ConneXium

TCSEFEA Tofino Firewall
User Manual

S1B76071.00

www.schneider-electric.com

Schneider Electric

Contents

Safety Information

Important Information

Notice: Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** minor or moderate injury.

PLEASE NOTE: Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel.
No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

About this Manual

Validity Note
The data and illustrations found in this book are not binding. We reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be construed as a commitment by Schneider Electric.

Product Related Information
Schneider Electric assumes no responsibility for any errors that may appear in this document. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of Schneider Electric.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, please follow the relevant instructions.

Failure to use Schneider Electric software or approved software with our hardware products may result in improper operating results.

Failure to observe this product related warning can result in injury or equipment damage.

User Comments
We welcome your comments about this document. You can reach us by e-mail at techpub@schneider-electric.com

Related Documents

Title	Reference number
TCSEFEA ConneXium Tofino Firewall User Manual	S1B76071
TCSEFEA ConneXium Tofino Firewall Installation Manual	S1B69349

Key

The designations used in this manual have the following meanings:

▶	List
☐	Work step
■	Subheading
Link	Cross-reference with link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
`Courier`	ASCII representation in user interface

1 Introducing the ConneXium Tofino Configurator

The ConneXium Tofino Industrial Security Solution is a comprehensive package for securing industrial control systems, particularly at the Local Area Network (LAN) level. The system consists of three core components:

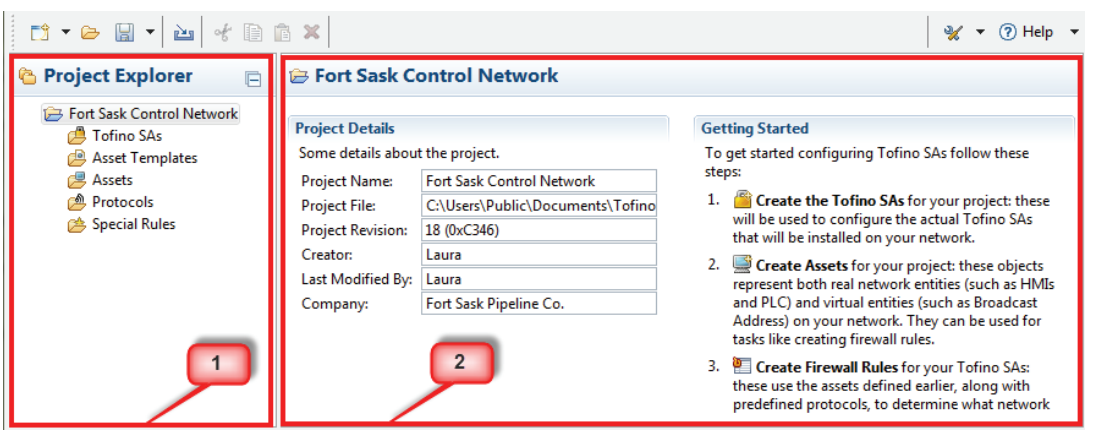
- ConneXium Tofino Firewall- Referred to in this manual as the Tofino Security Appliance or Tofino SA, these industrially hardened devices are installed in front of individual and/or clusters of Human Machine Interfaces (HMI), Distributed Control Systems (DCS), Programmable Logic Controllers (PLC) or Remote Terminal Units (RTU) control devices that require protection.
- Tofino Loadable Security Modules (LSM) - a variety of software modules providing security services such as Firewall and Event Logger. Each LSM is activated on the Tofino SAs to allow them to offer customizable security functions, depending on the requirements of the control system. ConneXium systems have the LSMs pre-loaded at the factory.
- ConneXium Tofino Configurator - a Windows-based off-line management system for the configuration of each Tofino SA.

Use the ConneXium Tofino Configurator off-line on your PC to define configuration data for each Tofino SA in your plant. When you have finished editing the configuration, you can save a copy of the configuration data to a USB storage device and then use this storage device to transfer the configuration into the Tofino SAs. You can also retrieve configuration details from a Tofino SA and load them back into the ConneXium Tofino Configurator to verify that the correct configuration is being used in the field.

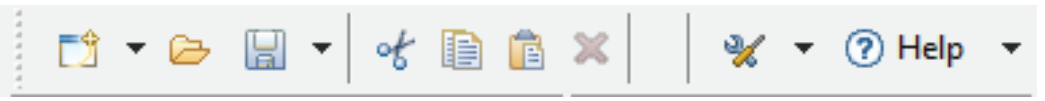
1.1 Navigating the ConneXium Tofino Configurator

The ConneXium Tofino Configurator is designed to look and operate just like Windows Explorer that you use to navigate files and folders on your computer. This way you can start using the ConneXium Tofino Configurator immediately.

- 1 - Project Explorer view: where Tofino SAs, Asset Templates, Assets, Protocols and Special Rules are listed in a tree format similar to the way that files are displayed in Windows Explorer. Any object in the Project Explorer view can be clicked on and details can be viewed in the Details view. Clicking on the root folder will display a table of defined objects of that type. For example, clicking on the Assets folder will present a table of the defined assets in the project.
- 2 - Details view: where the details of what is selected in the Project Explorer are displayed. This is where you can edit particular values for an object.



The ConneXium Tofino Configurator has a tool bar that allows you to perform actions on the objects in a project.



The toolbar contains 3 sections

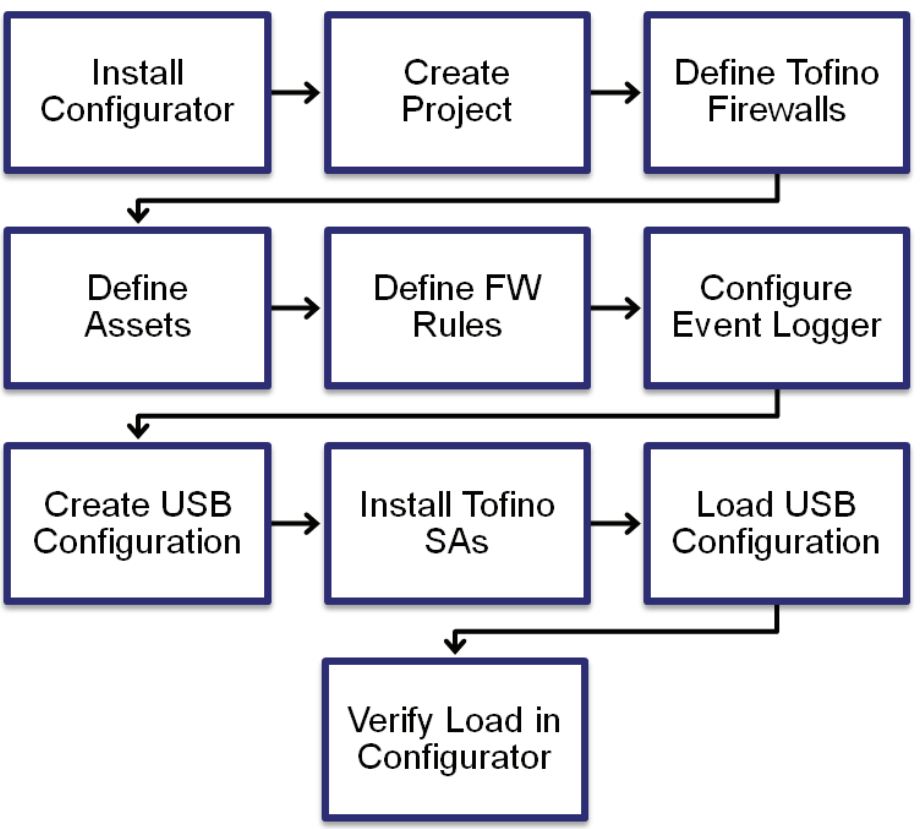
- Project Edit commands - This section appears at the far left of the toolbar and is for commands related to managing project files and their data. It includes:
  - Create new Projects, Assets, Asset Templates, Protocols, or Tofino SAs, using a wizard.
  - Open an existing project.
  - Save a project.
  - Import predefined Asset Templates, Protocols, Special Rules and Security Profiles
  - Cut/Copy/Paste/Delete of objects and fields.

- Context commands - This section appears in the center of the toolbar and is for commands related to the content that is currently being worked on. The list of commands which appears here changes depending on the type of object selected in the Project Explorer.

- Help and Configuration commands - This section appears at the far right of the toolbar and is for:
  - Audit Logs: Viewing and managing the audit system.
  - Preferences: Setting configurations, such as the location of the audit file.
  - Help menu commands (down arrow to the right of Help); including About and Display Help.

2 10 Steps to a Secure Control System

The ConneXium Tofino Configurator was designed to make the installation of security firewalls in an industrial control system as simple as possible. Follow the steps below to configure and install your ConneXium Tofino Industrial Security Solution.



☐ Install your ConneXium Tofino Configurator on your computer.
☐ Create a Tofino ConneXium project.
☐ Define the Tofino SAs for your project: This information will be used to configure the actual Tofino SAs that will be installed on your network.

- ☐ Define Assets for your project: These objects represent both real network entities (such as HMIs and PLCs) and virtual entities (such as Broadcast Addresses) on your network. They are used to simplify tasks like creating firewall rules.
- ☐ Define Firewall Rules for your Tofino SAs: These use the assets you created earlier, along with predefined protocols and special rules that are supplied with the ConneXium Tofino Configurator to determine what network traffic the Tofino SA will allow or block. The Modbus TCP Enforcer is accessed through the Firewall selection.
- ☐ Configure the Event Logger (Optional): Enter the details for your syslog server where you want Tofino SA alarms and events sent. Or configure the Tofino SA to save logs locally on the Tofino SA for later offloading via USB storage device.
- ☐ Create a configuration on a USB storage device: This builds encrypted configuration files for loading into Tofino SAs and stores them to a USB storage device.
- ☐ Install your Tofino SA hardware on the network, between the device(s) to be protected and the rest of the network.
- ☐ Load the configuration into the Tofino SAs: Insert the USB storage device containing your configuration files into the USB port on the matching Tofino SAs and then load the configuration.
- ☐ Verify the configuration: Retrieves the configuration load reports from the USB storage device that was used to load configurations onto one or more Tofino SAs. This will allow you to record the configuration of Tofino SAs in the field and save it in your project.

You have successfully installed the ConneXiumTofino Industrial Security Solution and significantly improved the security of your process network.

Note: The Tofino SA will pass network traffic freely during the initial configuration or when its configuration is being updated. Firewall rules take effect after completion of the initial configuration or update of the Tofino SA so that network operations are not affected before the full rule set can be loaded. A typical configuration load will finish in approximately 30 seconds.

3 Installing Your ConneXium Tofino Configurator

This section details the procedure for installing the ConneXium Tofino Configurator on a computer that has not previously had the ConneXium Tofino Configurator installed on it.
The steps for installing a new copy of the ConneXium Tofino Configurator are as follows:

☐ Run the ConneXium Tofino Configurator installer.
☐ Assign a License Activation Key (LAK), affixed to the CD envelope supplied with the ConneXium Tofino Firewall product.

Initial Preparation

Prior to installing your ConneXium Tofino Configurator software, please verify that you have the following materials ready:

- ConneXium Tofino Configurator Installer CD.
- License Activation Key (a 25 string of letters and numbers such as X4QP9-RMNRQ-B59SD-AG5H6-KSFRW).

Run the ConneXium Tofino Configurator Installer

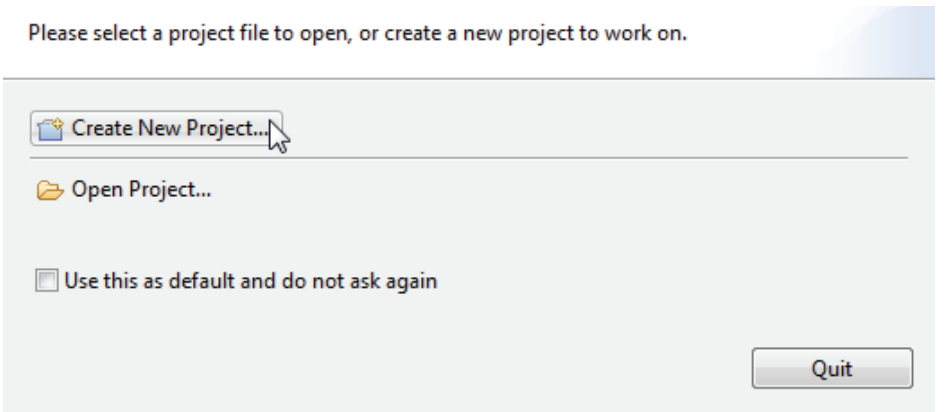
☐ Run the ConneXium Tofino Configurator installer from the CD.
☐ Follow the on-screen instructions to install the ConneXium Tofino Configurator.
☐ Enter your LAK, and required information on the `Activate Your License` screen.

4 Creating Projects

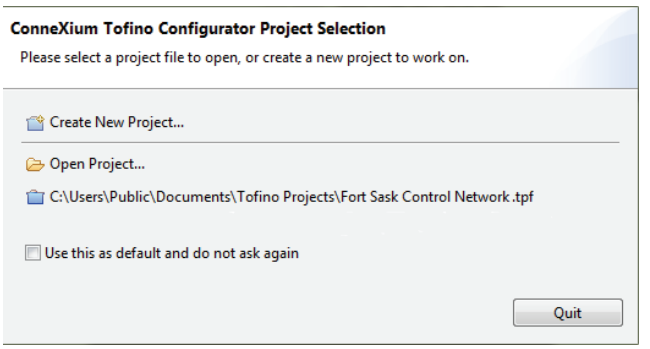
The ConneXium Tofino Configurator uses Project Files to coordinate one or more Tofino SAs that are being used for a common facility or project. Each Project File contains the configurations of the Tofino SAs it is managing along with other data such as network assets and common protocols.

The first time you start the ConneXium Tofino Configurator, you will be asked if you would like to:

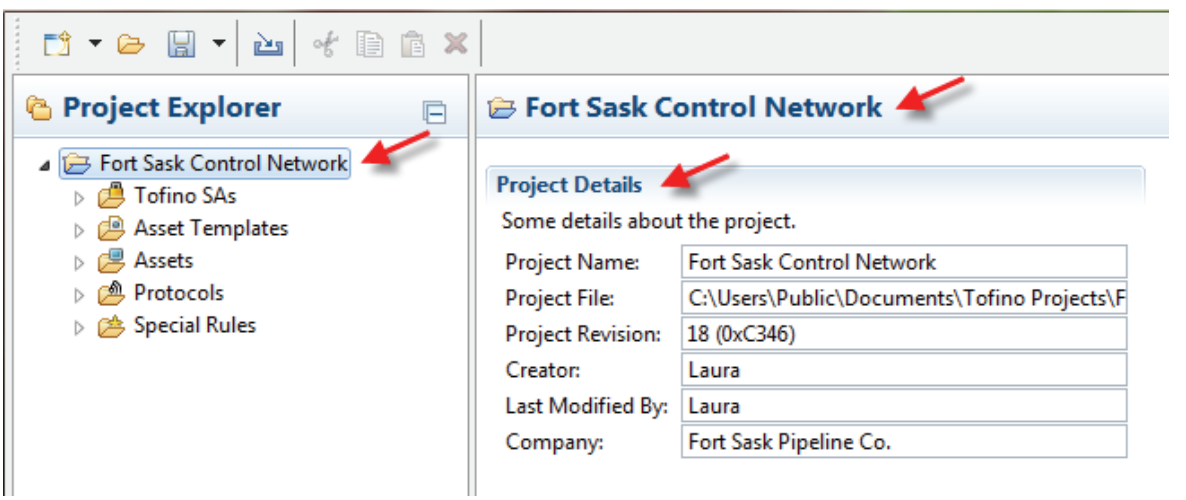
- Create a new Project, see “Creating a New Project”.
- Open an existing Project.



Once you have worked on a Project File, that file will be visible for you to open, with one click, on the start up window. You can also set a specific Project File as the default project so that it is opened every time the ConneXium Tofino Configurator is started. Clearing or changing the default project is done in the Project Preferences, see “Preferences”.

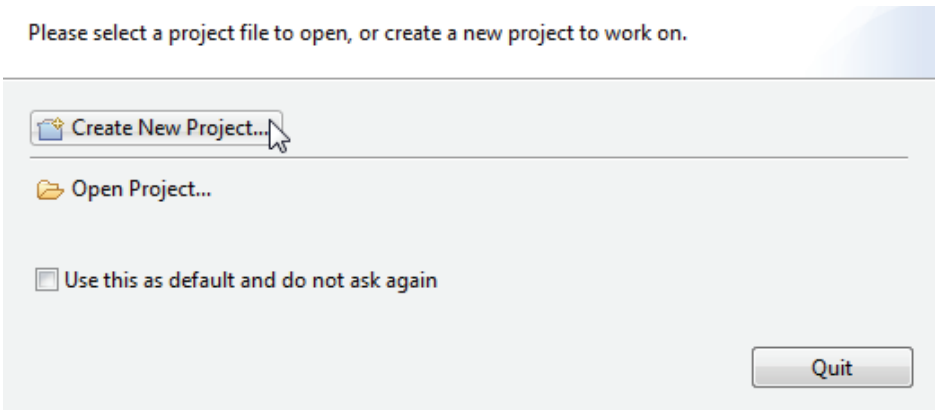


Once the project is open, the details about that project can be viewed in the Details view when the root folder in the Project Explorer is selected. This includes information such as the Project Name, Project File location on the PC, Project Revision, Creator and Company.

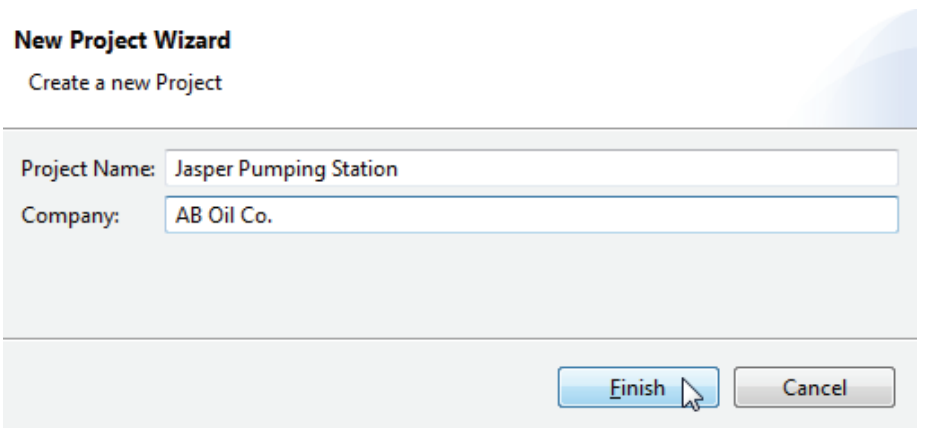


4.1 Creating a New Project

To begin using the ConneXium Tofino Configurator, create a Project. To launch the New Project Wizard, Select `Create a New Project` from the start-up screen. (You can also create a new project from the Project Explorer view by clicking the `New` button and selecting `Project`).



