Schneider Electric

Continuum® Network Security Module

Hardware Version: ACX series Rev 2a, NetController II Rev B
Firmware Version: ACX series v1.100021; NetController II v2.100021

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation

Document Version 1.3

Revision History

Version	Modification Date	Modified By	Description of Changes
1.0	09/28/2009	Richard Dubois	Release Version
1.1	03/22/2010	Richard Dubois	Corrected ThreadX version information in section 1.9 Updated Figure 3 in section 1.8
1.2	04/06/2010	Richard Dubois	Added clarification for firmware revisions in section 1.3
1.3	04/15/10	Richard Dubois	Added Hardware Revision to all descriptions of the controllers. Indicated that seals are installed at the factory in section 1.8

Table of Contents

Table of Figures

Table of Tables

Continuum® NetController II Rev B (left) and ACX Series Rev 2a Controllers (right)

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Continuum® Network Security Module from Schneider Electric. It provides detailed information relating to each of the FIPS 140-2 security requirements relevant to the Continuum® Network Security Module along with instructions on how to run the module in a secure FIPS 140-2 mode.

1.2 References

This document deals only with operations and capabilities of the cryptographic module in the technical terms of a FIPS 140-2 cryptographic module security policy. Refer to the sources in items 1-6 below for FIPS 140-2, and items 7-12 below for more information on the Continuum® Network Security Module.

[1] NIST Security Requirements for Cryptographic Modules, FIPS PUB 140-2, December 3, 2002

[2] NIST Security Requirements for Cryptographic Modules, Annex A: Approved Security Functions for FIPS PUB 140-2, May 19, 2007.

[3] NIST Security Requirements for Cryptographic Modules, Annex B: Approved Protection Profiles for FIPS PUB 140-2, November 4, 2004.

[4] NIST Security Requirements for Cryptographic Modules, Annex C: Approved Random Number Generators for FIPS PUB 140-2, March 19, 2007.

[5] NIST Security Requirements for Cryptographic Modules, Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2, March 19, 2007.

[6] NIST Derived Test Requirements for FIPS 140-2, Draft, March 24, 2004.

[7] ACX Series Access Controller for Ethernet
SDS-C-ACX-US TAC, LLC, September, 2007.

[8] NetController II CPU Module
SDS-C-NETCONTROLLER-II-US, TAC, LLC, January, 2007

[9] Andover Continuum® Power Supplies with UPS
SDS-C-POWERSUP-US, TAC, LLC, May, 2006

[10] ACX57xx Series Controller, Installation Instructions
Document Number 30-3001-998 Rev A, TAC, LLC, March, 2007

[11] ACX57xx Series Controller, Operation and Technical Reference Guide
Document Number 30-0001-999 Rev A, TAC, LLC, April, 2007

[10] NetController II Installation Instructions
Document Number 30-3001-994 Rev A, TAC, LLC, November, 2006

[11] NetController II Operation and Technical Reference Guide
Document Number 30-3001-995 Rev A, TAC, LLC, December, 2007

[12] Network Security Configuration Guide
Document Number 30-3001-996 Rev A, TAC, LLC, December, 2006

1.3 Product Overview

Continuum® Network Controllers are powerful Central Processing Units (CPUs) and network managers for the Continuum® facility management system. In combination with a Cyberstation Workstation and database server, the Continuum® family of products allows facilities to completely automate such building operations as HVAC, Lighting, and Physical Access Control. The Continuum® Network Security module is offered with the NetController II Rev B or the ACX Series Rev 2a of controllers to provide the most secure method of communications amongst peer controllers and Cyberstation Workstations on the Ethernet/IP network by providing FIPS 140-2 certified encryption algorithms that are used by the IPsec/IKE protocol built into these controllers. The ACX Series Rev 2a controller is a first generation hardware platform and its firmware revision is denoted by v1.100021. The NetController II Rev B is a second generation hardware platform and its firmware revision is denoted by v2.100021. An overview of the Continuum® Architecture is provided below in figure 1.

