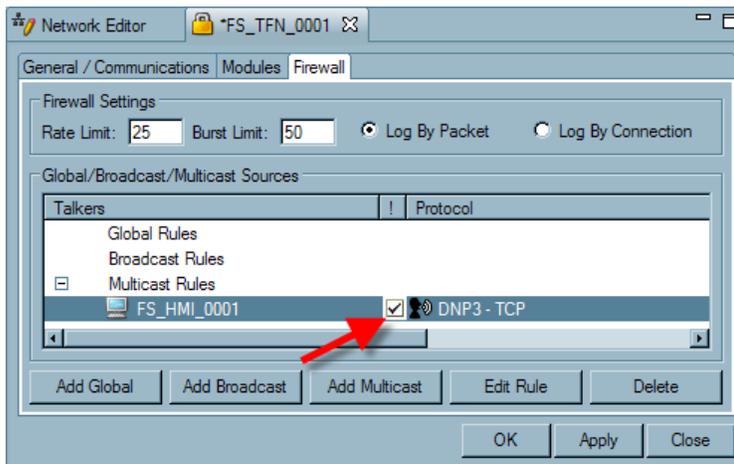
- Drag and drop a protocol from the protocol window onto the Multicast Rule text.



- Drag and drop a Node from the Network View window onto the protocol.



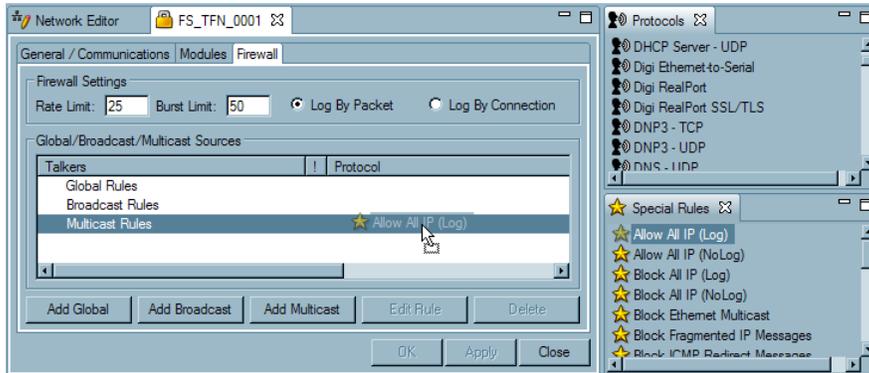
- The rule should now appear under Multicast Rules. The checked box is where the rule is activated or deactivated. A checked box means the rule is activated. An unchecked box indicates the rule is deactivated. A rule may be deactivated in order to test the rule or as a reminder of rules that have been in use.



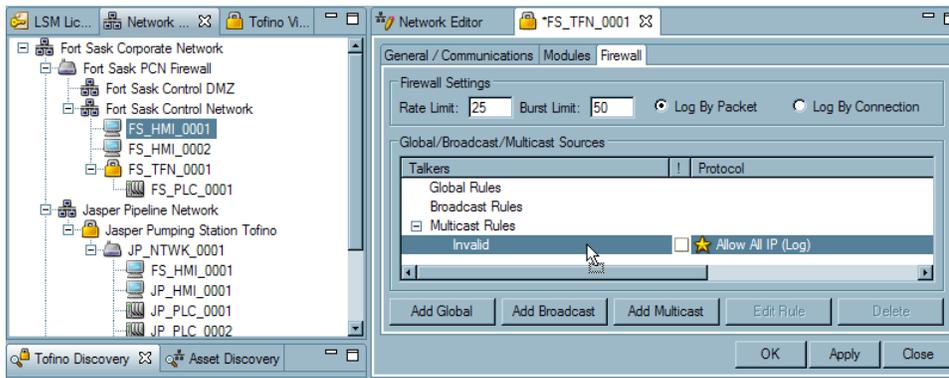
- Save your changes. See: [Saving Changes](#)

Drag and Drop Special Rule

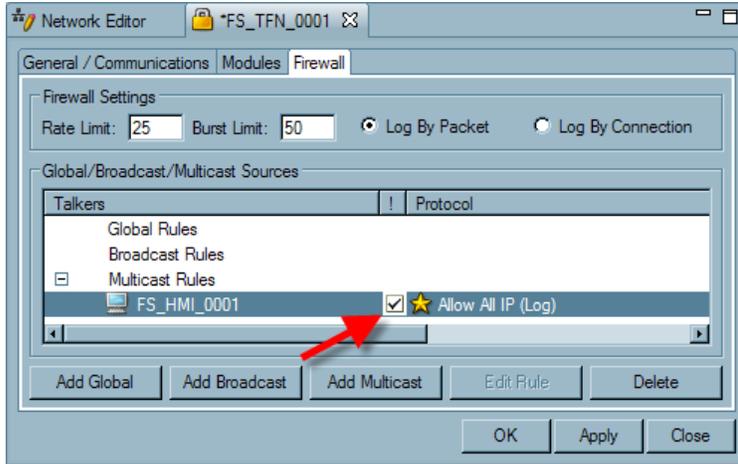
- Drag and drop a Special Rule from the Special Rule window onto the Multicast Rule text.



- Drag and drop a Node from the Network View window onto the Special Rule.



- The rule should now appear under Global Rules. The checked box is where the rule is activated or deactivated. A checked box means the rule is activated. An unchecked box indicates the rule is deactivated. A rule may be deactivated in order to test the rule or as a reminder of rules that have been in use.



- Save your changes. See: [Saving Changes](#)

6.3 Secure Asset Management LSM

6.3.1 About Asset Discovery

What is Asset Discovery?

Asset Discovery uses the Secure Asset Management [LSM](#) that can be installed on Tofino SAs to help the user "discover" what assets (nodes) are on the network. See: [Adding an LSM to a Tofino SA](#)

How does Asset Discovery work?

Once the Secure Asset Management LSM is added to and activated on the Tofino SA, the Tofino CMP begins receiving [exception heartbeats](#) from Tofino SAs in the field regarding nodes on the network.

Tofino SAs analyze network traffic passing through them and report back to the Tofino CMP in the form of an exception heartbeat, any new nodes on the network.

Note: These exception heartbeats do not show up in the [Event View](#) of the Tofino CMP.

Where do I see what Assets are being discovered?

The newly discovered assets are listed in the [Asset Discovery view](#).

When the Secure Asset Management LSM is first activated, all nodes on the network will show up in the Asset Discovery view. After the initial discovery however, only new nodes on the network will show up in the Asset Discovery view.

What happens once all my assets have been discovered?

The Secure Asset Management LSM continues to search for new nodes until it is deactivated or until the Tofino SA that it is installed on is put into decommissioned mode.

Can Asset Discovery impact my control operations in any way?

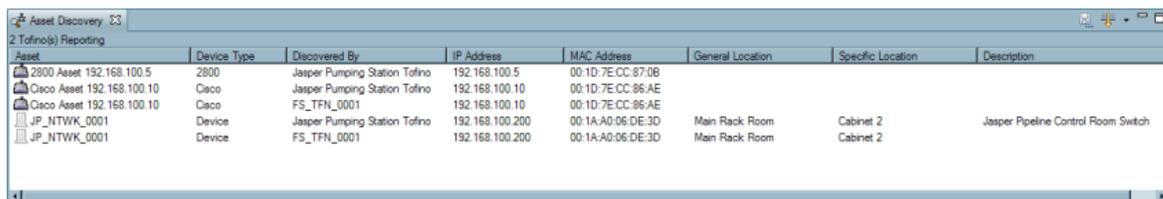
Absolutely not. The Tofino Secure Asset Management LSM uses an innovative technique that does not generate any network traffic.

Why do I see the same asset shown more than once in the Asset Discovery view?

Each Tofino SA that discovers an asset will report it in the Asset Discovery view. Thus if three Tofino SAs discover the same asset, it will appear three times in the view. However, once the asset is deployed into the network diagram all instances of it will be hidden.

6.3.2 Using Asset Discovery

Once the Secure Asset Management LSM has been installed and activated on an operational Tofino SA it will automatically begin to populate a list of "discovered" nodes in the Asset Discovery view. The Secure Asset Management LSM will continue to search for nodes, until it is deactivated or until the Tofino SA is put into decommissioned mode. See: [Adding an LSM to a Tofino SA](#)



The screenshot shows a window titled "Asset Discovery" with a sub-header "2 Tofino(s) Reporting". Below this is a table with the following columns: Asset, Device Type, Discovered By, IP Address, MAC Address, General Location, Specific Location, and Description. The table contains five rows of data.

Asset	Device Type	Discovered By	IP Address	MAC Address	General Location	Specific Location	Description
2800 Asset 192.168.100.5	2800	Jasper Pumping Station Tofino	192.168.100.5	00:1D:7E:CC:87:0B			
Cisco Asset 192.168.100.10	Cisco	Jasper Pumping Station Tofino	192.168.100.10	00:1D:7E:CC:86:AE			
Cisco Asset 192.168.100.10	Cisco	FS_TFN_0001	192.168.100.10	00:1D:7E:CC:86:AE			
JP_NTWK_0001	Device	Jasper Pumping Station Tofino	192.168.100.200	00:1A:A0:06:DE:3D	Main Rack Room	Cabinet 2	Jasper Pipeline Control Room Switch
JP_NTWK_0001	Device	FS_TFN_0001	192.168.100.200	00:1A:A0:06:DE:3D	Main Rack Room	Cabinet 2	

See: [Asset Discovery View Explained](#)

See: [Asset Discovery Right Click Menu](#)

See: [Adding Discovered Nodes to the Network Diagram](#)

Note: If a Tofino SA is configured using an IP address it will show up in the Asset Discovery view greyed out.

If you have discovered a Tofino SA using Asset Discovery and then delete or change that Tofino SA's IP address, the discovered Tofino SA will show up as an available device in the Asset Discovery list. It will have the same MAC address as the greyed out Tofino SA.

Asset Discovery View Explained

- Lists the number of Tofino SAs reporting on the network with the Secure Asset Management LSM installed.

Asset	Device Type	Discovered By
2800 Asset 192.168.100.5	2800	Jasper Pumping Station Tofino
Cisco Asset 192.168.100.10	Cisco	Jasper Pumping Station Tofino
Cisco Asset 192.168.100.10	Cisco	FS_TFN_0001
JP_NTWK_0001	Device	Jasper Pumping Station Tofino
JP_NTWK_0001	Device	FS_TFN_0001

- Allows the user to either show or hide the assets that are already in the network diagram (greyed out). **Note:** The default setting is for nodes that are already in the network diagram (greyed out) to be hidden. This menu also allows the user to show or hide duplicate nodes discovered on the network.

Asset	Device Type	Discover
2800 Asset 192.168.100.5	2800	Jasper Pumping Station
Cisco Asset 192.168.100.10	Cisco	Jasper Pumping Station
Cisco Asset 192.168.100.10	Cisco	FS_TFN_0001
JP_NTWK_0001	Device	Jasper Pumping Station
JP_NTWK_0001	Device	FS_TFN_0001

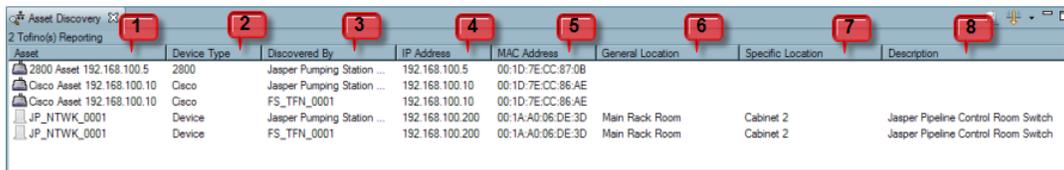
- This button allows the user to export the list of discovered assets to a .csv file. **Note:** The spreadsheet will be filtered and ordered as per the current Asset Discovery view. For example, if you do not want duplicate Nodes in a spreadsheet, then you will need to ensure that duplicates are not shown in the Asset Discovery view.

Asset	Device Type	Discovered By
2800 Asset 192.168.100.5	2800	Jasper Pumping Station
Cisco Asset 192.168.100.10	Cisco	Jasper Pumping Station
Cisco Asset 192.168.100.10	Cisco	FS_TFN_0001
JP_NTWK_0001	Device	Jasper Pumping Station
JP_NTWK_0001	Device	FS_TFN_0001

The Asset Discovery view has eight columns:

- ▶ See: [Asset Column](#)
- ▶ See: [Device Type Column](#)
- ▶ See: [Discovered By Column](#)
- ▶ See: [IP Address Column](#)
- ▶ See: [MAC Address Column](#)
- ▶ See: [General Location Column](#)
- ▶ See: [Specific Location Column](#)
- ▶ See: [Description Column](#)

Note: The columns can be sorted by clicking on the column header. Clicking the column sorts them in ascending order. Clicking the column again will sort them in descending order.

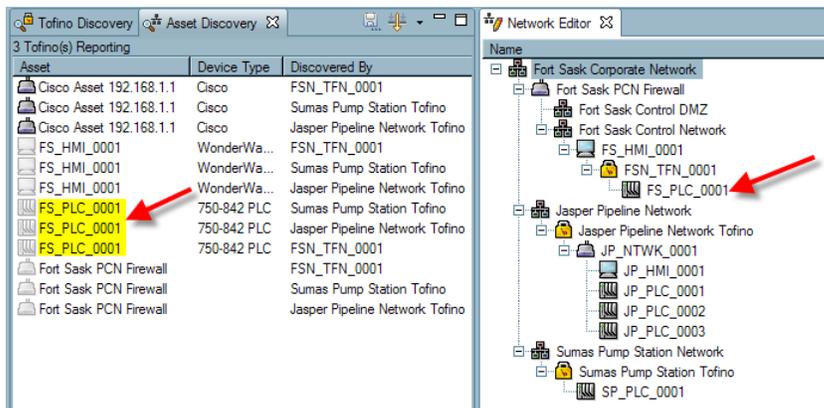


Asset	Device Type	Discovered By	IP Address	MAC Address	General Location	Specific Location	Description
2800 Asset 192.168.100.5	2800	Jasper Pumping Station ...	192.168.100.5	00:1D:7E:CC:87:0B			
Cisco Asset 192.168.100.10	Cisco	Jasper Pumping Station ...	192.168.100.10	00:1D:7E:CC:86:AE			
Cisco Asset 192.168.100.10	Cisco	FS_TFN_0001	192.168.100.10	00:1D:7E:CC:86:AE			
JP_NTWK_0001	Device	Jasper Pumping Station ...	192.168.100.200	00:1A:A0:06:DE:3D	Main Rack Room	Cabinet 2	Jasper Pipeline Control Room Switch
JP_NTWK_0001	Device	FS_TFN_0001	192.168.100.200	00:1A:A0:06:DE:3D	Main Rack Room	Cabinet 2	Jasper Pipeline Control Room Switch

Asset Column

This column lists the nodes that are discovered on the network. The Tofino CMP will list the discovered nodes in three possible ways:

- If a discovered node's IP address matches that of a node already present in the network diagram in the Network Editor, then the name displayed in the Asset Discovery view will be taken from the network diagram and the icon will either be hidden or greyed out.



The screenshot displays two windows side-by-side. On the left is the 'Tofino Discovery' window, which has a table with three columns: 'Asset', 'Device Type', and 'Discovered By'. The 'Asset' column lists various nodes, including 'FS_PLC_0001' which is highlighted in yellow. On the right is the 'Network Editor' window, showing a hierarchical network diagram. A red arrow points to a node labeled 'FS_PLC_0001' in the diagram, which is highlighted in red, indicating it is the same node as the one highlighted in the Tofino Discovery window.

- If the discovered node is not already in the network diagram, the Tofino CMP will attempt to name the node by analyzing the node's traffic characteristics and comparing them to a database of known device types. If a match is found the node will be named based on the match in the database in this format: <Vendor> <IP Address>.

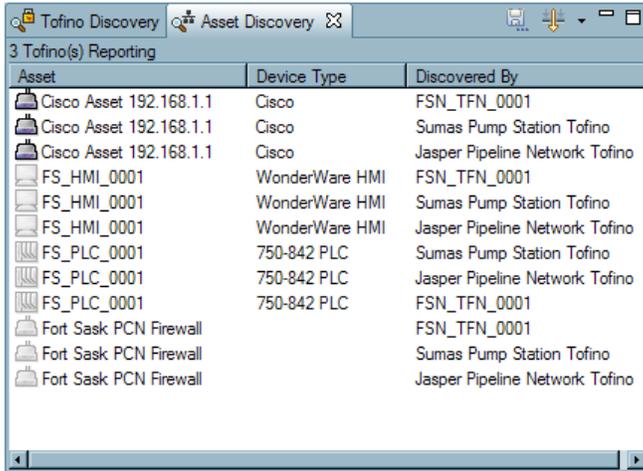
Asset	Device Type	Discovered By
Cisco Asset 192.168.1.1	Cisco	FSN_TFN_0001
Cisco Asset 192.168.1.1	Cisco	Sumas Pump Station Tofino
Cisco Asset 192.168.1.1	Cisco	Jasper Pipeline Network Tofino
FS_HMI_0001	WonderWa...	FSN_TFN_0001
FS_HMI_0001	WonderWa...	Sumas Pump Station Tofino
FS_HMI_0001	WonderWa...	Jasper Pipeline Network Tofino
FS_PLC_0001	750-842 PLC	Sumas Pump Station Tofino
FS_PLC_0001	750-842 PLC	Jasper Pipeline Network Tofino
FS_PLC_0001	750-842 PLC	FSN_TFN_0001
Fort Sask PCN Firewall		FSN_TFN_0001
Fort Sask PCN Firewall		Sumas Pump Station Tofino
Fort Sask PCN Firewall		Jasper Pipeline Network Tofino

- If the first two methods are unsuccessful the node will be named: Asset <IP address>. This most commonly occurs with devices that are general purpose computers or unusual control products. If you think the Tofino Asset Discovery feature is not correctly identifying a control device, contact your local sales representative.

Asset	Device Type	Discovered By
Asset 192.168.1.101		Tofino 00:00:11:8D:95:14
Asset 192.168.1.101		Jasper Pumping Station Tofino
Asset 192.168.1.101		FS_TFN_0001
Cisco Asset 192.168.1.1	Cisco	Tofino 00:00:11:8D:95:14
Cisco Asset 192.168.1.1	Cisco	Jasper Pumping Station Tofino
Cisco Asset 192.168.1.1	Cisco	FS_TFN_0001
FS_PLC_0001	750-842 PLC	Jasper Pumping Station Tofino
FS_PLC_0001	750-842 PLC	Tofino 00:00:11:8D:95:14
FS_PLC_0001	750-842 PLC	FS_TFN_0001
Linksys Asset 192.168.1.12	Wireless AP	FS_TFN_0001
Linksys Asset 192.168.1.12	Wireless AP	Jasper Pumping Station Tofino
Linksys Asset 192.168.1.12	Wireless AP	Tofino 00:00:11:8D:95:14

Device Type Column

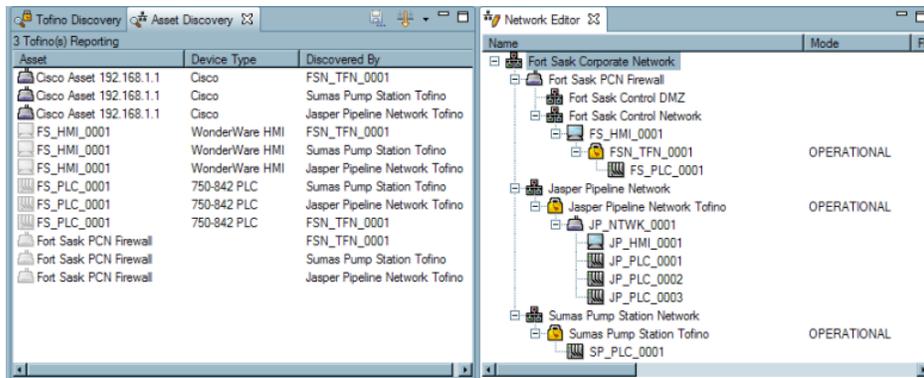
This column displays what type of device the node is. This entry should be verified by the user and adjusted as appropriate. Once a discovered node is deployed in the network diagram, the type can not be changed, so it is important that it is set correctly here. See: [Adding Discovered Assets to the Network Diagram](#)



Asset	Device Type	Discovered By
Cisco Asset 192.168.1.1	Cisco	FSN_TFN_0001
Cisco Asset 192.168.1.1	Cisco	Sumas Pump Station Tofino
Cisco Asset 192.168.1.1	Cisco	Jasper Pipeline Network Tofino
FS_HMI_0001	WonderWare HMI	FSN_TFN_0001
FS_HMI_0001	WonderWare HMI	Sumas Pump Station Tofino
FS_HMI_0001	WonderWare HMI	Jasper Pipeline Network Tofino
FS_PLC_0001	750-842 PLC	Sumas Pump Station Tofino
FS_PLC_0001	750-842 PLC	Jasper Pipeline Network Tofino
FS_PLC_0001	750-842 PLC	FSN_TFN_0001
Fort Sask PCN Firewall		FSN_TFN_0001
Fort Sask PCN Firewall		Sumas Pump Station Tofino
Fort Sask PCN Firewall		Jasper Pipeline Network Tofino

Discovered By Column

Lists the Tofino SA that "discovered" the node on the network.

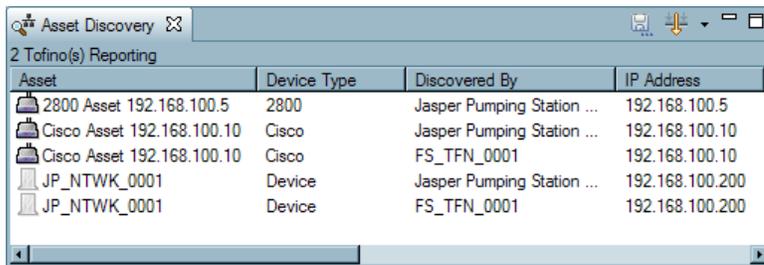


Asset	Device Type	Discovered By
Cisco Asset 192.168.1.1	Cisco	FSN_TFN_0001
Cisco Asset 192.168.1.1	Cisco	Sumas Pump Station Tofino
Cisco Asset 192.168.1.1	Cisco	Jasper Pipeline Network Tofino
FS_HMI_0001	WonderWare HMI	FSN_TFN_0001
FS_HMI_0001	WonderWare HMI	Sumas Pump Station Tofino
FS_HMI_0001	WonderWare HMI	Jasper Pipeline Network Tofino
FS_PLC_0001	750-842 PLC	Sumas Pump Station Tofino
FS_PLC_0001	750-842 PLC	Jasper Pipeline Network Tofino
FS_PLC_0001	750-842 PLC	FSN_TFN_0001
Fort Sask PCN Firewall		FSN_TFN_0001
Fort Sask PCN Firewall		Sumas Pump Station Tofino
Fort Sask PCN Firewall		Jasper Pipeline Network Tofino

Name	Mode	Plc
Fort Sask Corporate Network		
Fort Sask PCN Firewall		
Fort Sask Control DMZ		
Fort Sask Control Network		
FS_HMI_0001		
FS_PLC_0001	OPERATIONAL	
Jasper Pipeline Network		
Jasper Pipeline Network Tofino	OPERATIONAL	
JP_NTWK_0001		
JP_HMI_0001		
JP_PLC_0001		
JP_PLC_0002		
JP_PLC_0003		
Sumas Pump Station Network		
Sumas Pump Station Tofino	OPERATIONAL	
SP_PLC_0001		

IP Address Column

Lists the IP address of the discovered node.

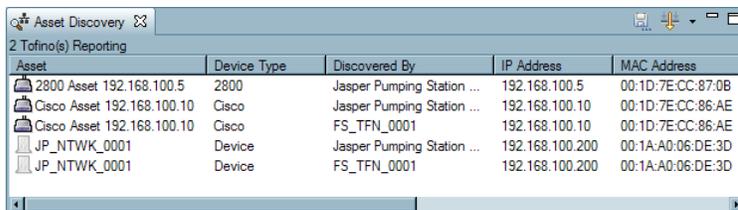


The screenshot shows a window titled "Asset Discovery" with a sub-header "2 Tofino(s) Reporting". It contains a table with the following data:

Asset	Device Type	Discovered By	IP Address
2800 Asset 192.168.100.5	2800	Jasper Pumping Station ...	192.168.100.5
Cisco Asset 192.168.100.10	Cisco	Jasper Pumping Station ...	192.168.100.10
Cisco Asset 192.168.100.10	Cisco	FS_TFN_0001	192.168.100.10
JP_NTWK_0001	Device	Jasper Pumping Station ...	192.168.100.200
JP_NTWK_0001	Device	FS_TFN_0001	192.168.100.200

MAC Address Column

Lists the MAC address of the discovered node.

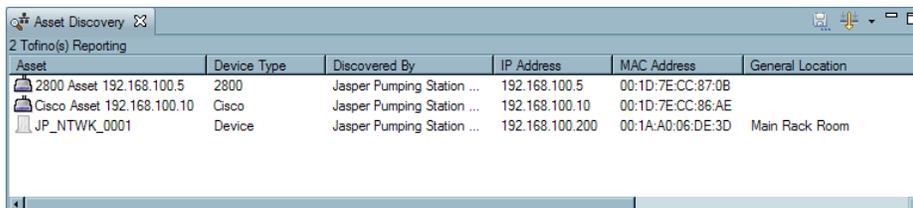


The screenshot shows a window titled "Asset Discovery" with a sub-header "2 Tofino(s) Reporting". It contains a table with the following data:

Asset	Device Type	Discovered By	IP Address	MAC Address
2800 Asset 192.168.100.5	2800	Jasper Pumping Station ...	192.168.100.5	00:1D:7E:CC:87:0B
Cisco Asset 192.168.100.10	Cisco	Jasper Pumping Station ...	192.168.100.10	00:1D:7E:CC:86:AE
Cisco Asset 192.168.100.10	Cisco	FS_TFN_0001	192.168.100.10	00:1D:7E:CC:86:AE
JP_NTWK_0001	Device	Jasper Pumping Station ...	192.168.100.200	00:1A:A0:06:DE:3D
JP_NTWK_0001	Device	FS_TFN_0001	192.168.100.200	00:1A:A0:06:DE:3D

General Location Column

Once the Node has been added into the network diagram, and the General Location of the node has been specified in the Node's Properties page, the location will be displayed in this column.