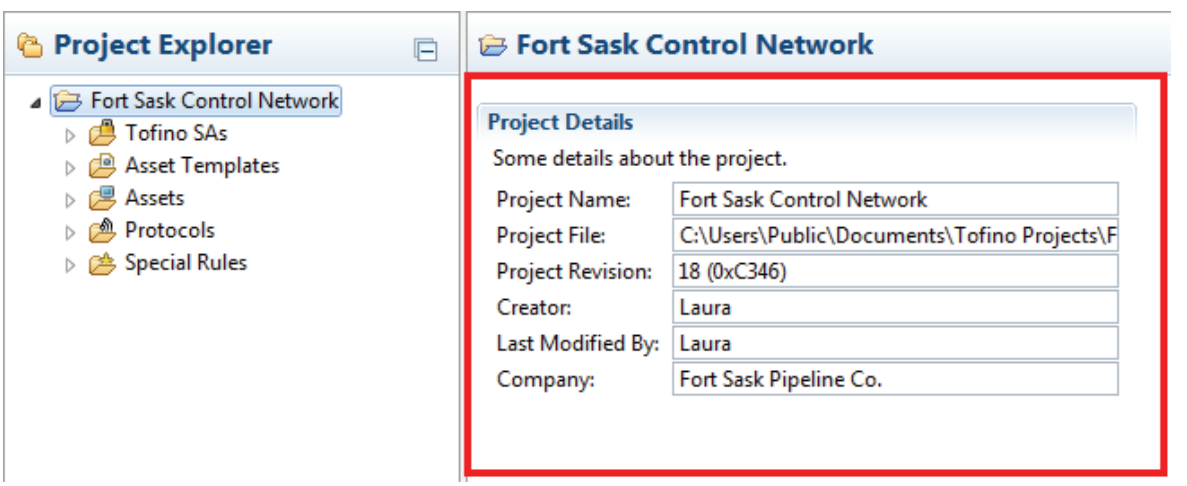
Once the user has started the wizard, it will ask you to complete two fields: `Project Name` and `Company`.



4.2 Viewing and Editing a Project

Clicking on the project name in the Project Explorer view will open the Project Details view. Here you can edit the details and check the current project version, creator and editors.

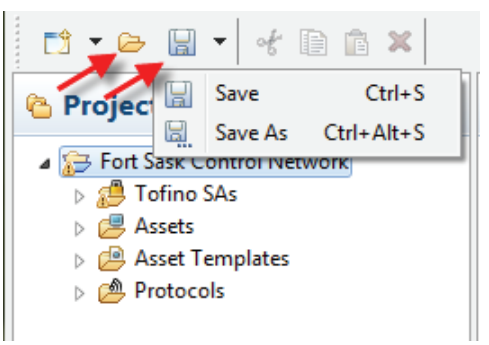
- Project Name - User editable project name. Defaults to "My Project".
- Project File - The file name and location where the Project File was loaded from or lasted saved to. This is also the location where the project will be stored the next time it is saved. It appears as "<unsaved>" for new, unsaved projects.
- Project Revision - The number of the current version of this project, along with a specially calculated hash code to reduce the chance of accidental duplication of revision numbers. The project revision number is incremented each time the project is saved.
- Creator - Uses the Windows username that was logged in at the time the project was created.
- Last Modified By - Uses the Windows username that was logged in at the time the project was last saved.
- Company - User editable company name.



4.3 Managing Project Files

Project Files can be managed just like any Windows' files. Using the ConneXium Tofino Configurator you can do the following:

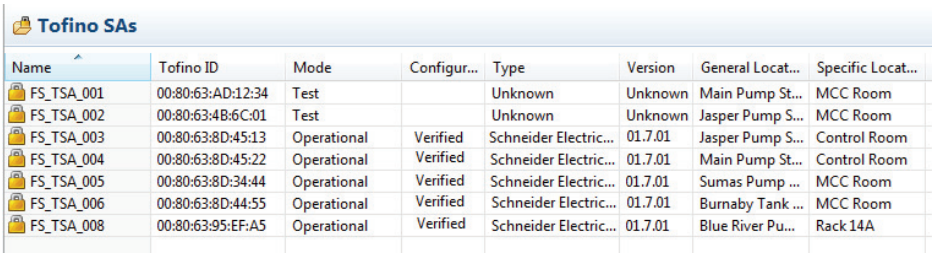
- Open - Open an existing Project File.
- Save - Save the current project to the Project File.
- Save As - Save the current project to a different Project File with a new name.



If you want to delete the Project File, you can use Windows Explorer to delete it, just like you would for any other computer file.

5 Defining Tofino SA Configurations

The Tofino SA management features allow you to create, edit, and delete the configuration data for multiple Tofino SAs contained in a single project.



Tofino SAs

Name	Tofino ID	Mode	Configur...	Type	Version	General Locat...	Specific Locat...
FS_TSA_001	00:80:63:AD:12:34	Test		Unknown	Unknown	Main Pump St...	MCC Room
FS_TSA_002	00:80:63:4B:6C:01	Test		Unknown	Unknown	Jasper Pump S...	MCC Room
FS_TSA_003	00:80:63:8D:45:13	Operational	Verified	Schneider Electric...	01.7.01	Jasper Pump S...	Control Room
FS_TSA_004	00:80:63:8D:45:22	Operational	Verified	Schneider Electric...	01.7.01	Main Pump St...	Control Room
FS_TSA_005	00:80:63:8D:34:44	Operational	Verified	Schneider Electric...	01.7.01	Sumas Pump ...	MCC Room
FS_TSA_006	00:80:63:8D:44:55	Operational	Verified	Schneider Electric...	01.7.01	Burnaby Tank ...	MCC Room
FS_TSA_008	00:80:63:95:EF:A5	Operational	Verified	Schneider Electric...	01.7.01	Blue River Pu...	Rack 14A

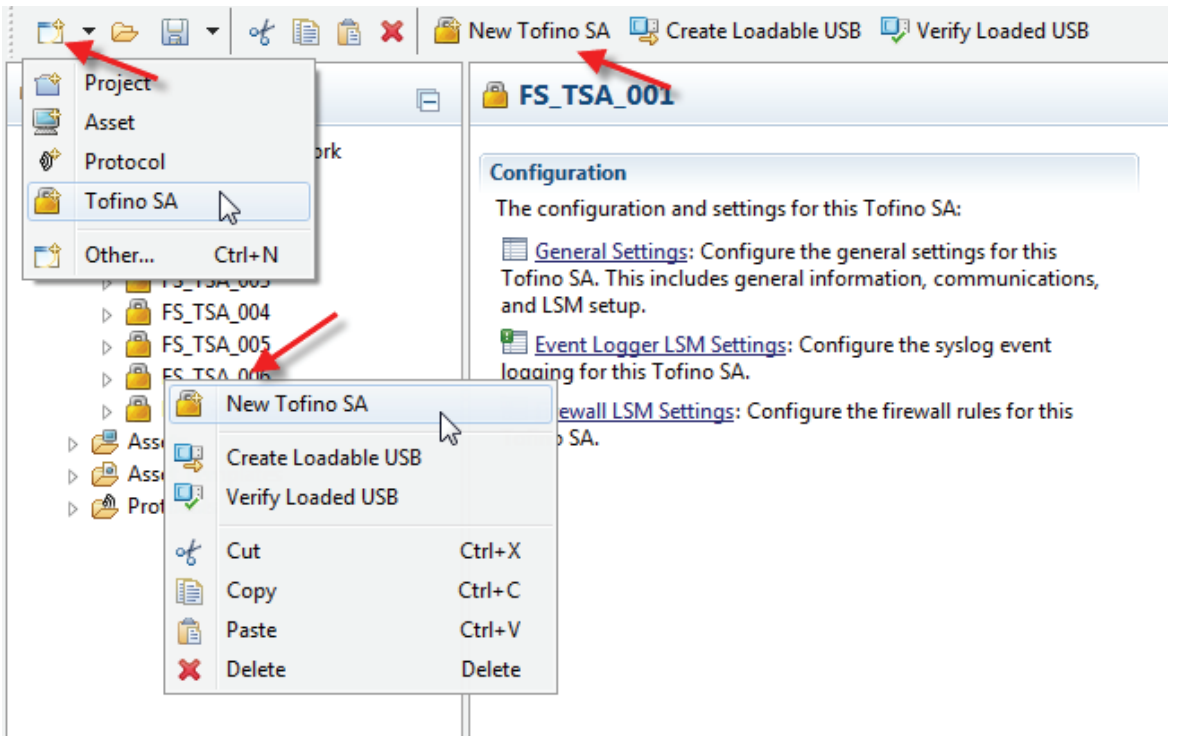
By selecting a specific Tofino SA in the Project Explorer view, you can do the following:

- ☐ Create a new Tofino SA.
- ☐ View and edit the Tofino SA configuration.
- ☐ Create a loadable configuration which you can save on a USB storage device. You can then insert the USB storage device into the USB port of a Tofino SA and load the configuration.
- ☐ Verify the load report from a USB storage device which was used to load a configuration. This will allow you to review and record successful USB loads.

5.1 Creating a New Tofino SA

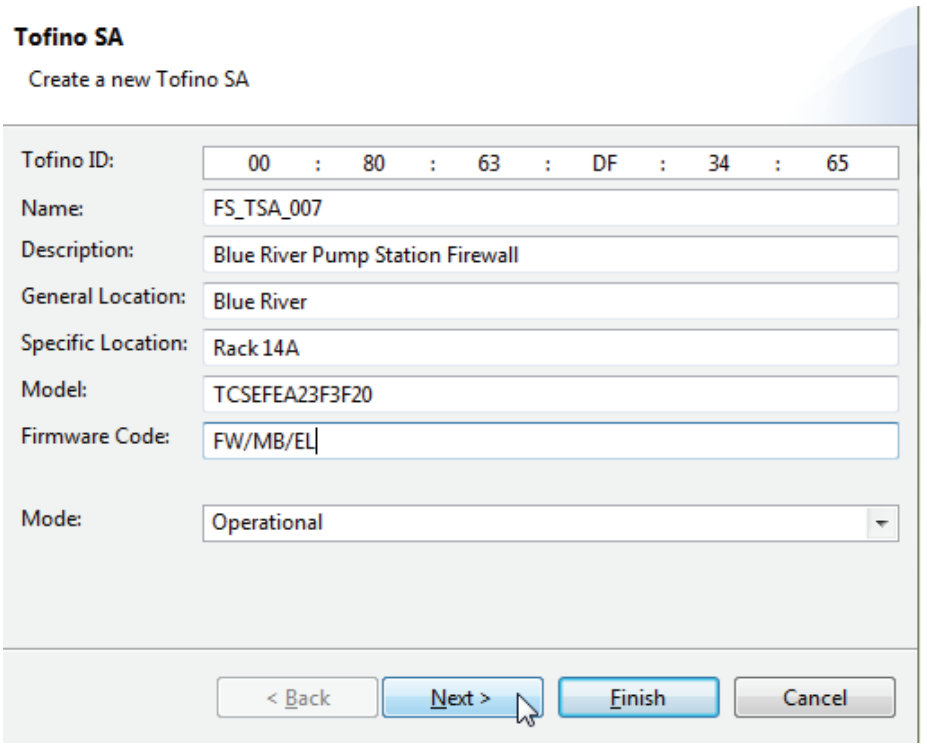
New Tofino SAs are created using the New Tofino SA Wizard. There are three ways to launch the New Tofino SA Wizard:

☐ Click the `New` button and select `Tofino SA`.
☐ Click the `New Tofino SA` button in the middle section of the tool bar.
☐ Right click on an existing Tofino SA and select `New Tofino SA`.

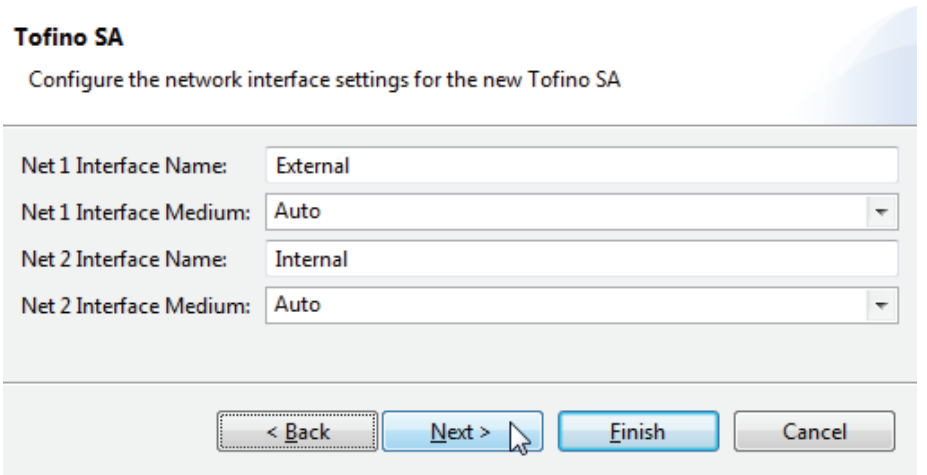


New Tofino SA Wizard

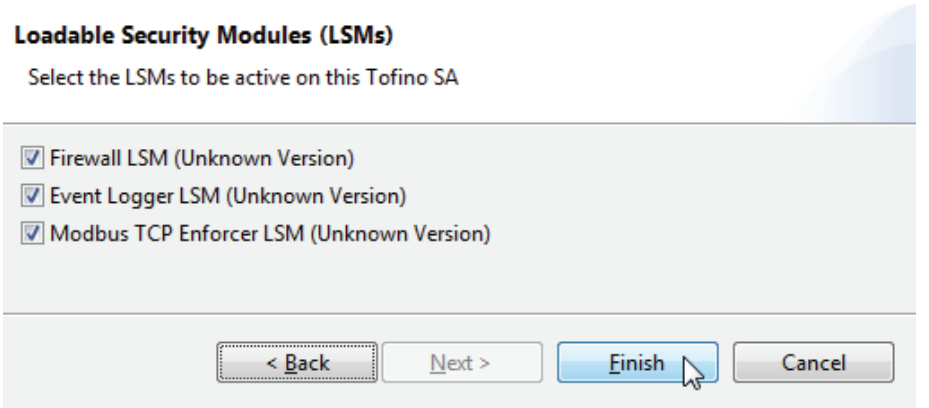
Once the wizard has started, it will ask you to enter the Tofino ID, Name, Description, General Location, Specific Location and Model. The Firmware Code will be automatically calculated based on the Model Number you enter. Lastly select the Mode (Operational or Test) you want the Tofino SA to run in when the configuration is loaded.



The second page of the wizard allows you to name the Tofino SA interfaces and set the configuration of each interface.



The third page of the wizard allows you to select which LSMs you would like to have activated on the Tofino SA.



For more information on these fields, see “Tofino SA General Settings”.

5.2 Viewing and Editing a Tofino SA

Clicking on the Tofino SA name in the Project Explorer view will open the Tofino SA Details view. Here you can navigate to pages for configuring the Tofino SA and launch wizards to perform actions such as creating a configuration on a USB storage device.

The configuration and setting options available for a Tofino SA will depend on the LSMs selected earlier. Typically, the available settings include:

- General Settings - Configure the general settings for the selected Tofino SA. This includes general information, communications parameters, and LSM selection.
- Event Logger LSM Settings - Configure alarm and event logging for the selected Tofino SA.
- Firewall LSM Settings - Configure firewall rules for the selected Tofino SA.

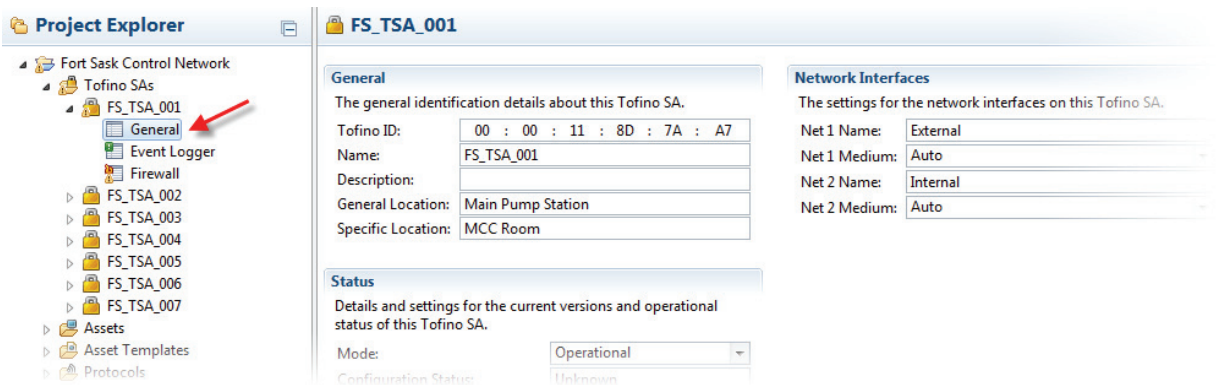
Some actions that can be performed for the selected Tofino SA are:

- Create Loadable USB Drive - Builds a loadable configuration and stores it to a selected USB storage device. This storage device can then be inserted into the USB port on the selected Tofino SA and the configuration loaded.

- Verify Loaded USB Drive - Retrieves the configuration report from a USB drive which was used to load a configuration onto the selected Tofino SA. This will allow you to review and record successful USB loads.

5.3 Tofino SA General Settings

The Tofino SA General Settings view allows you to view and configure the common settings for the selected Tofino SA. This includes general information, communications parameters, status and LSM selection.



General

- Tofino ID:
  The ID number found on the right hand side of the Tofino SA‘s face. This number is used to confirm that the configuration is loaded into the correct Tofino SA.
- Name:
  Insert a name or identifier that uniquely identifies the Tofino SA. (i.e. Jasper Pump Station Tofino or JP-TFN-001). Each Tofino SA needs to have a unique name for clarity and ease of deployment.
- Description:
  A text field that can be used to describe the function of this Tofino SA.
- General Location:
  A text field for reference.
- Specific Location:
  A text field for reference.

Network Interfaces

- Net 1 Name:
  A name or identifier that describes the upper Ethernet port on the Tofino SA. For example, you could name it after the network it connects to (such as "Business Network") or it could be named by function (such as "Untrusted").
- Net 1 Medium:
  This sets the interface settings on the upper 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 in the Tofino SA, you can manually set the Ethernet ports to the following:
  – Auto (auto-negotiate)
  – 10baseT-HD (Twisted pair, 10 Mb/s, half duplex)
  – 10baseT-FD (Twisted pair,10 Mb/s, full duplex)
  – 100baseTX-HD (Twisted pair,100 Mb/s, half duplex)
  – 100baseTX-FD (Twisted pair,100 Mb/s, full duplex)
  The default value is "Auto".
- Net 2 Name:
  A name or identifier that describes the lower Ethernet port on the Tofino SA. For example, you could name it after the network it connects to (such as "Control Network") or you could name it by function (such as "Trusted").
- Net 2 Medium:
  This sets the interface settings on the lower 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, you can also manually set the Ethernet ports to:
  – Auto (auto-negotiate)
  – 10baseT-HD (Twisted pair, 10 Mb/s, half duplex)
  – 10baseT-FD (Twisted pair,10 Mb/s, full duplex)
  – 100baseTX-HD (Twisted pair,100 Mb/s, half duplex)
  – 100baseTX-FD (Twisted pair,100 Mb/s, full duplex)
  The default value is "Auto".