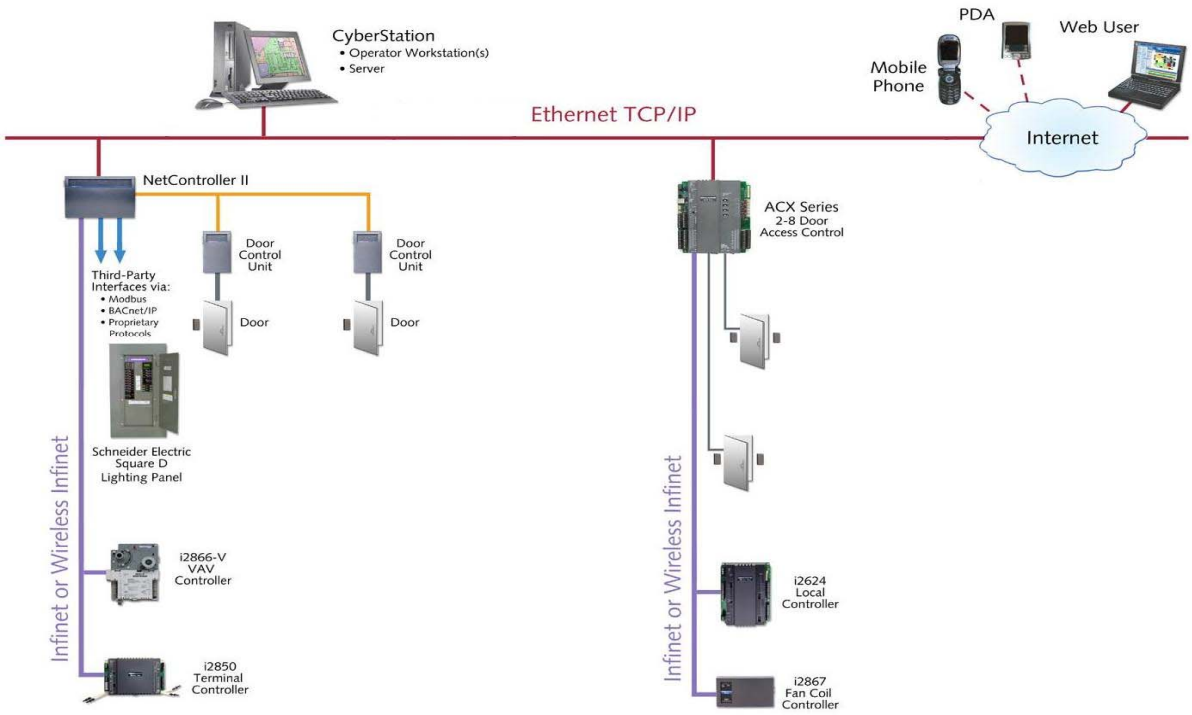
Controller Features include:

- Native Ethernet TCP/IP network connectivity
- High-speed processing
- Programmable communications ports for flexible interconnect and third-party communications
- Flash memory for easy on-line software updates
- Built-in web server capabilities
- FIPS 140-2 validated Continuum® Network Security Module

Cyberstation Workstation Features include:

- Complete building automation configuration tool
- Alarm and Event handling
- Report generation
- Graphics based building operation