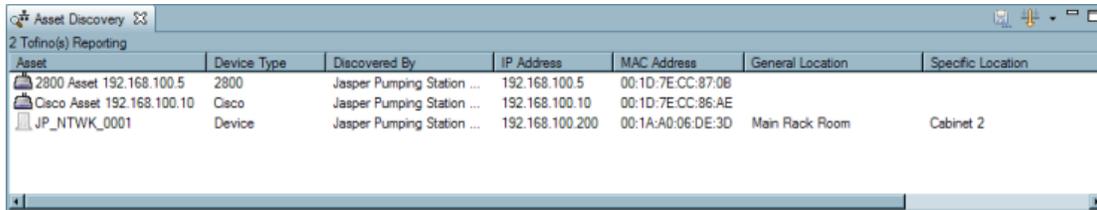


The screenshot shows a window titled "Asset Discovery" with a sub-header "2 Tofino(s) Reporting". It contains a table with the following data:

Asset	Device Type	Discovered By	IP Address	MAC Address	General Location
2800 Asset 192.168.100.5	2800	Jasper Pumping Station ...	192.168.100.5	00:1D:7E:CC:87:0B	
Cisco Asset 192.168.100.10	Cisco	Jasper Pumping Station ...	192.168.100.10	00:1D:7E:CC:86:AE	
JP_NTWK_0001	Device	Jasper Pumping Station ...	192.168.100.200	00:1A:A0:06:DE:3D	Main Rack Room

Specific Location Column

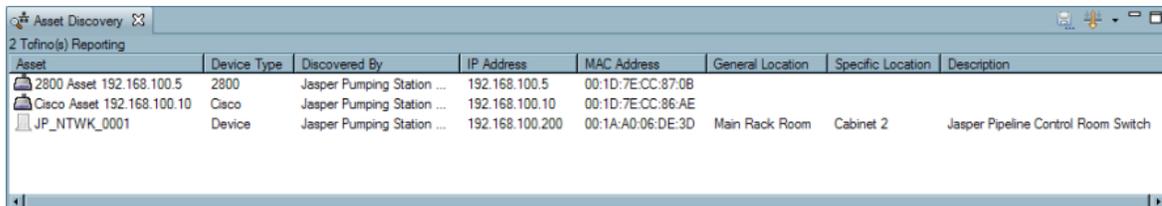
Once the Node has been added into the network diagram, and the Specific Location of the Node has been specified in the Node's Properties page, the location will be displayed in this column.



Asset	Device Type	Discovered By	IP Address	MAC Address	General Location	Specific Location
2800 Asset 192.168.100.5	2800	Jasper Pumping Station ...	192.168.100.5	00:1D:7E:CC:87:0B		
Cisco Asset 192.168.100.10	Cisco	Jasper Pumping Station ...	192.168.100.10	00:1D:7E:CC:86:AE		
JP_NTWK_0001	Device	Jasper Pumping Station ...	192.168.100.200	00:1A:A0:06:DE:3D	Main Rack Room	Cabinet 2

Description Column

Once the Node has been added into the network diagram, and a description of the Node has been specified in the Node's Properties page, the description will be displayed in this column.



Asset	Device Type	Discovered By	IP Address	MAC Address	General Location	Specific Location	Description
2800 Asset 192.168.100.5	2800	Jasper Pumping Station ...	192.168.100.5	00:1D:7E:CC:87:0B			
Cisco Asset 192.168.100.10	Cisco	Jasper Pumping Station ...	192.168.100.10	00:1D:7E:CC:86:AE			
JP_NTWK_0001	Device	Jasper Pumping Station ...	192.168.100.200	00:1A:A0:06:DE:3D	Main Rack Room	Cabinet 2	Jasper Pipeline Control Room Switch

Asset Discovery Right Click Menu



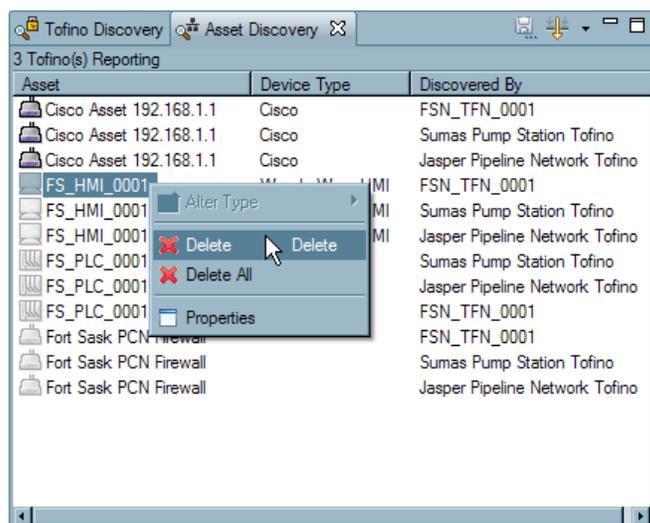
See: [Deleting Assets](#)

See: [Properties](#)

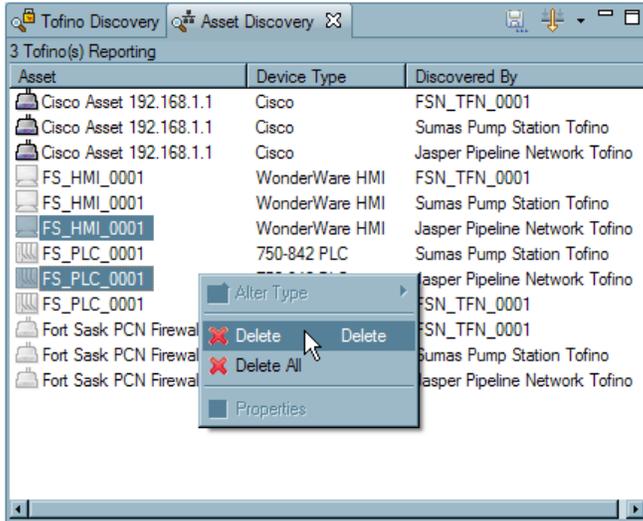
Deleting Assets

The user has the option to delete nodes from the Asset Discovery view. This has no impact on the network diagram. One or multiple entries can be deleted at a time.

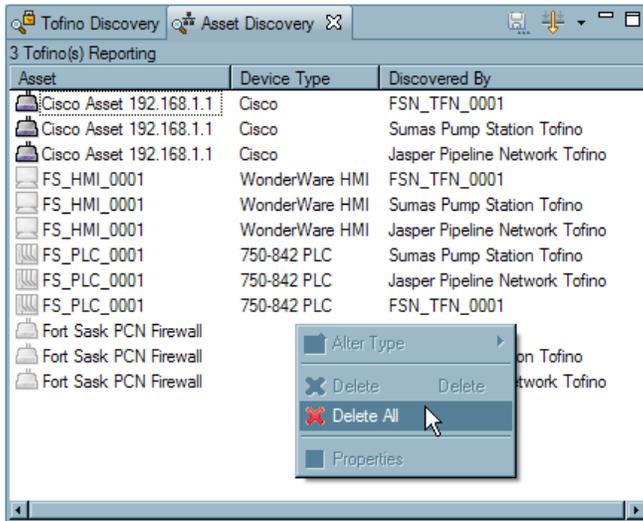
- ▶ To delete one entry select the node name and hit "Delete" on the keyboard, or right click and select "Delete".



- ▶ To delete multiple entries, select the entries to be deleted and hit "Delete" on the keyboard, or right click anywhere in the Asset Discovery view and select "Delete".

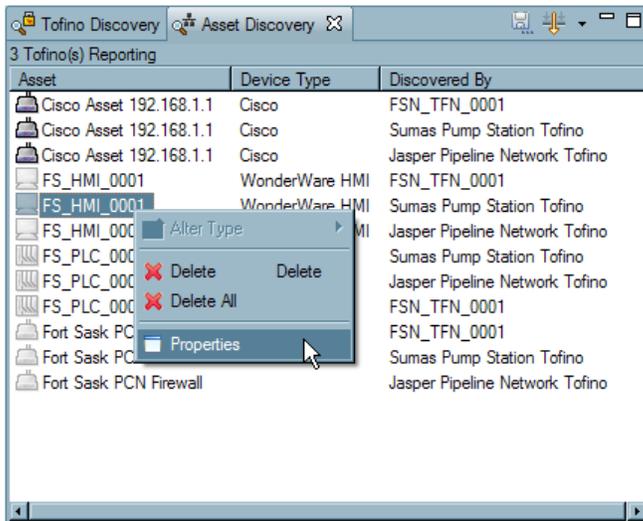


- ▶ To delete the entire list, select all the entries and press "Delete" on the keyboard or right click and select "Delete All".



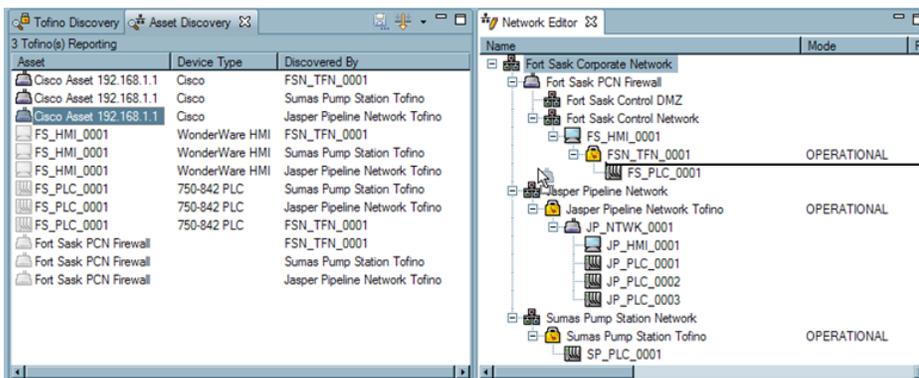
Properties

To view a particular node's properties, double click on the node's name or right click on the name and select "Properties".

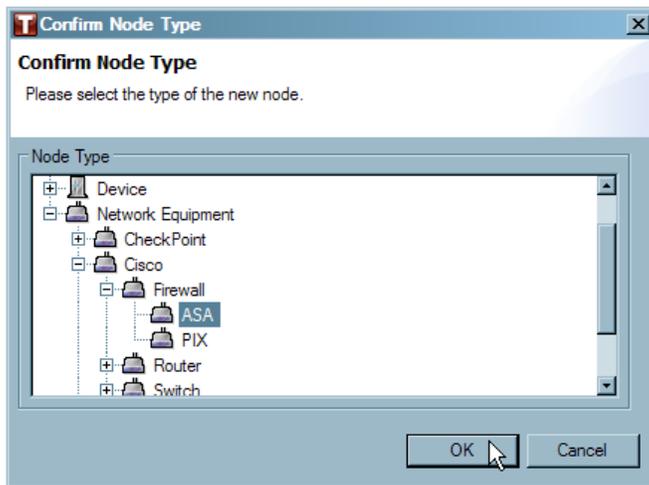


Adding Discovered Assets to the Network Diagram

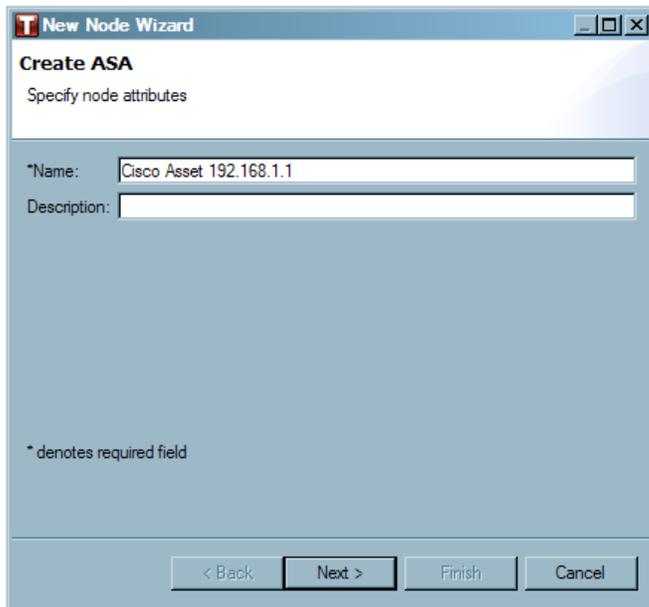
Any discovered node that is not already in the network diagram can be dragged and dropped into the network diagram. Make sure that the Node type is correct as once it is deployed this can not be changed. If the node is already present in the network diagram, the node will either be hidden or greyed out in the Asset Discovery view.



- Once a Node has been dragged and dropped into the network diagram, a Confirm Node Type window will open to allow the user to ensure the Node type has been set, as once the Node has been added into the network diagram, the type can not be altered.



- Next, a New Node Wizard will open to guide the user through the setup of the node type. Because the node was discovered and is known by the Tofino CMP some of the pages in the wizard will already be filled in, although they can be changed by the user during the set up or at any other time by opening the node's properties page.



See: [Editing a Node's Properties](#)

6.3.3 About Assisted Rule Generation

What is Assisted Rule Generation?

The Assisted Rule Generation feature helps the user to create firewall rules for the purpose of protecting devices on their network.

How do I activate Assisted Rule Generation?

The Assisted Rule Generation (ARG) feature is included as a part of the Secure Asset Management LSM.

How does Assisted Rule Generation work?

Note that both the Secure Asset Management LSM and the Firewall LSM must be loaded into the Tofino SAs being used in order for the Assisted Rule Generation to function. See: [Using Assisted Rule Generation](#)

Do I have to use Assisted Rule Generation to set firewall rules?

ARG uses [exception heartbeats](#) that are sent to the Tofino CMP, by Tofino SAs in the field, to create rules based on the information coming in from devices in the field.

Assisted Rule Generation is optional, firewall rules can be created manually.

See: [Firewall Rule Configuration of a Tofino SA](#) or [Firewall Rule Configuration for a Node](#)

6.3.3.1 Using Assisted Rule Generation

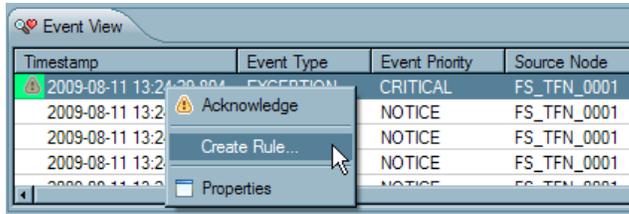
Once the user has installed the Secure Asset Management LSM and the Firewall LSM onto the Tofino SAs in the field, the Assisted Rule Generation feature is available to assist in creating firewall rules using IP based protocols. See: [Adding an LSM to a Tofino SA](#)

Note: Assisted Rule Generation simplifies the task of creating firewall rules for IP based protocols only. Non-IP (Ethernet) protocols are currently not supported by this feature.

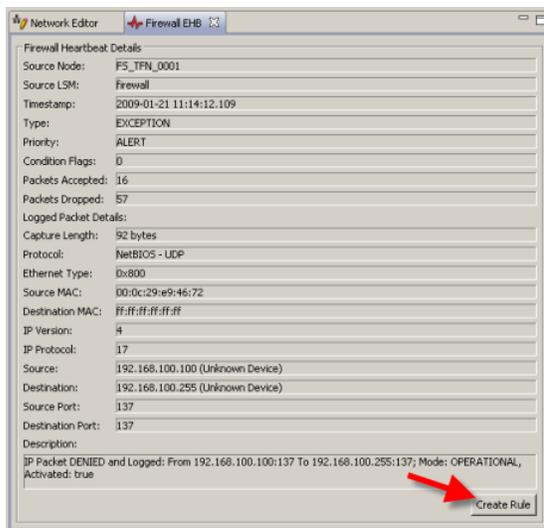
How to Access Assisted Rule Generation

There are two ways to access the Assisted Rule Generation feature:

- Right Clicking on an exception heartbeat in the Event View and selecting "Create Rule". This will open the Firewall Rule Wizard. See: [Event View](#)



- Double Clicking on an exception heartbeat in the Event View which opens the heartbeat's properties page and then clicking the "Create Rule" button. This will open the Firewall Rule Wizard.



One of three Firewall Rule Generation Wizards will open when initiating the Assisted Rule Generation feature. The wizard that opens is dependant on whether the packet that passed through the Tofino SA, and thus created the exception heartbeat, contained unicast, broadcast or multicast destination IP addresses:

See: [Unicast traffic Assisted Rule Generation Wizard](#)

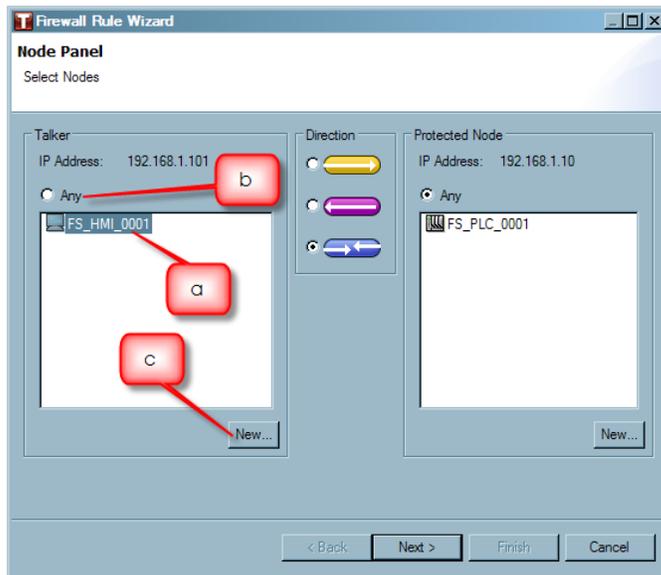
See: [Broadcast traffic Assisted Rule Generation Wizard](#)

See: [Multicast traffic Assisted Rule Generation Wizard](#)

Assisted Rule Generation Wizard for Unicast Traffic

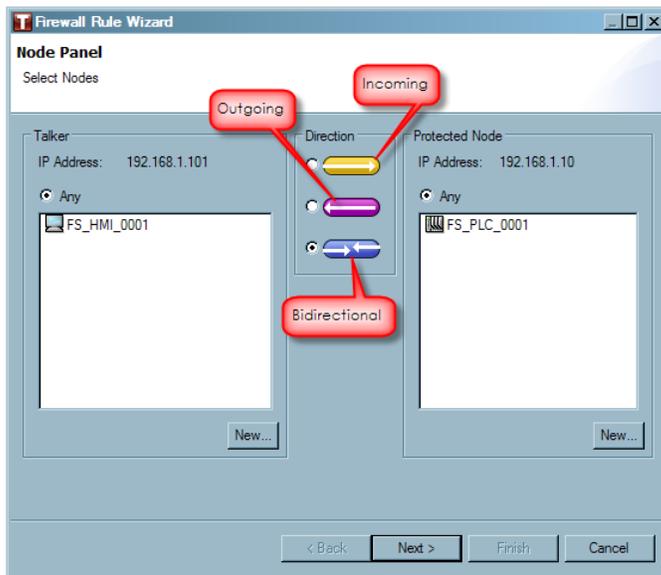
A selection list is displayed that contains the name of all devices in the network model whose IP address match those contained in the packet.

- Select the [Talker](#) associated with the shown IP address by clicking on the name.
- Or to allow traffic to come from any *Talker* on the untrusted side of the Tofino SA the user can select "Any".
- If there is no Talker in the list that matches the shown IP address the user can create a new Talker by clicking "New" and following the Node Creation Wizard. See: [Assisted Rule Generation New Node Wizard](#)



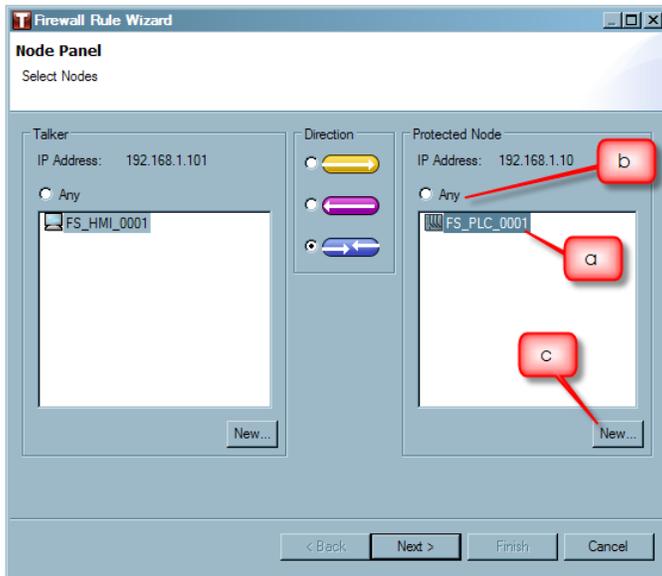
- Select the direction for the rule: incoming, outgoing or bidirectional.

Note: This direction indicates the direction that a connection between two nodes is set up. It does not refer to packet flow. See: [Incoming versus Outgoing versus Bidirectional](#)

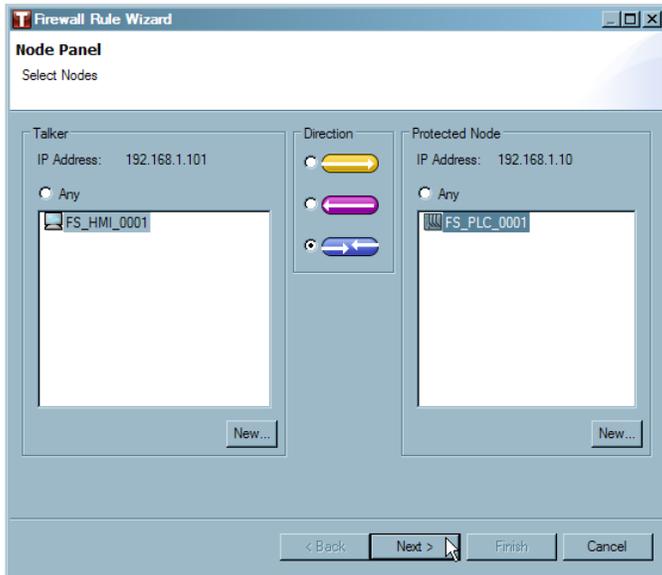


- Select the target node:
- Select the Protected Node associated with the shown IP address by clicking on the name.
- Or to allow the previously selected Talker(s) on the untrusted interface of the Tofino SA to communicate to any protected node, select "Any".

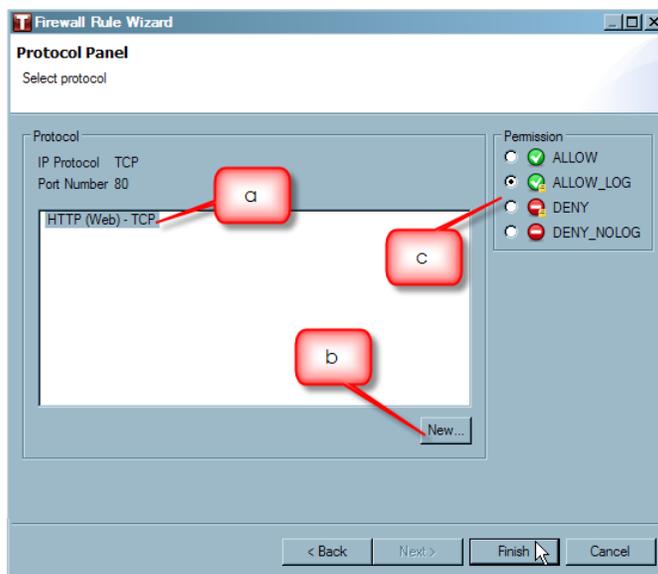
- If there is no *Protected Node* in the list that matches the shown IP address the user can create a new *Protected Node* by clicking *New...* and following the Node Creation Wizard. See: [Assisted Rule Generation New Node Wizard](#)



- Once the Node Panel has been completed, click "Next".



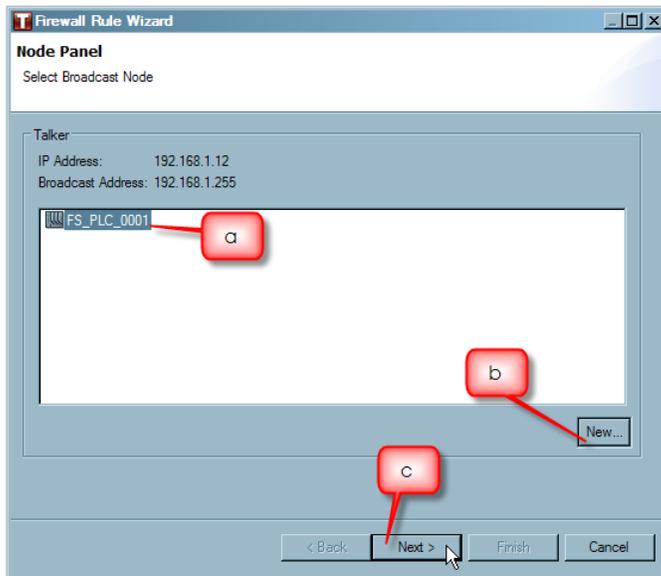
- A Protocols window will appear. This window displays a list of protocols that are in the Tofino CMP Protocols database that match the IP protocol and the port number of the packet in the heartbeat.
- Select the desired protocol for communications between the nodes selected on the previous window or create a new protocol by clicking "New..." at the bottom of the protocols window. See: [Protocol Wizard](#)
- Select the permission of the rule:
 - ▶ Allow: Traffic matching the rule is allowed through the Tofino SA with no logging or alarms reported to the Tofino CMP.
 - ▶ Allow Log: Traffic matching the rule is allowed through the Tofino SA. This traffic is logged and exception heartbeats are generated.
 - ▶ Deny No Log: Traffic matching the rule is blocked by the Tofino SA with no logging or alarms reported to the Tofino CMP.
 - ▶ Deny: Traffic matching the rule is blocked by the Tofino SA. This traffic is logged and exception heartbeats are generated.



- Click "Finish" to finish creating the firewall rule.

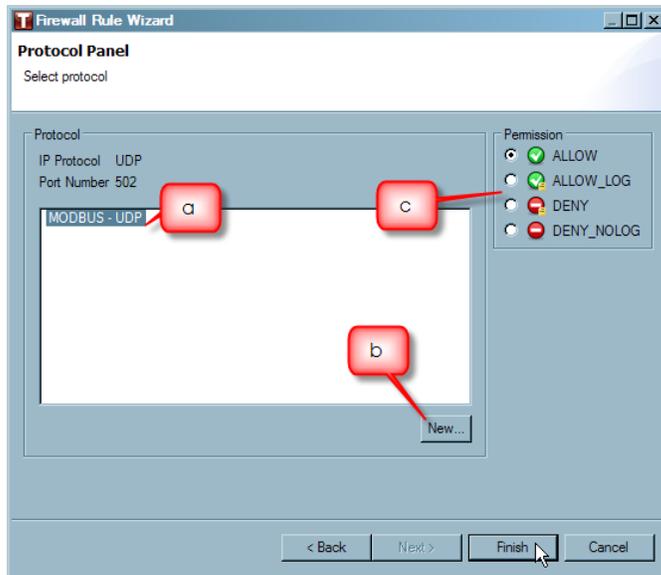
Assisted Rule Generation Wizard for Broadcast Traffic

- A selection list is displayed that contains the name of all devices in the network model whose IP address and broadcast addresses match those contained in the packet. Select the node from the list associated with the listed IP address.
- If there is no node in the list that matches the shown IP address, the user can create a new one by clicking "New..." and following the Node Creation Wizard. See: [Assisted Rule Generation New Node Wizard](#)
- Once the Select Devices window has been completed, click "Next".