Status

- Mode:
  You can set the Tofino SA to one of two modes:
  - Test:
    The Tofino SA is fully operational, processes traffic but will not drop any network traffic. You can use this mode to test if the Tofino SA is correctly configured before you use it to filter control system traffic.
  - Operational:
    The Tofino SA provides full-packet processing and protection.
- Configuration Status:
  This is the current status of the actual Tofino SA in the field, as determined by the last USB verification:
  - Unknown:
    The configuration has either not been loaded into the Tofino SA or has not been verified.
  - Verified:
    A USB configuration was successfully loaded onto the Tofino SA and the Verify Loaded USB command was run to read the results back into ConneXium Tofino Configurator.
  - Failed:
    The result of the Verify Loaded USB command shows that there was an unsuccessful load the last time the USB Load command was executed on this Tofino SA.
- Latest Configuration Revision:
  The number of the current version of this Tofino SA‘s configuration in this Project File, along with a specially calculated hash code to reduce the chance of accidental duplication of revision numbers. The configuration revision number is incremented each time you modify the settings of the Tofino SA and the project is saved. This is calculated separately from the Project Revision number by the ConneXium Tofino Configurator.
- Verified Configuration Revision:
  The number of the last version of this Tofino SA‘s configuration that has been verified by the Verify Loaded USB command as installed in the Tofino SA. There is also a specially calculated hash code to reduce the chance of accidental duplication of revision numbers. If the Verified Configuration Revision is different than the Latest Configuration Revision, then the Tofino SA in the field may contain an outdated configuration.
- Hardware Type:

This field is updated by the Verify Loaded USB command based on the Tofino type reported by the Tofino SA.

- Model:
  This field is updated by the Verify Loaded USB command based on the model reported by the Tofino SA
- Firmware Code:
  This field indicates the available LSMs pre-loaded in this product.
- Firmware Version:
  This field is updated by the Verify Loaded USB command based on the firmware version reported by the Tofino SA.

Loadable Security Modules (LSMs)

Here you can select the LSMs you wish to have activated on your Tofino SA during the USB Load. These include:

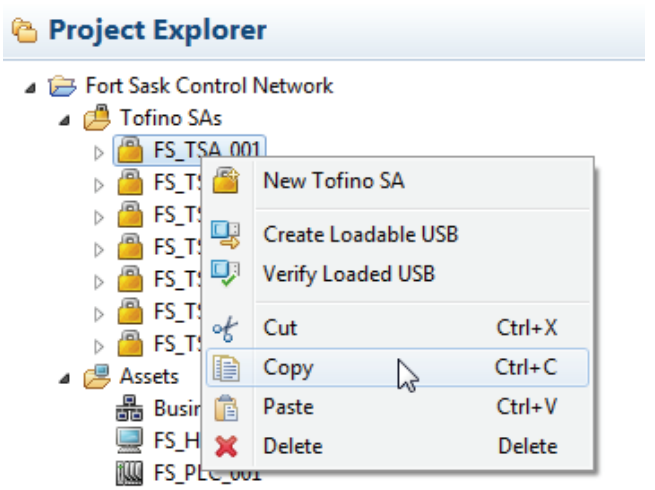
- Firewall LSM
- Event Logger LSM
- Modbus TCP Enforcer LSM

When an LSM is selected, additional sub-folders may appear below the Tofino SA folder. These allow you to configure the specific LSM. Keep in mind that settings for the Enforcer LSMs are included in the Firewall subfolder.

5.4 Managing Tofino SAs

You can manage your Tofino SAs just like any Windows' object. By right clicking on a Tofino SA, or using the tool bar, you have the following options:

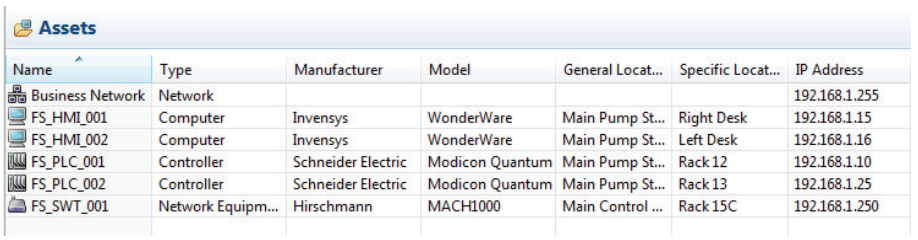
- New Tofino SA - Launches the New Tofino SA wizard.
- Create Loadable USB - Create a loadable configuration which can be saved on a USB storage device. The USB storage device can then be inserted into the USB port of a Tofino SA and the configuration loaded.
- Verify Loaded USB- Verify the load report from a USB storage device which was used to load a configuration. This will allow you to review and record successful USB loads.
- Cut - Removes the highlighted Tofino SA from the project and saves it in the clipboard for later pasting in a different location.
- Copy - Makes a copy of the highlighted Tofino SA from the project and saves it in the clipboard for later pasting in a different location.
- Paste - Pastes the contents of the clipboard into the project.
- Delete - Removes the highlighted Tofino SA from the project.



6 Defining Assets

In the ConneXium Tofino Configurator, you have "Assets" that include both physical devices such as PLCs, computers and network equipment, as well as "virtual" assets such as a broadcast address range, a network or a multicast address. This provides flexibility in the creation of firewall rules.

The Asset management features allow you to create, edit, and delete assets representing real world devices and systems on the control network. You can also use Asset Templates to help create a standard for commonly used assets.



Name	Type	Manufacturer	Model	General Locat...	Specific Locat...	IP Address
Business Network	Network					192.168.1.255
FS_HMI_001	Computer	Invensys	WonderWare	Main Pump St...	Right Desk	192.168.1.15
FS_HMI_002	Computer	Invensys	WonderWare	Main Pump St...	Left Desk	192.168.1.16
FS_PLC_001	Controller	Schneider Electric	Modicon Quantum	Main Pump St...	Rack 12	192.168.1.10
FS_PLC_002	Controller	Schneider Electric	Modicon Quantum	Main Pump St...	Rack 13	192.168.1.25
FS_SWT_001	Network Equipm...	Hirschmann	MACH1000	Main Control ...	Rack 15C	192.168.1.250

By selecting a specific asset in the Project Explorer view, you can:

- Create a new asset or folder.
- View and edit the asset's details.
- Delete an asset.
- Cut, Copy and Paste assets.

Computer, Controller, Device, and Network Equipment Assets

Most assets used in the ConneXium Tofino Configurator are real devices. These typically use messages known as Unicast messages. A Unicast message is network traffic directed from a specific device to another specific device. When you define an asset to be a computer, controller, device or network equipment, the ConneXium Tofino Configurator assumes it is a physical device on your network and helps create rules appropriate for that type of device.

Network Assets

Network assets are a virtual representation of the devices contained in a specific network or subnetwork. When you define an asset to be a network, the ConneXium Tofino Configurator assumes it is a collection of devices on your network that belong to a group of IP addresses known as a subnet. Thus, if you use a network asset in a rule, the ConneXium Tofino Configurator helps create rules that allow or deny traffic from that range of addresses.

Broadcast and Multicast Assets

In most 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 ConneXium Tofino Configurator has special assets designed to handle these types of messages.

- Broadcast:
  This asset represents an address that is used for IP broadcasts. Broadcast packets, which are a normal part of network operation, are transmitted by a device to a broadcast address that many devices listen to. For example, IP networks use broadcasts to resolve network addresses using Address Resolution Protocol (ARP). The exact broadcast address is dependent on the subnet defined for a given network. 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 type of asset is required if you wish to provide broadcast filtering rules in the Firewall LSM.
- Multicast:
  This asset represents an address that is used for IP multicasts. Multicast packets are transmitted to a multicast address that a set of devices listen to. 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.

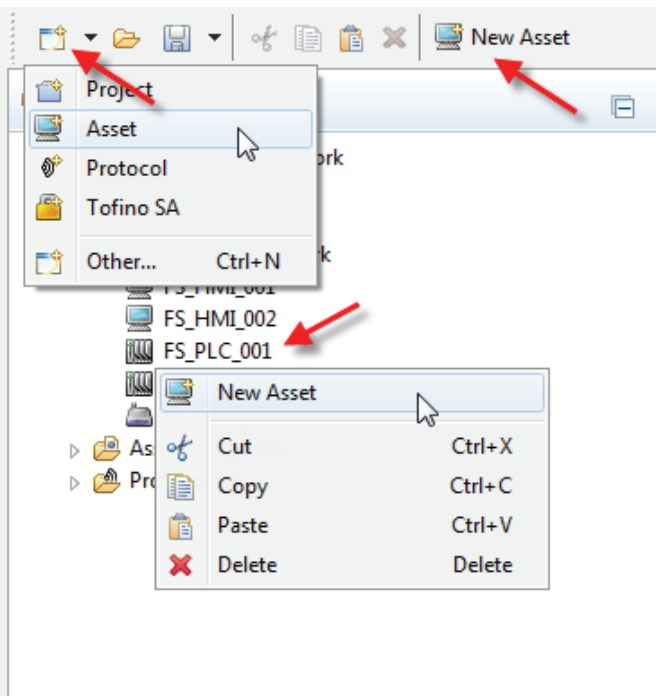
6.1 Creating an Asset

You can create new assets using the New Asset Wizard. You can launch the New Asset Wizard in four ways:

- Click the `New` button and select `Asset`.
- Click the `New Asset` button in the middle section of the tool bar.
- Right click on an existing asset and select `New Asset`.
- Creating an asset from an Asset Template.

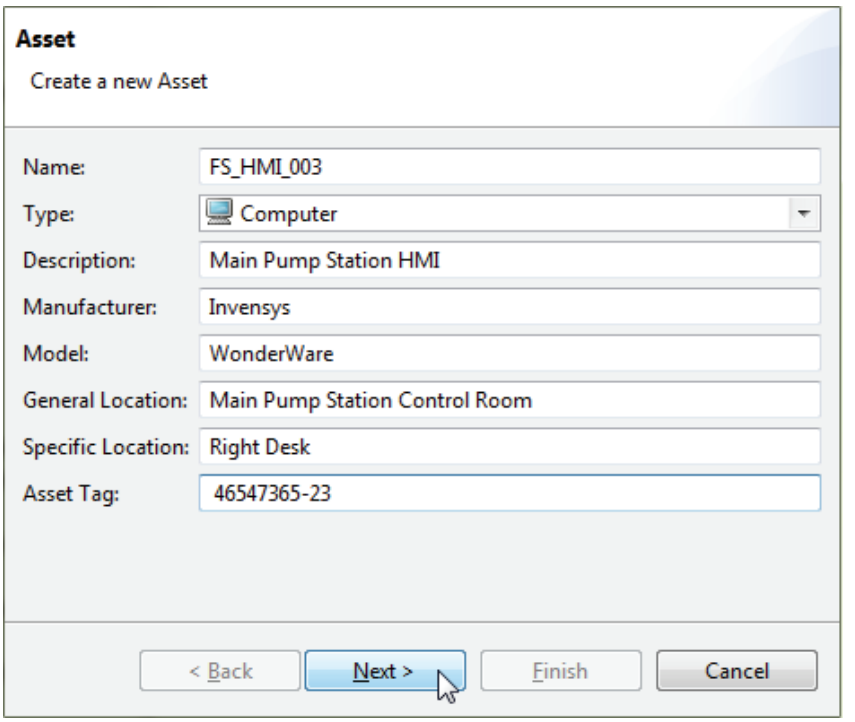
The fourth method is available when the Asset Template folder is selected.

You can also copy and paste from existing assets or asset templates to the asset folder. However this will not run the wizard, so you will have to manually edit the appropriate fields such as name and IP address.

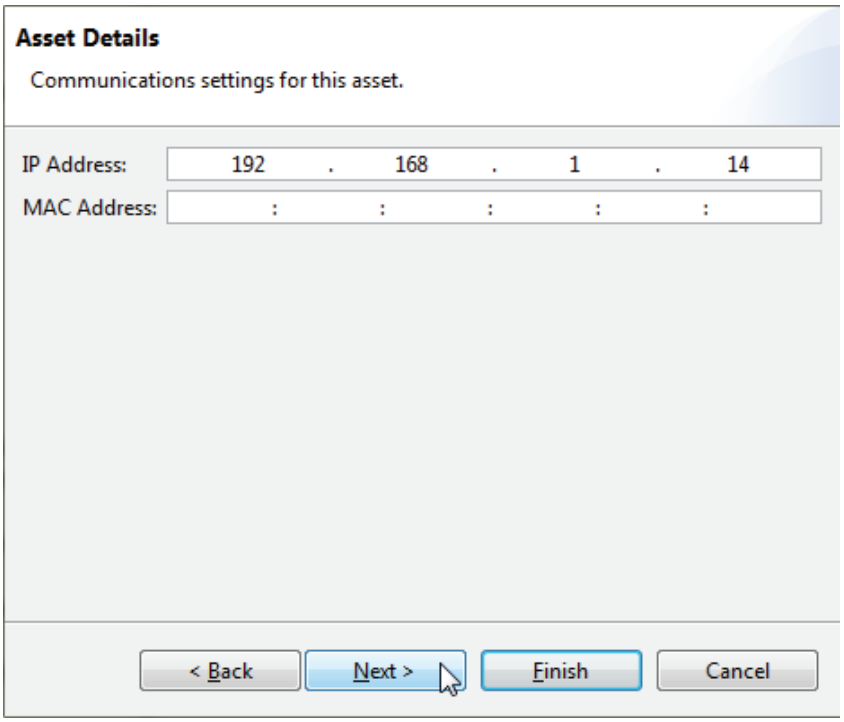


New Asset Wizard

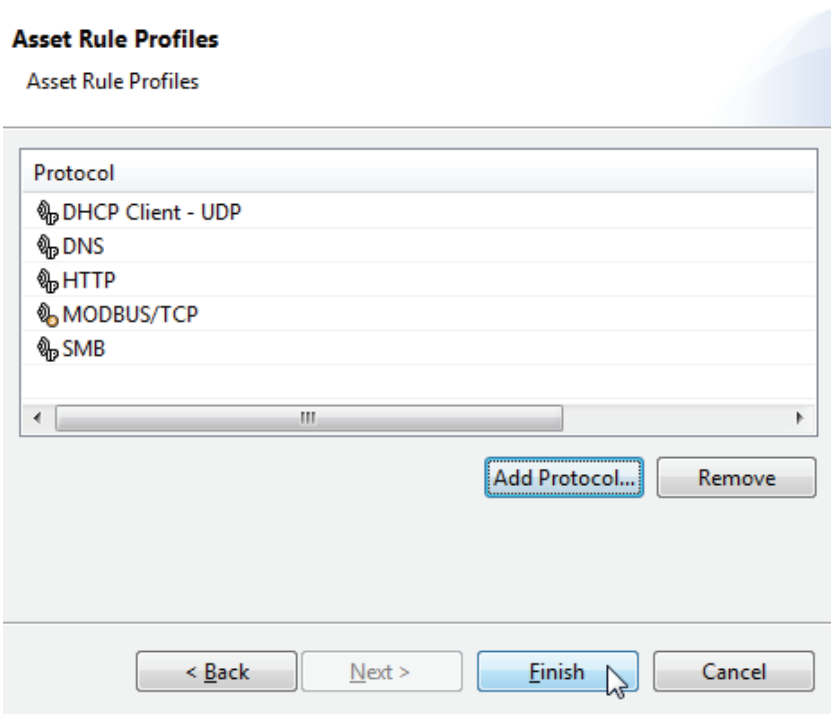
Once you start the wizard, it will ask you to enter the Name, Asset Type, and a number of optional fields. For more information on these fields, see “Viewing and Editing Assets”



The second page of the wizard allows you to enter the address information for the asset. This information will be used by the ConneXium Tofino Configurator when creating firewall rules for this asset.



The third page of the wizard allows you to define rule profiles by selecting protocols that the asset typically uses to communicate. These rule profiles are used in the firewall rule generation to suggest possible rules.



6.2 Asset Templates

Asset Templates are a tool to help you create multiple Assets quickly. They contain pre-defined fields that can be used to rapidly create similar assets. For example, if you have 10 PLCs in your plant that are a similar make and model, you can create an Asset Template (or use a pre-existing Asset Template) to represent that type of PLC. Then you can quickly generate Assets to represent the10 PLCs. Each time you use the `New Asset From Template` tool, a new Asset will be created with the fields filled out except for the Name, Location and Address information.

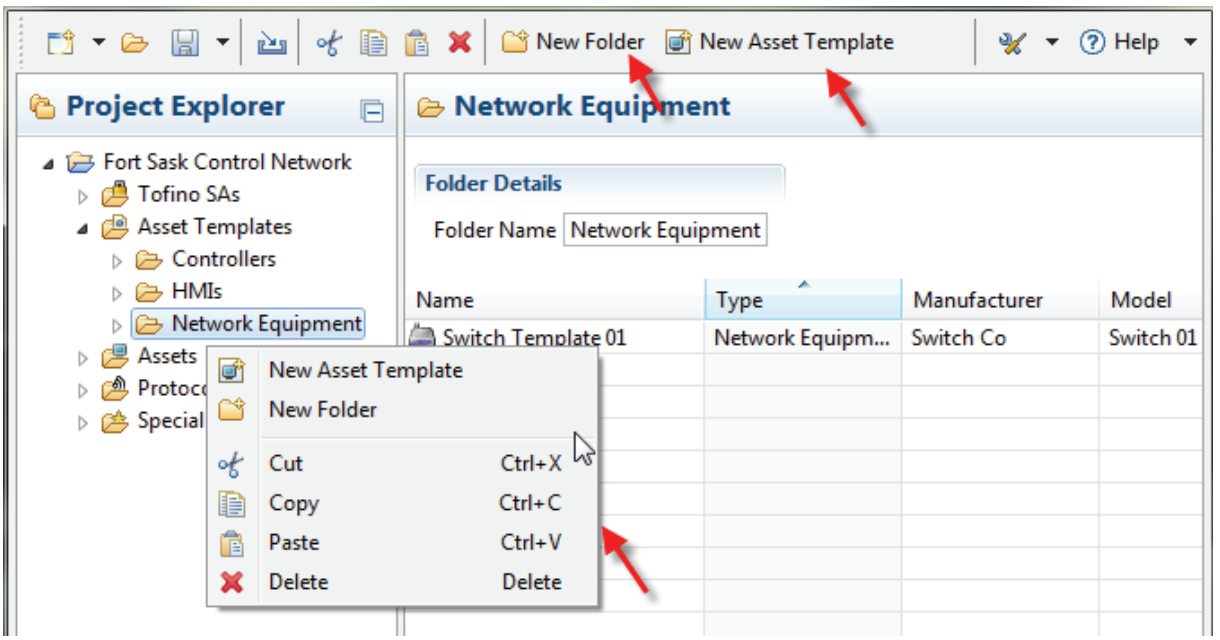
The ConneXium Tofino Configurator comes with a number of templates pre-loaded for Schneider Automation products. You can also import new templates using the Import command or create templates of your own.