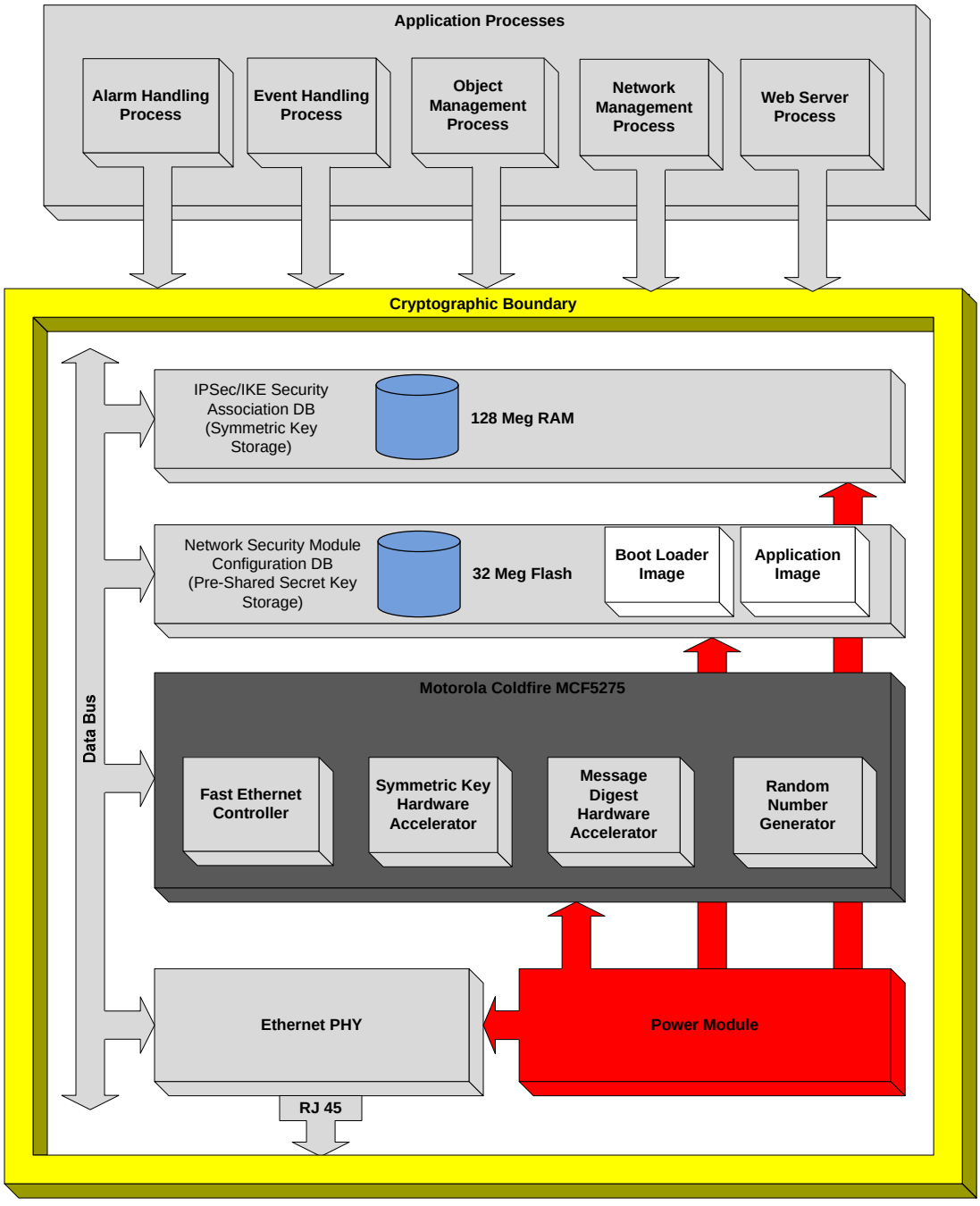
Figure 1 – Continuum® Architecture



1.4 Cryptographic Module Specification

The Continuum® Network Security Module is a hardware module developed by Schneider Electric. The Continuum® NetController II Rev B and ACX Series Rev 2a of Controllers provide services for building automation in such areas as HVAC, Lighting, and Physical Access Security. The controller series maintains a set of building automation objects in an internal database as configured through a Cyberstation workstation front end. In addition to performing building automation tasks, the controller series provides secure communication using IPsec/IKE protocols between peer controllers and Cyberstation workstations for the delivery of alarms, access events, and configuration data. The physical cryptographic boundary of the Continuum® Network Security Module is defined by the plastic enclosure. The logical cryptographic boundary is illustrated in figure 2 below:

Figure 2 – Logical Cryptographic Boundary



The physical device consists of the following hardware components:

- NetController II Rev B or ACX Series Rev 2a General Control Module (GCM)
- Onboard power management module
- External 12-28V DC or 24V AC Power Supply
- 10/100Mbs Fast Ethernet Controller
- RJ-45 Ethernet Port