- A Protocols and Permissions window will appear. This window displays a list of protocols that are in the Tofino CMP Protocols database that match the IP protocol and the port number of the packet in the heartbeat. Select the desired protocol for communications between the nodes selected on the previous page.
- Or create a new protocol by clicking "Next..." at the bottom of the protocols window. See: [Protocol Wizard](#)

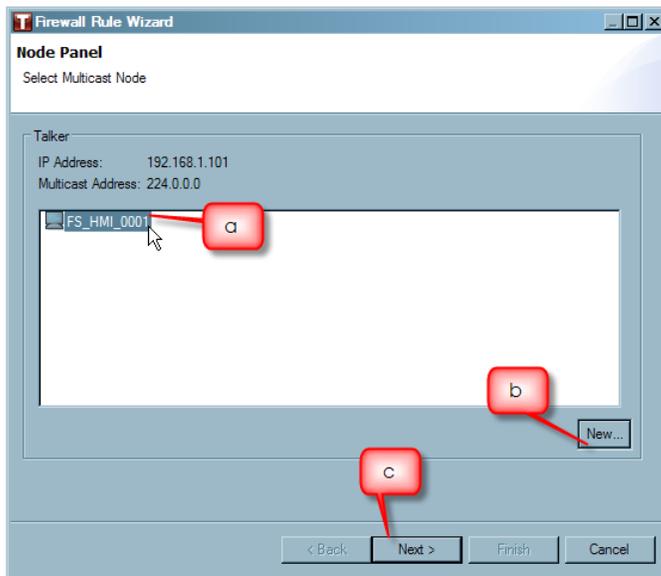
- Select the permission of the rule:
 - ▶ Allow: Traffic matching the rule is allowed through the Tofino SA with no logging or alarms reported to the Tofino CMP.
 - ▶ Allow Log: Traffic matching the rule is allowed through the Tofino SA. This traffic is logged and exception heartbeats are generated.
 - ▶ Deny No Log: Traffic matching the rule is blocked by the Tofino SA with no logging or alarms reported to the Tofino CMP.
 - ▶ Deny: Traffic matching the rule is blocked by the Tofino SA. This traffic is logged and exception heartbeats are generated.



- Click "Finish" to finish creating the firewall rule.

Assisted Rule Generation Wizard for Multicast Traffic

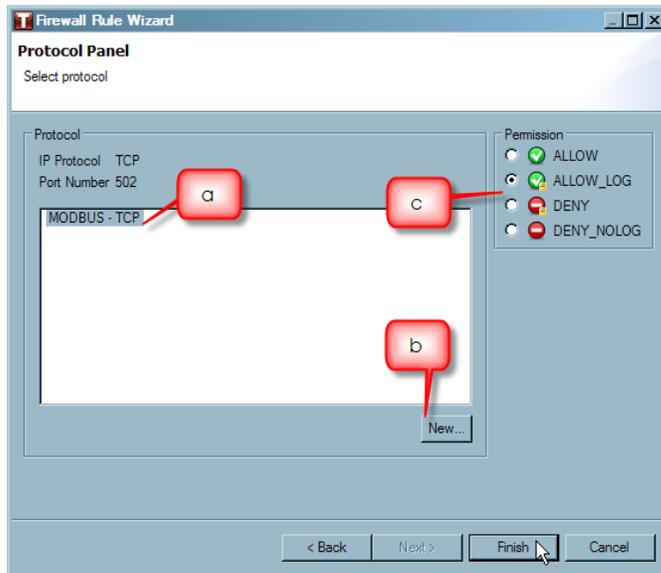
- A selection list is displayed that contains the name of all devices in the network model whose IP address and multicast addresses match those contained in the packet. Select the node from the list associated with the listed IP address.
- If there is no node in the list that matches the shown IP address, the user can create a new one by clicking "New..." and following the Node Creation Wizard. See: [Assisted Rule Generation New Node Wizard](#)
- Once the Select Devices window has been completed, click "Next".



- A Protocols and Permissions window will appear. This window displays a list of protocols that are in the Tofino CMP Protocols database that match the IP protocol and the port number of the packet in the heartbeat. Select the desired protocol for communications between the nodes selected on the previous page.
- Or create a new protocol by clicking "Next..." at the bottom of the protocols window. See: [Protocol Wizard](#)

□ Select the permission of the rule:

- ▶ Allow: Traffic matching the rule is allowed through the Tofino SA with no logging or alarms reported to the Tofino CMP.
- ▶ Allow Log: Traffic matching the rule is allowed through the Tofino SA. This traffic is logged and exception heartbeats are generated.
- ▶ Deny No Log: Traffic matching the rule is blocked by the Tofino SA with no logging or alarms reported to the Tofino CMP.
- ▶ Deny: Traffic matching the rule is blocked by the Tofino SA. This traffic is logged and exception heartbeats are generated.



□ Click "Finish" to finish creating the firewall rule.

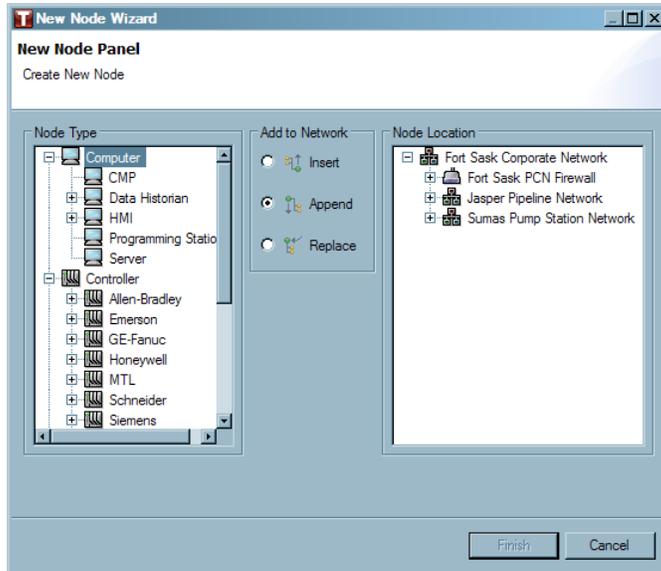
6.3.3.2 ARG New Node Wizard

When clicking "New..." on the Unicast, Broadcast or Multicast Assisted Rule Generation Create Node page, a New Node Wizard will open. See: [Using Assisted Rule Generation](#)

See: [Inserting or Appending a Node in the Network Diagram](#)

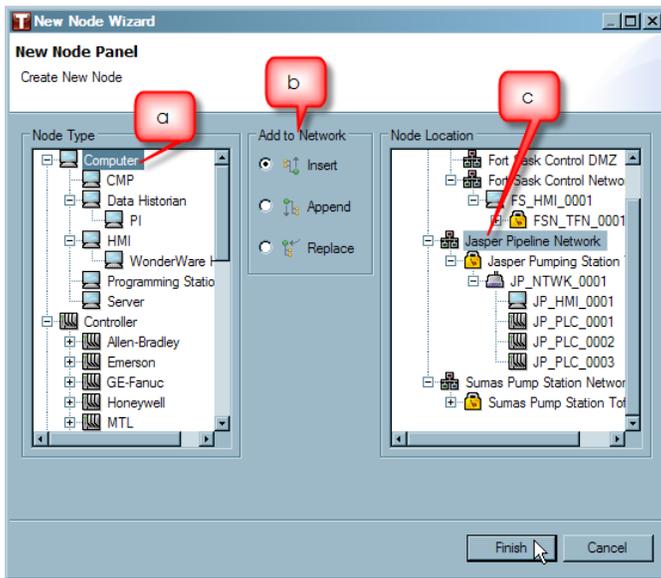
See: [Replacing a Node in the Network Diagram](#)

Inserting or Appending a Node in the Network Diagram

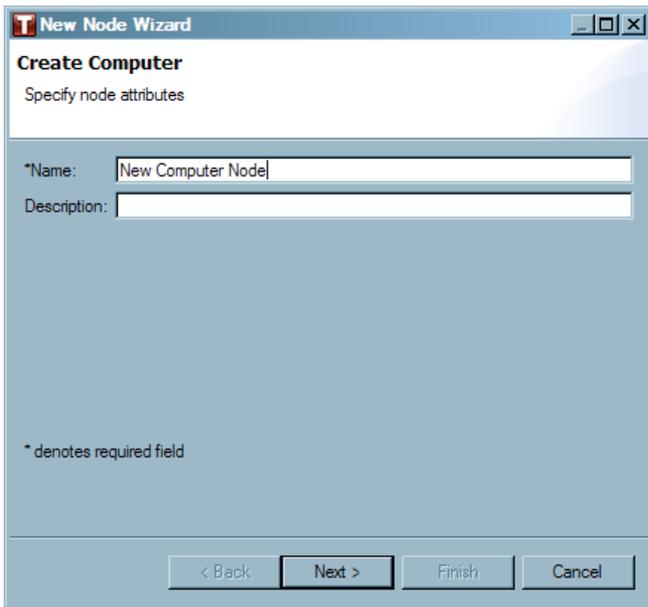


- To create a new node select the node type to be created.
- Select how the node will be added to the network diagram:
 - ▶ Insert: adds the new node as a sibling of the node selected in the right tree view.
 - ▶ Append: adds the new node as a child of the node selected in the right tree view.

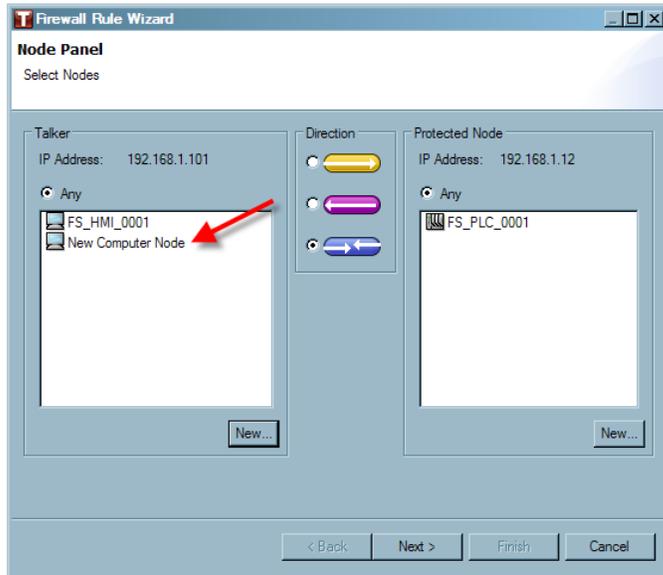
- Select the location for the new node in the network diagram.



- Click "Finish".
- A New Node Wizard will open to guide the user through the setting up of the new node's properties.



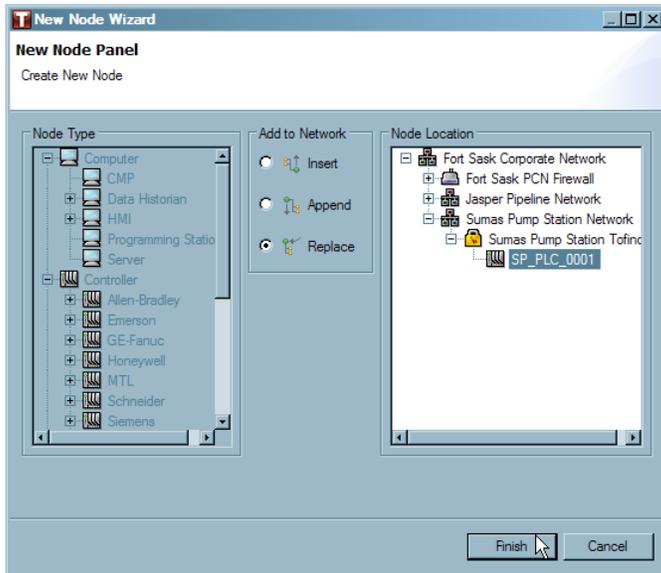
- Once the New Node Wizard has completed the creation of the new node, the new node will now appear in the panel where it was created as well as in the network diagram.
- Continue through the Firewall Rule Wizard to be made. See: [Using Assisted Rule Generation](#)



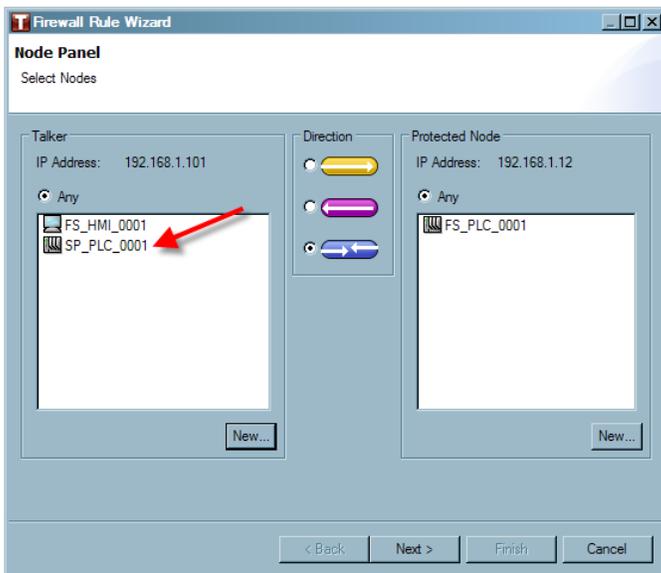
Replacing a Node in the Network Diagram

If Replace was chosen, the IP address(es) of the highlighted node are replaced by the address(es) extracted from the exception heartbeat. The node type will not be changed. The Node Type panel is disabled (greyed out) when "Replace" is selected.

- Select "Replace".
- Next, select the node from the Node Location and then click "Finish".



- The node that was chosen to take over the IP address will now be shown in the appropriate window, depending on where the "New..." button was selected.
- Continue through the Firewall Rule Wizard. See: [Using Assisted Rule Generation](#)



6.4 Modbus TCP Enforcer LSM Management

6.4.1 About Modbus TCP Enforcer LSM

What is Modbus TCP?

Modbus is now the most commonly available means of connecting industrial electronic devices. Modbus allows for communication between many devices connected to the same network and is often used to connect a supervisory computer with a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems. <http://en.wikipedia.org/wiki/Modbus>

What is the Modbus TCP Enforcer LSM?

It is an advanced firewall for the Modbus TCP protocol that allows you to filter traffic based on specific Modbus function codes and the data content of those codes. The Modbus TCP Enforcer LSM is an add-on to the standard Tofino Firewall LSM.

How does it work?

The Modbus TCP Enforcer LSM provides many security features for managing Modbus TCP traffic:

- ▶ Checks to ensure that each Modbus packet conforms to the Protocol specification and then allows or rejects this packet.
- ▶ Allows you to specify Modbus function codes or register ranges that should be allowed or denied by the Tofino SA.
- ▶ Monitors the state of Modbus TCP connections to ensure that incoming messages are expected and in sequence.

What does the Tofino SA do when it detects an illegal or filtered Modbus message?

You can set the Tofino SA to perform a variety of actions when it detects an illegal or filtered Modbus message. These include:

- ▶ Drop the message and do nothing
- ▶ Drop the message and send a TCP reset message to both Modbus devices
- ▶ Drop the message and send an exception response to the Modbus device that created the illegal message

Which one you choose depends on the nature of your Modbus equipment.

What is Modbus sanity checking?

For well known Modbus commands, the Tofino SA can check if the messages are

properly formed and follow the Modbus specification. If they do not, the Tofino SA can be directed to block the message. For example, if a Modbus Write Multiple Registers command (Function Code 16) has a value in its length field that is either illegal or does not match the amount of data being sent, then it would be considered an illegal message and could be dropped. **Note:** The Modbus TCP Enforcer LSM always performs sanity checking on the Modbus MBAP header - this can not be turned off.

Will the Modbus TCP Enforcer LSM work for Modbus over UDP?

Yes, provided that the UDP implementation follows the Modbus TCP 1.1b specification.

6.4.2 Using the Modbus TCP Enforcer LSM

The Modbus TCP Enforcer LSM is an advanced deep packet inspection firewall for the Modbus TCP protocol that allows you to filter traffic based on specific Modbus function codes and the data content of those codes. The Modbus TCP Enforcer LSM is an add-on to the standard Tofino Firewall LSM.

Note: Deleting or deactivating either the Firewall LSM or the Modbus TCP Enforcer LSM while the Modbus TCP Enforcer LSM is operating may have unexpected results.

See: [Activating the Modbus TCP Enforcer LSM](#)

See: [Configuring Modbus TCP Enforcer Firewall Rules](#)

See: [Deleting a Function Code](#)

See: [Deleting a Talker](#)

Activating the Modbus TCP Enforcer LSM

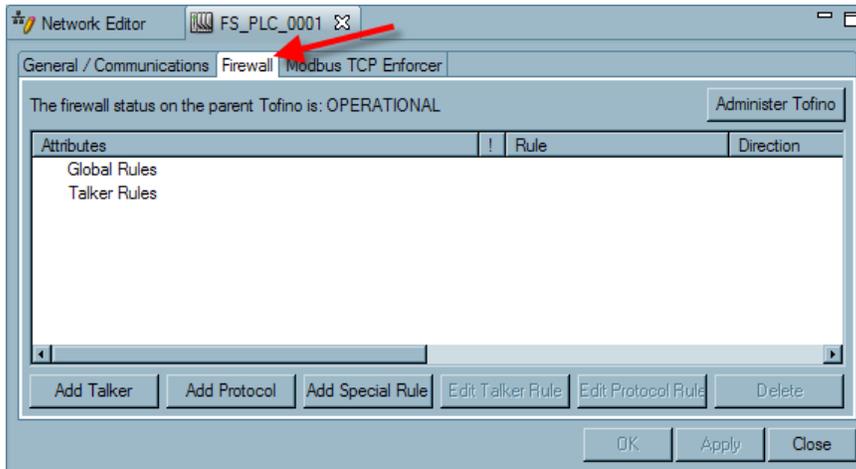
Before Modbus TCP Enforcer is available on a Tofino SA, both the Firewall LSM and the Modbus TCP Enforcer LSM must be installed and activated.

- ▶ Install and activate the Firewall LSM on a Tofino SA.
- ▶ Install and activate the Modbus TCP Enforcer LSM on the same Tofino SA. See: [Adding an LSM to a Tofino SA](#)

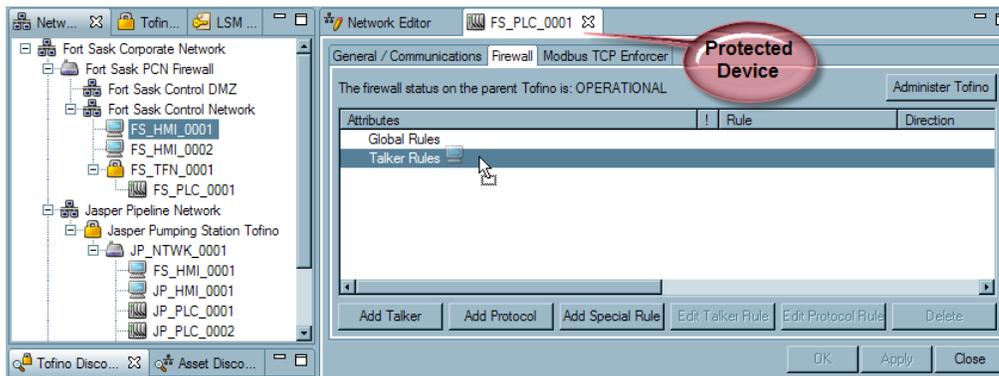
Configuring Modbus TCP Enforcer Firewall Rules

With both the Firewall LSM and Modbus TCP Enforcer LSM installed and activated on a Tofino SA, you can follow these steps to configure Modbus TCP Enforcer firewall rules:

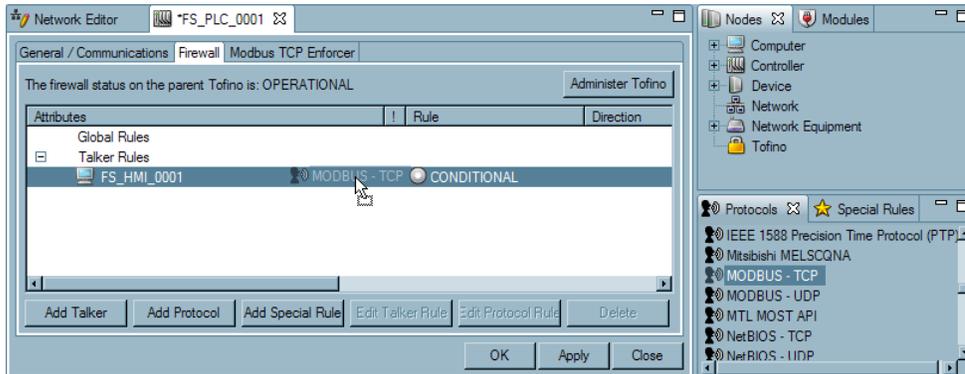
- Open the Firewall page of a node, downstream from a Tofino SA, that you wish to protect using the Modbus TCP Enforcer. (The Protected Device)



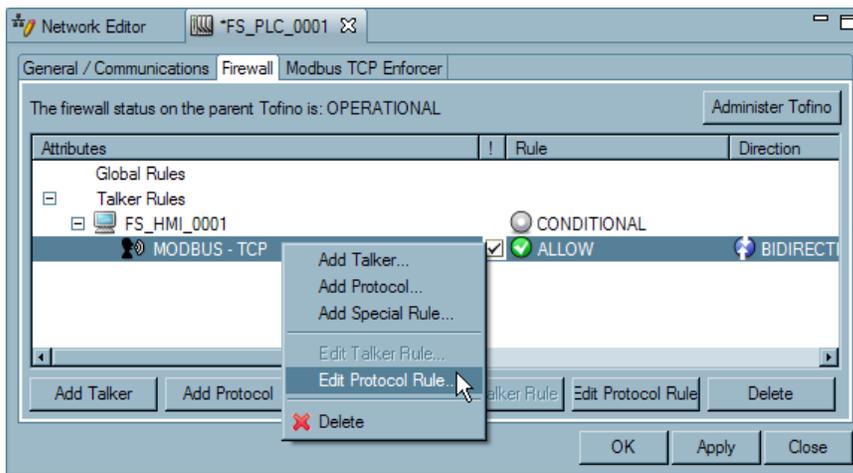
- Drag a talker onto the Talker Rules text on the Firewall page of the Protected Device. (A talker is a node that is able to communicate with the protected device).



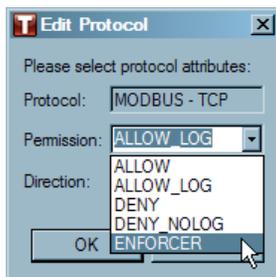
- Next, drag the appropriate Modbus protocol from the Protocols view onto the Talker icon on the Firewall page of the protected device. You can select either Modbus-TCP or Modbus-UDP for use with the Modbus TCP Enforcer.



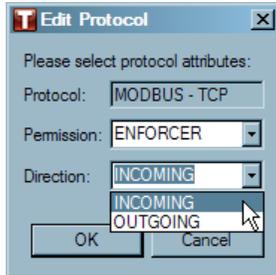
- Next, you will need to set the direction and permission of the rule. Right click on the Modbus protocol and select "Edit Protocol Rule..."



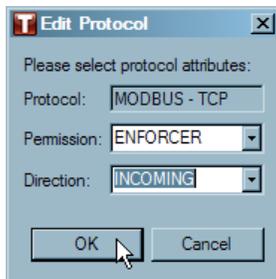
- Set the Permission to ENFORCER in order to activate the Modbus TCP Enforcer LSM. **Note:** If you select ALLOW or DENY, the Modbus traffic between the Talker and Protected Device will simply be allowed or blocked accordingly without reference to the Modbus TCP Enforcer LSM.



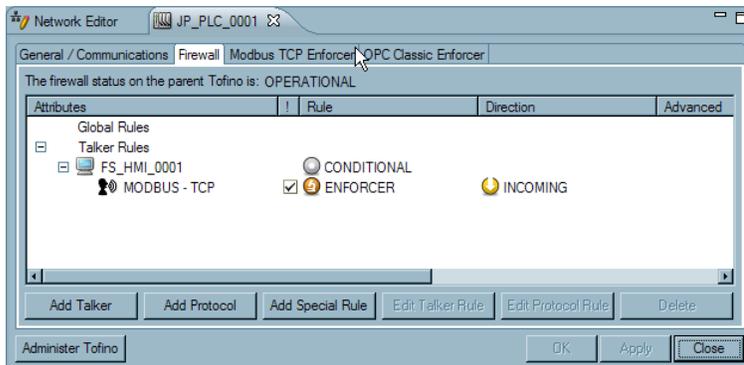
- Set the Direction to either INCOMING (ie: The Talker is the Modbus Master) OUTGOING (ie: The Talker is the Modbus Slave) For example, the FS_HMI_001 acts as a Modbus master to the Protected PLC FS_PLC_001 and thus the traffic direction should be set to INCOMING. **Note:** BIDIRECTIONAL can not be used with the Modbus TCP Enforcer LSM.



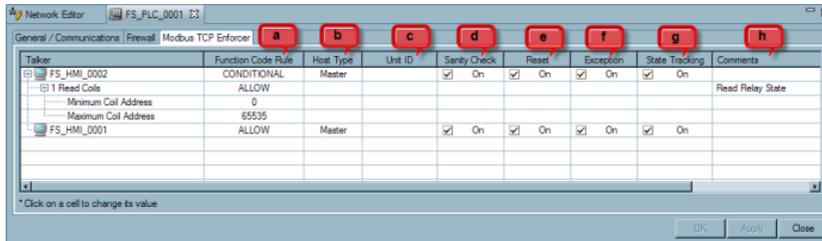
- Click "OK" once the Permission and Direction have been set.



- Now click on the Modbus TCP Enforcer tab.



- You will notice that the Talker (FS_HMI_0001) that you dragged onto the Firewall tab is already on the Modbus TCP Enforcer page. It is here that you can now define the specifics of the Modbus TCP Enforcer rule for this talker. (FS_HMI_0002 is an example of a another talker with function codes already defined.)