You can also create Asset Templates by copying an existing Asset and pasting it into the Asset Template folder.

By selecting a specific Asset Template in the Project Explorer view, you can:
- Create a new asset template or folder.
- Create a new asset from the selected template.
- View and edit the asset templates's details.
- Delete an asset.
- Cut, Copy and Paste asset templates.

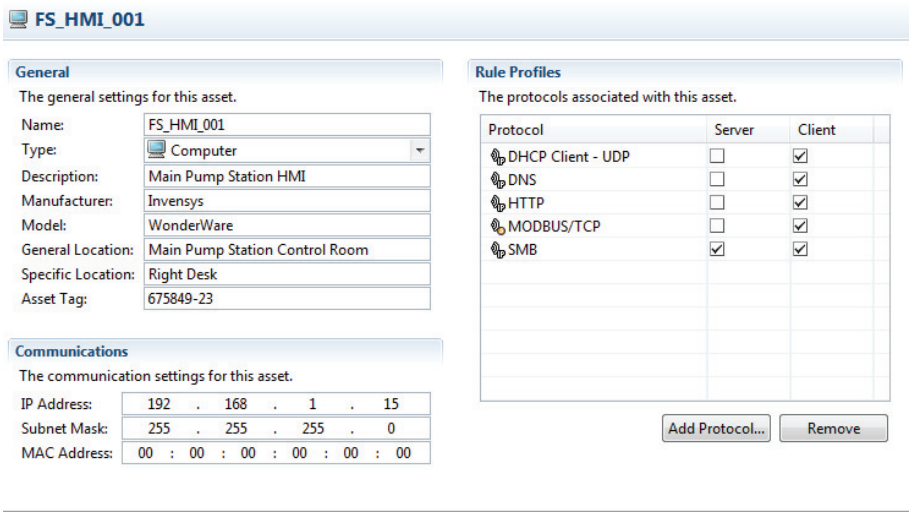
Some templates are factory defined, and cannot be cut or deleted.

In order to use an Asset Template as the basis for an asset, select the template you wish to use and then select the `New Asset From Template` button. This will start the New Asset wizard with most of the fields already completed.


New Folder
New Asset Template
Help
Project Explorer
Network Equipment
Fort Sask Control Network
Tofino SAs
Asset Templates
Controllers
HMIs
Network Equipment
Assets
Folder Details
Folder Name
Network Equipment
Name
Type
Manufacturer
Model
Switch Template 01
Network Equipm...
Switch Co
Switch 01
New Asset Template
New Folder
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Delete Delete

6.3 Viewing and Editing Assets

Clicking on an asset name in the Project Explorer view will open the Asset Details view. This allows you to view and configure the settings for the selected asset. This includes general information and communications parameters.



General

- Name:
  Insert a name or identifier that uniquely identifies the asset. (i.e. Jasper Pump Station PLC or JP-PLC-001). Each Asset needs to have a unique name to avoid confusion.
- Type:
  Select an asset type.The fields available for input, will be determined by the asset chosen. Asset types include:
  - Computer
  - Controller
  - Device
  - Network
  - Network Equipment
  - Broadcast
  - Multicast
- Description:
  A text field you can use to describe the function of this asset.
- Manufacturer:
  The make or company that manufactured or sold this asset (for example, Schneider Electric).
- Model:
  The model of this asset (for example, Quantum).
- General Location:
  A text field for reference.
- Specific Location:
  A text field for reference.
- Asset Tag:
  User defined field for corporate asset tags.

Communications

- IP Address:
  This is the IP address of the asset. In order for the firewall rules to operate properly, check that the address is correct.
- Subnet Mask:
  The subnet mask is used by the Tofino SA 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.
- MAC Address:
  This is the Ethernet MAC or physical address of the asset. For most assets this is an optional field and should be left blank. However if you are creating rules for non-IP protocols such as GOOSE, then enter a MAC address.

Rule Profiles

When you create an asset you can also specify the protocols that this asset typically uses. You can also specify whether the asset uses these protocols as a client (i.e.: it initiates the communications) or as a server (i.e.: it responds to requests from clients). The New Firewall Rule Wizard can use this information to automatically create rules for the asset.

- Protocol:
  A list of protocols that this asset can use for network communications.

  Note: that if you select an application layer protocol such as Modbus or HTTP you do not have to select the lower layer protocols such as Ethernet, TCP and IP.

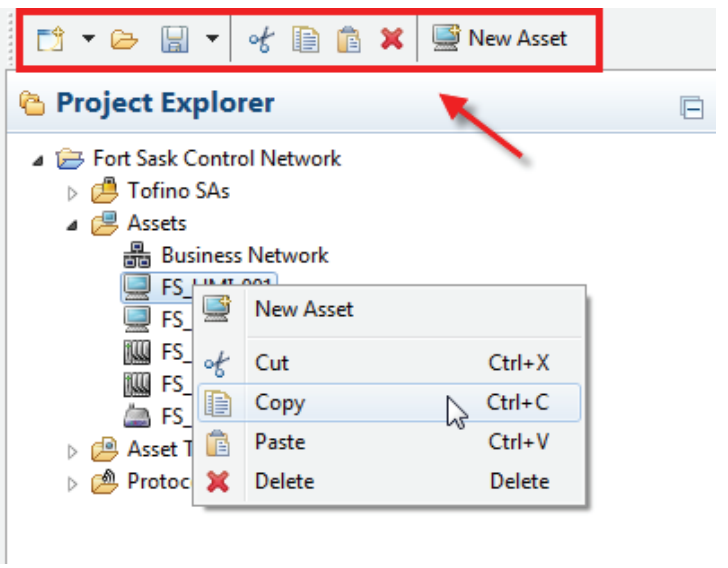
- Server:
  Selecting this box indicates that the asset acts as a server and responds to requests from clients. For example, a web server or a Modbus slave device (such as a PLC) would be selected as a server.
- Client:
  Selecting this box indicates that the asset acts as a client and initiates requests to servers. For example, a web browser or a Modbus client device (such as a HMI) would be selected as a client.

Protocols can be set as both client and server on an asset if appropriate. For example, a computer may contain both web server software and web browser software and thus could be designated as both a HTTP client and an HTTP server.

6.4 Managing Assets

You can manage assets just like any Windows' object. By right clicking on an asset, or using the tool bar, you have the following options:

- New Asset - Launches the New Asset wizard.
- New Folder- Creates a new folder for organizing your assets.
- Cut - Removes the highlighted asset from the project and saves it in the clipboard for later pasting in a different location.
- Copy - Makes a copy of the highlighted asset from the project and saves it in the clipboard for later pasting in a different location.
- Paste - Pastes the contents of the clipboard into the project.
- Delete - Removes the highlighted asset from the project.



7 Defining Firewall Rules

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) to help protect 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 devices (or networks) in need of protection and other systems - such as the corporate network, or another portion of a site's control network.

The Tofino Firewall is an LSM that is activated on the Tofino SA to process traffic. It is a stateful deep-packet inspection firewall.

What is an Enforcer?

An Enforcer is an advanced firewall for specific SCADA and ICS protocols. It allows you to filter traffic based on specific function codes and message content. Enforcers are designed to be add-ons to the standard Tofino Firewall LSM. Enforcers include:

- Modbus TCP Enforcer:
  This LSM provides security features for managing Modbus TCP traffic such as:
  - Checks to determine if each Modbus packet conforms to the protocol specification and then allows or rejects this packet.
  - Allows you to specify Modbus functions that should be allowed or denied by the Tofino SA.
  - Monitors the state of Modbus TCP connections to determine that incoming messages are expected and in sequence.

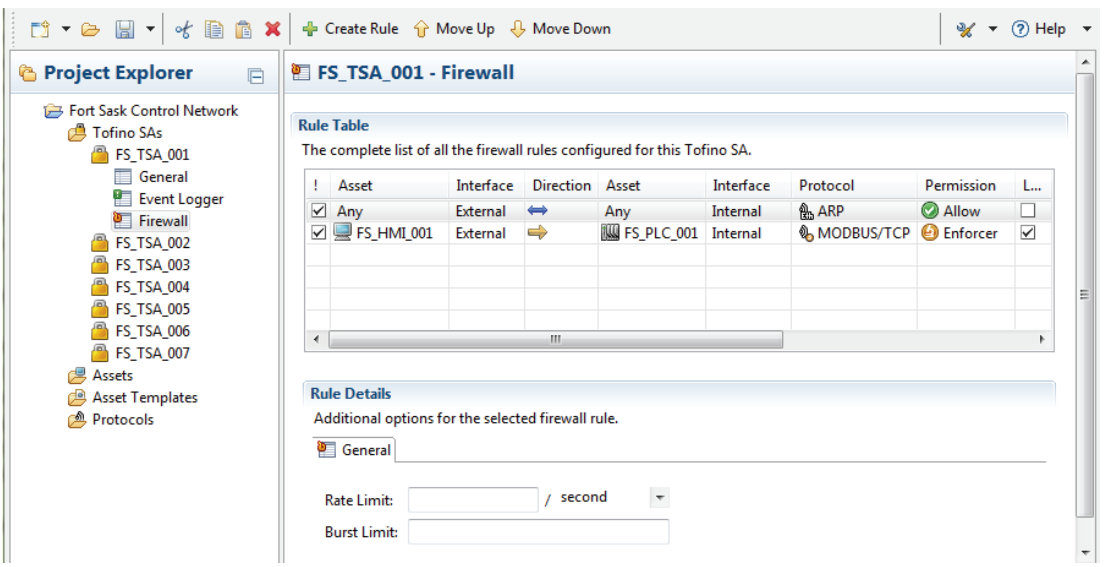
7.1 Managing Firewall Rules

The Firewall details page contains a list of firewall rules configured for the selected Tofino SA. It also allows you to:

- Create a new firewall rule.
- View and edit the rules.
- Reorder rules.
- Cut, Copy and Paste rules.
- Delete rules.

For the Cut, Copy, Paste and Delete commands you can select multiple firewall rules and perform mass operations. For example you can copy a block of rules from one Tofino SA and paste it into another.

If you select a rule, a Rule Details section will appear with options for that specific rule and protocol.

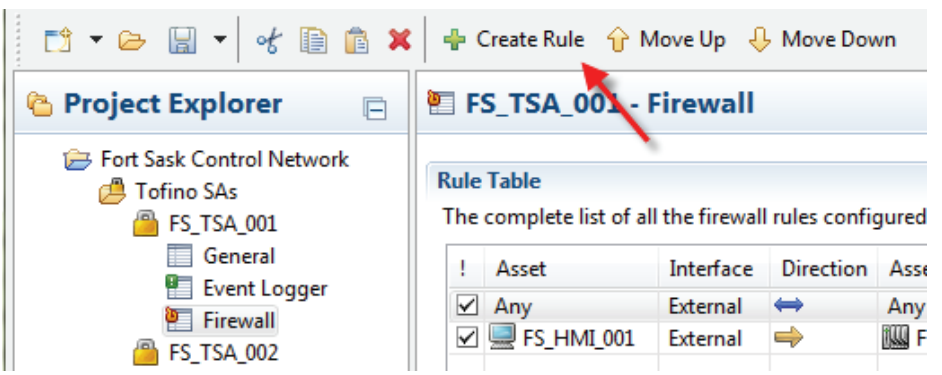


Creating Firewall Rules

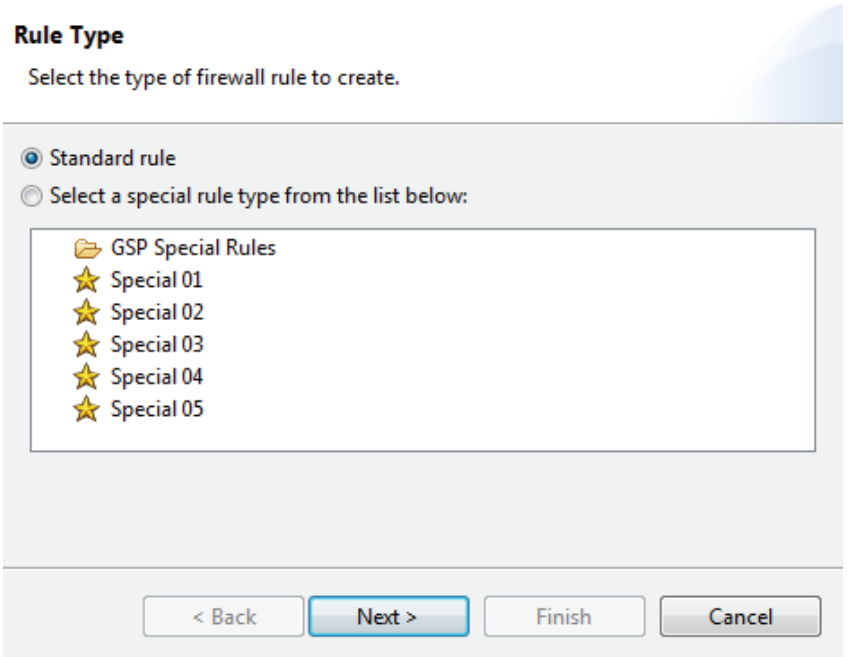
The ConneXium Tofino Configurator allows you to create two types of firewall rules:

- Standard firewall rules are designed to allow or deny specific protocols passing through the firewall. They allow you to set the source, destination, direction, permission and rate limits for traffic of a particular protocol type. For example, if you want to allow Modbus/TCP traffic between two devices, a standard rule can be used. Use standard rules for most applications.
- Special Rules are highly complex rules that go beyond simple allow or deny. For example, a Special Rule could be used to block a subset of a particular type of traffic. The available Special Rules can be viewed in the Special Rules folder. You should only use these rules in exceptional cases.

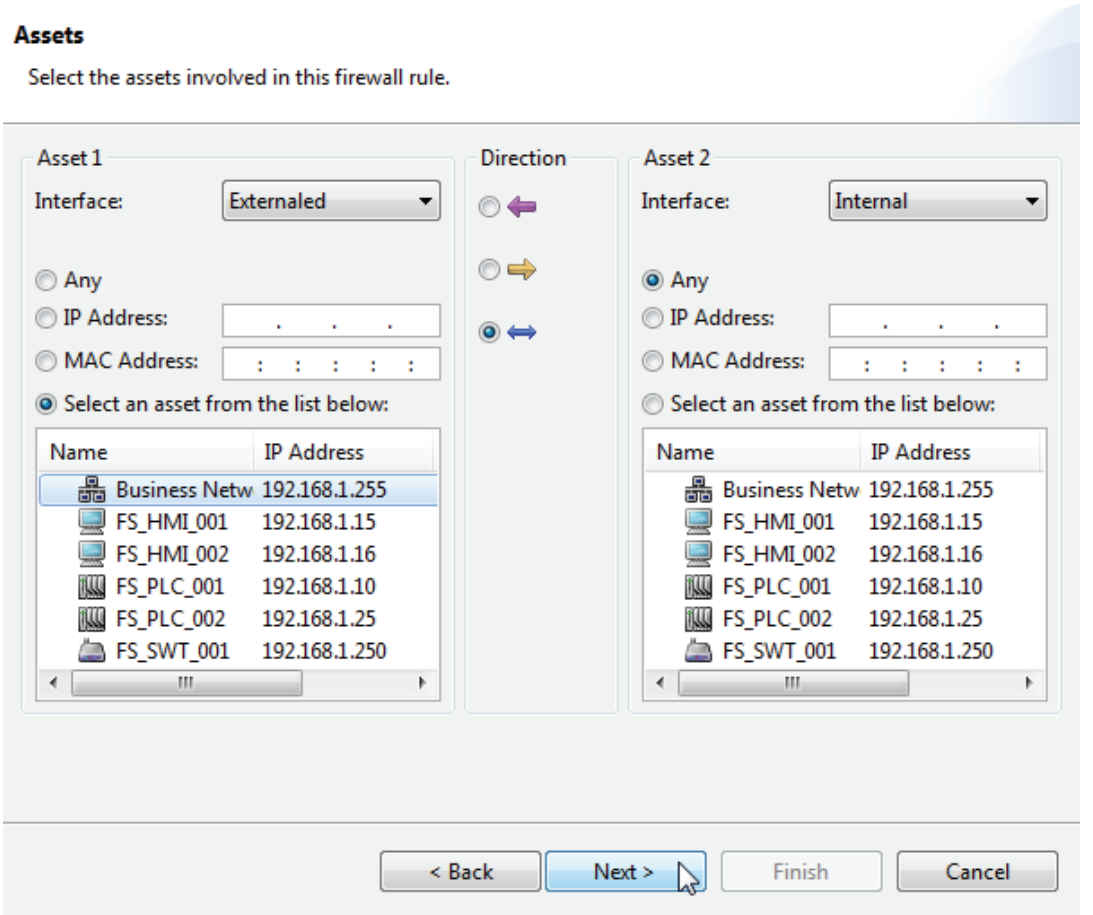
New rules are created using the New Firewall Rule Wizard.You can launch the wizard by selecting the Firewall Details view for the Tofino SA you wish to create a rule for and then by clicking the `Create Rule` button in the middle section of the tool bar.



Once the wizard has started, it will ask you if you want to create your rule based on a standard rule or a Special Rule. If you select Special Rule, you will be asked to choose from a list of available Special Rule templates.