The following are excluded from the cryptographic boundary:

- RS232/485 Ports
- Internal Modem

Per FIPS 140-2 terminology, the Continuum® Network Security Module is a multi-chip standalone module that meets overall level 2 FIPS 140-2 requirements. The Continuum® Network Security module includes the following that are common to both the NetController II Rev B and ACX Series Rev 2a controllers:

- 150MHz Processor
- 128Mb DDR SDRAM
- 32 Mb Flash

The Continuum® Network Security Module is validated at the following FIPS 140-2 Section levels:

Table 1 - Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

1.5 Module Ports and Interfaces

The module's logical interfaces are contained within the IPsec/IKE stack. Physically, ports and interfaces are located on the periphery of the cryptographic module boundary and include only the 10/100 Ethernet port and the Power Interface. The NetController II Rev B and ACX Series Rev 2a controllers also contain an LED bank for communication, CPU, Ethernet, and IO Bus status. The interfaces can be categorized into following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Out Interface
- Control Interface
- Status Output Interface
- Power Interface

Since the Data Input, Data Output, Control Input and Status Output interfaces share the same physical port, they are logically divided by the IPSec protocol stack using different IP sockets for both inbound and outbound communications.

All of these logical interfaces are described in the following table:

Table 2 - FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Continuum® Network Security Port/Interface	Physical Port/Interface
Data Input	IP Packet Buffer on Inbound IP Socket port via IPsec/IKE stack	Ethernet Port
Data Output	IP Packet Buffer on Outbound IP Socket port via IPsec/IKE stack	Ethernet Port
Control Input	IP Packet Buffer on Inbound IP Socket via IPsec/IKE stack Clear Memory/Reset Button	Ethernet Port Clear Memory/Reset Button
Status Output	IP Packet Buffer on Outbound IP Socket via IPsec/IKE stack Persistent Error Log LED Interface	Ethernet Port Flash Device LED Panel
Power Interface	External Power Connector	External Power Connector

1.6 Roles, Services and Authentication

Two roles are supported by the module: a Crypto-Officer (CO) role and a User role using role-based authentication. The Crypto Officer role is assumed by a user that is configuring the system. The User role is automatically assumed by the NetController II Rev B and ACX Series Rev 2a controller's processes that take advantage of the crypto module. Both of the roles and their responsibilities are described below.

1.6.1 Crypto Officer Role

The Crypto-Officer (CO) role is responsible for the configuration and initialization of the cryptographic functions provided by the Continuum® Network Security Module.

Descriptions of the services available to the Crypto-Officer role are provided in the table below.

Table 3 – Mapping of Crypto Officer Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Configure the module	Configure the module's IP address via a direct connection to the controller's Ethernet port.	IP and address data using standard web browser	None	None
Configure FIPS mode of operation. (commissioning)	Configure the module for FIPS-approved mode of operation	Selection of Network Security policy via standard web browser	None	None
Restart the module (reboot)	Command the module to restart.	Selection of restarting the controller via standard web browser	Module restarts. If FIPS-approved mode is configured, initiates power up self-tests.	None
Establish a secure IPsec/IKE session	Establish a secure IPsec/IKE session with web browser client and ACX Series Rev 2a/NetController II Rev B web server	Diffie Hellman pre-shared key	Secure IKE and IPsec SA's	3DES key read/write SHA1 key read/write

Service	Description	Input	Output	CSP and Type of Access
Review status	Module status information	Status read via web browser connection to the ACX Series Rev 2a/NetController II Rev B Status read via log database via client application	Module status displayed in web browser. Module status displayed in client application	None
Update Module Firmware	Update the module firmware NOTE: The module will NOT operate in FIPS 140-2 mode unless the revision that the controller is being updated to has been FIPS 140-2 validated.	Firmware binary image	Module firmware revision	None

1.6.2 User Role

The User role is assumed by application processes running in the controller. These processes access the module's cryptographic services for the establishment of IPsec and IKE security associations in order to provide secure communication over those channels on behalf of the processes.