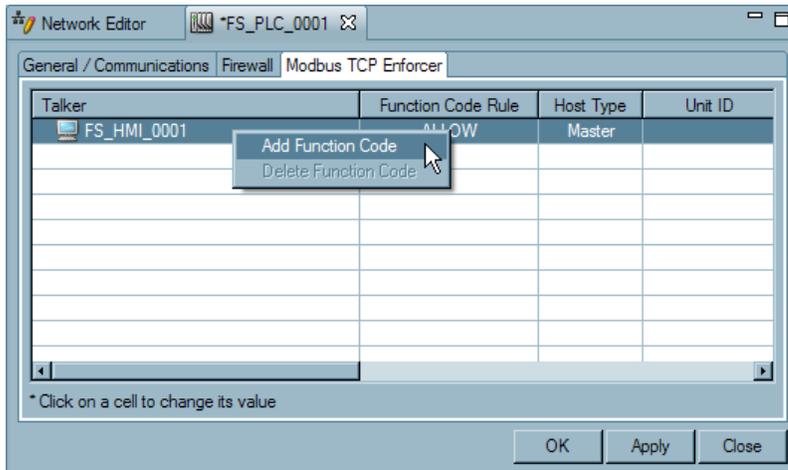


Set the general Modbus TCP filtering rules for this talker. These are:

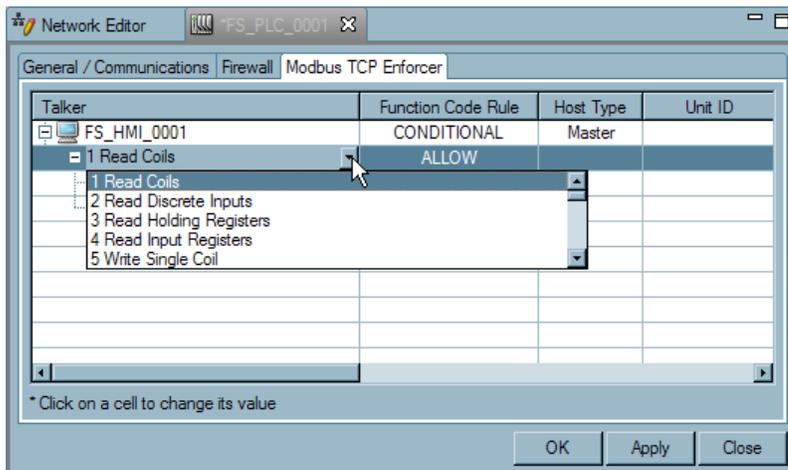
- ▶ (a) Function Code Rule: This is either set to ALLOW, which means all Modbus function codes are permitted from this Talker, or CONDITIONAL which means that only the listed function codes are permitted. This field is set automatically by the system depending on whether function codes have been added or not.
- ▶ (b) Host Type: This identifies the Talker as either the Master or the Slave. This is automatically set based on how the direction of the traffic was set on the Firewall page. This can be changed by clicking in the cell under the Host Type heading and selecting either "Master" or "Slave" from the pull down menu. Note: The direction can also be changed on the Firewall page. Please ensure when you are making a change to the Direction or Host Type that the changes have been saved before continuing with other changes.
- ▶ (c) Unit ID: The 'Unit Identifier' is used to communicate via devices such as bridges, routers and gateways that use a single IP address to support multiple independent Modbus end units. For most Modbus TCP applications this should be set to the default which is 1. If you don't want the Unit ID to be checked, clear this field.
- ▶ (d) Sanity Check: For well known Modbus commands (1-6, 15, 16, 20-24), the Tofino SA can check if the messages are properly formed and follow the Modbus specification. If they do not, the Tofino SA can be directed to block the message. For example, if a Modbus Write Multiple Registers command (Function Code 16) has a value in its length field that is either illegal or does not match the amount of data being sent, then it would be considered an illegal message and would be dropped if this box is checked. This option may have to be disabled for Modbus devices that do not conform to the Modbus/TCP 1.1b specification. Note: The Modbus TCP Enforcer LSM always performs sanity checking on the Modbus MBAP header - this can not be turned off.
- ▶ (e) Reset: If this box is checked, the Tofino SA will send a TCP reset message to both Modbus devices when it blocks a message. This can prevent session lock up on certain loosely written Modbus systems.
- ▶ (f) Exception: If this box is checked, the Tofino SA will send a Modbus TCP exception response (if appropriate) to the Modbus device that generated a blocked message. This can prevent session lock up on certain loosely written Modbus systems. Note that not all illegal Modbus TCP messages have a defined exception response.
- ▶ (g) State Tracking: When checked, this box will cause the Tofino SA to block and report any Modbus command or response that is out of sequence for the current state of the connection. Examples of some 'out-of-state' traffic include: two Modbus commands issued by the master without an intervening response from the slave, a command issued by the slave device to the master, or a response issued by the master device to the slave. If this box is unchecked, then the Tofino SA will not block these out-of-state commands or responses.
- ▶ (h) Comments: This field is available as a convenience, so the control engineer may add text to

help describe or document the Modbus rules that have been set up on the Tofino security appliance.

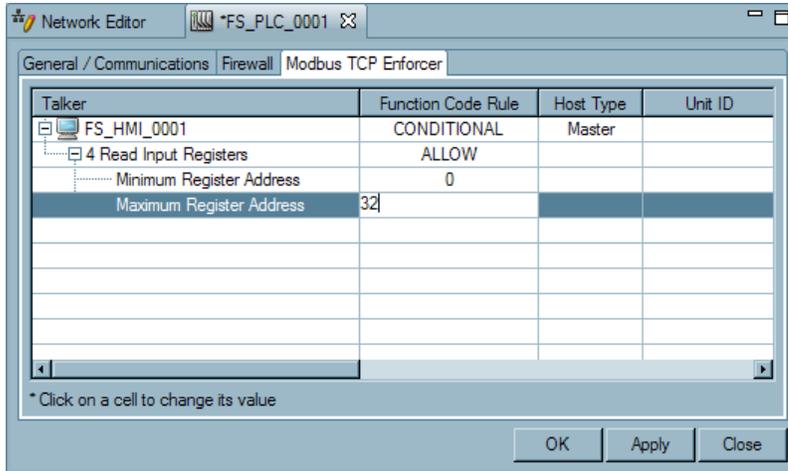
- Next, select the function codes and register/coil ranges that you wish to allow for this Talker/Protected node pair. To do this, right click on the Talker node and select "Add Function Code". Note that you can add as many Function Codes as needed to one Talker but each function code should only be entered once for a given talker.



- Select the appropriate function code from the drop down menu by clicking on the function code to activate the drop down menu.



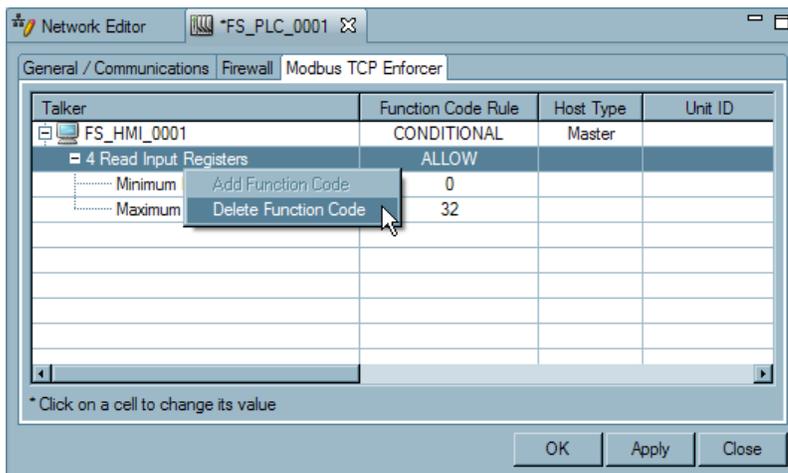
- If appropriate, set the range of addresses that you wish to allow communications to by supplying the Minimum Address and the Maximum Address. For example, if you wish to allow access to addresses in the range from 8 to 31, you would enter 8 for the Minimum Address and 31 for the Maximum Address. Note that the first address in any memory location is designated address zero, so some conversions may be needed depending on the Modbus equipment used.



- Continue adding function codes as appropriate.
- Once you have completed your configurations, ensure that the Modbus rule direction on the Firewall page matches the Host Type on the Modbus TCP Enforcer page. If they are not matching make the appropriate change so that they are matching, and save your changes.

Deleting a Function Code

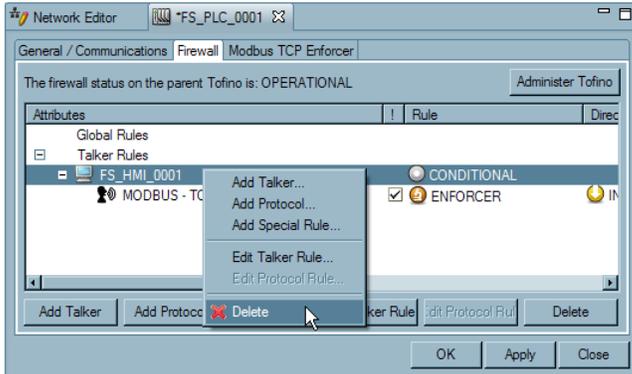
To delete a function code, right click on the function code that you want to delete and select "Delete Function Code".



Deleting a Talker

To delete a Talker from the Modbus TCP Enforcer page, you must click on the Firewall tab and delete the talker from the Firewall page. To do so right click on the Talker on the Firewall page and select "Delete".

Note: Any Talker will automatically be removed from the Modbus TCP Enforcer page if the Permission of the Modbus rule on the Firewall page is set to anything other than ENFORCER (i.e.: ALLOW, ALLOW_LOG, DENY, DENY_NO LOG) or if the Modbus protocol is deleted from the Firewall page.



6.5 OPC Classic Enforcer LSM Management

6.5.1 About OPC Classic Enforcer LSM

What is OPC Classic?

OPC Classic, based on Microsoft COM/DCOM technology, is widely used in control systems as an interoperability solution, interfacing control applications from multiple vendors. It includes a variety of OPC specifications including Data Access (DA), Alarms and Events (A&E), Historical Data Access (HDA), and Data Exchange (DE).

Why is OPC security an issue?

The DCOM technologies underlying OPC Classic were designed before network security issues were widely understood. As a result, OPC Classic is almost impossible to secure using a conventional firewall.

What is the difference between OPC Classic and OPC UA?

OPC UA is the next generation OPC specification. Rather than being based on DCOM, it is based on HTTP and Simple Object Access Protocol (SOAP).

What is the difference between OPC Classic and OPC DA, A&E, HDA and DE?

Nothing. DA, A&E, HDA and DE are all subsets of the OPC Classic specification.

What is the relationship between OPC Classic and COM, DCOM and RPC?

OPC Classic is based on Microsoft's Distributed Component Object Model (DCOM) technology, which is the culmination of a number of other technologies including Component Object Model (COM) and the Object Linking and Embedding (OLE). These in turn, are based on the Remote Procedure Call (RPC) protocol. Many people have heard of OLE and have used its capabilities when adding a spreadsheet to a word processing document. OLE allows the spreadsheet application to dynamically update the information in the word processing document. Typically the user isn't required to do even the slightest configuration beyond the click of a mouse. The OLE specification defines how the spreadsheet (in this case the OLE server) will format and send data to the word processor document (the OLE client).

What does the OPC Classic Enforcer LSM do?

The Tofino OPC Classic Enforcer Loadable Security Module (LSM) inspects, tracks and secures every connection that is created by an OPC application. It

dynamically opens only the TCP ports that are required for each connection, and only between the specific OPC client and server that created the connection. It's simple to use – no configuration changes are required on the OPC clients and servers – and offers superior security over what can be achieved with conventional firewall or tunneler solutions.

What is OPC Sanity Checking?

For all OPC session connection requests, the Tofino SA can check if the messages are properly formed and follow the RPC specification. If they do not, the Tofino SA can be directed to block the message.

What is OPC Fragment Checking?

Many attacks against OPC and DCOM take advantage of message fragments. In most network settings there is little need for fragmented messages, so for all OPC session connection requests, the Tofino SA can check if the messages are fragmented. If they are, the Tofino SA can be directed to block the message.

6.5.2 Using the OPC Classic Enforcer LSM

The Tofino OPC Classic Enforcer Loadable Security Module (LSM) inspects, tracks and secures every connection that is created by an OPC application. It dynamically opens only the TCP ports that are required for each connection, and only between the specific OPC client and server that created the connection. It's simple to use – no configuration changes are required on the OPC clients and servers – and offers superior security over what can be achieved with conventional firewall or tunneler solutions. The OPC Classic Enforcer LSM is an add-on to the standard Tofino Firewall LSM.

Note: Deleting or deactivating either the Firewall LSM or the OPC Classic Enforcer LSM while the OPC Classic Enforcer LSM is operating may have unexpected results.

See: [Activating the OPC Classic Enforcer LSM](#)

See: [Configuring the OPC Classic Enforcer Firewall Rules](#)

See: [Configuring OPC Classic Enforcer Settings](#)

See: [Deleting a Talker](#)

Activating the OPC Classic Enforcer LSM

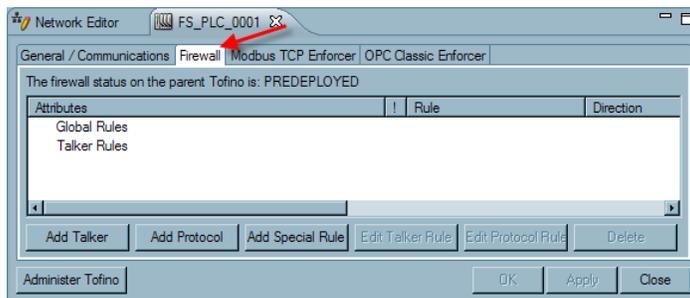
Before OPC Classic Enforcer LSM is available on a Tofino SA, both the Firewall LSM and the OPC Classic Enforcer LSM must be installed and activated.

- ▶ Install and activate the Firewall LSM on a Tofino SA.
- ▶ Install and activate the OPC Classic Enforcer LSM on the same Tofino SA. See: [Adding an LSM to a Tofino SA](#)

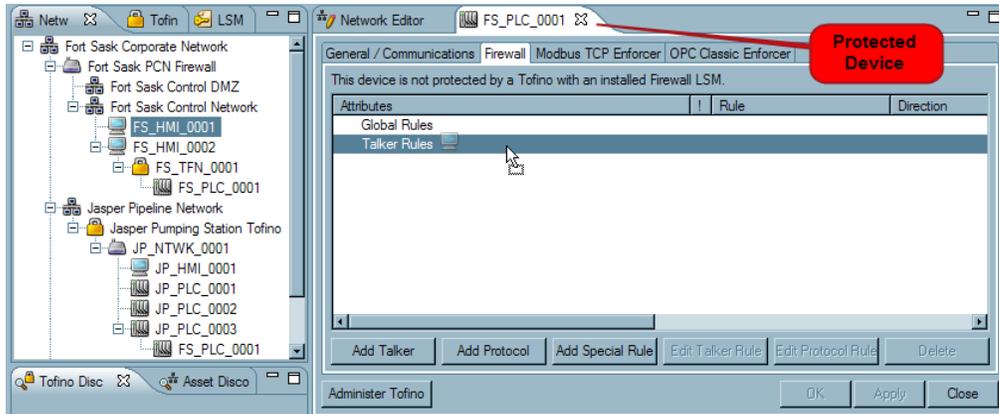
Configuring the OPC Classic Enforcer Firewall Rules

With both the Firewall LSM and OPC Classic Enforcer LSM installed and activated on a Tofino SA, you can follow these steps to configure OPC Classic Enforcer LSM rules:

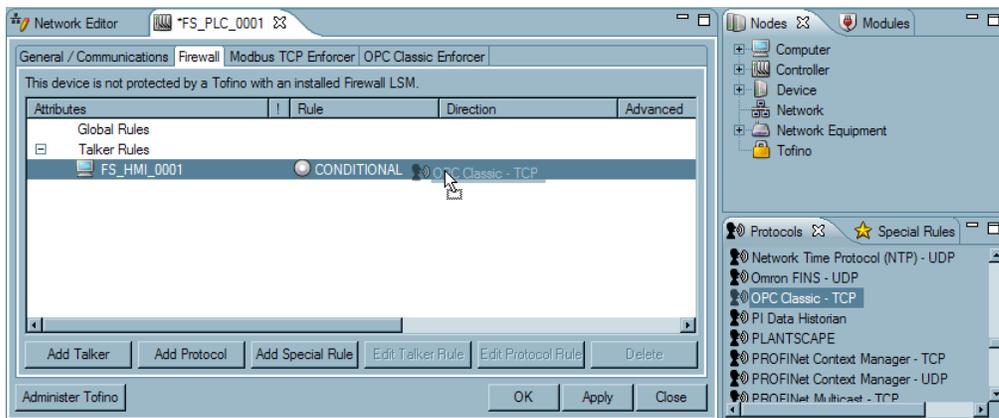
- Open the Firewall page of a node, downstream from a Tofino SA, that you wish to protect using the OPC Classic Enforcer LSM. (The Protected Device)



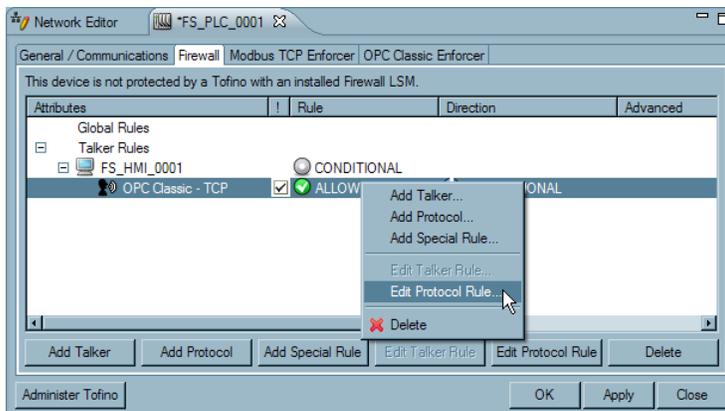
- Drag a talker onto the Talker Rules text on the Firewall page of the Protected Device. (A talker is a node that is able to communicate with the protected device).



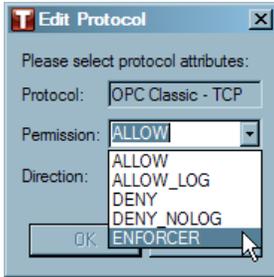
- Next, drag the OPC Classic TCP protocol from the Protocols view onto the Talker icon on the Firewall page of the protected device.



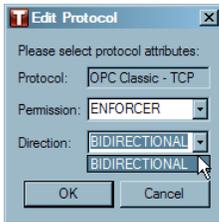
- Next, you will need to set the direction and permission of the rule. Right click on the OPC Classic TCP protocol and select "Edit Protocol Rule..."



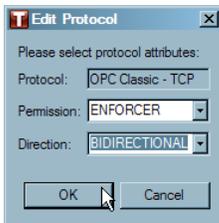
- Set the Permission to ENFORCER. **Note:** If you select ALLOW or DENY, the OPC traffic between the Talker and Protected Device will simply be allowed or blocked accordingly without reference to the OPC Classic Enforcer LSM.



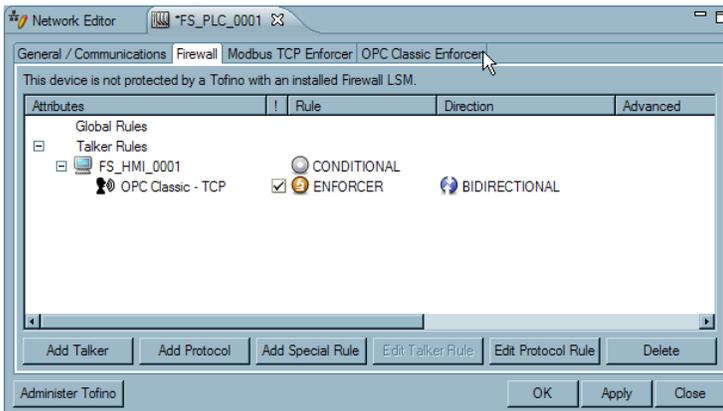
- BIDIRECTIONAL is automatically set when using the OPC Classic Enforcer LSM to allow OPC call backs from servers.



- Click "OK" once the Permission and Direction have been set.

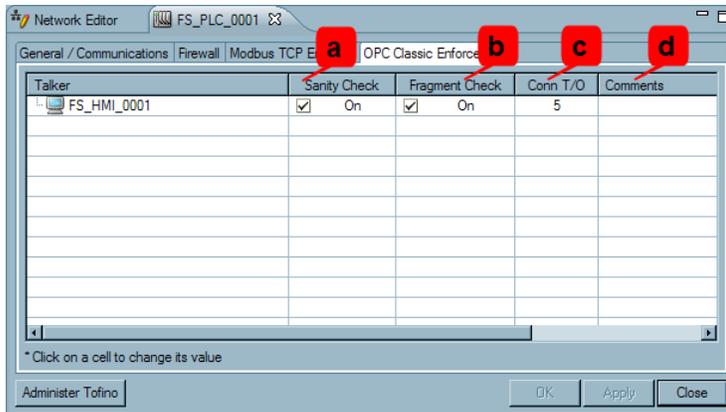


- Now click on the OPC Classic Enforcer tab.



Configuring OPC Classic Enforcer Settings

You will notice that the Talker (FS_HMI_0001) that you dragged onto the Firewall tab is already on the OPC Classic Enforcer page. It is here you can fine tune the checks that the OPC Classic Enforcer will carry out on each connection.



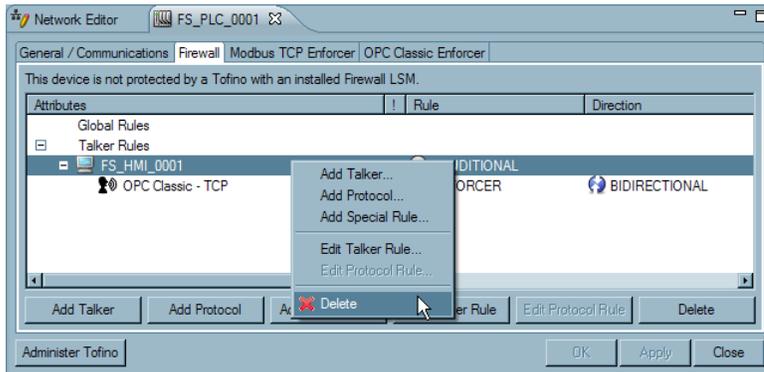
Set the general OPC Classic Enforcer filtering rules for this talker. These are:

- ▶ (a) Sanity Check: The Tofino SA can check if the connection establishment messages are properly formed and follow the RPC specification. If they do not, the Tofino SA can be directed to block the message.
- ▶ (b) Fragment Check: The Tofino SA can check if the connection establishment messages have been fragmented. If they are, the Tofino SA can be directed to block the message.
- ▶ (c) Conn T/O: OPC Connection timeout in seconds. The amount of time the Tofino SA will wait for for an OPC connection after a port has been requested
- ▶ (d) Comments: This field is available as a convenience, so the control engineer may add text to help describe or document the OPC rules that have been set up on the Tofino SA.

Deleting a Talker

To delete a Talker from the OPC Classic Enforcer page, you must click on the Firewall tab and delete the talker from the Firewall page. To do so right click on the Talker on the Firewall page and select "Delete".

Note: Any Talker will automatically be removed from the OPC Classic Enforcer page if the Permission of the OPC TCP rule on the Firewall page is set to anything other than ENFORCER (i.e.: ALLOW, ALLOW_LOG, DENY, DENY_NO LOG) or if the OPC Classic TCP protocol is deleted from the Firewall page.



6.6 VPN LSM Management

6.6.1 About VPN LSM

What is a VPN?

A virtual private network (VPN) is a network technology that uses a (possibly) insecure public network (often the Internet) to securely connect remote sites or users together.

How does a VPN protect my control data over an insecure network like the Internet?

VPNs first validate the identity of a device or person wishing to join the network (authentication) and then encrypt the traffic that is being passed between VPN endpoints (tunneling).

Why would I want to install a VPN in my control network?

A VPN provides the same type of security on a network as an armored car can for securely transporting company information between physical premises. It protects information in transport from the "outside" world. For the IACS environment, the outside world typically includes both the Internet and corporate LAN users who are not authorized to operate control equipment. (ANSI/ISA-TR99.00.01-2007 pg.60)

What are some common ways I can use a VPN?

- ▶ Securely connect remote plants to a central facility over the corporate WAN or Internet
- ▶ Provide secure remote access to your plant for maintenance personnel
- ▶ Allow older, non-IP equipment to communicate on IP networks

What does the Tofino VPN Server LSM do?

The VPN Server LSM enables multiple VPN clients to connect to a specific Tofino SA. The clients can be either Tofino SA or computers with a VPN PC Client package and license installed.

What does the Tofino VPN Client LSM do?

The VPN Client LSM enables a Tofino SA to securely connect to another Tofino SA that is acting as a VPN Server.

What does the Tofino VPN PC Client License do?

The VPN PC Client license enables a computer to securely connect to a Tofino SA that is acting as a VPN Server.

Why are there separate VPN Client and Server LSMs?

Making separate LSMs both simplify the configuration for users and lower the costs of the LSMs to users.

I have heard that VPNs can be difficult to configure. Is that true for Tofino?

Tofino VPN configuration is simple in most cases— just drag and drop client devices

Why does my Tofino need an IP address to have the VPN LSM operate?

How do the Tofino SA modes affect the VPN LSMs?

Can I use VLANs with the VPN LSMs?

What limitations are there in using VLANs with the VPN LSMs?

onto the VPN Server tab in the Tofino SA Central Management Platform to create the VPN connections. There may be some cases that more complex.

The VPN LSM functions as a server/client pairing; this requires a contact point between devices to establish the encrypted tunnel.

- ▶ In PREDEPLOYED mode you can activate and configure the VPN LSMs in the Tofino CMP, but they are not pushed out to the Tofino SA. This is useful for pre-configuring Tofino SAs or setting up USB loaded configurations.
- ▶ In PASSIVE mode you can install and configure the VPN LSMs on the Tofino SA, but they have no impact on the network.
- ▶ In TEST mode, the VPN LSMs establish a VPN tunnel between client and server, but do not route traffic through this tunnel. This allows you to test the viability of the connection before committing control traffic to it.
- ▶ In OPERATIONAL mode, all traffic is directed through the encrypted tunnel. If the tunnel is not functional, all traffic will be blocked.

Yes, the Tofino SA VPN will transport VLAN-tagged messages over a routed network, allowing VLANs to persist over wide area network like the Internet.

The Tofino VPN will encrypt and then transport VLAN-tagged messages from the trusted/unencrypted network. However the encrypted VPN (SSL) traffic on the untrusted or wide area network interface of the Tofino SA must be untagged.

6.6.2 Using the VPN LSMs

The VPN Client LSM and the VPN Server LSM allow encrypted communications tunnels to be set up from Tofino SA to Tofino SA, as well as between Tofino SAs and PCs and 3rd party VPN servers. These tunnels can both offer protection to critical network traffic traveling over unsecured networks (such as the Internet) as well as allow older non-IP protocols to be transported seamlessly over modern IP-based networks.

Ensure that the VPN Client and/or VPN Server LSM(s) are installed and activated.