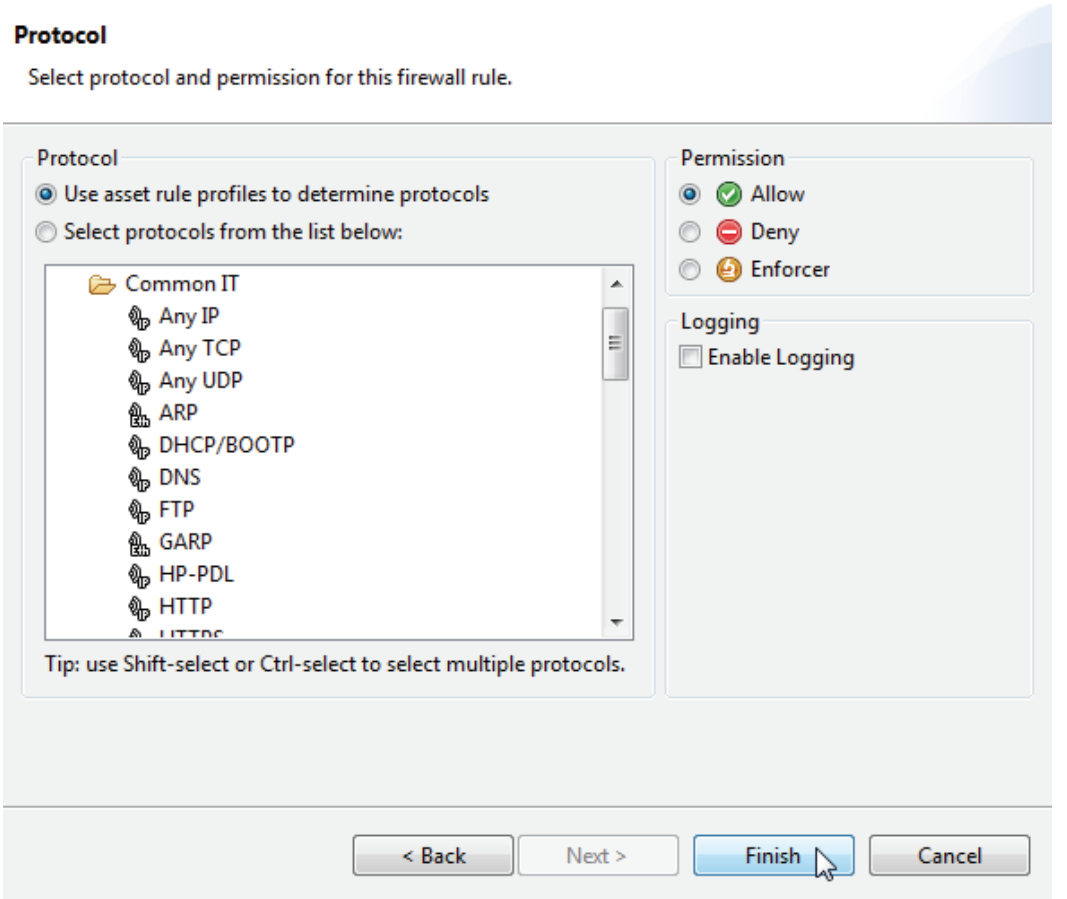
Next you will be asked to enter the Interfaces, Direction and either Assets or Addresses. For more information on these fields, see “Viewing and Editing Firewall Rules”



The second page of the wizard asks you to select one or more protocols for the rules. You can either allow the wizard to:

- Use the rule profiles associated with the assets you just selected to automatically generate the rules
- Manually select the protocols you want rules created for. If more than one protocol is selected, then a rule will be created for each protocol.

Finally, you select the permission (i.e.: Allow, Deny or Enforcer) and whether you want logs created whenever this rule is triggered.

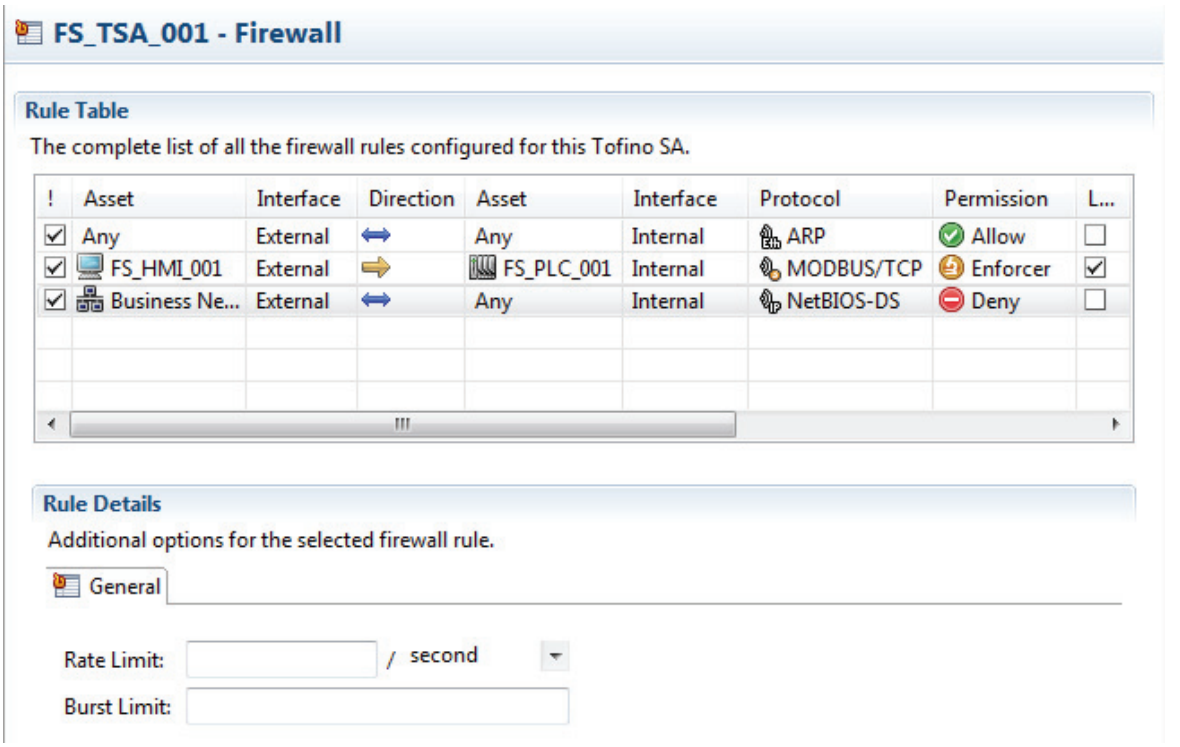


Note: When the option to automatically generate rules is selected, the ConneXium Tofino Configurator will check both of the assets selected earlier in the wizard for protocols listed in the rule profiles. The automatic rule generator will then create one rule for every protocol the two assets have in common. If the two assets do not have any protocols in common or if they have a protocol in common but are either both clients or both servers then a warning will be sent and no rules generated.

7.2 Viewing and Editing Firewall Rules

Clicking on the Firewall sub-folder for a Tofino SA in the Project Explorer view will open the Firewall Details view. Here you can view and edit the firewall rules for this Tofino SA including rule details (See “Firewall Rule Details”). You can also change the order rules are evaluated (See “Firewall Rule Order”). The ConneXium Tofino Configurator will also prompt you to create firewall rules that it deems necessary (See “Assisted Firewall Rule Creation”).

Editing Firewall Rules



- ! : This Active Rule check box will activate (selected) or deactivate (not selected) the rule. If the checkbox is not selected, the rule will not be loaded into the firewall. This allows you to create rules in advance that you wish to activate at a later time.It also allows you to quickly deactivate rules for testing, without having to delete them.
- Asset (#1)
  An asset or address that the rule applies to. The following are valid entries:
  – Any.
  – A defined asset name.
  – IP or MAC Address
    Keep in mind, that certain protocols require a specific address type or a predefined address.
- Interface:
  This is the Tofino SA interface where the left asset or address is found.

- Direction:
  The direction a session is initiated (See “Right versus Left versus Bidirectional”). There are three possible selections to choose from in the table:
  – Right.
  – Left.
  – Bidirectional.
- Asset (#2):
  An asset or address that the rule applies to. The following are valid entries:
  – Any.
  – A defined asset name.
  – IP or MAC Address.
    Keep in mind, that certain protocols require a specific address type or a predefined address.
- Interface:
  This is the Tofino SA interface where the correct asset or address is found.
- Protocol
  The protocol that you define when setting up the firewall rule in the ConneXium Tofino Configurator. There is a list of protocols found in the Protocol folder.
- Permission:
  What the firewall does with a packet, based on the defined rules. There are three options:
  – Allow: Traffic matching the rule is allowed through the Tofino SA.
  – Deny: Traffic matching the rule is blocked by the Tofino SA.
  – Enforcer: Traffic matching the rule in the Tofino SA will be further inspected and filtered based on Deep Packet Inspection settings. This option is available for protocols such as Modbus that have Enforcer LSMs installed.

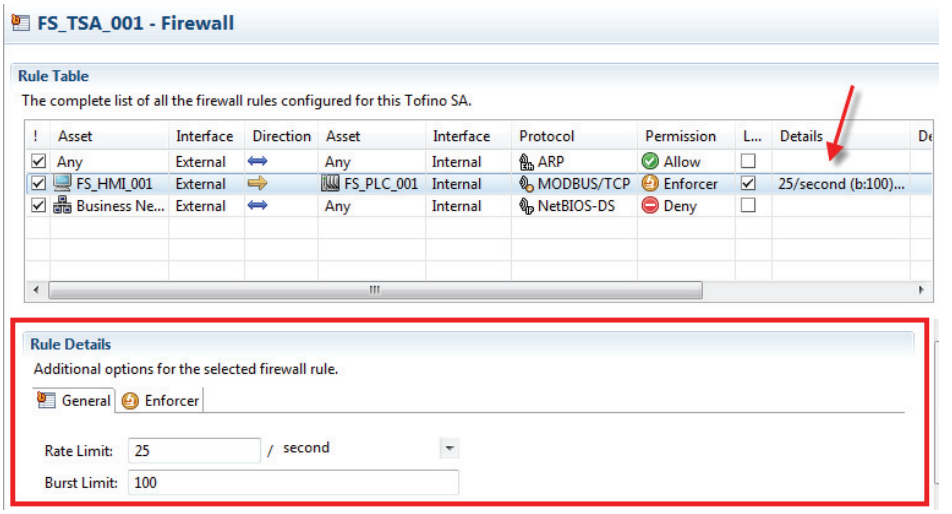
- Type:
  - Standard: These rules are designed to simply allow or deny specific protocols passing through the firewall. They allow the user to set the source, destination, direction and permission for traffic of a particular protocol type. For example, if the user wants to allow Modbus/TCP traffic between two devices, a standard rule can be used.
  - Special: These rules are highly complex rules that go beyond simple allow or deny. For example, a Special Rule could be used to block a subset of a particular type of traffic. The available Special Rules can be viewed in the Special Rules folder.
- Log:
  A checkbox for setting Logging on the rule.

  Note: By default, denied packets are logged and allowed packets are not logged. Selecting Logging on an Allow rule results in messages for permitted traffic being logged. De-selecting the logging option on a Deny rule results in the blocked traffic being dropped without any logs. This option is useful for blocking broadcast traffic that can create excessive nuisance alarms.

- Details:
  A short form summary of special Firewall Rule Details such as "RO" for Modbus Read-Only.
- Description:
  This field is available as a convenience, so the controls engineer may add text to document the rules that you have set up on the Tofino SA.

Firewall Rule Details

Many firewall rules allow you to adjust advanced settings such as traffic rate limiting. The settings for a selected rule are displayed in one or more tabs below the rule table in the ConneXium Tofino Configurator. A summary of these settings are also shown in the Details column of the Firewall table.

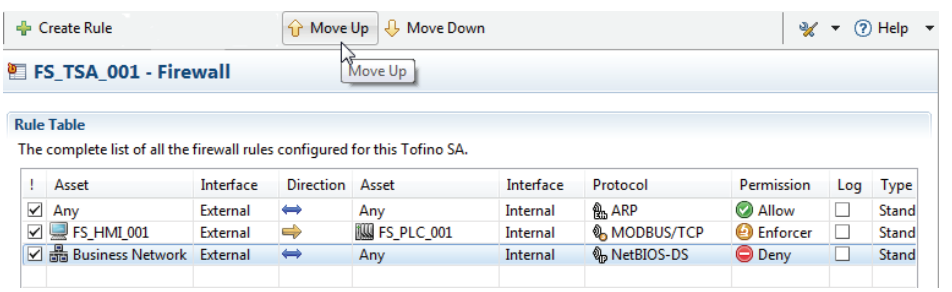


Firewall Rule Order

The Tofino SA inspects packets in a sequential manner according to the order that the rules are displayed in the firewall rule table. Having the same rules, but placing them in a different order, can radically alter how the Tofino SA manages traffic.

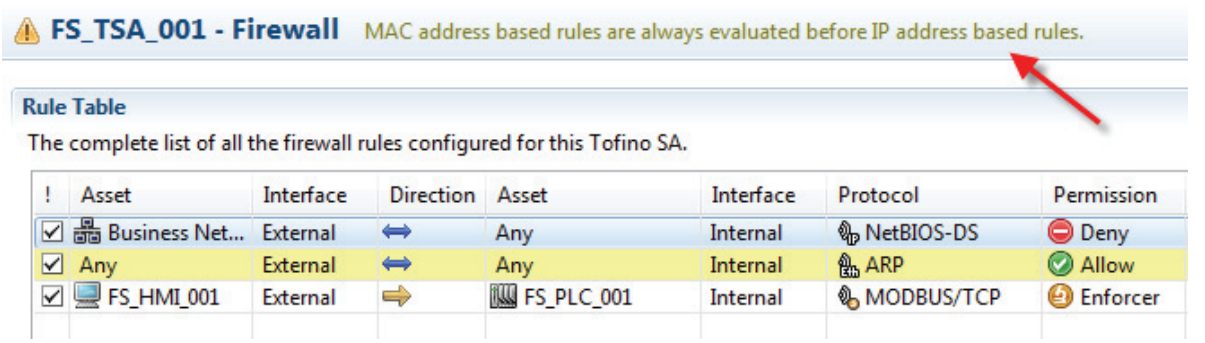
When the Tofino SA receives a packet, it compares it against the first rule, then the second, then the third, etc. When it finds a rule that matches, it stops checking and applies that rule. If the packet goes through each rule without finding a match, then that packet is denied.

You can manually reorder the rules by selecting a rule and clicking the `Move Up` and `Move Down` buttons in the middle tool bar.



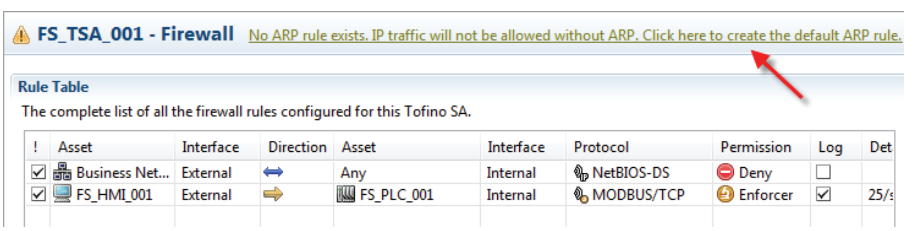
Keep in mind that the first rule in the Tofino SA that matches, is applied to the packet, not the rule that best matches. Based on this, set the more specific rules at the top of the list, followed by the more general rules. This helps to prevent a general rule being matched before hitting a more specific rule.

There are certain exceptions to this strategy - for example, rules using MAC addresses need to be evaluated before rules using IP addresses. The ConneXium Tofino Configurator advises you if this is required.



Assisted Firewall Rule Creation

Some firewall rules are needed for other rules to work correctly. For example, for a TCP rule to work an ARP Allow rule is needed. This is because the devices using the TCP protocol use the ARP protocol to determine each other's addresses. The Tofino SA detects when an additional rule is needed and prompts you to insert it.



Firewall Rate Limiting

Three advanced settings that are available for rules are the Rate Limiting settings. These define the rate at which packets that have met the other criteria for a given rule are allowed through the firewall. The rate limiting uses a token bucket filter algorithm with three settings:

- Rate Limit: The average packet allow rate over the defined time interval.
- Interval: The time interval used for the Rate Limit (Second, Minute, Hour).
- Burst Limit: Maximum initial number of packets allowed. This will be greater than or equal to the Rate Limit.

To understand how token bucket filtering works, picture a 'bucket' of 'tokens'. It costs one token for the firewall to forward one packet. If the bucket is out of tokens, then the firewall will drop packets until there are more tokens in the bucket. The number of tokens (and thus the number of forwarded packets) is controlled by two settings; Rate limit and Burst Limit.

The Rate Limit is the rate at which the bucket is refilled with tokens. The rate limit setting is calculated over an interval set by the user (such as per second or per minute). Thus if the rate limit is 50 and the interval is "per second", then 50 tokens per second will be placed in the bucket and 50 packets per second will be let through the firewall. Keep in mind, that the refilling of the bucket is done gradually over an interval (not at the start of the interval).

The Burst Limit is the initial number of tokens in the bucket, as well as the maximum number of tokens the bucket can hold. In other words, this helps to prevent the number of tokens from building up during times of low traffic.

The firewall will immediately allow through any burst of packets equal to the number of tokens in the bucket. Once the bucket is empty, the firewall can only forward 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 100 and your rate limit is 25 per second and 1000 packets are sent to the firewall, then the first 100 will be allowed, followed by another 25 packets per second after that. Any other packets will be dropped.

Right versus Left versus Bidirectional

Many firewall rules have a direction associated with them. This displayed arrow direction indicates which device establishes a connection between the two nodes. It does not refer to packet flow. For example, if an 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 setting up (i.e. establishing) the connection. Once the other person (Person 2) answers the phone, then speech can flow both ways.

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

- Right: Connections can only be established by the left asset (as defined in the rule table) and will flow to the right. For example, an HMI could be the left asset and a PLC the right asset and the direction set to "Right". This would allow the HMI to initiate the connection and the PLC to respond, but the PLC would not be allowed to initiate a session.

- Left: Connections can exclusively be established by the right asset (as defined in the rule table) and will flow to the left. For example, a Workstation with a browser client could be the right asset and a Web Server the left asset and the direction set to "Left". This would allow the Workstation to initiate web sessions and the Web Server to respond, but the Web Server would not be allowed to initiate a session.

- Bidirectional: The connections can be established by either device.

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

7.3 Using Modbus TCP Enforcer Rules

The Modbus TCP Enforcer LSM is an advanced deep packet inspection firewall for the Modbus TCP protocol. It allows you to filter traffic based on specific Modbus function codes, register ranges and the validity of the Modbus messages. The Modbus TCP Enforcer LSM is a security software module to the standard ConneXium Tofino Firewall.

Activating the Modbus TCP Enforcer LSM

Before Modbus TCP Enforcer capabilities are available, activate both the Firewall LSM and the Modbus TCP Enforcer LSM on theTofino SA “Tofino SA General Settings”.

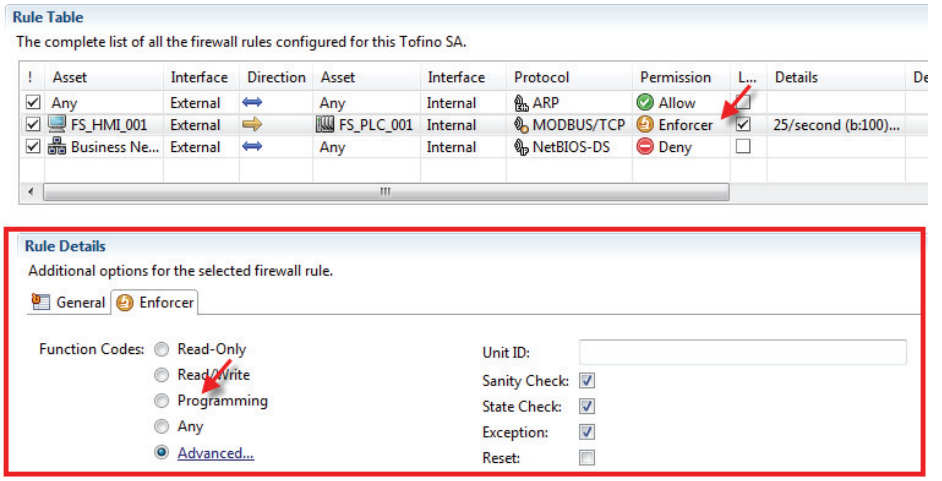
Creating Modbus TCP Enforcer Rules

Follow these steps to create a Modbus Enforcer firewall rule:

- ☐ Create a firewall rule between two assets.
- ☐ Set the protocol to either Modbus TCP or Modbus UDP.
- ☐ Set the direction of the rule so that it is FROM the Modbus Master TO the Modbus Slave. (Keep in mind that the Bidirectional option cannot be used with the Modbus TCP Enforcer LSM).
- ☐ Set the Permission to Enforcer.

  Note: If you select ALLOW or DENY, the Modbus traffic between the two assets will simply be allowed or blocked accordingly by the Tofino SA, without reference to the Modbus TCP Enforcer.

Once you create a Modbus Enforcer rule, the next step is to configure it.



Configuring Modbus TCP Enforcer Rules

Follow these steps to configure the Modbus TCP Enforcer firewall rule you have created:

☐ Click on the Enforcer Details tab.
☐ Set the following fields as needed:

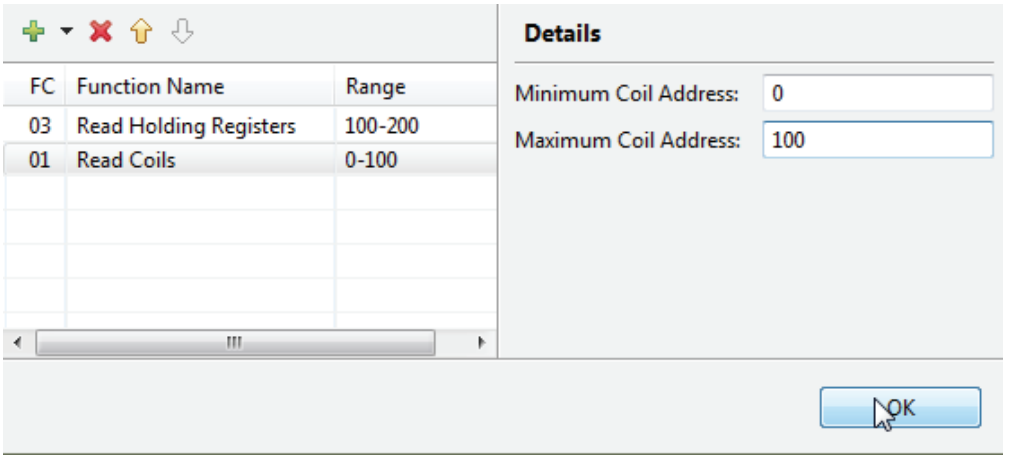
- Function Codes. This is either set to one of the following:

  Read-Only: only function codes that are data read commands are permitted.
  Read/Write: only function codes that are data read or data write commands are permitted.
  Programming/OFS: only function codes that are either data read write or programming commands are permitted.
  Any: all Modbus function codes are permitted.
  Advanced: opens a new window so you can individually select function codes and ranges.

- Unit ID:
  The Tofino SA uses the 'Unit Identifier' 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 either 0 or 1. If you don't want the Unit ID to be checked, clear this field.

- 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 will 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 the message would be dropped. This option may have to be disabled for Modbus devices that do not conform to the Modbus/ TCP 1.1b specification (Keep in mind that sanity checking of the Modbus MBAP header is performed regardless of whether this option is selected).
- State Check: When selected, 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 sent by the master without an intervening response from the slave, a command sent by the slave device to the master, or a response sent by the master device to the slave. If this box is not selected, then the Tofino SA will not block these out-of-state commands or responses.
- Exception: If this box is selected, the Tofino SA will send a Modbus TCP exception response (if appropriate) to the Modbus device that generated a blocked message. Keep in mind that some illegal Modbus TCP messages have a defined exception response.
  For Modbus UDP it is recommended that the Exception option be off (not selected) and the Reset option be on (selected).
- Reset: If this box is selected, the Tofino SA will send a TCP reset message to both Modbus devices when it blocks a message. This can help to prevent session lock up on certain poorly designed Modbus products.

☐ If you selected Advanced for the function code, the Advanced Modbus TCP Function Code Filtering window will open. This will allow you to specify the function codes and register/coil ranges that you wish to allow for this rule. To do this, select the `Add Function Code` button on the tool bar. Then, select the function code you want to allow, and optionally add a register or coil range. You can add as many Function Codes as needed to one rule but each function code should only be entered once for a given rule.


FC
Function Name
Range
03
Read Holding Registers
100-200
01
Read Coils
0-100
Details
Minimum Coil Address:
0
Maximum Coil Address:
100
OK

8 Configuring Event Logging

The Event Logger LSM is a security module used to provide external alarm and event logging for the Tofino SA to a syslog server. It offers two methods for saving event logs:

- Via the syslog protocol to forward Tofino SA exception events to a remote Syslog server
- Saving exception events to long term memory in theTofino SA for offloading via USB Storage Device

Activating the Event Logger LSM

Before Event Logger capabilities are available, activate the Event Logger LSM on theTofino SA “Tofino SA General Settings”.

Setting up the Event Logger

You can configure the Event Logger by clicking on the Event Logger folder displayed in the Project View.

- Syslog Server IP Address:
  This is the address of the Syslog server where you would like your logs sent to. In order to disable the remote syslog feature, set this field to all zeros.
- Default Gateway:
  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 on a **different** network than the Tofino SA. If the syslog feature is not being used, or if the Tofino SA and the Syslog server are on the same subnet, set this field to all zeros.

- Destination Port:
  This is the UDP port number your syslog server is listening for log messages on (usually Port 514). To disable the syslog feature, leave the field blank.
- Lowest Priority Logged:
  This is the cut-off as to the lowest logging level you would like the Tofino SA to record. Setting the priority to 0 would result in just the emergency events being recorded while setting the priority to 7 would result in every detected event being recorded. The default setting is 5.

	Lowest Priority Message to be Logged
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

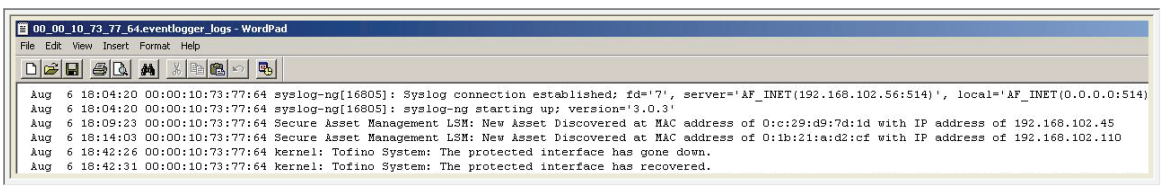
Table 1: Lowest Priority Message to be Logged setting options for the Event Logger.

Note: Keep in mind that the Tofino SA does not require an IP address to communicate to a remote Syslog server. The Tofino SA uses special stealth technology to communicate without having an IP address. The Syslog server will see the messages coming from either address 0.0.0.0 or 169.254.2.2.

Retrieving Logs Using a USB Storage Device

To retrieve the logs stored on the Tofino SA, insert a USB storage device into the USB port on the Tofino SA and then initiating the USB save operation. For more detail see: “USB Save from Your Tofino SA”.

Once the logs are transferred to the USB storage device, install it in a computer and view the storage device to find the file containing the logs. The logs will be stored in <tofino id>_evt.log files and <tofino id>_evt.<X>.gz files. The evt.log files contain the latest events and are uncompressed. The evt.X.gz files are compressed and contain older event logs. You can open the evt. log files using a syslog viewer or WordPad for better formatting. The evt.X.gz can be uncompressed using a gzip capable tool such as WinRAR or 7-zip. Below is an example of the log file opened with WordPad.



9 Loading and Verifying Configurations

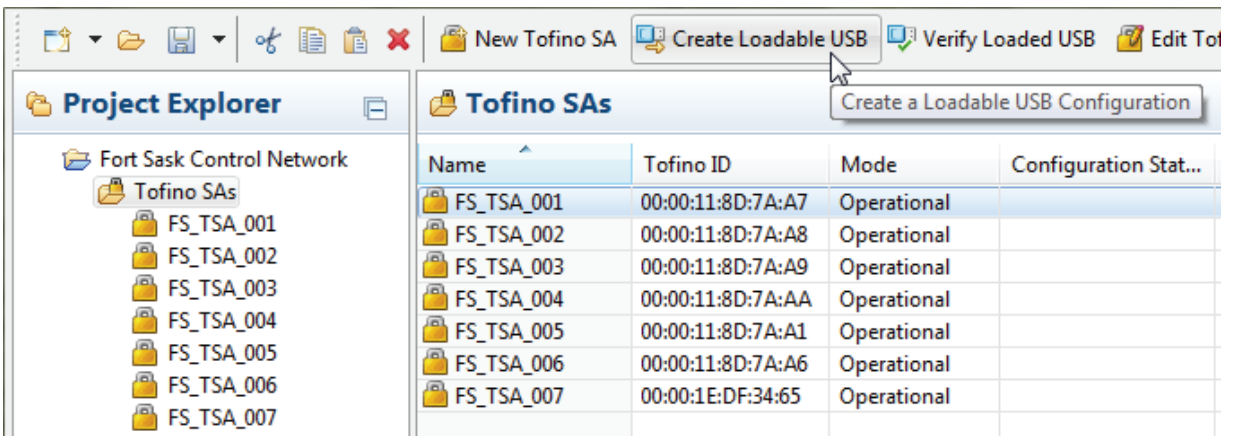
Once your Tofino SAs are configured in the ConneXium Tofino Configurator, these configurations need to be transferred to the Tofino SAs in the field. This is a three step process:

- ☐ Create a configuration on a USB storage device: This builds encrypted configuration files for loading into Tofino SAs and stores them to a USB storage device.
- ☐ Transfer the configuration to the Tofino SAs: Insert the USB storage device containing your configuration files into the USB port on the matching Tofino SAs and then load the configuration.
- ☐ Verify a configuration from a USB storage device: Retrieves the configuration load reports from the USB storage device that was used to load configurations onto one or more Tofino SAs. This will allow you to record and verify the configuration of Tofino SAs in the field and save it in your project.

9.1 Creating a USB Configuration

To configure a Tofino SA in the field, the `Create Loadable USB Drive` action is used in the ConneXium Tofino Configurator. This builds a loadable configuration for a Tofino SA and stores it to a selected USB storage device. You can insert the storage device into the USB port on the matching Tofino SA and load the configuration.

☐ Select the Tofino SAs that you would like a USB configuration created for. You can store multiple Tofino SA configurations on the same USB storage device.
☐ Click the `Create Loadable USB` button on the middle tool bar.



☐ Select the USB storage device that you will save the configuration files to.

The option to create a USB configuration load file will only be possible if the following conditions are met:

- The Tofino SA configuration is free of errors.
- You have write access to the Project File.
- Any changes to the Project have been saved.

The write access requirement helps to prevent users, without sufficient privileges, from modifying Tofino SAs in the field.

The final requirement reduces the possibility that the configurations being loaded into the Tofino SAs in the field are different from the configuration in the Project File.

9.2 USB Loading Your Tofino SA

The Save Load Reset button on the Tofino SA provides three functions depending on the number of times it is pressed.

- Once: Saves diagnostics files and log files to a USB storage device.
- Twice: Loads configuration files from a USB storage device.
- Three times: Performs a factory reset and returns the Tofino SA back to its default state as shipped from the factory.

The USB Load function allows either configuration files generated by the ConneXium Tofino Configurator's Create Loadable USB function or firmware updates to be loaded to a Tofino SA using a USB storage device (See “Creating a USB Configuration”).

Note: The following version 2.0 USB storage devices are known to work: Kingston Data Traveler, SanDisk Cruzer, Sony Microvault, Lexar and Schneider TCSEAM0100. Other brands and models may work, but have not been tested.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Follow these configuration loading steps carefully.

- ☐ Power on the Tofino SA for at least one minute.
- ☐ Insert the USB storage device containing the prepared files into one of its USB ports.
- ☐ Press the Save Load Reset button twice.
- ☐ Both the 1/S and the 2/L LEDs will illuminate to indicate a Load.
- ☐ After a few seconds the marquee will move from right to left to indicate a USB Load is in progress.
- ☐ When the flashing sequence stops remove the USB storage device.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

If the load was successful, the Tofino SA‘s Fault LED will be off.

Following a successful USB Load function, five or more files should be stored on your USB storage device for each Tofino SA loaded (<tofino id> is replaced with the actual ID of the Tofino SA):

- <tofino id>_tc_data
  “USB Verification” data indicating if the configuration was successful or not.
- <tofino id>_diagnostics.txt
  Diagnostics information on the Tofino SA (See “Tofino SA Diagnostics”).
- <tofino id>_evt.log and <tofino id>_evt.<X>.gz.
  Event logs from the Tofino SA (See “Configuring Event Logging”).
- <tofino id>_kernel_evt.enc:
  Encrypted kernel diagnostics information (For factory troubleshooting use only).
- <tofino id>_diagnostics.enc
  Encrypted module diagnostics information (For factory troubleshooting use only).

Note: The Tofino SA will pass network traffic freely during the initial configuration or when its configuration is being updated. Firewall rules take effect after completion of the initial configuration or update of the Tofino SA so that network operations are not affected before the full rule set can be loaded. A typical configuration load will finish in approximately 30 seconds.

9.3 USB Save from Your Tofino SA

The Save Load Reset button on the Tofino SA provides three functions depending on the number of times it is pressed.

- Once: Saves diagnostics files and log files to a USB storage device.
- Twice: Loads configuration files from a USB storage device.
- Three times: Performs a factory reset and returns the Tofino SA back to its default state as shipped from the factory.

The USB Save function copies diagnostics and validation files from the Tofino SA to the USB storage device. You can then validate these files using the ConneXium Tofino Configurator‘s Verify Loaded USB function, or they can be sent to technical support for analysis.

To create these files you will need to perform a USB Save. Keep in mind that a USB Load will also execute a USB Save in order to record the results of the Load and the status of the Tofino SA after the load is finished.

☐ Power on the Tofino SA for at least one minute.
☐ Insert the USB storage device into one of its USB ports.
☐ Press the Save Load Reset button once.
☐ The 1/S LED will illuminate.
☐ After a few seconds the marquee will move from left to right to indicate a USB Save is in progress.
☐ When the flashing sequence stops remove the USB storage device.
☐ If the save was successful the Tofino SA LEDs will revert to the state they were in prior to the saving action.

Note: The following version 2.0 USB storage devices are known to work: Kingston Data Traveler, SanDisk Cruzer, Sony Microvault, Lexar and Schneider TCSEAM0100. Other brands and models may work, but have not been tested.

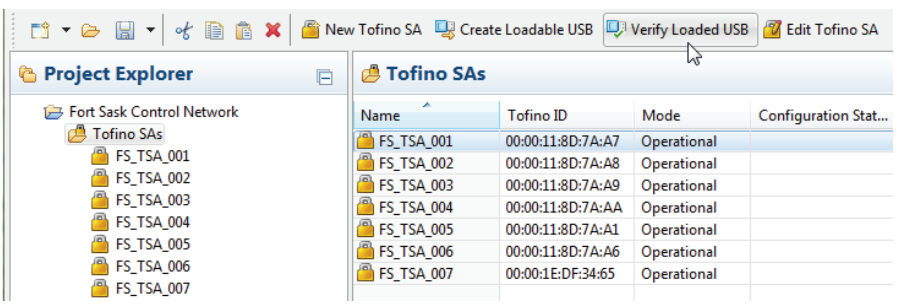
Following a successful USB Save function, five or more files should be stored on your USB storage device for each Tofino SA. These are (<tofino id> is replaced with the actual ID of the Tofino SA):

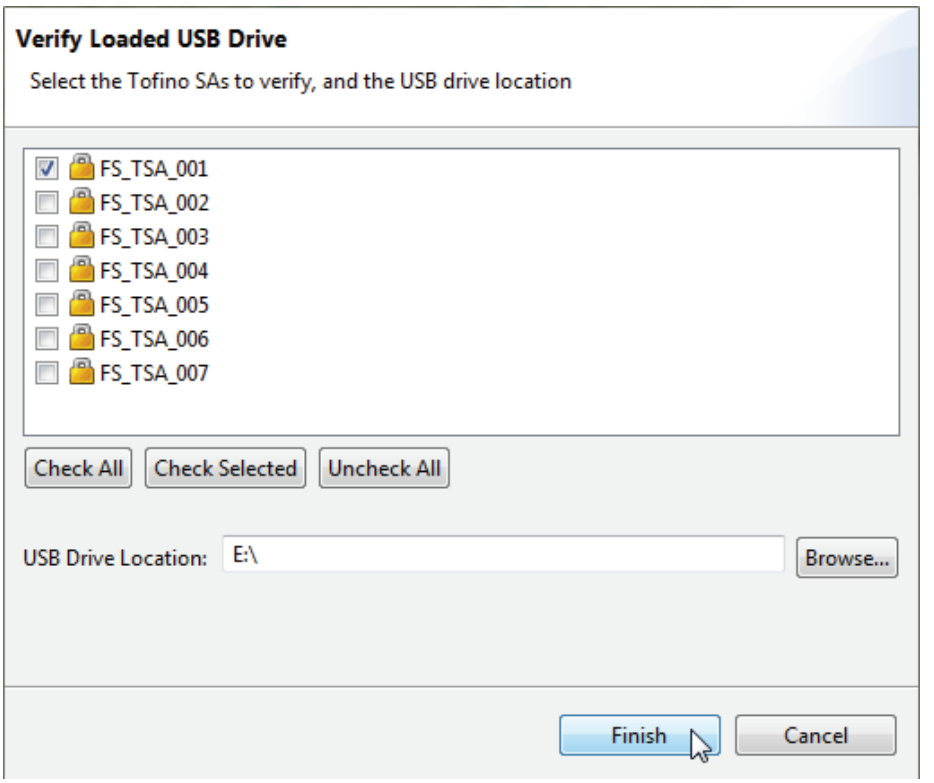
- <tofino id>_tc_data
  "USB Verification" data indicating if the configuration was successful or not.
- <tofino id>_diagnostics.txt
  Diagnostics information on the Tofino SA (See "Tofino SA Diagnostics").
- <tofino id>_evt.log and <tofino id>_evt.<X>.gz
  Event logs from the Tofino SA (See "Configuring Event Logging").
- <tofino id>_kernel_evt.enc
  Encrypted kernel diagnostics information (For factory troubleshooting use only).
- <tofino id>_diagnostics.enc
  Encrypted module diagnostics information (For factory troubleshooting use only).