To set up VPN connections between a Tofino SA VPN Server and either a Tofino SA VPN Client or VPN PC Client, it is recommended that the following steps be taken:

- Configure the Tofino SA acting as the VPN server. See: [Setting up a Tofino SA as a VPN Server](#)
- Configure any Tofino SAs acting as VPN clients. See: [Setting up a Tofino SA as a VPN Client](#)
- Set up any VPN tunnels between the Tofino SA server and Tofino SA clients. See: [Setting up a VPN Tunnel between a Tofino SA Server and a Tofino SA Client](#)
- Set up any VPN tunnels between the Tofino SA server and VPN PC Clients. See: [Setting up a VPN Tunnel between a Tofino SA Server and a VPN PC Client](#)
- Install the VPN PC Client Software and configuration files in appropriate PCs. See: [Installing the VPN PC Client on Your Computer](#)
- Test the connectivity of the VPN tunnels. See: [Testing Your VPN Tunnel](#)
- Activate the VPN tunnels. See: [Activate Your VPN Tunnel](#)

Important: Your Tofino SA must have a valid IP address assigned to it before it is configured to act as a VPN Server or VPN Client. Failure to have a an address that is reachable from the Tofino CMP may mean loss of all connectivity to that Tofino SA. For information on setting a Tofino SA's IP Address see: [Tofino SA Contact Devices](#)

Setting up a Tofino SA as a VPN Server

To set up a Tofino SA as a server, complete the following steps:

- Locate the Tofino SA in your network diagram that will be the VPN server and double click on it's icon. The Tofino SA properties page will open.
- Ensure that the IP address and the subnet mask of the Tofino SA is correctly set. This IP address should be the local network address of the Tofino SA. For example, if the Tofino SA is located on a control network with an IP address range of 192.168.1.0/24 then the IP address should be in this range. Also See: *Public IP Address* below.

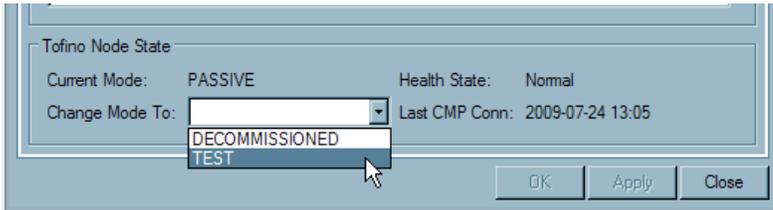
WARNING: Failure to have a an IP address that is reachable from the Tofino CMP may mean loss of all connectivity to that Tofino SA, including Tofino CMP connectivity.

The screenshot shows the 'VPN Server' configuration window in the Network Editor. The window title is 'Jasper Compressor Station Tofino'. The 'General Settings' tab is active. The configuration includes:

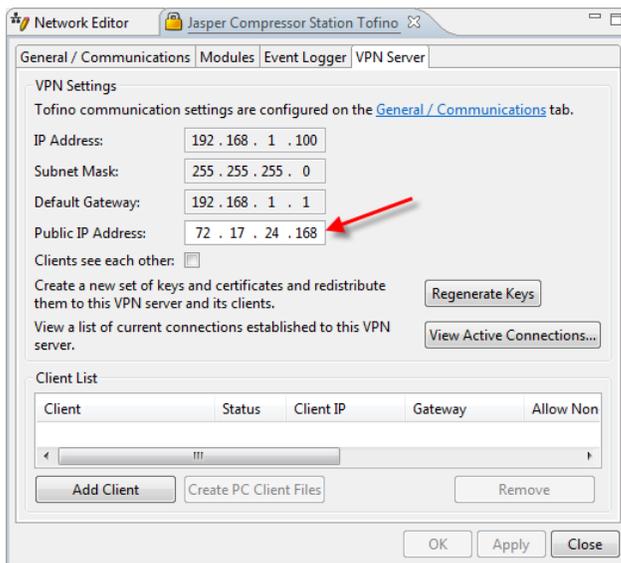
- Name: Jasper Compressor Station Tofino
- General Location: (empty)
- Specific Location: (empty)
- Tofino ID: 00 : 00 : 11 : 8D : B1 : 34
- Primary Contact: JP_PL_C_0002
- Backup Contact: -- NONE --
- Heartbeat Interval (s): 10
- USB Load Config: Enabled
- Untrusted Media Type: auto
- Trusted Media Type: auto
- Mode Button Behavior: Toggle
- Mode Button Timeout (m): 60
- IP Address: 192 . 168 . 1 . 100
- Subnet Mask: 255 . 255 . 255 . 0
- Default Gateway: 192 . 168 . 1 . 1
- Link State Pass Through:

A note on the right side of the IP address field states: 'The IP address details are not required unless the VPN Client, VPN Server, or Event Logger LSM is activated.'

- Ensure the Tofino SA is in TEST or PASSIVE mode. We do not recommend attempting to set up a VPN on a Tofino SA that is in OPERATIONAL mode.

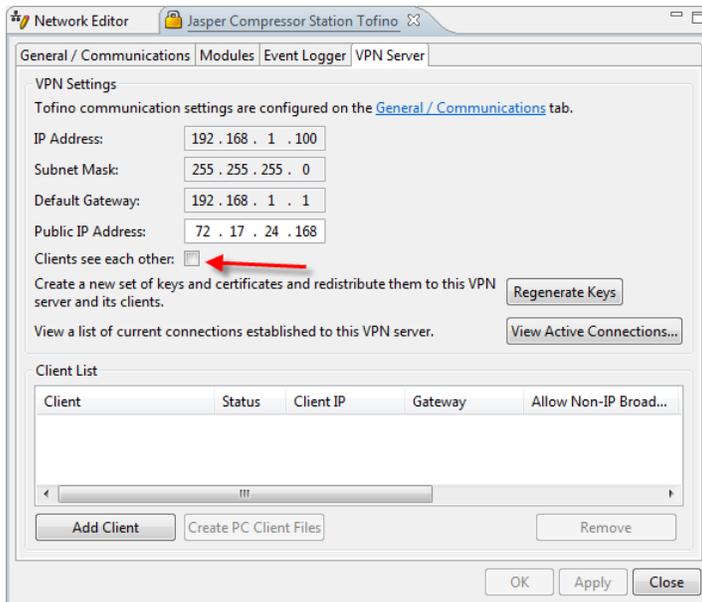


- Select the VPN Server tab.
- Set the *Public IP Address* for the VPN Server. This address is used when the IP address of the Tofino VPN Server, as seen by the outside world, is not the same as the IP address used by the Tofino SA on the internal network. For example, if the internal IP Address of the Tofino SA is 192.168.1.100, but because of Network Address Translation (NAT) in an Internet-facing router, the outside world might see the Tofino SA as having the Internet routable address of 72.17.24.168.
Note: If NAT is not used, this address should be set to either 0.0.0.0 or the same IP address as the Tofino SA's actual address.



- If you want this Tofino SA's remote clients to be able to communicate to each other via this Server, check the *Clients Can See Each Other* box; otherwise Clients will only be able to communicate to the network behind the Tofino VPN Server.

WARNING: When using the “Clients see each other” option, the remote networks may not share address spaces either via explicit IP segment or classless subnet masking. For example, two remote networks may not be both set at 192.168.1.x. with a subnet of 255.255.255.0 or within the entire network of 10.x.x.x when the subnet mast is 255.0.0.0. Advanced network design assistance is available from your authorized Tofino representative. (The above guidance is only applicable to networks that are truly remote and not while making a secure encrypted connection to a Tofino SA that is on the local network).



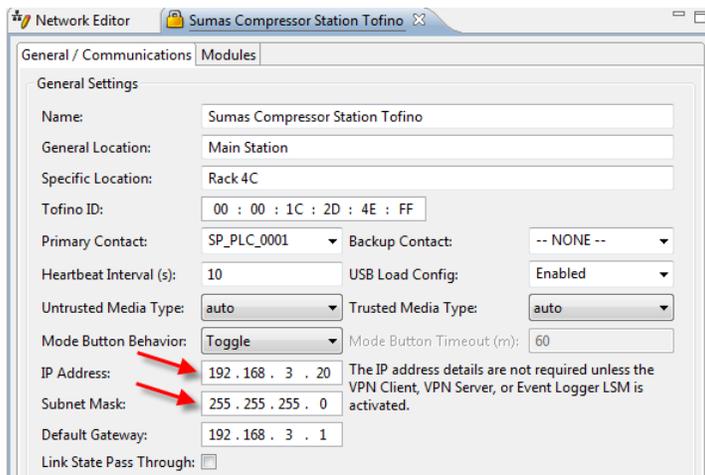
- Click "OK".

Setting up a Tofino SA as a VPN Client

To set up a Tofino SA as a client, complete the following steps:

- Locate the Tofino SA in your network diagram that will be a VPN client and double click on it's icon. The Tofino SA properties page will open.
- Ensure that the IP address and the subnet mask of the Tofino SA is correctly set. This IP address should be the local network address of the Tofino SA. For example, if the Tofino SA is located on a control network with an IP address range of 192.168.3.0/24 then the IP address should be in this range. The Public IP Address of the Tofino SA that is acting as the VPN Client, is not required.

WARNING: Failure to have a an IP address that is reachable from the Tofino CMP may mean loss of all connectivity to that Tofino SA, including Tofino CMP connectivity.

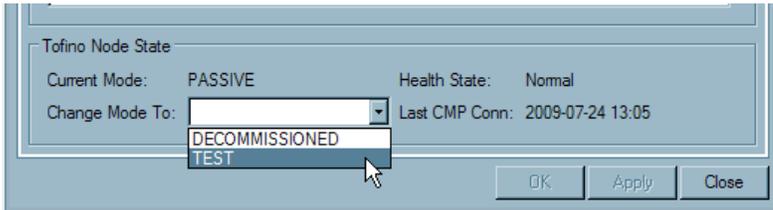


The screenshot shows the 'Network Editor' window for a device named 'Sumas Compressor Station Tofino'. The 'General / Communications' tab is active, and the 'Modules' section is expanded to show 'General Settings'. The following fields are visible:

- Name: Sumas Compressor Station Tofino
- General Location: Main Station
- Specific Location: Rack 4C
- Tofino ID: 00 : 00 : 1C : 2D : 4E : FF
- Primary Contact: SP_PLC_0001 (dropdown)
- Backup Contact: -- NONE -- (dropdown)
- Heartbeat Interval (s): 10
- USB Load Config: Enabled (dropdown)
- Untrusted Media Type: auto (dropdown)
- Trusted Media Type: auto (dropdown)
- Mode Button Behavior: Toggle (dropdown)
- Mode Button Timeout (m): 60
- IP Address: 192 . 168 . 3 . 20
- Subnet Mask: 255 . 255 . 255 . 0
- Default Gateway: 192 . 168 . 3 . 1
- Link State Pass Through:

Two red arrows point to the IP Address and Subnet Mask fields. A note next to the IP Address field states: 'The IP address details are not required unless the VPN Client, VPN Server, or Event Logger LSM is activated.'

- Ensure the Tofino SA is in TEST or PASSIVE mode. We do not recommend attempting to set up a VPN on a Tofino SA that is in OPERATIONAL mode.



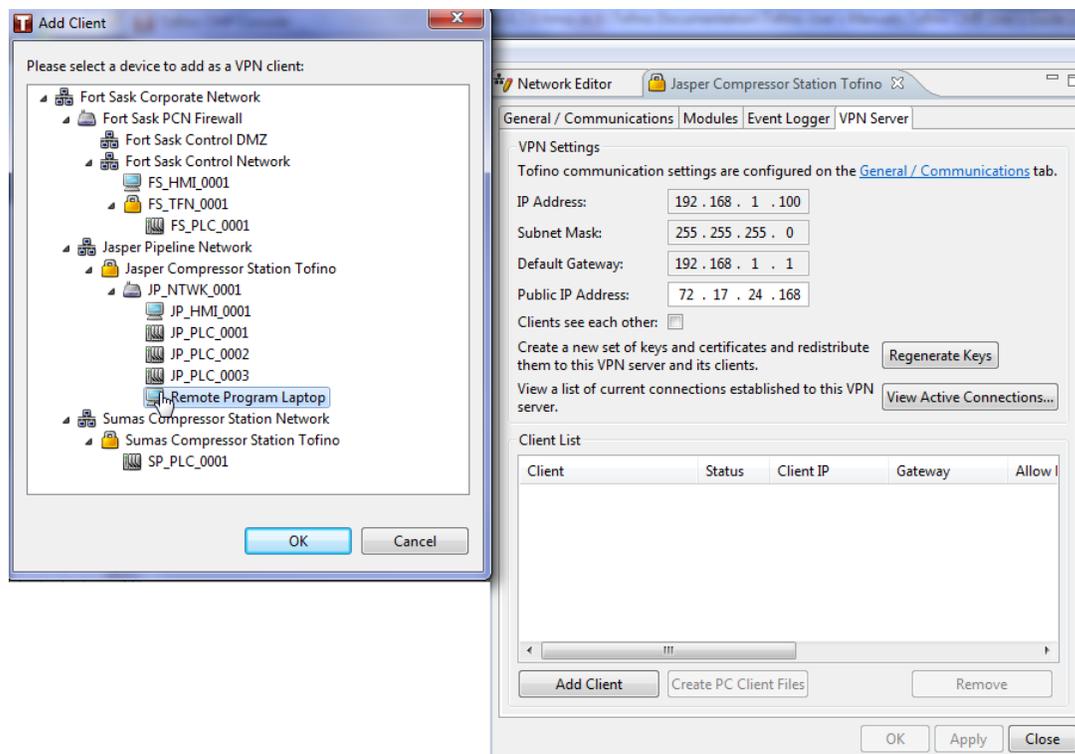
- Click "OK".

Setting up a VPN Tunnel between a Tofino SA Server and a VPN PC Client

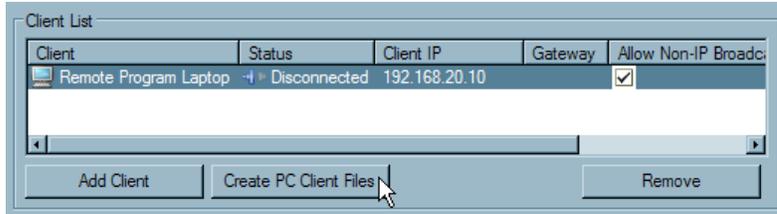
Many users require the capability to have maintenance laptops connect to a Tofino SA VPN to allow remote support for the control system. To make this easy for the user, the Tofino CMP contains a built-in software wizard that will enable Windows' computers to act as clients. The Tofino CMP will create custom install packages for each PC that contain both a free VPN client package and all required VPN configuration files so they can be installed on a Windows PC in a single process. (**Note:** VPN PC Client licenses are required to use this feature).

This section explains how to configure the tunnel between a VPN Server and VPN PC client.

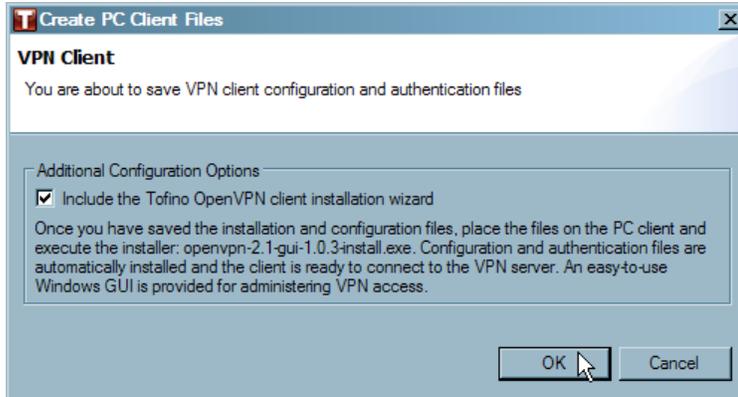
- Create nodes in the Network Editor to represent each remote PC.
- Set the IP address and subnet mask of each remote PC to unique IP addresses within the subnet range defined on the Tofino SA VPN Server tab. Note that this is a virtual IP address. The actual IP address set on the remote PC should not be entered. For example, if the Tofino SA has an addresses of 192.168.1.100 and a subnet mask of 255.255.255.0 then the remote PC should be assigned an unused address in the range of 192.168.1.1 to 192.168.1.254. Also note that the real IP address of the remote PC must not be in this range.
- Double click on the Server Tofino SA icon in the Network Editor.
- Click on the VPN Server tab.
- Now you will need to select the PC Client(s) you would like to establish VPN tunnels with. To do this, drag the desired VPN PC Clients from the *Network View* and drop them onto the *Client List*.
Note: Alternatively, you can add a client to the client list by clicking on the Add Client button.



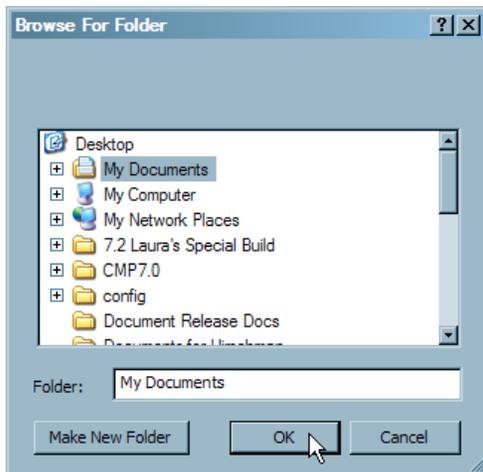
- Once you have added in the clients you wish to establish connections to, click "Apply".
- Once a VPN PC Client has been added to the Client List on a Tofino SA VPN Server Tab, the VPN PC Client needs to have a configuration file and security certificates created. At the same time, a VPN PC Client installation program can be created and included with the configuration/certificate files. Click on the VPN PC Client you wish to create files for.



- Click on the "Create PC Client Files" button and a window will open
- If you would like to install the Tofino VPN PC Client software on your remote computer, check the box that says Include the Tofino OpenVPN client installation wizard; otherwise, to simply save the config files to a location of your choice, click "OK".



- Regardless of the route you choose, a Browse for Folder window will open, allowing you to choose the location to save the configuration files or the combined installation wizard and configuration files. Click "OK" once the location has been chosen.

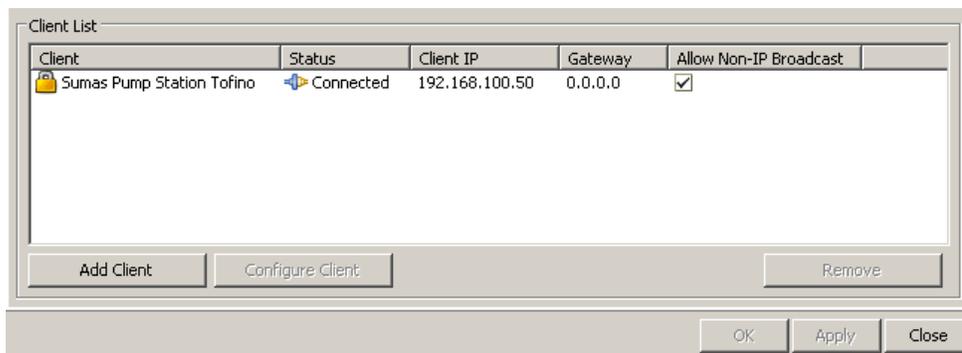


- Either the configuration files or the installation wizard will be saved to the location of your choice. These files can then be moved to the remote computer of your choice. See: [Installing the VPN PC Client on Your Computer](#)
- Note:** For each client you configure, you will require a VPN PC Client license. See: [VPN PC Client Licensing](#)
- Click "OK" to have the final configurations pushed out to the Tofino SA.

Testing Your VPN Tunnel

To test your VPN tunnel follow these steps:

- Change all Tofino SAs running VPN LSMs to TEST mode.
- Watch the *Status* column on the *Client List* on the VPN Server tab. Once this is set to *Connected* the VPN tunnel has been successfully established. If an error appears the error status should indicate the type of problem that exists. **Note:** You can also watch the Heartbeats in the *Event View* for up-to-date information on the VPN status.



WARNING: We do not recommend putting the Tofino SA into OPERATIONAL mode until the connection is proven in TEST mode.

Activating Your VPN Tunnel

Once you have tested your VPN tunnel and the status is *Connected*, follow these steps:

- Place both client and server Tofino SAs into OPERATIONAL mode. It is strongly recommended that you change the mode of the Tofino SA furthest from the Tofino CMP first. Use the following to remember the order for setting up and taking down a VPN tunnel.
 - ▶ When putting the VPN into OPERATIONAL mode, build your defenses from the outside inward towards the Tofino CMP
 - ▶ When taking the VPN out of OPERATIONAL mode, tear down your defenses from the inside outward away from the Tofino CMP

WARNING: All network traffic between the Tofino SA VPN Client and the VPN Server will be temporarily blocked until the modes are matched.

- Wait until the status says *Connected*.

With your VPN activated, all traffic directed through the VPN client from the non-VPN side (the trusted interface) will be encrypted and routed to the VPN server (and vis-versa).

6.6.2.1 3rd Party Servers

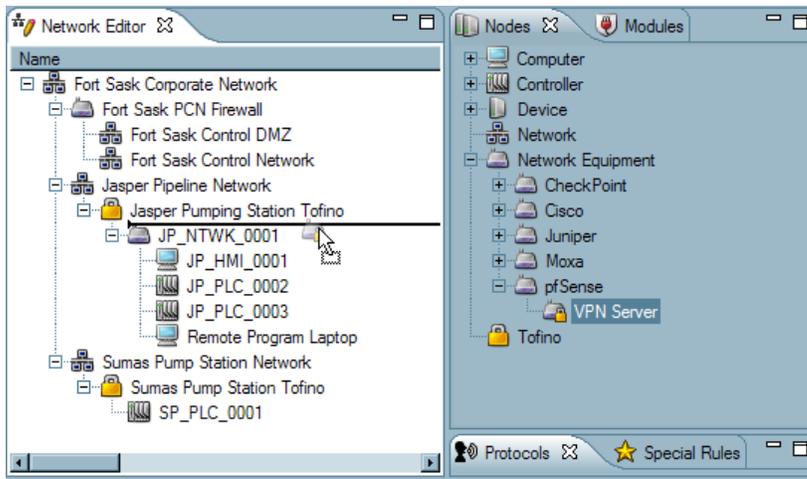
Currently the Tofino CMP supports pfSense VPN servers. If you would like to use a different type of VPN server, please contact support@tofinosecurity.com.

Ensure that the VPN Client LSM is installed and activated.

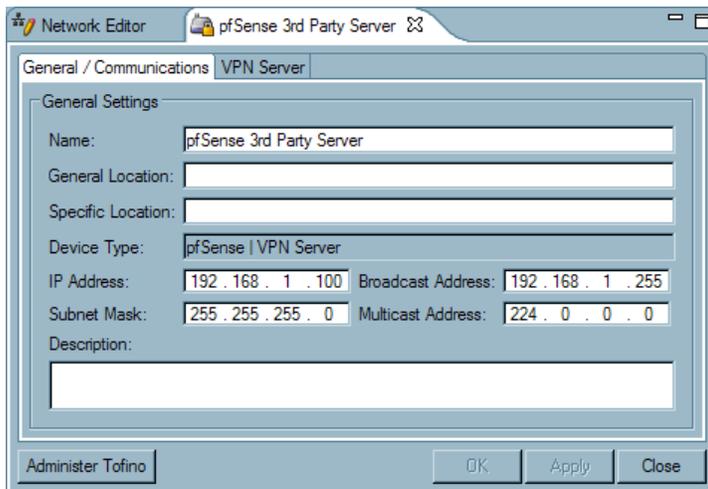
Setting Up a 3rd Party Server

To set up a 3rd party VPN server follow these steps:

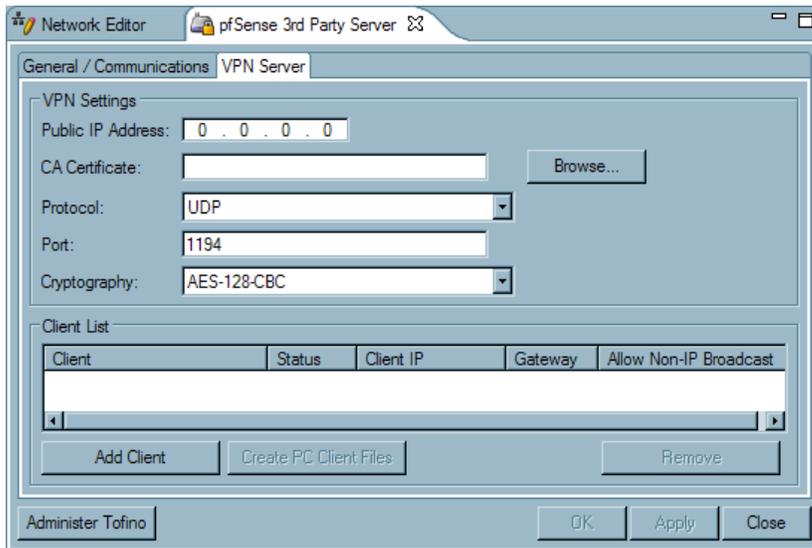
- Drag the appropriate 3rd party server icon from the Nodes window into the Network Editor.



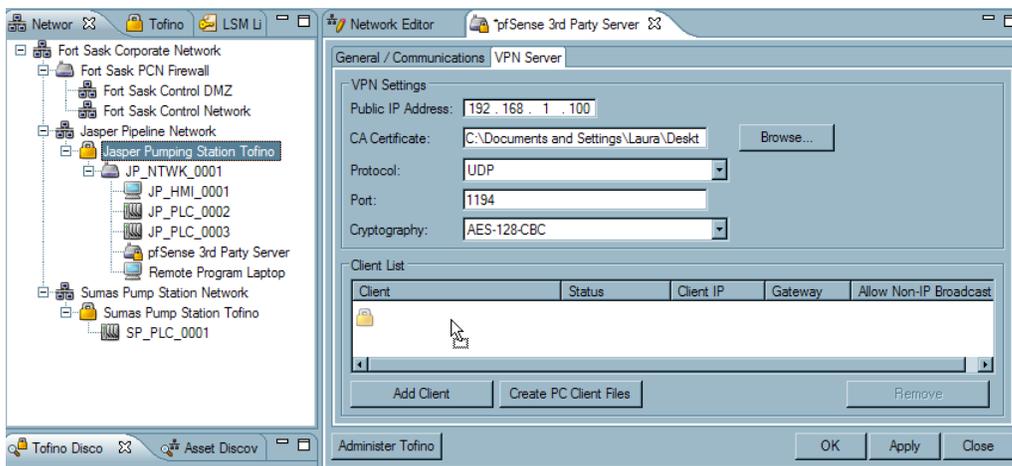
- Next, double click on the 3rd party server icon to open the Properties page.



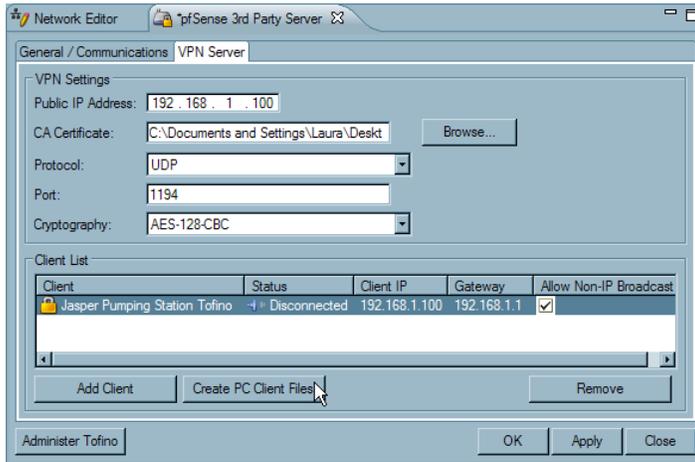
- ❑ Click on the VPN Server tab.