9.4 USB Verification

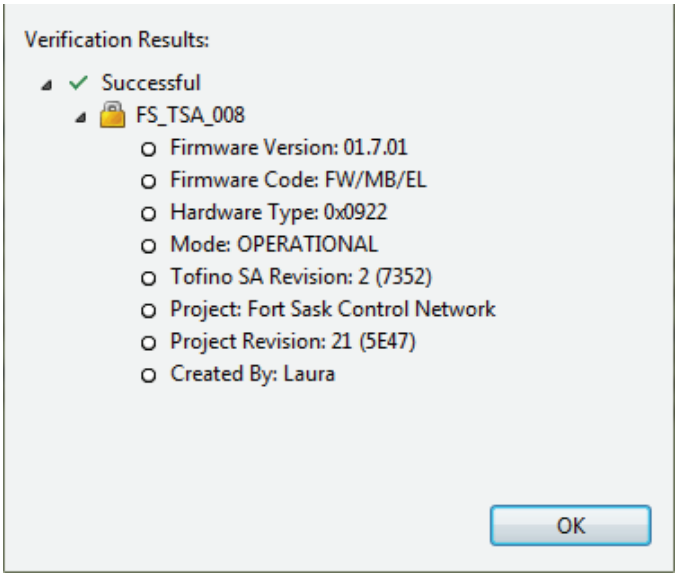
To verify the configuration of one or more Tofino SAs in the field, use the `Verify Loaded USB` action. This retrieves the configuration load reports from the USB storage device that was used to load configurations onto one or more Tofino SAs. This will allow you to record and verify the configuration of Tofino SAs in the field.

- ☐ Insert the USB storage device, on which the files are contained, into your computer.
- ☐ Select one or more Tofino SAs that you would like to verify.
- ☐ Click the `Verify Loaded USB` button on the middle tool bar. A Wizard to guide you through verifying the configuration on the selected USB drive will open.
- ☐ Select the Tofino SAs you want to verify.
- ☐ Select the USB drive location.





The verification data will be displayed and logged by the ConneXium Tofino Configurator. The Verified Configuration Revision, Hardware Type, and Firmware Version for the verified Tofino SAs will be updated in the Project File. You can also view the verification information on the "Tofino SA General Settings" folder of each Tofino SA.

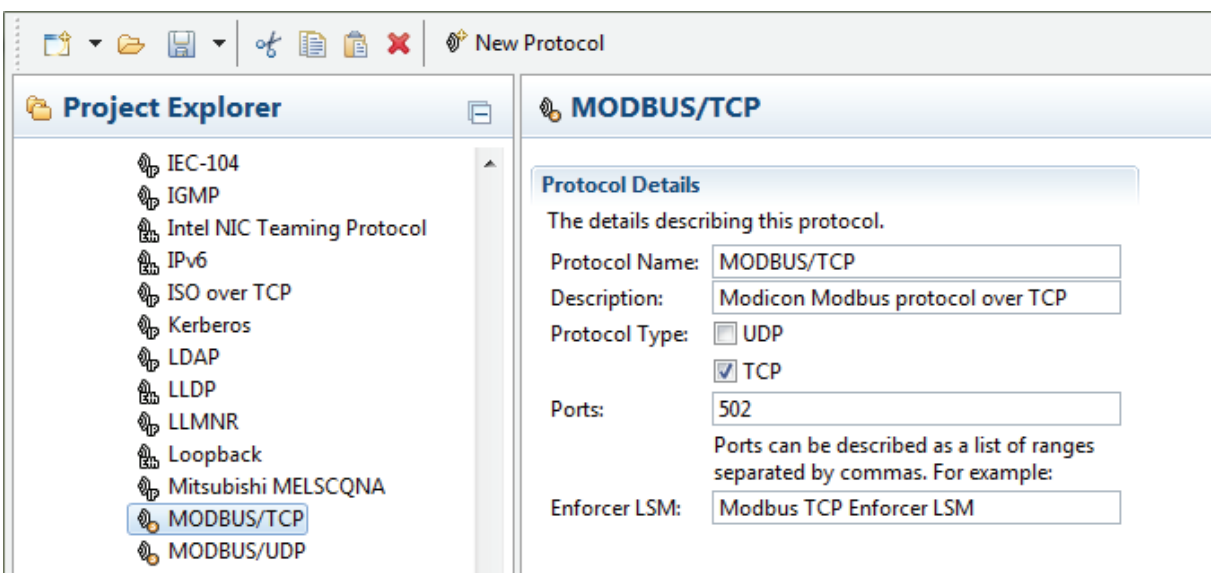

Verification Results:
Successful
FS_TSA_008
Firmware Version: 01.7.01
Firmware Code: FW/MB/EL
Hardware Type: 0x0922
Mode: OPERATIONAL
Tofino SA Revision: 2 (7352)
Project: Fort Sask Control Network
Project Revision: 21 (5E47)
Created By: Laura
OK

10 Advanced Topic - Creating and Managing Protocols

In the ConneXium Tofino Configurator, "Protocols" define the particular services that are communicated between devices on the network. For example, the use of web traffic on a network would use the HyperText Transport Protocol (HTTP) for communications between a web server and a web client. Similarly, a HMI might use the Modbus/TCP protocol to communicate to a PLC.

The Tofino SA comes with a complete set of protocols already defined. However, in special cases you may want to create new protocols for specific types of equipment or situations.

The Protocol management features allow you to create, edit, and delete protocols. The ConneXium Tofino Configurator comes with a number of pre-defined protocols that are common to many industrial systems. These factory defined protocols cannot be cut or deleted.



By selecting a specific Protocol in the Project Explorer view, you can:

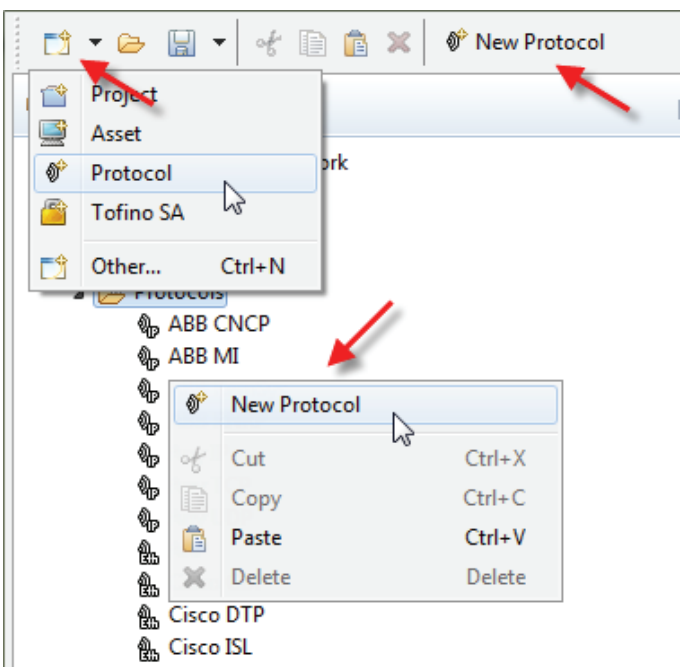
- Create a new protocol or folder.
- View and edit the protocol's details.
- Delete a protocol.
- Cut, Copy and Paste protocols.

Some protocols are factory defined and cannot be edited, cut or deleted.

10.1 Creating a Protocol

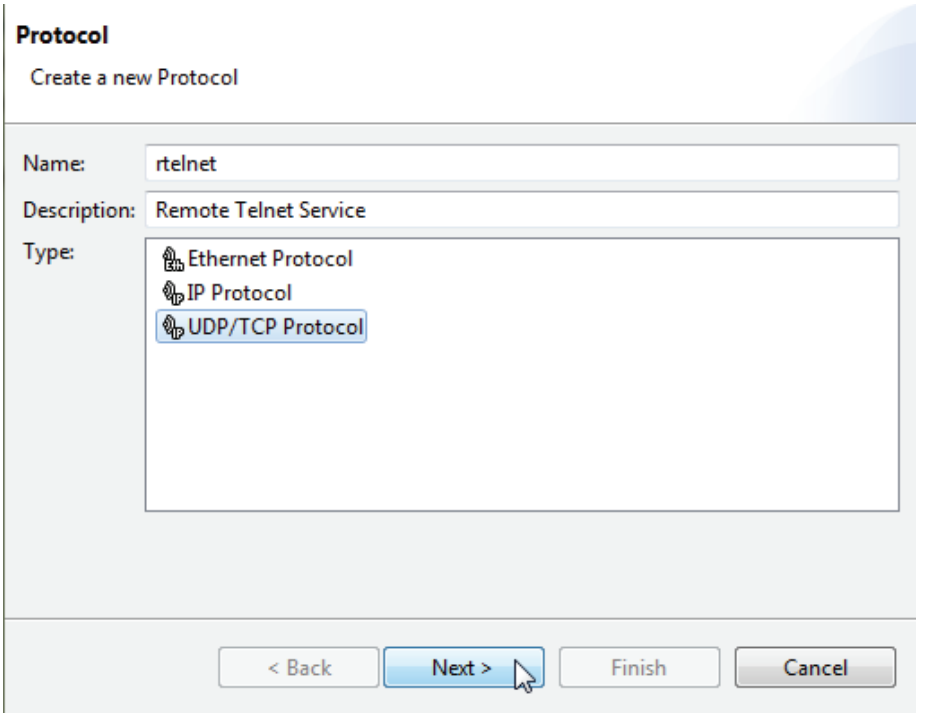
New protocols are created using the New Protocols Wizard. There are three ways to launch the New Protocols Wizard:

- Click the `New` button and select `Protocol`.
- Click the `New Protocol` button in the middle section of the tool bar.
- Right click on an existing protocol and select `New Protocol`.

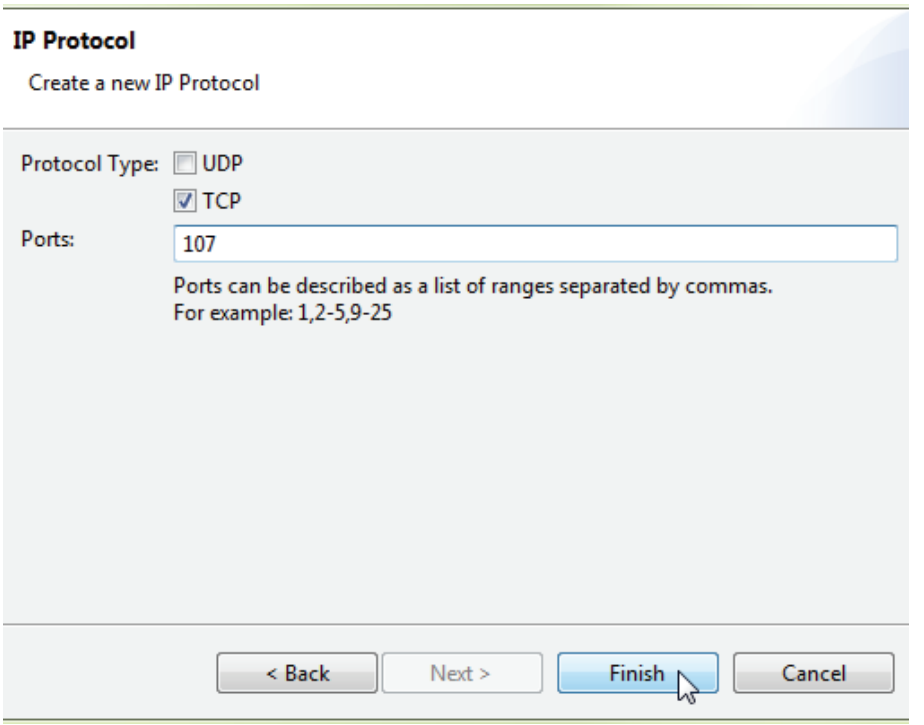


New Protocol Wizard

Once the wizard has started, it will ask you to enter a name, description and select the protocol type.



The second page of the wizard allows you to enter specific details for the protocol. This page will vary depending on the type of protocol selected on the first page.

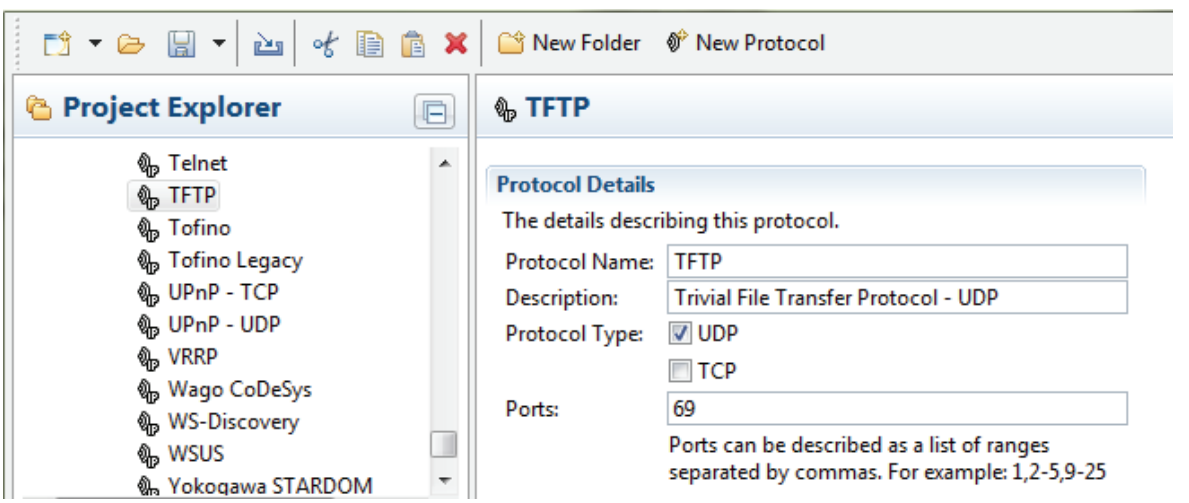


For more information on these fields, see “Viewing and Editing Protocols”.

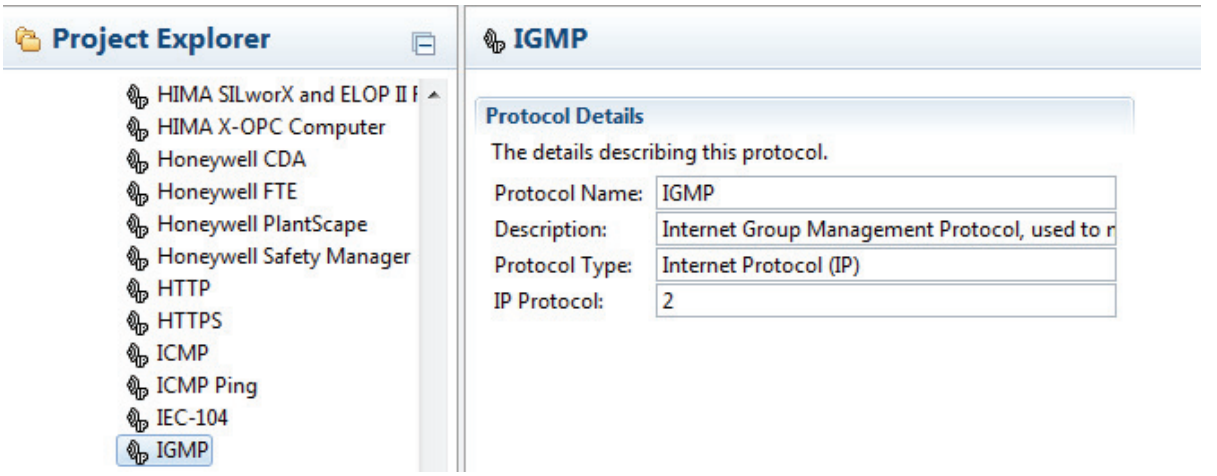
10.2 Viewing and Editing Protocols

Clicking on a protocol name in the Project Explorer view will open the Protocol Details view. This allows you to view and configure the settings for the selected protocol. This includes general information and specific parameters. The details vary depending on the type of protocol selected. Below are three typical protocols of different types.

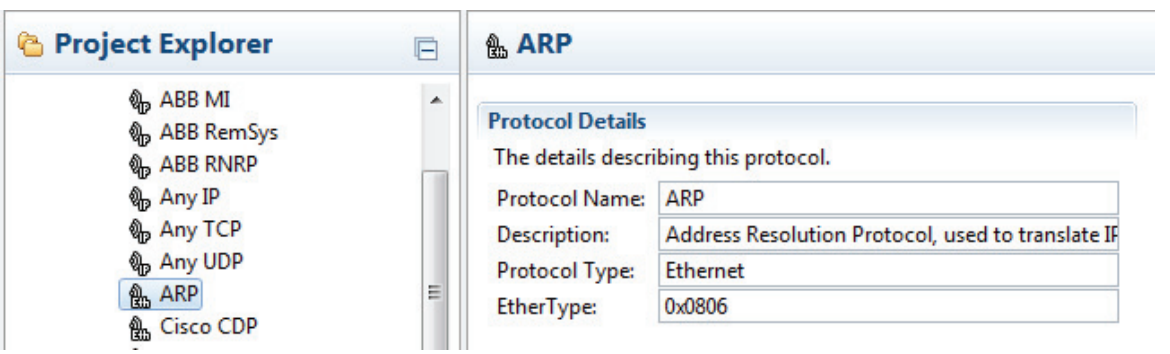
UDP/TCP Protocol



IP Protocol



Ethernet Protocol



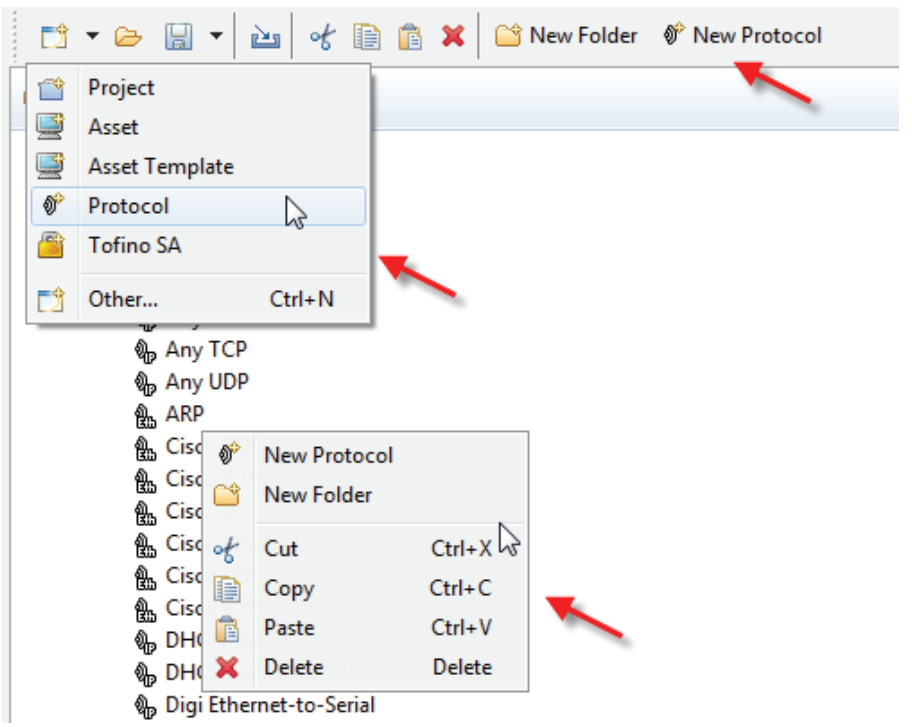
General

- Protocol Name: Insert a name or identifier that uniquely identifies the protocol. Remember that each protocol needs to have a unique name to avoid confusion.
- Description: A text field for reference only and may be used to describe the function of this protocol.
- Protocol Type: The general classification of this protocol and determines the fields available for input. (UDP, TCP, IP or Ethernet).
- Ports: 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. Exclusivley use the numbers 0 through 9 and commas and dashes.
- IP Protocol: The IP protocol number (in hexadecimal format).
- EtherType: The Ethernet type number (in hexadecimal format). For more information see: http://www.iana.org/assignments/ethernet-numbers.