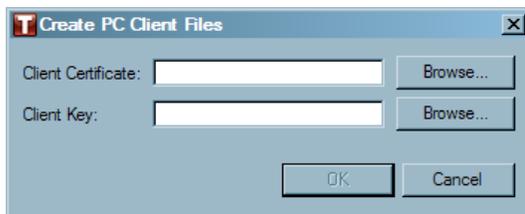
- ❑ Set the Public IP Address, if different than the IP Address.
- ❑ Click "Browse..." to select a CA certificate. This must be configured on the Tofino SA.
- ❑ Select a protocol, enter a port number and select the type of cryptography the server uses. This information will be used to automatically configure Tofino SA VPN clients.
- ❑ Add the clients, you wish to connect to the server, onto Client List. This can be done by dragging and dropping from the Network View, or by using the Add Client button. Note that only Tofino SAs can be clients to 3rd party servers.



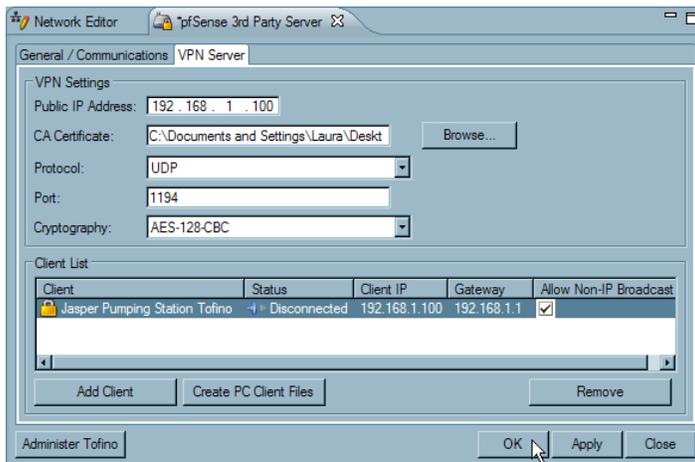
- Once you have added all the clients to the client list that you wish to add, click on a client to highlight it and then click the "Create PC Client Files" button.



- Click "Browse..." to find the Client Certificate and the Client Key for this client and select these files. Click "OK". **Note:** The Client Certificate and the Client Key must be supplied by the administrator of the 3rd party VPN server.



- Click "OK" to push the configuration out to the Tofino SA.



- The Tofino SA will now attempt to establish a connection to the 3rd party VPN server, provided it is in TEST or OPERATIONAL mode.

6.6.2.2 VPN Server and Client Tabs

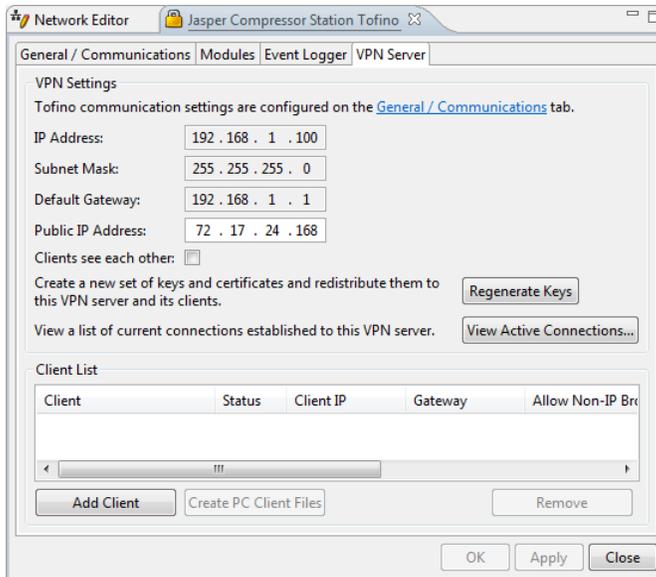
See: [Working with the VPN Server Tab](#)

See: [Working with the VPN Client Tab](#)

See: [Working with the VPN \(3rd Party\) Server Tab](#)

Working with the VPN Server Tab

This tab allows you to modify various VPN server settings, add and remove VPN clients for that server, view all active connections and regenerate VPN certificates



VPN Settings

- ▶ **IP Address:** This is configured on the General/Communications page. This IP address should be a local address in subnet used on the trusted network.
- ▶ **Subnet Mask:** This is configured on the General/Communications page. The subnet mask for the IP address of the Tofino SA on the network it is physically connected to.
- ▶ **Default Gateway:** This is configured on the General/Communications page. The default gateway for the Tofino SA on the network. This is where traffic will be directed if the Tofino SA cannot identify the destination node for an IP of a packet it must deliver.
- ▶ **Public IP Address:** This address is the IP address of the Tofino VPN Server as seen by the outside world when a router is used to isolate the VPN server from an external untrusted network and to give the Tofino a routable IP address. For example, the internal IP Address of the Tofino SA might be 192.168.1.100, but the outside world might see the Tofino as having the external address of 72.17.24.168. If NAT (Network Address Translation) is not used, this address should be set to either 0.0.0.0 or the same IP address as the Tofino SA's actual address. This must be set in order for a VPN tunnel to be established.
- ▶ **Clients see each other:** If checked, a pathway is created between all clients and server (i.e. a mesh network); clients may receive and direct traffic destined for other clients instead of just with the server. **WARNING: When using the "Clients see each other" option, the remote networks may not share address spaces either via explicit IP segment or classless subnet masking.**
- ▶ **Regenerate Keys:** This button will create a new set of keys and certificates and redistributes them

to the VPN server and its clients.

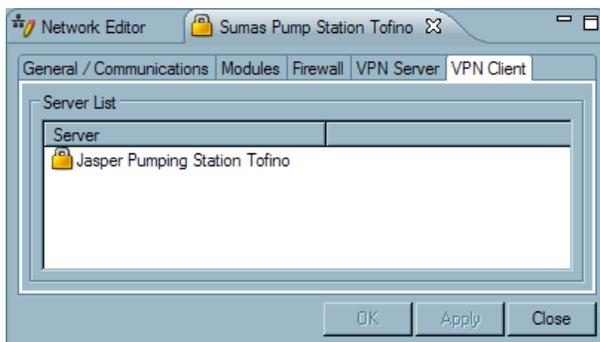
- ▶ View Active Connections: This button will open a window that lists the clients that are currently connected to the server.

Client List

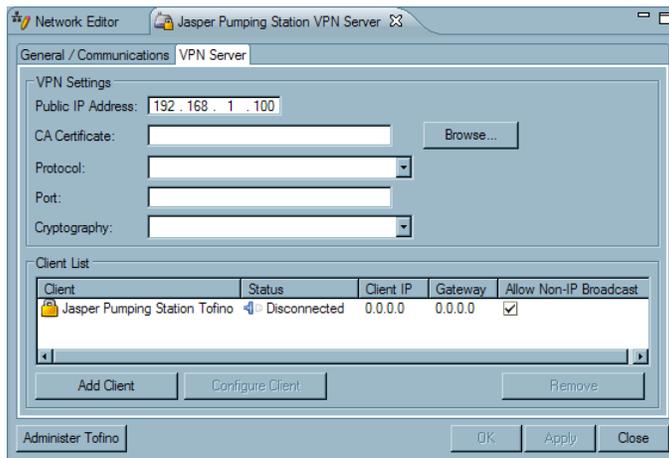
- ▶ Client: Lists the client(s) name(s).
- ▶ Status: Indicates the condition of the client LSM in relation to the server. For example, if the status is Host Unreachable this would indicate that the Client LSM is unable to communicate with the server.
- ▶ Client IP: Lists the client(s) IP address.
- ▶ Gateway: Lists the client(s) gateway.
- ▶ Allow Non-IP Broadcast: The default setting is for this box to be checked. If this box is not checked it will block non-IP broadcast traffic from devices behind the client from going into the tunnel.
- ▶ Use Public IP Address: The default setting is for this box to be unchecked. If this box is checked the the VPN Server Tofino SA Public IP address will be used when connecting. Otherwise, the private address will be used.
- ▶ Comments: This area is used to make comments about the Client List.

Working with the VPN Client Tab

- ▶ Server: Lists the server the client is connected to.



Working with the VPN (3rd Party) Server Tab



VPN Settings

- ▶ **Public IP Address:** This address is the IP address of the Tofino VPN Server as seen by the outside world when a router is used to isolate the VPN server from an external untrusted network and to give the Tofino a routable IP address. For example, the internal IP Address of the Tofino might be 192.168.1.100, but the outside world might see the Tofino as having the external address of 72.17.24.168. **Note:** If NAT (Network Address Translation) is not used, this address should be set to either 0.0.0.0 or the same IP address as the Tofino SA's actual address. This must be set in order for a VPN tunnel to be established.
- ▶ **CA Certificate:** These certificates are created by the user, Browse and search for certificate.
- ▶ **Protocol:** The protocol to be used by all clients of the VPN server (UDP or TCP).
- ▶ **Port:** The remote port that the client uses to connect to the server. Only numeric values can be accepted (Such as 1194).
- ▶ **Cryptography:** The type of cryptography used by the server.

Client List

- ▶ **Client:** Lists the client('s) name(s).
- ▶ **Status:** Indicates the condition of the client LSM in relation to the server. For example, if the status is Host Unreachable this would indicate that the Client LSM is unable to communicate with the server.
- ▶ **Client IP:** Lists the client('s) IP address.
- ▶ **Gateway:** Lists the client('s) gateway.
- ▶ **Allow Non-IP Broadcast:** The default setting is for this box to be checked. If this box is not checked it will block non-IP broadcast traffic from devices behind the client from going into the tunnel.
- ▶ **Use Public IP Address:** The default setting is for this box to be unchecked. If this box is checked the Public IP address will be used to connect to the VPN Server otherwise the private address will be used.
- ▶ **Comments:** This area is used to make comments about the Client List.

6.6.2.3 Installing the VPN PC Client

When a PC Client has been added to the Client List on a Tofino SA VPN Server Tab, configuration files and security certificates are created. Optionally, a VPN PC Client installation program can be created and included with the configuration/certificate files. This section explains how to install these files and software on a remote computer.

See: [Using the Installation Wizard](#)

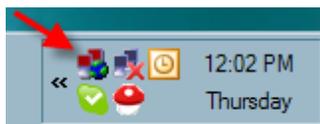
See: [Using the Configuration Files](#)

Using the Installation Wizard

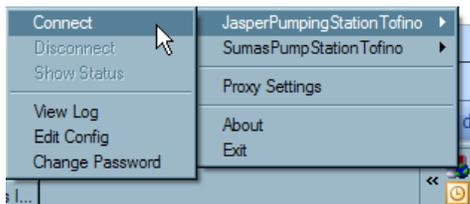
- Use a USB key to transport the configuration files to the appropriate remote computer.
- Once you have placed the USB key in the remote computer, double click on the ".exe" icon to start the installation process. To learn how to obtain the installation wizard and the configuration files, see: [Using the VPN LSMs](#)
- Follow the Tofino OpenVPN Installation wizard.



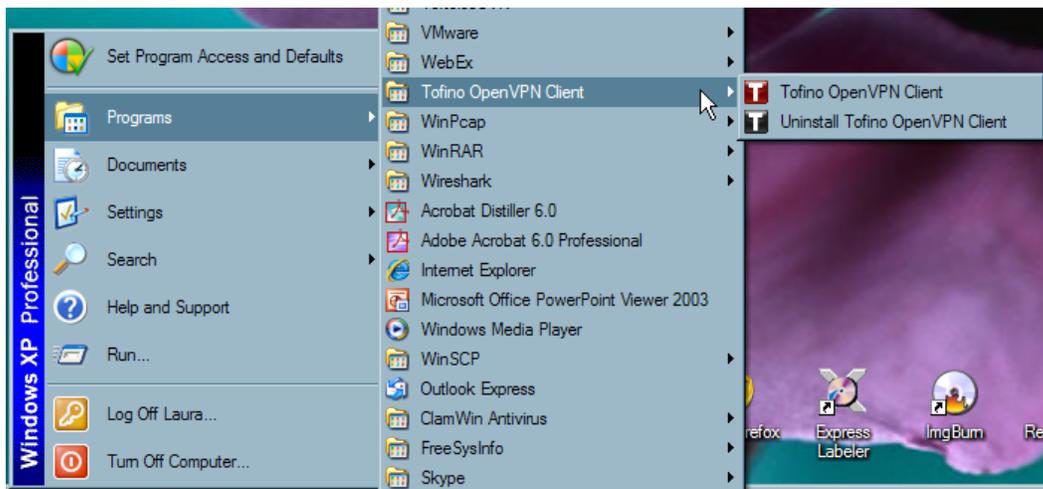
- Once the Tofino OpenVPN program has been installed on your computer, it will appear in the bottom right-hand side of your screen.



- From this icon, you can connect to the Tofino SA server(s) that you have set up.



- Also note, that the Tofino OpenVPN Client can be run and uninstalled from the Start menu.



Using the Configuration Files

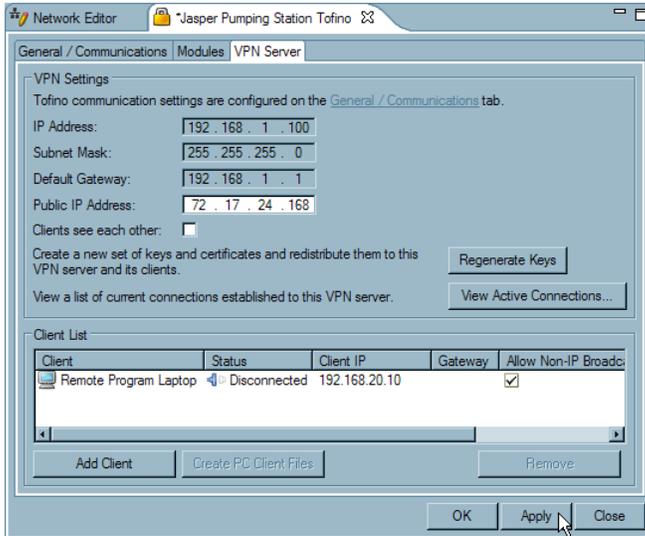
If a VPN PC Client software package (or equivalent OpenVPN software package) is already installed on the remote computer, then the software can be configured to communicate with the Tofino SA VPN Server by simply installing the configuration files in the correct location.

- Take the files that are in the config folder and place them in the folder C:\Program Files\Tofino OpenVPN Client\config on the remote computer.
- Restart the remote computer.

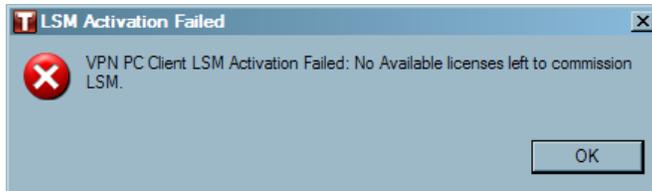
6.6.2.4 VPN PC Client Licensing

In order to use a VPN PC Client, a license needs to be obtained. See: [LSM Licensing](#)

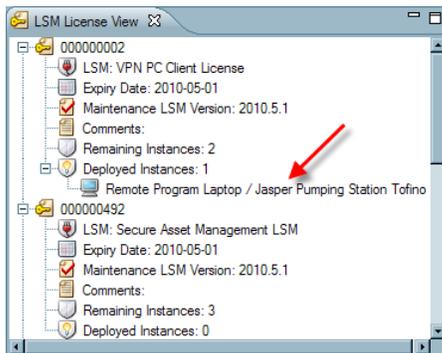
Once a VPN PC Client has been added to the Client List on a Tofino VPN Server tab and this is applied, by clicking the "Apply" button, a license will be used.



If there are insufficient licenses available, an error will display and the system will not add any new PC Clients. You must then modify the list of PC Clients to match the available number of licenses before you can save your changes.



If a license is used, it will display in the License View, and the deployed instance will indicate the VPN Tofino SA Server and the VPN PC Client.



6.6.3 Locating the Tofino CMP when Using the VPN

The location of the Tofino CMP computer in the network is an important factor when using the Tofino VPN LSMs. There are two cases for the Tofino CMP computer locations:

- The Tofino CMP is located on the untrusted (i.e. encrypted) side of all Tofino SAs. This is the simplest case and no modifications are required.
- The Tofino CMP is located on the trusted (i.e. unencrypted) side of one or more Tofino SAs.

If case #2 applies to your network, you must make the following changes so that the Tofino CMP computer can manage both the local and remote Tofino SA.

Note: Make these changes while both Tofino SAs are in Passive or Test mode. Making these changes while the VPN is active may cause loss of communications.

- Ensure there is a global firewall rule on the local Tofino SA (i.e. the Tofino SA closest to the Tofino CMP) to allow the "Tofino CMP" protocol. This rule should have the direction set to Bidirectional.
- Select a protected device that is on the trusted interface of the remote Tofino SA as the primary contact device for that Tofino SA.
- Select the same protected device (i.e. on the trusted interface of the remote Tofino SA) as the primary contact device for the local Tofino SA. To do this, Select "More..." on Primary Contact combo box, then select the device from network tree.
- On the Tofino CMP computer you must add a static ARP entry for the remote Tofino SA. This ARP entry must be in place whenever the Tofino CMP is running, so enter this command in a DOS batch file and configure the PC to run the batch file automatically each time the computer is re-started.

See: [Tofino 220](#)

See: [Tofino 100](#)

Tofino 220

The command is of the form

```
arp -s [Tofino ID] [MAC]
```

where [Tofino ID] and [MAC] are the Tofino ID and MAC address of the remote Tofino SA

For example, if the IP address of the remote Tofino SA is 172.18.1.77 and the Tofino ID is 00-80-63-a7-84-c1 then the command should be:

```
arp -s 172.18.1.77 00-80-63-a7-84-c1
```

Tofino 100

The command is of the form

```
arp -s [IP] [MAC]
```

where [IP] and [MAC] are the IP and MAC address of the remote Tofino SA

For example, if the IP address of the remote Tofino SA is 172.18.1.77 and the MAC address is 00-80-63-a7-84-c1 then the command should be:

```
arp -s 172.18.1.77 00-80-63-a7-84-c1
```

For more on how to find your Tofino SA's MAC address see: [Appendix A](#)

Mode Change – ‘Test’ to ‘Operational’

When changing modes from Test to Operational, you must change the mode on the remote Tofino SA FIRST, then change the mode of the local Tofino SA.

All connections between remote and local PCs will be broken as soon as the remote Tofino SA enters Operational mode, and it may take up to 4-5 minutes after BOTH Tofino SA's enter Operational mode before the VPN tunnel is established and passing traffic.

Even after the tunnel is established, the remote Tofino SA may be displayed as ‘Missing’ in the Tofino CMP Network Editor View. To rectify this, open the General/Communications settings page for the remote Tofino SA and change the Heartbeat Interval setting. This will create a connection through the tunnel from the Tofino CMP to the remote Tofino SA, and the Tofino SA will begin sending heartbeat status messages through the tunnel to the Tofino CMP. After this has been completed, the VPN tunnel will be used to manage and monitor both Tofino SA devices, and no further operator intervention should be required for the system to operate correctly.

Mode Change – ‘Operational’ to ‘Test’

When changing modes from Operational to Test, change the mode in the reverse order – that is, change the mode on the local Tofino SA FIRST, then change the mode on the remote Tofino SA. When this is done, the remote Tofino SA may go missing and communications between local and remote PCs will be interrupted until both Tofino SA's are in Test mode.

Additional Notes

When changing modes, you may encounter an error dialog reporting a connection timeout. Please close this dialog and check to see if the Tofino CMP indicates that the mode change was successful. If so, then you can safely ignore this error dialog. This error occurs because the Tofino SA's internal bridge is re-configured during the mode change, and the control connection from Tofino CMP is broken when this happens. However the connection is only broken after all configuration changes have been sent to the Tofino SA, so it is of no consequence. The connection is immediately re-established the next time the Tofino CMP contacts the Tofino SA.

6.7 Event Logger LSM Management

6.7.1 About Event Logger LSM

What is the Event Logger LSM?

The Event Logger LSM records security events on a Tofino SA.

Where does the Event Logger LSM record events?

The Event Logger LSM enables each Tofino SA to log events and alarms simultaneously to any of the following:

- ▶ A remote IT syslog server
- ▶ USB key in the Tofino SA
- ▶ Text files on the Tofino CMP computer

What is syslog?

Syslog is a standard for forwarding log messages in an IP network. The term "syslog" is often used for both the actual syslog protocol, as well as the application or library sending syslog messages. Syslog is a client/server protocol: the syslog sender sends a small (less than 1KB) textual message to the syslog receiver. The receiver is commonly called "syslogd", "syslog daemon" or "syslog server". Syslog messages can be sent via UDP and/or TCP. The data is sent in cleartext; although not part of the syslog protocol itself, an SSL wrapper can be used to provide for a layer of encryption through SSL/TLS. <http://en.wikipedia.org/wiki/Syslog>

Does the Tofino SA require an IP address in order to send syslog messages?

No! Starting with Tofino version 1.7.0, the Tofino SA uses special stealth technology to send syslog messages to a remote server without the Tofino SA being assigned an IP address. The syslog server will see the messages coming from either address 0.0.0.0 or 169.254.2.2, tagged with the Tofino SA's ID number. Note that this feature is only available for syslog transported over UDP (the most common form of syslog).

What happens if my Tofino SA loses its connection to the remote syslog server?

The Event Logger LSM is designed specifically for SCADA environments where communications may be sporadic and yet data loss is not tolerated. If communications between the Tofino SA in the field and the syslog server are disconnected, events can be automatically stored locally until

Why would I want to install an Event Logger LSM in my control network?

I don't have a syslog server and yet I want to record the security logs. Can I still use the Event Logger LSM?

How many logs can the Tofino SA hold without downloading?

communications are reestablished. Note that in certain conditions, logs that were already queued for transmission may not be buffered and thus not sent to the syslog server on re-connection. However, these logs will still be available via USB save and the Tofino CMP Retrieve active logs feature.

The Event Logger LSM allows you to collect complete security event logs for compliance to security standards such as NERC CIP and ANSI/ISA-99.

Yes! The Event Logger LSM will record to either a USB key or to a Tofino CMP.

The Tofino SA can hold up to 20,000 event and alarm records in its memory (enough to last over a full month if security events occur every minute).

6.7.2 Using Event Logger LSM

The Event Logger LSM offers three methods for saving event logs.

- ▶ Using the syslog protocol to forward Tofino SA exception events(heartbeats) to a remote syslog server See: [Setting up the Event Logger](#)
- ▶ Saving events to a USB key in the Tofino SA See: [Retrieving Logs Using a USB Storage Device](#)
- ▶ Sending locally logged events to a text file on the Tofino CMP computer See: [Retrieving Logs Using the Tofino CMP](#)

Any combination of these methods can be used simultaneously. Ensure the Event Logger LSM is installed and activated.

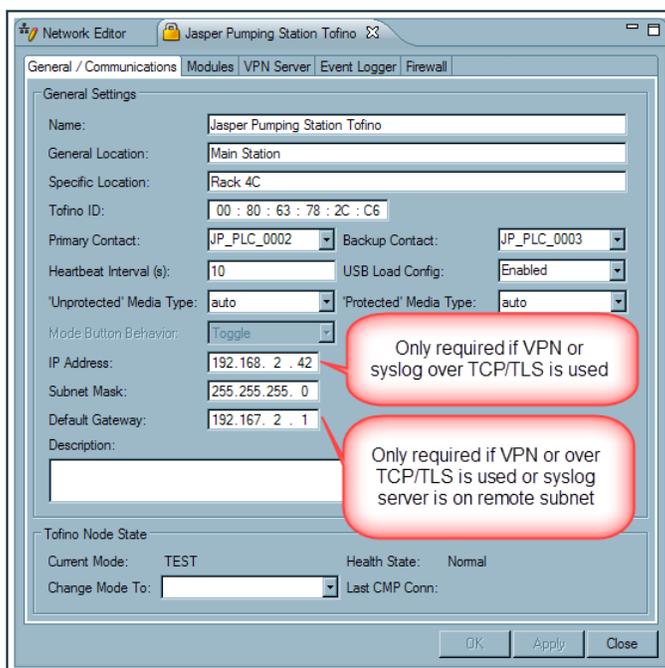
IP Addressing for Tofino SA Event Logging

Tofino's unique address-free management capability lets Tofino SAs report security events directly to 3rd party event logging and incident management systems via syslog, even if no IP address is assigned to the Tofino SA. An IP address and subnet mask on the Tofino SA is only required if logs are to be sent using the TCP or TLS transport options.

If the syslog server is located on a different subnet from the Tofino SA, then a Default Gateway address must be provided. This is the IP address of the forwarding router on the network where the Tofino SA is located. This is only required if the syslog server is NOT on the same network as the Tofino SA. If the remote syslog feature is not being used, or if the Tofino SA and the syslog server are on the same subnet, this field can remain blank.

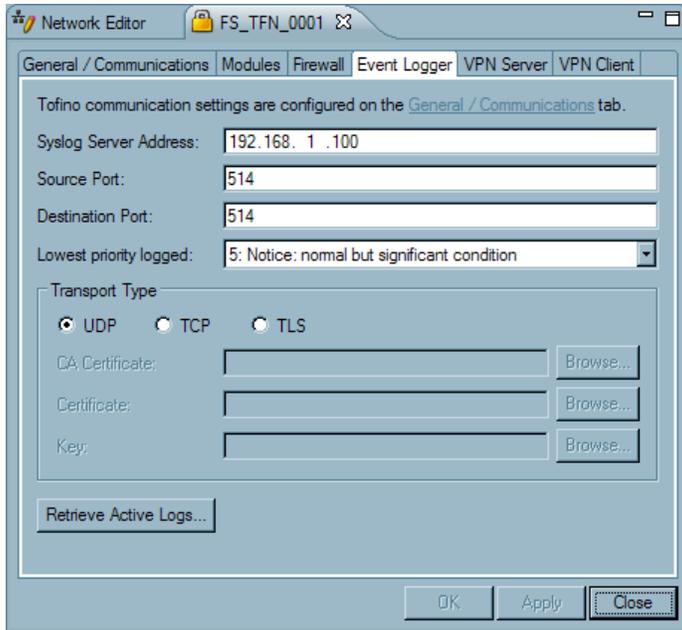
The both the Default Gateway and the Tofino SA IP address are set on the General/Communications tab. See: Working with Your Tofino SA

Note: If VLANs are being used for device management, the syslog server and the Tofino CMP must be located on the same management VLAN. Defining two VLANs for Tofino SA management and reporting can cause intermittent communications.



Setting up the Event Logger

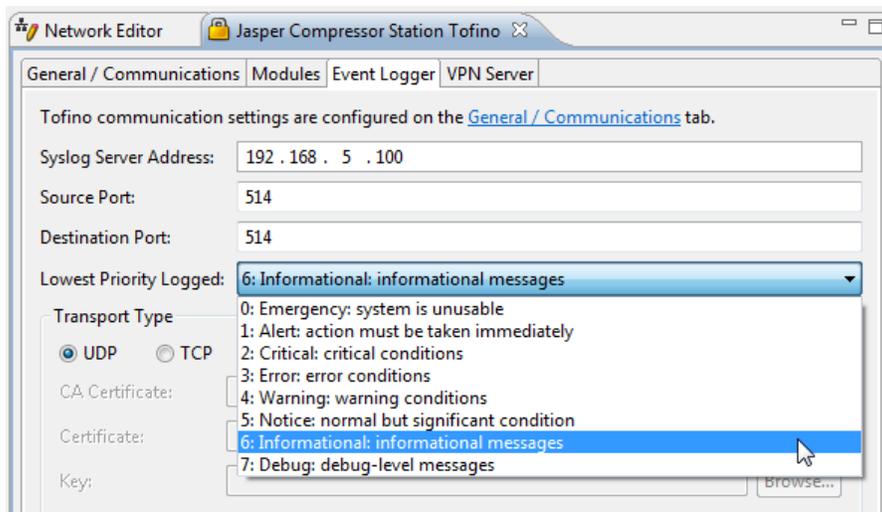
- ▶ Syslog Server Address: This is the address of the syslog server where you would like your logs sent to. If the syslog feature is not being used, this field can remain blank.
- ▶ Source Port: This is the source port the Tofino SA uses to send logs to your syslog server. If the syslog feature is not being used, this field can remain blank.
- ▶ Destination Port: This is the port your syslog server is receiving logs on. If the syslog feature is not being used, this field can remain blank.
- ▶ Lowest priority logged: This is the cut-off as to the lowest logging level you would like the Tofino SA to record.
- ▶ Transport Type:
 - ▶ UDP: logs will be sent to the syslog server using the transport layer protocol UDP. Note that when using UDP, if your syslog server was to go offline then logs sent to it during that time will not be recorded. However, the logs will still be available via local USB key save and as text files on the Tofino CMP computer. Also note that the transmitted logs are not encrypted in UDP mode.
 - ▶ TCP: logs will be sent to the syslog server using the transport layer protocol TCP. Using TCP gives you a log buffer so that if your syslog server was to go offline, the Tofino SA will automatically send the buffered logs when the server comes back online.* Also note that the transmitted logs are not encrypted in TCP mode.
 - ▶ TLS: Logs will be sent to the syslog server using the application layer protocol TLS (which is built on top of TCP). Using TLS also gives you a log buffer so that if your syslog server was to go offline, the Tofino SA will automatically send the buffered logs when the server comes back online.* The logs are encrypted. Note: The syslog server you are using must use TLS in order for this to work. You also have to ensure the common name in your server certificate includes the server's IP address.
- ▶ Browse... to find the CA Certificate, Certificate, and Key in order to use the TLS transport type. If the syslog feature is not being used, this field can remain blank.
- ▶ Retrieve Active Logs... by clicking this button the Event Logger logs will be immediately retrieved from the Tofino SA and stored in a location of your choice on the Tofino CMP computer. A window will open asking where you would like them to be saved. Note that logs are automatically stored to a location based on the CMP Preferences any time the log files exceed 1 MB in size.



***Note:** in certain conditions when using TCP or TLS transport, logs that were already queued for transmission may not be buffered and thus not sent to the syslog server on re-connection. However, these logs will still be available via USB save and the Tofino CMP Retrieve active logs feature.

Syslog Heartbeats

The Event Logger can be configured to send a periodic syslog heartbeat to a syslog server. This allows the syslog server to detect if a Tofino SA has gone offline. In order to send this message, the Event Logger 'Lowest Priority Logged' must be changed to "6: Informational: informational messages."



The message format received by the syslog server will be in the form of:

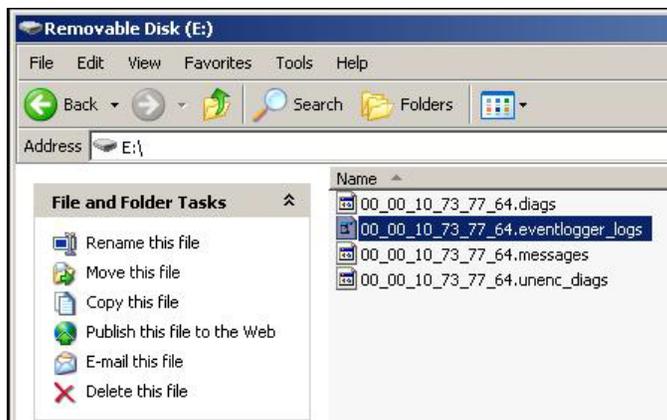
```
02-15-2012 15:03:48 User.Info 169.254.2.2 Feb 15 15:03:48 00:50:C2:B3:20:0A Tofino: System:
```

Healthy. Mode: OPERATIONAL

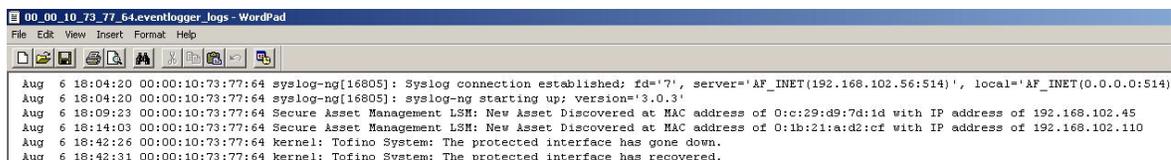
The time period between syslog heartbeats is the same as the periodic heartbeat setting. The reporting interval is set in the Tofino SA's Properties page. To prevent over-writing the local event logs on the Tofino SA we recommend that you change the default periodic heartbeat interval from 10 seconds to a higher value, such as 300 seconds.

Retrieving Logs Using a USB key

- To retrieve the logs stored on the Tofino SA, insert a USB key into the USB port on the Tofino SA and then press the Load/Save button or S/L/R button once, initiating the USB save. A marquee will flash in a downward direction or left to right, indicating files are being saved to the USB key, wait until the lights have finished flashing before removing the USB key.
- Open the the USB key to find the file containing the logs. The logs will be stored in a .eventlogger_logs file; open the file using a syslog viewer or Word Pad for the best formatting.



- When the .eventlogger_logs file is opened, the logs can be viewed. Below is an example of the log file opened with Word Pad.



If you are using Event Logger with VPN in OPERATIONAL Mode, the syslog server must be upstream of the Tofino SA and NOT within the encryption tunnel.

Retrieving Logs Using the Tofino CMP

The Tofino Event Logger automatically saves all logs recorded by the Tofino SA onto the Tofino CMP computer hard drive. These logs can be found in the directory specified in the CMP Preferences/Logs Settings.

Tofino SA to CMP log off load is performed automatically whenever the Tofino CMP is running and the log files on the Tofino SA exceed 4 MB in size. The Tofino CMP does not have to be powered on when the 4 MB threshold is reached - the Tofino SA will continue to retain the files until it detects the Tofino CMP is available for off loading the log files. The Tofino SA is capable of locally saving 8 MB of log events without losing any information.

Note that the logs are only transferred to the Tofino CMP when the 4 MB threshold is reached. However clicking Retrieve Active Logs button on the Event Logger tab will force the logs to be immediately retrieved from the Tofino SA and stored in a location of your choice on the Tofino CMP computer.

Sending CMP Event Logs to a Syslog Server

Heartbeat and local Tofino CMP console events can also be sent to a remote syslog server. These preferences are set in [CMP Preferences](#). They also allow you to determine the facility levels of the heartbeat syslog events.

Section 7

Troubleshooting

7 Troubleshooting

7.1 Tofino Argon 100 or 220 Diagnostics

The Tofino SA has the capability to save diagnostic files to a USB key for troubleshooting purposes. To create these files you will need to perform a USB Save. These files can then be viewed with a standard text editor or sent to technical support for analysis.

See: [Tofino SA 220](#)

See: [Tofino SA 100](#)

Tofino SA 100

To create these files you will need to perform a USB Save.

- Insert a USB key into one of the USB ports.
- Press and hold the Config button for 1-2 (but less than 5) seconds
- The Fault-Event-Mode LEDs will begin to flash, in downward sequence, to indicate a "Save."
- When the flashing sequence stops remove the USB key
- If the save was successful the Tofino SA LEDs will revert to the state they were in prior to the saving action.
- Send copies of these files to technical support for analysis.

If the USB Diagnostic Save is successful there will be three or four files on the USB key similar* to this:

```
00_00_11_8D_95_14_diagnostics.txt
00_00_11_8D_95_14_diagnostics.enc
00_00_11_8D_95_14_kernel_evt.enc
00_00_11_8D_95_14_evt.log (will appear only if the Event Logger LSM is installed and activated).
```

*The prefix of the file name will be equal to the Tofino ID.

If you examine the file ending in *_diagnostics.txt* using a standard text editor such as WordPad, you should see something like the following:

```
=====
=
2     Tofino Version information:
3     Tofino Firmware version: Tofino Linux: 1.4.0
4     Tofino Hardware Info:
5     Hardware : Arcom VULCAN
6     Processor : XScale-IXP42x Family rev 2 (v5b)
7     Flash Type: P-Flash
8     Tofino ID:  00:00:10:73:77:64
9
=====
10    Network Statistics
11    unsecured IF ifconfig
12    eth0      Link encap:Ethernet  HWaddr 00:80:66:04:65:2C
13            inet6 addr: fe80::280:66ff:fe04:652c/64 Scope:Link
```

```

14         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
15         RX packets:2776 errors:0 dropped:0 overruns:0 frame:0
16         TX packets:3900 errors:0 dropped:0 overruns:0 carrier:0
17         collisions:0 txqueuelen:100
18         RX bytes:419084 (409.2 KiB)  TX bytes:586268 (572.5 KiB)
19
20     secured IF ifconfig
21 eth1     Link encap:Ethernet  HWaddr 00:80:66:04:65:2D
22         inet6 addr: fe80::280:66ff:fe04:652d/64 Scope:Link
23         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
24         RX packets:15 errors:0 dropped:0 overruns:0 frame:0
25         TX packets:716 errors:0 dropped:0 overruns:0 carrier:0
26         collisions:0 txqueuelen:100
27         RX bytes:846 (846.0 B)  TX bytes:95002 (92.7 KiB)
28
29     unsecured IF Settings
30     Basic registers of MII PHY #0:  1000 782d 0013 7a11 01e1 45e1 0005
6001.
31     The autonegotiated capability is 01e0.
32     The autonegotiated media type is 100baseTx-FD.
33     Basic mode control register 0x1000: Auto-negotiation enabled.
34     You have link beat, and everything is working OK.
35     Your link partner advertised 45e1: Flow-control 100baseTx-FD 100baseTx
10baseT-FD 10baseT, w/ 802.3X flow control.
36     End of basic transceiver information.
37
38     secured IF Settings
39     Basic registers of MII PHY #1:  1000 782d 0013 7a11 01e1 45e1 0005
6001.
40     The autonegotiated capability is 01e0.
41     The autonegotiated media type is 100baseTx-FD.
42     Basic mode control register 0x1000: Auto-negotiation enabled.
43     You have link beat, and everything is working OK.
44     Your link partner advertised 45e1: Flow-control 100baseTx-FD 100baseTx
10baseT-FD 10baseT, w/ 802.3X flow control.
45     End of basic transceiver information.
46
47
=====
48     Memory
49
50     total      used      free      shared    buffers
51     cached
52     Mem:      62952    17952    45000         0       140
53     9060
54     -/+ buffers/cache:      8752    54200
55     Swap:         0         0         0
56
-----
57     MemTotal:      62952 kB
58     MemFree:      44992 kB
59     Buffers:       140 kB
60     Cached:       9060 kB
61     SwapCached:    0 kB

```

```

59 Active:          9288 kB
60 Inactive:       1996 kB
61 SwapTotal:      0 kB
62 SwapFree:       0 kB
63 Dirty:          0 kB
64 Writeback:      0 kB
65 AnonPages:      2100 kB
66 Mapped:         1744 kB
67 Slab:           3176 kB
68 SReclaimable:   752 kB
69 SUnreclaim:     2424 kB
70 PageTables:     260 kB
71 NFS_Unstable:   0 kB
72 Bounce:         0 kB
73 WritebackTmp:   0 kB
74 CommitLimit:    31476 kB
75 Committed_AS:   5200 kB
76 VmallocTotal:   958464 kB
77 VmallocUsed:    33436 kB
78 VmallocChunk:   917500 kB
79

```

```

=====
80 Flash
81 Filesystem      Size      Used Available Use% Mounted on
82 rootfs          31.5M     8.1M     23.4M   26% /
83
=====

```

The files ending in .enc are encrypted files and should be sent to support@tofinosecurity.com

The file ending in .evt.log is a log file created by the Event Logger LSM. See: [Using Event Logger LSM](#)

Tofino SA 220

To create these files you will need to perform a USB Save.

- Insert a USB key into one of the USB ports.
- Push the button labeled 'S/L/R' one time.
- The marquee will move from left to right to indicate a USB Save.
- When the flashing sequence stops remove the USB key
- If the save was successful the Tofino SA LEDs will revert to the state they were in prior to the saving action.
- Send copies of these files to technical support for analysis.

If the USB Diagnostic Save is successful there will be three or four files on the USB key similar* to this:

00_00_11_8D_95_14_diagnostics.txt

00_00_11_8D_95_14_diagnostics.enc

00_00_11_8D_95_14_kernel_evt.enc

00_00_11_8D_95_14_evt.log (will appear only if the Event Logger LSM is installed and activated).

*The prefix of the file name will be equal to the Tofino ID.

If you examine the file ending in *_diagnostics.txt* using a standard text editor such as WordPad, you should see something like the following:

```
=====
Tofino Version information:
  Tofino Firmware version: Tofino Linux: 1.5.2
Tofino Hardware Info:
  Hardware : Hirschmann EAGLE20 Development Platform
  Processor : XScale-IXP42x Family rev 2 (v5b)
  Flash Type: P-Flash
  Tofino ID: 00:80:63:95:EF:B1
=====
Network Statistics
  unsecured IF ifconfig
eth0      Link encap:Ethernet  HWaddr 00:80:63:95:EF:B1
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:953 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:83690 (81.7 KiB)  TX bytes:0 (0.0 B)

          secured IF ifconfig
eth1      Link encap:Ethernet  HWaddr 00:80:63:95:EF:B2
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

          unsecured IF Settings
Basic registers of MII #0: 1000 782d 0040 61e4 01e1 45e1 0005 2001.
The autonegotiated capability is 01e0.
The autonegotiated media type is 100baseTx-FD.
Basic mode control register 0x1000: Auto-negotiation enabled.
You have link beat, and everything is working OK.
Your link partner advertised 45e1: Flow-control 100baseTx-FD 100baseTx
10baseT-FD 10baseT, w/ 802.3X flow control.
End of basic transceiver information.

          secured IF Settings
Basic registers of MII PHY #1: 1000 7809 0040 61e4 01e1 0000 0004 2001.
Basic mode control register 0x1000: Auto-negotiation enabled.
Basic mode status register 0x7809 ... 7809.
Link status: not established.
End of basic transceiver information.

=====
Memory
          total          used          free          shared          buffers          cached
Mem:          63028          15192          47836              0              0              7136
-/+ buffers/cache:          8056          54972
Swap:           0              0              0
-----
MemTotal:          63028 kB
=====
```

```
MemFree:          47828 kB
Buffers:          0 kB
Cached:           7136 kB
SwapCached:       0 kB
Active:           7156 kB
Inactive:         2136 kB
SwapTotal:        0 kB
SwapFree:         0 kB
Dirty:            0 kB
Writeback:        0 kB
AnonPages:        2172 kB
Mapped:           1748 kB
Slab:             2912 kB
SReclaimable:     892 kB
SUnreclaim:       2020 kB
PageTables:       272 kB
NFS_Unstable:     0 kB
Bounce:           0 kB
WritebackTmp:     0 kB
CommitLimit:      31512 kB
Committed_AS:     4820 kB
VmallocTotal:     958464 kB
VmallocUsed:      17144 kB
VmallocChunk:     925692 kB
```

```
=====
```

Flash					
Filesystem	Size	Used	Available	Use%	Mounted on
rootfs	6.4M	5.1M	1.3M	80%	/

```
=====
```

The files ending in .enc are encrypted files and should be sent to support@tofinosecurity.com

The file ending in .evt.log is a log file created by the Event Logger LSM. See: [Using Event Logger LSM](#)

7.2 Asset Discovery Shows Removed Devices

You have either physically removed a device from your network or changed its IP address and yet the old device is still listed in the Asset Discovery view. How do you remove it?

All assets remain in the Asset Discovery view until either deleted or deployed to the Network Editor. Physically removing the device from the network will not clear it from the Asset Discovery view as there is no way to determine if the asset is truly removed or just offline for a time. Thus, if you want a device to no longer appear in the Asset Discovery view, you must use the [deleting asset feature](#).

7.3 Asset Discovery is Not Discovering Assets

If expected assets are not showing up in the Asset Discovery view try the following:

- Ensure your Tofino SA has the Firewall LSM and the Secure Asset Management LSM installed and activated. See: [Adding an LSM to a Tofino SA](#)
- Change the mode on your Tofino SA to another mode, and then back into the mode you were originally in. WARNING: Putting your Tofino SA into OPERATIONAL mode will enact any firewall rules in place.
- When a VPN link is active between two Tofino SAs, only the assets on the trusted side of each Tofino SA (i.e: communicating over the VPN tunnel) will be discovered. Any traffic coming from the untrusted interface and outside the VPN tunnel will not be discovered as it will be unencrypted and thus immediately rejected by the Tofino SA.

7.4 Expired Licenses

There are two types of licenses needed to use the Tofino Industrial Security Solution: Tofino CMP Licenses and LSM Licenses. See: [Tofino CMP Licensing](#) and [LSM Licensing](#).

See: [Expired Tofino CMP Licenses](#)

See: [Expired LSM Licenses](#)

Expired Tofino CMP Licenses

There are two dates attached to the Tofino CMP license: the Maintenance Contract Expiry Date and Expiry Date.

See: [Maintenance Contract Expiry Date](#)

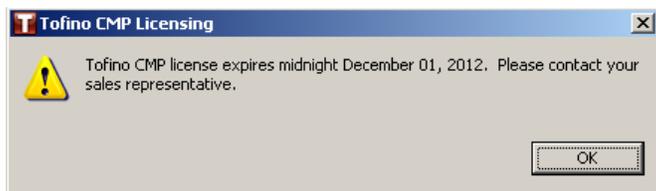
See: [Expiry Date](#)

Maintenance Contract Expiry Date

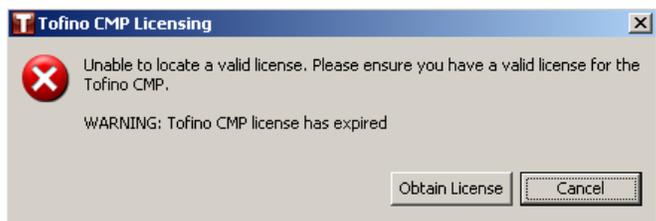
The maintenance date indicates the maintenance contract expiry date, if a newer version of the Tofino CMP is released after this date, the license does not cover the new release. **Note:** once the maintenance contract expiry date has passed, the Tofino Industrial Security Solution will continue to run as normal. Also note: if a maintenance contract was not purchased, the maintenance contract expiry date is 90 days after the purchase date.

Expiry Date

The expiry date is the day the Tofino CMP license will expire, and as a result the Tofino CMP will stop functioning. 31 days prior to this day a window will open any time the Tofino CMP is closed and re-opened indicating how many days are left until the Tofino CMP license expires. To renew the Tofino CMP license, contact support@tofinosecurity.com



Once the Tofino CMP license has expired, and the user attempts to open the Tofino CMP, a window will open prompting the user to obtain a license. See: [Tofino CMP Licensing](#)



Expired LSM Licenses

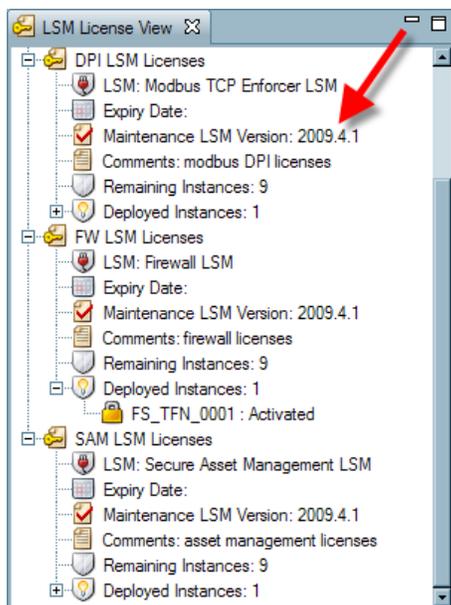
There are two dates attached to the LSM licenses: the Maintenance Contract Expiry Date and Expiry Date.

See: [Maintenance Contract Expiry Date](#)

See: [Expiry Date](#)

Maintenance Contract Expiry Date

The maintenance date, which can be found in the LSM License View, indicates the maintenance contract expiry date; if a newer version of the LSM is released after this date, the license does not cover an update to the new release. **Note:** once the maintenance contract expiry date has passed, the Tofino Industrial Security Solution will continue to run as normal. Also note: if a maintenance contract was not purchased, the maintenance contract expiry date is 90 days after the purchase date.



Expiry Date

The expiry date is the day the LSM license will expire, and as a result the LSM will stop functioning. This date can be seen in the LSM License view; this date will be displayed in red when the license is expired. To renew the LSM license, contact support@tofinosecurity.com

7.5 Firewall Not Blocking Traffic

If the Tofino Firewall LSM does not appear to be blocking traffic that you think it should, first check the following:

- The Tofino Firewall LSM status (is the Firewall LSM installed and activated?).
- The mode of the Tofino SA (is the Tofino SA in Operational mode?).
- Does the configuration of the Tofino SA REALLY match the CMP? If in doubt, synchronize the Tofino SA with the Tofino CMP.

Next, check the rules on both the protected device firewall tab and the Tofino SA's firewall tab for the following:

- Are the device IP addresses correct? See the General/Communications tab of the Talker devices sending the traffic. See: [Editing a Node's Properties](#)
- Are the protocols and direction correct on the Firewall tab of the protected device? See: [Firewall Rule Configuration for a Node](#)
- Are the protocols and direction correct on the Firewall tab of the Tofino SA? See: [Firewall Rule Configuration for a Tofino SA](#)
- Are there conflicting rules between protected devices and the Tofino SA. For example, does the Tofino SA have a global allow rule for a protocol that the protected device is supposed to deny?
- Was the connection established BEFORE the rule was applied? For safety reasons, the Tofino SA will not break established connections between a talker and protected device. If you think this is the case, try breaking the connection by restarting the talker.

7.6 Licensing

In order to use the Tofino system two different types of licenses must be acquired.

- ▶ A Tofino CMP License.
- ▶ An LSM License for each LSM that you wish to activate.

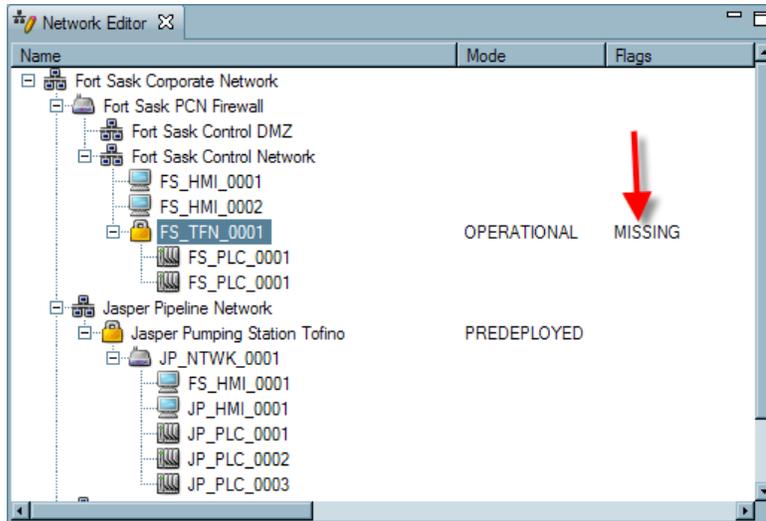
Typically these are combined together in a single License Grant file.

See: [Tofino CMP Licensing](#)

See also: [LSM Licensing](#)

7.7 Missing Tofino SA

When a Tofino CMP fails to receive two heartbeats in a row from a Tofino SA it will be reported as MISSING. The length of time this will take depends on the heartbeat rate.



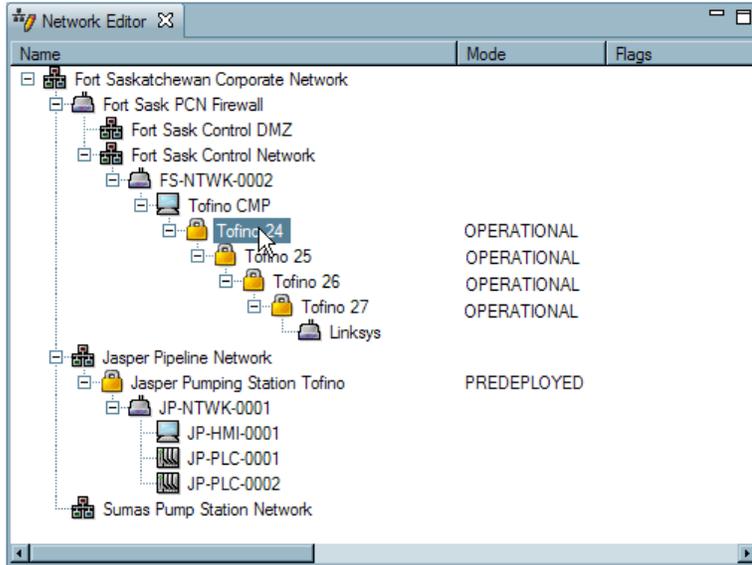
Possible causes of a MISSING Tofino SA include:

- ▶ The Tofino SA has been physically removed from the network or has failed or has powered off.
- ▶ All contact devices behind the Tofino SA have failed or have been removed. This would result in the Tofino SA no longer having a valid IP address to use to send heartbeats to the Tofino CMP. To see what the contact devices are see: [Tofino View](#)
- ▶ Something in the network is preventing the heartbeats from reaching the Tofino CMP. For example, a failed switch or a firewall that has been reconfigured.
- ▶ The Tofino SA has been replaced with a different Tofino SA that has a different ID number from what the Tofino CMP expects.

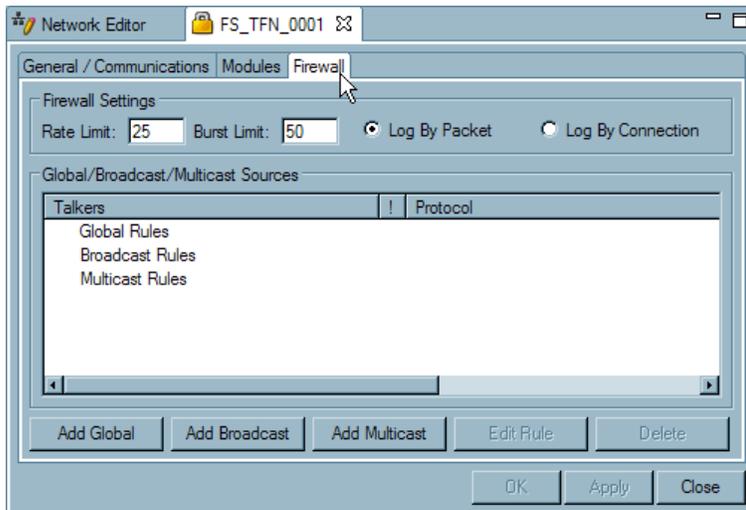
7.8 Serial Tofino SAs

If you have two or more Tofino SAs serially connected (i.e.: the Tofino CMP communications must pass through one Tofino SA in order to reach another) then you must install a firewall rule in the first Tofino SA to allow the Tofino CMP communications to pass through.