10.3 Managing Protocols

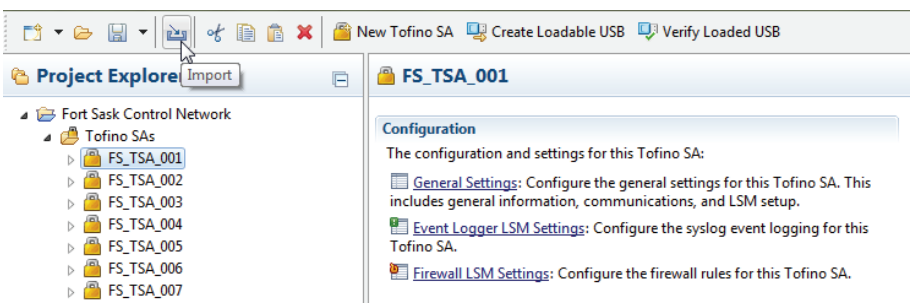
You can manage protocols just like any Windows' object. By right clicking on a protocol, or using the tool bar, you have the following options:

- New Protocol - Launches the New Protocol Wizard.
- Create New Folder - Creates a folder to organize your protocols.
- Cut - Removes the highlighted protocol from the project and saves it in the clipboard for later pasting in a different location.
- Copy - Makes a copy of the highlighted protocol from the project and saves it in the clipboard for later pasting in a different location.
- Paste - Pastes the contents of the clipboard into the project.
- Delete - Removes the highlighted protocol from the project. Keep in mind that certain pre-defined protocols are read-only and are unable to be moved or deleted.



11 Advanced Topic - Importing Templates and Security Profiles

The ConneXium Tofino Configurator allows you to import pre-defined objects that can be used as building blocks for your security design. The following types of objects can be imported:



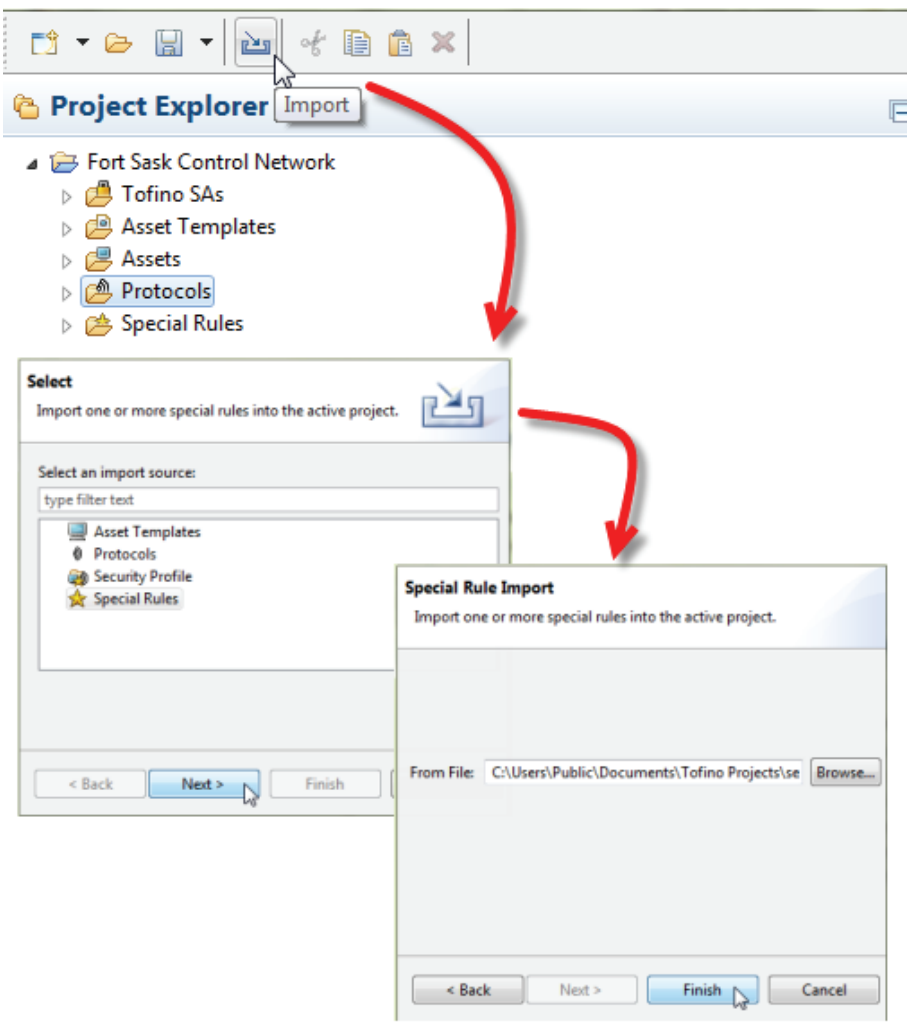
- Asset Templates
- Protocols
- Special Rules
- Security Profiles

Importing Asset Templates, Protocols or Special Rules allow you to update existing definitions or add new ones to your project. Importing new versions of Asset Templates, Protocols or Special Rules will not automatically update the rules in your firewalls.

Security Profiles are predefined combinations of Asset Templates, Special Rules, and Protocol definitions, bundled into a single Security Profile (.tsp) file. They allow you to import the related objects needed to help secure PLCs, DCS and other devices against published vulnerabilities as a single file.

Note: If the Asset Templates or the Security Profiles in an imported file reference Protocols or Special Rules, these will be imported during the import operation.

To import a pre-defined object follow these steps:
☐ Click the `Import` button.
☐ Select the type of object you would like to import.
☐ Browse for and select the object file.
☐ Click `Finish`.



12 Advanced Topic - ConneXium Tofino Configurator Settings

Your ConneXium Tofino Configurator can be adjusted using the following advanced settings:

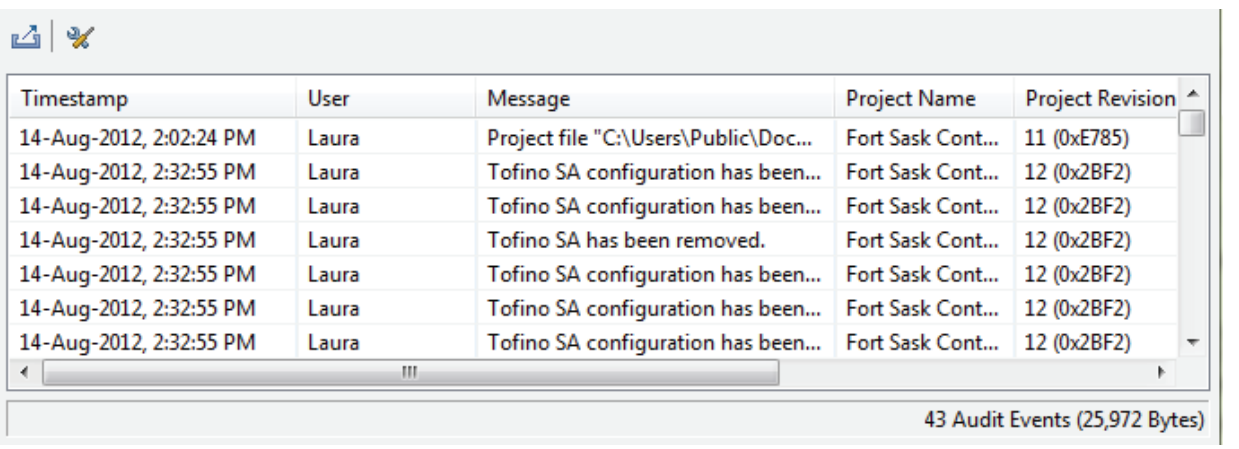
☐ Defining the Audit preferences and Project Preferences, see “Preferences”.

☐ Setting user administration rights, see: “User Administration”.

12.1 User Administration

The User Identification and Administration system for the ConneXium Tofino Configurator is based on the Windows Account Management system. When you make changes to a project, the Windows user name for the active account on the computer is the user name recorded against any ConneXium Tofino Configurator activities. This user name is recorded in the audit logs for key changes to a project by the ConneXium Tofino Configurator.

Similarly, user access control for a ConneXium Tofino Configurator project is based on the Windows File Management security settings for the Project File. For example, if a person is given read-only access to the folder where a Project File is stored, then the ConneXium Tofino Configurator will also give the user read-only access to project tasks. These settings extend beyond basic file management. For example, they can keep an unauthorized user from loading a new USB configuration into the Tofino SA.

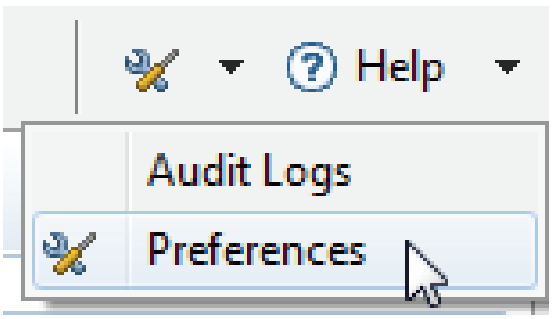


Timestamp	User	Message	Project Name	Project Revision
14-Aug-2012, 2:02:24 PM	Laura	Project file "C:\Users\Public\Doc...	Fort Sask Cont...	11 (0xE785)
14-Aug-2012, 2:32:55 PM	Laura	Tofino SA configuration has been...	Fort Sask Cont...	12 (0x2BF2)
14-Aug-2012, 2:32:55 PM	Laura	Tofino SA configuration has been...	Fort Sask Cont...	12 (0x2BF2)
14-Aug-2012, 2:32:55 PM	Laura	Tofino SA has been removed.	Fort Sask Cont...	12 (0x2BF2)
14-Aug-2012, 2:32:55 PM	Laura	Tofino SA configuration has been...	Fort Sask Cont...	12 (0x2BF2)
14-Aug-2012, 2:32:55 PM	Laura	Tofino SA configuration has been...	Fort Sask Cont...	12 (0x2BF2)
14-Aug-2012, 2:32:55 PM	Laura	Tofino SA configuration has been...	Fort Sask Cont...	12 (0x2BF2)

43 Audit Events (25,972 Bytes)

12.2 Preferences

The Preferences command allows you to view and edit preferences that are not project specific.



- Audit - The location and size of the audit file.
- Project - Determines the default project that opens on start-up.

Audit Preferences

This Preference page allows you to set the maximum size of the audit file and where it is stored.

Help

This Preference page allows you to select how ConneXium Tofino Configurator Help information is displayed on your computer. For example, you can select whether Help is displayed in a ConneXium Tofino Configurator window or in an external browser.

Project Preferences

This Preference page allows you to set the default project that opens on start-up.

13 Troubleshooting

13.1 Tofino SA Diagnostics

The Tofino SA has the capability to save diagnostics files to a USB storage device for troubleshooting purposes. To create these files you will need to perform a USB Save. You can also view these files with a standard text editor or they can be sent to technical support for analysis.

To create these files you will need to perform a USB Save.

- ☐ Power on the Tofino SA for at least one minute.
- ☐ Insert the USB storage device into one of its USB ports.
- ☐ Press the Save Load Reset button once.
- ☐ The 1/S LED will illuminate.
- ☐ After a few seconds the marquee will move from left to right to indicate a USB Save is in progress.
- ☐ When the flashing sequence stops remove the USB storage device.
- ☐ 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.

Note: The following version 2.0 USB storage devices are known to work: Kingston Data Traveler, SanDisk Cruzer, Sony Microvault, Lexar and Schneider TCSEAM0100. Other brands and models may work, but have not been tested.

Interpreting Diagnostics Files

If the USB Diagnostics Save is successful there will be three or four files on the USB storage device similar to this:[1]

- **<tofino id>_tc_data**: “USB Verification” data indicating if the configuration was successful or not.
- **<tofino id>_diagnostics.txt:** Diagnostics information on the Tofino SA.

1. The prefix of the file name will be equal to the Tofino ID.

- **<tofino id>_evt.log and <tofino id>_evt.<X>.gz:** Event logs from the Tofino SA (See “Configuring Event Logging”).
- **<tofino id>_kernel_evt.enc:** Encrypted kernel diagnostics information (For factory troubleshooting use only).
- **<tofino id>_diagnostics.enc:** Encrypted module diagnostics information (For factory troubleshooting use only).

If you examine the file ending in .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: 1.7.0
4  Tofino Hardware Info:
5    Hardware : Schneider ConneXium Development Platform
6    Processor : XScale-IXP42x Family rev 2 (v5b)
7    Flash Type: P-Flash
8    Tofino ID:  00:80:63:73:77:649
================================================================
10  Network Statistics
11    unsecured IF ifconfig
12  eth0      Link encap:Ethernet  HWaddr 00:80:63:73:77:64
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 00:80:63:73:77:65
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           total       used       free     shared    buffers     cached
50 Mem:        62952      17952      45000          0        140       9060
51 -/+ buffers/cache:        8752      54200
52 Swap:             0          0          0
53------------------------------------------------------------------
54 MemTotal:         62952 kB
55 MemFree:          44992 kB
56 Buffers:            140 kB
57 Cached:            9060 kB
58 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 product technical support.

The files ending in .evt.log and <tofino id>_evt.<X>.gz are log files created by the Event Logger LSM and can be opened and viewed with any event management system, see: “Configuring Event Logging”.

13.2 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 activated?). See: "Tofino SA General Settings"
- The mode of the Tofino SA (is the Tofino SA in Operational mode?). The Tofino SA's Mode LED should be on steady.
- Does the configuration of the Tofino SA REALLY match what is stored on the ConneXium Tofino Configurator? If in doubt, verify using the Verify Loaded USB feature (See "USB Verification").

Next, check the rules on the Tofino SA's firewall details view for the following (See "Managing Firewall Rules"):

- Are the device IP addresses correct?
- Are the protocols and direction correct?
- Are there conflicting rules? For example, does the Tofino SA have an "Allow All" rule as well as a protocol specific rule?
- Was the connection between devices established BEFORE the rule was loaded? The Tofino SA will not break established connections between two devices. If you think the connection was made before the rule was loaded, try breaking the connection by restarting one of the devices.

13.3 USB Storage Device Recommendations

If you are experiencing difficulties doing USB Loads or USB Saves, check to see if you are using a version 2.0 USB storage device. USB storage devices that are version 1.1 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 a version 1.1 USB storage device.

The tested and approved USB storage devices include: Kingston Data Traveler, SanDisk cruzer, Sony Microvault, Lexar, Schneider TCSEAM0100.

No. of Flashes	During Load Sequence	During Save Sequence
2	No USB memory device isconnected to the USB connection, orthe file system of the memory device is not formatted as FAT16 or FAT32.	No USB memory device is connected to the USB connection, or the file system of the memory device is not formatted as FAT16 or FAT32.
3	The files on the USB memorydevice are invalid.	The device was unable to create any diagnostic files. Please contact yourtechnical support.
4	The device was unable to encrypt the configuration files. It is possible that the files were damaged during the copying operation. Repeat the copying operation. If the condition persists, please contact your technical support	The device was unable to encrypt the diagnotic files. Please contact your technical support.
5	The device was unable to load the files. It is possible that the files weredamaged during the copying operation. Repeat the copying operation. If the condition persists, please contact your technical support	The device was unable to copy the encrypted diagnostic files to the USB memory device. It is possible that the memory device is full.
6	The device was unable to deactivatethe USB connection. Please contactyour technical support.	The device was unable to deactivatethe USB connection. Please contactyour technical support.
7		The file system of the device does not have enough memory capacity to save the files temporarily before they are copied to the USB memory device. Please contact your technical support.

Table 2: Fault LED Activity During Load/Save

13.4 Factory Resetting Your Tofino SA

To reset the Tofino SA back to its default state as shipped from the factory, you can perform a 'Factory Reset'.

- ☐ Confirm that power is applied to the Tofino SA and it has completed its start-up initialization.
- ☐ Press, then release the "Save Load Reset" button three times so that the three LEDs are illuminated. On the first press, the " 1/s" indicator will be illuminated; on the second press, the " 2/L" indicator will be illuminated; and on the third press, the "V.24/R" indicator will be illuminated.
- ☐ After a few seconds, the Tofino SA will start its factory reset sequence. The " 1/s", " 2/L", "V.24/R", "Mode" and "Fault" indicators will flash simultaneously while the factory reset is being performed.

Once the factory reset is complete, the " 1/s", " 2/L", "V.24/R", "Mode" and "Fault" indicators will turn off. This LED pattern confirms that the Tofino SA is passive and passing traffic without filtering. If the Mode LED is ON, repeat steps 1 through 3 above. If the LEDs are different from the above, please contact technical support.

14 Glossary

ACL	Access Control List: List of rules specifying access privileges to network resources.
ARG	Assisted Rule Generation: a feature that helps you to create firewall rules for the purpose of helping to protect devices on your 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).
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.
Firewall	A set of security schemes that helps to 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 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.
HMI	Human Machine Interface: This interface enables the interaction of human 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 protocol that uses encryption to transfer Web documents from a server to a browser.
IDS	Intrusion Detection System: A system to detect suspicious patterns of network traffic.

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 business computer systems and their applications.
LAN	Local Area Network: A network that interconnects computers in a limited area such as a home, office, laboratory or factory.
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), and Diagnostics.
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.
Asset	The objects used to represent the devices (or groups of devices) installed in your control system. They can be broken down into seven categories: Computers, Controllers, Devices, Networks, Networking equipment, Broadcast and Multicast.
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.
PLC	Programmable Logic Controller: A PLC is a small dedicated computer used for controlling industrial machinery and processes.
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.
SA	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.
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.
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 encrypted communications created by Netscape Incorporated.
TCP	Transmission Control Protocol: A transport level protocol that provides a connection-oriented 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.
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.