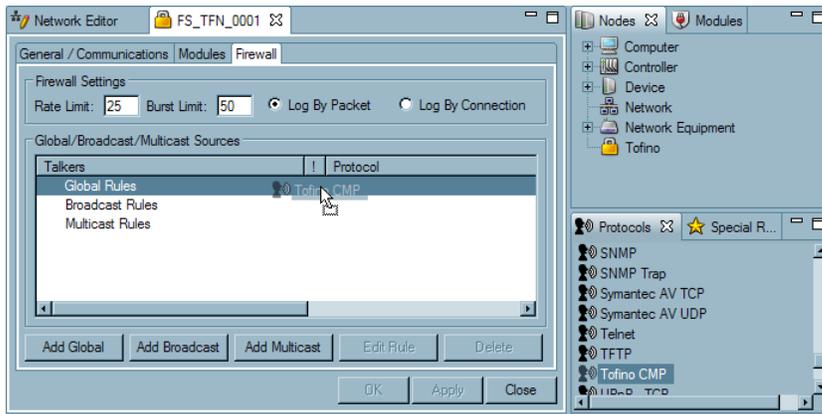
- Open the first Tofino SA's Properties page (by double clicking on the icon in the Network Editor diagram).



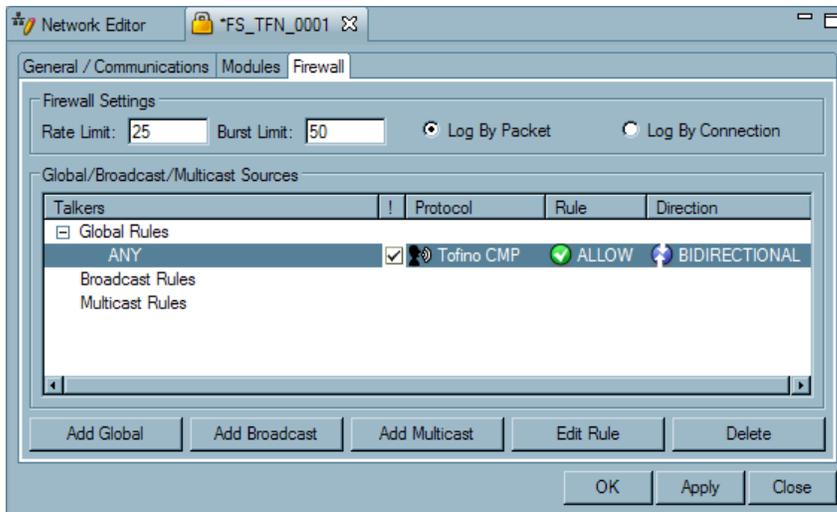
- Click on the Firewall tab.



- Add the Tofino CMP protocol to the Global rules.



- Set the rule to ALLOW and BIDIRECTIONAL.

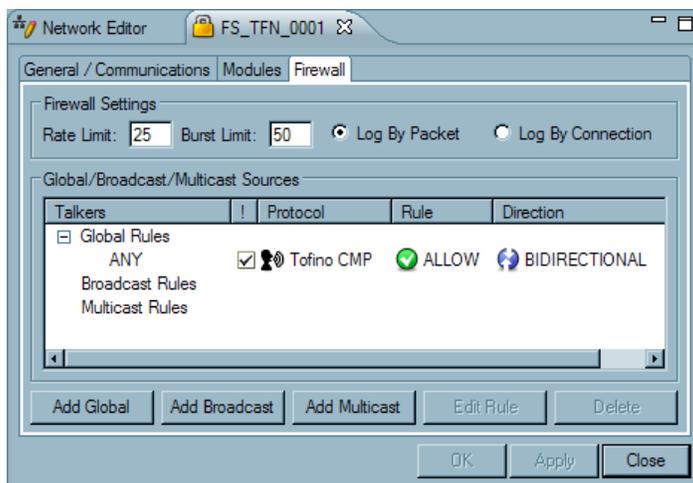


- Click "OK".

7.9 Tofino Discovery is Not Discovering Tofino SAs

If Tofino Discovery scans are not discovering Tofino SAs on your network try the following solutions:

- ▶ Delete the Tofino Discovery scan and create a new scan.
- ▶ Ensure the Tofino SAs you are trying to discover were new Tofino SAs direct from the factory or factory reset.
- ▶ If you have a Tofino SA on your network that was originally USB loaded and there are Tofino SAs downstream from it, the USB loaded Tofino SA needs a Tofino CMP Global rule added to it. This will allow the request traffic through, otherwise the USB loaded Tofino SA will prevent downstream Tofino SAs from being discovered.
- ▶ If you have a Tofino SA on your network that has an installed and activated firewall and there are Tofino SAs downstream from it, the Tofino SA with the firewall installed needs a Tofino CMP Global rule added to it. This will allow the request traffic through, otherwise the Tofino SA's firewall will prevent downstream Tofino SAs from being discovered.



7.10 USB Key Problems

If you are experiencing problems doing USB Loads or USB Saves, ensure you are using a version 2.0 USB storage device that has been formatted as FAT32. USB storage devices that are either version 1.1 or a non-FAT32 formatted device are not compatible and will not work with the Tofino SA. The Tofino SA Fault LED will flash twice (indicating invalid USB storage device), if it detects either a version 1.1 USB storage device or a non-FAT32 formatted device.

Many low cost USB storage devices are known to have quality issues. The tested and approved USB storage devices include:

- ▶ Kingston Data Traveler
- ▶ SanDisk cruzer
- ▶ Sony Microvault
- ▶ Lexar

7.11 Why Can't I Enter the %\$@#! Character?

Valid characters for most fields on the Tofino CMP include:

- ▶ a-z
- ▶ A-Z
- ▶ 0-9
- ▶ Dashes “ - ”
- ▶ Periods “ . ”
- ▶ Underscores “ _ ”
- ▶ Colons “ : ”

If you try to enter invalid characters into a field, nothing will happen.

7.12 VPN Troubleshooting

VPNs are inherently difficult security solutions. Because the VPN Client and VPN Server must interact not only with each other, but also with other network devices that sit in between them (such as routers and firewalls), it is necessary to configure your VPN carefully.

7.12.1 My VPN Client will not connect to my VPN Server

This can be caused by several factors, but the primary cause is that the VPN Client and VPN Server do not have a communications path available to connect over.

First, ensure that the VPN Client and VPN Server are both in TEST mode and follow the directions in [Testing Your VPN Tunnel](#). If they do not connect, confirm the path by using a port scanning tool (such as SuperScan or Nmap) on the trusted side of the Tofino SA VPN Client to scan port UDP 1194 at the Tofino SA VPN Server's Public IP Address (if NAT is used) or the Tofino SAs regular IP Address (if NAT is not used). If the port scanner can not connect:

- ▶ Ensure that any firewalls or routers in between the VPN Client and VPN Server have port forwarding enabled for UDP port 1194 and directed to the Tofino VPN Server's regular IP Address.
- ▶ If there is an internet gateway router between the Tofino VPN Server and the internet, ensure that the Public IP Address of the Tofino SA is the same as the gateway's WAN side IP Address.
- ▶ Ensure that SSL messages BETWEEN the VPN client and VPN server are not VLAN-tagged. The VLAN-tagged messages on the trusted (unencrypted) interface are allowed.

7.12.2 The Client Certificates Have Time Expired

VPN Client certificates are time stamped by the Tofino CMP when they are created. If they are not installed in the Tofino SA VPN Client and the VPN tested within seven days, they will expire for security reasons. Once the Tofino SA VPN Client has communicated to the Tofino CMP, the timestamps are coordinated. This condition is most likely to occur if a Tofino SA's configuration is loaded using a USB key or if a Tofino SA has been powered off for more than seven days.

7.12.3 PC Client Can't Connect to my VPN Client's Devices

Under default operating conditions, VPN Clients (including PC Clients) only can communicate to devices on the trusted side of a Tofino SA VPN Server. If a PC Client wants to connect to devices downstream from a VPN Client, the Clients see each other option must be enabled on the Tofino SA VPN Server as described in [Using the VPN LSM](#). **Note that when using the “Clients see each other” option, the remote networks may not share address spaces either via explicit IP segment or classless subnet masking.**

7.12.4 PC Client Can't Connect to my Tofino VPN Server

Make sure that you have no other VPN software active on your PC Client computer. Conflicts between different VPN Clients on the same PC are very common. There should only be one VPN running or loaded in memory at a time, and very often they can't even be active in the task bar.

Ensure that there is no overlapping or conflicting IP addressing between the real address of the PC Client and the VPN assigned IP address. For example, if the Tofino SA has an address of 192.168.1.100 and a subnet mask of 255.255.255.0 then the remote PC will be assigned a virtual address in the range of 192.168.1.1 to 192.168.1.254 via the Tofino CMP configuration. Also note that the real IP address of the remote PC must not be in this range. For example, if a remote internet service provider in a hotel assigns an IP address such as 192.168.1.100 to the remote laptop, the VPN will not work due to the conflict between the virtual address and the real address.

Ensure that the Public IP address assigned to the VPN Server matches the address in the PC Client

configuration files. For example, if the PC Client configuration files are created with the VPN Server having a public address of 72.23.100.1 and then this address is later changed in the Tofino CMP Network Editor, the old files will not work correctly. You can check the Public IP address of the VPN Server in the PC Client configuration file by running the Tofino Open VPN software and on the systray icon, right click and select "Edit Config". If there are two server configurations, select the server configuration desired and right click "Edit Config". The configuration file should open and the IP address marked "Remote" is the Public IP address of the VPN Server.

7.13 Event Logger Troubleshooting

7.13.1 Syslog Over UDP

The most common configuration for communications to a syslog server is syslog over UDP. If you are using this transport option, then no IP address needs to be assigned on the Tofino SA.

- ▶ **If the syslog server is on the same subnet as the Tofino SA confirm the following:**
 - ▶ UDP transport is selected on the [Event Logger](#) tab
 - ▶ The destination port set on the Event Logger tab matches the port number used on the syslog server (this is usually 514)
 - ▶ The IP address of the syslog server set on the Event Logger tab is correct
 - ▶ That syslog server and the Tofino CMP are located on the same management VLAN (if VLANs are used). Defining two VLANs for Tofino SA management and reporting can cause intermittent communications
 - ▶ If VLAN Tagging or VPN LSMs are deployed, then CMP and syslog server are on the 'same side' of the Tofino SA
- ▶ **If the syslog server is on a different subnet from Tofino SA do the above and then confirm:**
 - ▶ The Default Gateway address on the Tofino SA's General settings page is set to the address of the subnet router

7.13.2 Syslog Over TCP

Syslog over TCP allows the event messages to be confirmed on delivery. If you are using this transport option, then an IP address must be assigned on the Tofino SA.

- ▶ **If the syslog server is on the same subnet as the Tofino SA confirm the following:**
 - ▶ TCP transport is selected on the [Event Logger](#) tab
 - ▶ An IP address and subnet mask is set on the Tofino SA's General settings page
 - ▶ The Default Gateway address on Tofino SA General settings page is set to the address of the subnet router
 - ▶ The destination port set on the Event Logger tab matches the port number used on the syslog server (this is usually 514)
 - ▶ The IP address of the syslog server set on the Event Logger tab is correct
 - ▶ That syslog server and the Tofino CMP are located on the same management VLAN (if VLANs are used). Defining two VLANs for Tofino SA management and reporting can cause intermittent communications
 - ▶ If VLAN Tagging or VPN LSMs are deployed, then CMP and syslog server are on the 'same side' of the Tofino SA

7.13.3 Syslog Over TLS

Syslog over TLS allows the event messages to be encrypted. If you are using this transport option, then an IP address must be assigned on the Tofino SA.

- ▶ **If the syslog server is on the same subnet as the Tofino SA confirm the following:**
 - ▶ TLS transport is selected on the [Event Logger](#) tab
 - ▶ An IP address and subnet mask is set on the Tofino SA's General settings page
 - ▶ The Default Gateway address on Tofino SA General settings page is set to the address of the subnet router
 - ▶ The destination port set on the Event Logger tab matches the port number used on the syslog server (this is usually 514)
 - ▶ The IP address of the syslog server set on the Event Logger tab is correct
 - ▶ That syslog server and the Tofino CMP are located on the same management VLAN (if VLANs are used). Defining two VLANs for Tofino SA management and reporting can cause intermittent communications
 - ▶ If VLAN Tagging or VPN LSMs are deployed, then CMP and syslog server are on the 'same side' of the Tofino SA
 - ▶ Ensure that your server's hostname/IP address is used in the common name of the server certificate. Syslog-ng 3.0 documentation states this as a configuration requirement for specific TLS configuration support, you may refer to: <http://www.balabit.com/dl/html/syslog-ng-v3.0-guide-admin-en.html/ch03s12.html> and http://www.balabit.com/dl/html/syslog-ng-admin-guide_en.html/ch08s10.html

Section 8

Glossary

8 Glossary

ACL: Access Control List: List of rules specifying access privileges to network resources.

Append: Appending a new node will place the new node below the node currently selected in the Network Editor window. This function is designed to be used to add children to a network.

ARG: (Assisted Rule Generation): a feature that helps the user to create firewall rules for the purpose of protecting devices on their network. This feature comes with the Secure Asset Management LSM.

Children: A child node is one that is connected under another node (known as its parent).

CIP: Common Industrial Protocol: CIP is an open standard for industrial network technologies. It is supported by an organization called Open DeviceNet Vendor Association (ODVA).

CMP:(Central Management Platform): The CMP is a Windows-based centralized management server. It provides a database for monitoring, supervision and configuration of each security appliance.

CSP: Client Server Protocol: An Allen-Bradley protocol used to communicate to PLCs over TCP/IP.

DCOM: Distributed Component Object Model: This is an extension to the Component Object Model that Microsoft made to support communication among objects on different computers across a network.

DCS: Distributed Control System: A Distributed Control System allows for remote human monitoring and control of field devices from one or more operation centers.

DMZ: Demilitarized Zone: A small network inserted as a "neutral zone" between a trusted private network and the outside untrusted network.

DNP3: Distributed Network Protocol 3: A protocol used between components in process automation systems.

DNS: Domain Name System: A distributed database system for resolving human readable names to Internet Protocol addresses.

DPI: Deep Packet Inspection

EHB: (Exception Heartbeats) Messages that have been generated because a specific event has occurred such as a packet being blocked by the Firewall LSM.

Firewall: A set of security schemes that prevent unauthorized persons or devices from gaining access to protected nodes on a network. A firewall essentially works as a control point that blocks invalid connections to nodes protected behind the firewall while still allowing trusted communications to pass through unaffected.

FTP: File Transfer Protocol.

GUI: Graphical User Interface: Graphical, as opposed to textual, interface to a computer.

Heartbeats: Messages sent back to the Tofino CMP from each Tofino SA, as well as locally generated events such as a Tofino SA being reported as missing by the Tofino CMP. There are two types of heartbeats: Periodic heartbeats which are regular reporting messages from each Tofino SA and Exception

heartbeats which are messages that have been generated because a specific event has occurred (such as a packet being blocked by the firewall LSM).

HMI: Human Machine Interface: This interface enables the interaction of man and machine.

HTML: Hypertext Markup Language: The authoring software language used on the Internet's World Wide Web.

HTTP: HyperText Transfer Protocol: The protocol used to transfer Web documents from a server to a browser.

HTTPS: HyperText Transfer Protocol over SSL: A secure protocol used to transfer Web documents from a server to a browser.

IDS: Intrusion Detection System: A system to detect suspicious patterns of network traffic.

Insert: Inserting a new node will place the new node above the node currently selected in the Network Editor window. This function is designed to be used to add Children to a network.

IP: Internet Protocol: The standard protocol used on the Internet that defines the datagram format and a best effort packet delivery service.

IT: Information Technology: The development, installation and implementation of applications on computer systems.

LAN: Local Area Network: A computer network that covers a small area.

LDAP: Lightweight Directory Access Protocol: Protocol to access directory services.

LSM:(Loadable Security Module): Software plug-ins providing security services such as: Firewall, Intrusion detection system (IDS), Diagnostics, and VPN encryption.

Modbus: A communications protocol designed by Modicon Incorporated for use with its PLCs.

MySQL: A relational database management system (RDBMS) that runs as a server providing multi-user access to a number of databases.

NETBEUI: NetBIOS Extended User Interface: An enhanced version of the NetBIOS protocol.

NetBIOS: Network Basic Input Output System: A de facto IBM standard for applications to use to communicate over a LAN.

Node Type: A node type is a category of devices that have common properties. For example, a node type may be "Allen Bradley PLC5."

Node: Nodes are the objects used to build a network diagram and represent the devices installed in your control system. They can be broken down into six categories: Computers, Controllers, Devices, Networks, Networking equipment, and Tofino SAs.

OLE: Object Linking and Embedding: A precursor to COM, allowing applications to share data and manipulate shared data.

OPC: OLE for Process Control: A standard based on OLE, COM and DCOM, for accessing process control

information on Microsoft Windows systems.

Parent: A parent node is one that has nodes connected to it (known as children).

PCN: Process Control Network: A communications network used to transmit instructions and data to control devices and other industrial equipment.

PHB: (Periodic Heartbeats) Regular reporting messages (heartbeats) from each Tofino SA. The reporting interval is set in the Tofino SAs properties page.

PLC: Programmable Logic Controller: A PLC is a small dedicated computer used for controlling industrial machinery and processes.

Protected Node: A node that is protected by a Tofino

Protocol: A convention or standard that controls or enables the connection, communication, and data transfer between two computing endpoints. In its simplest form, a protocol can be defined as the rules governing the syntax, semantics, and synchronization of communication. Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behavior of a hardware connection.

RPC: Remote Procedure Call: A standard for invoking code residing on another computer across a network.

SCADA: Supervisory Control And Data Acquisition: A system for industrial control consisting of multiple Remote Terminal Units (RTUs), a communications infrastructure, and one or more Control Computers.

Scan Object: A range of IP addresses set to scan in the Tofino Discovery view in order to search for configured Tofino SAs on the network.

Sibling: Siblings are two or more nodes that have the same parent, and are on the same level of the network tree (just as with a family tree).

SNMP: Simple Network Management Protocol: A protocol used to manage devices such as routers, switches and hosts.

SQL: A database computer language designed for managing data in relational database management systems.

SSL: Secure Socket Layer: A de facto standard for secure communications created by Netscape Incorporated.

Talkers: Nodes located upstream from a Tofino SA that need to communicate to a protected node (located downstream from a Tofino SA) using a specified protocol.

TCP: Transmission Control Protocol: The standard transport level protocol that provides a reliable stream service.

TFTP: Trivial File Transfer Protocol.

Tofino Security Appliance: An industrially hardened security appliance designed to be installed in front of individual and/or networks of HMI, DCS, PLC or RTU control devices that require protection.

UDP: User Datagram Protocol: Connectionless network transport protocol.

URL: Uniform Resource Locator: The address of a resource on the Internet.

VPN: A virtual private network (VPN) is a network technology that uses a (possibly) insecure public network (often the Internet) to securely connect remote sites or users together.

XML: eXtensible Markup Language: A general-purpose markup language for creating special purpose markup languages that are capable of describing many different kinds of data.

Section 9

Technical Support

9 Technical Support

Please contact the local representative in your region.

or

e-mail: support@tofinosecurity.com

web: www.tofinosecurity.com

Section 10

Appendix A: Finding Your MAC Address

10 Appendix A: Finding Your MAC Address

To determine the MAC address of your Tofino SA you will need to perform a USB save, as outlined in the steps below:

- Insert a USB key into one of the USB ports.
- Press and hold the Config button for 1-2 (but less than 5) seconds
- The Fault-Event-Mode LEDs will begin to flash, in downward sequence, to indicate a "Save."
- When the flashing sequence stops remove the USB key.
- If the save was successful the Tofino SA LEDs will revert to the state they were in prior to the saving action.

If the USB Diagnostic Save is successful there will be three or four files on the USB key similar* to this:

- 00_00_11_8D_95_14_diagnostics.txt
- 00_00_11_8D_95_14_diagnostics.enc
- 00_00_11_8D_95_14_kernel_evt.enc
- 00_00_11_8D_95_14_evt.log (will appear only if the Event Logger LSM is installed and activated).

*The prefix of the file name will be equal to the Tofino ID.

If you examine the file ending in *_diagnostics.txt* using a standard text editor such as WordPad, you should see something like the following. The MAC address is found in the location highlighted in yellow.

```
=====
2      Tofino Version information:
3      Tofino Firmware version: Tofino Linux: 1.4.0
4      Tofino Hardware Info:
5      Hardware : Arcom VULCAN
6      Processor : XScale-IXP42x Family rev 2 (v5b)
7      Flash Type: P-Flash
8      Tofino ID:  00:00:10:73:77:64
9
=====
10     Network Statistics
11     unsecured IF ifconfig
12     eth0      Link encap:Ethernet  HWaddr 00:80:66:04:65:2C
13             inet6 addr: fe80::280:66ff:fe04:652c/64 Scope:Link
14             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
15             RX packets:2776 errors:0 dropped:0 overruns:0 frame:0
16             TX packets:3900 errors:0 dropped:0 overruns:0 carrier:0
17             collisions:0 txqueuelen:100
18             RX bytes:419084 (409.2 KiB)  TX bytes:586268 (572.5 KiB)
```

Index

- 3 -

3rd Party Server 259

- A -

Acknowledge 84
Adding an LSM to a Tofino 168
Alarms 126
Alter Type 203
Always run in background 101
ANSI/ISA-99 270
Appending Network Nodes 29
ARG 214
Asset Column 203
Asset Discovery 93
Asset Discovery Right Click Menu 203
Assisted Rule Generation 214

- B -

Backing up and Restoring Databases 127
Beginning a Scan 116
Bidirectional 174
Broadcast 174
Broadcast Traffic 214
Burst Limit 177

- C -

Characters 295
CMP Basics 6
CMP Database 16
CMP General Settings 101
CMP Log Settings 101
CMP Preferences 22
CMP Windows 25
Computer Properties 52
Computer Wizard 58
Configuring Modbus/TCP DPI Firewall Rules 230
Contact Devices 138

Continuous Scanning 116
Controller Properties 52
Controller Wizard 58
Copy 8
Create Loadable USB Key 34
Create New Scan 116
Create Protocol 74
Creating a Node 47
Creating and Editing a Network 113
Creating Your Network Diagram 112
Cut 8

- D -

Database 16, 101
Database Backup and Restore 12
Debug 24
Default Password 111
Delete 8
Delete Protocol 74
Deleting a Function Code 230
Deleting a Node Type 47
Deleting a Talker 230
Deleting Assets 203
Deployed Instances 46
Device Database 16
Device Properties 52
Device Type Column 203
Device Wizard 58
Disconnect 8
Discovered By Column 203
Discovered Nodes view 116

- E -

Edit Menu 8
Editing a Network 29
Editing a Node's Properties 52
Event Capture 25, 91
Event Capture Button 84
Event Priority 84
Event Type 84
Event View 25, 84
Event View Buttons 84
Exports 126

Exception Heartbeats 126
Exit 8

- F -

File Menu 8
Filter Heartbeats Button 84
Firewall 174
Firewall Not Blocking Traffic 288
Firewall Rule Configuration for a Node 178
Flags 27
Function Code Rule 230

- G -

Global Rules 174
Glossary 301
Go Into Go Back Go Home 94

- H -

Heartbeat Right Click Menu 84
Heartbeat syslog 101
Heartbeats 126
Help 7
Help Contents 24

- I -

Importing Special Rules 82
Inserting Network Nodes 29
IP address 138

- L -

Licensing 289
Log By Connection 177
Log By Packet 177
Log Type 177
LSM License Management 12
LSM License Updating 12
LSM License View 25, 46
LSM Licensing 167, 172

- M -

Maintenance LSM Version 46
Managing LSMs 167
Menus 7
Missing Tofino 290
Modbus/TCP Deep Packet Inspection 230
Modes 27
Modules 73
Multicast 174
Multicast Traffic 214

- N -

NERC CIP 270
Network diagrams 27
Network Editor 25, 27
Network Editor Right Click Menus 28
Network Equipment Properties 52
Network Equipment Wizard 58
Network Node Menu 40
Network Properties 52
Network ReBuild Wizard 114
Network View 25, 41
Network Wizard 58
Networking Equipment 112
Networks 112
Node Properties Wizard 58
Nodes 25, 47

- P -

Paste 8
PC Client 245, 265
Periodic Heartbeats 126
Progress 25, 92
Protocol Right Click Menu 74
Protocol Wizard 79
Protocols 25, 74

- R -

Rate Limit 177
Reloading LSM Packages 12

Remaining Instances 46
Replacing a Tofino 144
Rescanning 116
Restoring a database 16

- S -

Sanity Check 230
Save Diagnostics 34
Saving Changes 128
Scan Continuously 116
Scan Details 116
scan object 116
Scan Properties 116
Scanning 116
Secure Asset Management LSM 93
Serial Tofino 291
Setting Broadcast Rules 195
Setting Global Rules 179, 192
Setting Talker Rules 178, 182
Source Node 84
Special Rules 25, 82, 174
State Tracking 230
Sync CMP 34, 114
Sync Tofino 34
Synchronizing Your Tofino's Configuration 148

- T -

Talker Rules 174
TCP/UDP Protocol 74
Technical Support 307
Timestamp 84
Tofino Auto Discovery 116
Tofino Central Management Platform (CMP) 6
Tofino CMP Database 127
Tofino CMP Licensing 98, 286
Tofino CMP Preferences 97, 101
Tofino CMP Tab Management 152
Tofino Device Database 127
Tofino Discovery 92, 116, 293
Tofino Discovery View 92
Tofino ID 58
Tofino Loadable Security Modules (LSM) 6
Tofino SA Wizard 58

Tofino Update Wizard 147
Tofino View 25, 42
Tofino View Right Click Menu 42
Tofino100 268
Tofino™ Security Appliance Firmware Update Process 147
Tools Menu 12

- U -

Unicast Traffic 214
Unprotected Media Type 58
Updating the Firmware 12
USB Load Config 58
User Administration 97
Using Asset Discovery 203
Using Tofino Discovery 116

- V -

Valid Characters 111
Validating Databases 16
Vendor 27
Version and copyright information 24
VPN 247
VPN Client 245, 247
VPN PC Client 247, 265, 267
VPN PC Client Licensing 267
VPN Server 247

- W -

Windows Menu 22