The user role actions that cause data to be shared in the system include:

1. Alarm handling process
2. Event handling process
3. Object management process
4. Network management process
5. Web server process

Table 4 – Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Alarm event	securely transfer alarm information to the workstation	Diffie Hellman pre-share secret	Initiate an IPsec/IKE security association with a peer controller or Workstation	Diffie Hellman pre-shared secret – read 3DES key – read/write SHA1 key– read/write
Access Events	transfer access event information to the workstation	Diffie Hellman pre-share secret	Initiate an IPsec/IKE security association with a peer controller or Workstation	Diffie Hellman pre-shared secret – read 3DES key – read/write SHA1 key– read/write
Update of object values	transfer updates of object values to the workstation	Diffie Hellman pre-share secret	Initiate an IPsec/IKE security association with a peer controller or Workstation	Diffie Hellman pre-shared secret – read 3DES key – read/write SHA1 key– read/write
Online/Offline detection	detect the presence of other controllers or workstations on the network by sending/receiving heartbeat messages	Diffie Hellman pre-share secret	Initiate an IPsec/IKE security association with a peer controller or Workstation	Diffie Hellman pre-shared secret – read 3DES key – read/write SHA1 key– read/write
Web Server	responses to http requests	Diffie Hellman pre-share secret	Initiate an IPsec/IKE security association with a peer controller or Workstation	Diffie Hellman pre-shared secret – read 3DES key – read/write SHA1 key– read/write

1.7 Non – FIPS

The following operate in the NetController II Rev B and ACX Series Rev 2a controllers in a non-FIPS mode:

- SNMP Protocol
- SMTP Protocol
- Boot Loader

1.8 Physical Security

The physical security requirements do apply to this module since it meets the overall level 2 FIPS 140-2 requirements for Physical Security. The NetController II Rev B and ACX Series Rev 2a controller's crypto module is protected by a plastic enclosure which is opaque to the visible spectrum. Components on the PCB board such as the CPU, Flash Chip, and RAM chips have been coated as to prohibit the ability to read the component type and model. Further, the plastic body is protected with tamper evident seals in order to reveal any tampering by removal of the plastic enclosure. The tamper evident seals are installed at the factory. The tamper evident seals are displayed in Figure 3 below.

Figure 3 – Physical Security – Tamper Evident Seals

Figure 3 depicts the ACX Series Rev 2a Controller (left) with a tamper evident seal on the top of the enclosure and a second tamper evident seal on the bottom of the enclosure. Figure 3 also depicts The NetController II Rev B Controller (right) with a tamper evident seal on the left side of the enclosure and a second tamper evident seal on the bottom of the enclosure.

The NetController II Rev B and ACX Series Rev 2a of controllers have been tested for and meet applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and

Electromagnetic Compatibility (EMC) requirements for business use as defined in Subpart B of FCC Part 15.

1.9 Operational Environment

The module contains the Multi-Threaded Real Time Operating System ThreadX, version G3.0e.3.0b. The RTOS is stored in and executed in flash memory and is non-modifiable.

1.10 Cryptographic Key Management

The Continuum® Network Security Module implements the following FIPS-approved algorithms:

- Triple-DES (CBC) mode for IPsec and IKE encryption (certificate #752)
- SHA1 for message hash (certificate #924)
- HMAC-SHA-1 for IPsec and IKE authentication (certificate #528)
- Deterministic Random Number Generator (certificate #537)

Additionally, the cryptographic module utilizes the following non-FIPS-approved algorithm implementation:

- Diffie-Hellman (key agreement: key establishment methodology provides 80-bits of encryption strength)[1]
- Non-deterministic Random Number Generator (used to seed the DRNG)

[1] In order to operate in an Approved mode of operation compliant to FIPS 140-2, keys of 80-bits are used.

The module supports the following critical security parameters:

Table 5 - List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Diffie Hellman Pre-shared secret	16-32 character string	Set to default value at factory. Changed by Crypto Officer during configuration	Never	Stored in Flash	N/A	Diffie Hellman authenticated key agreement protocol
Skeyid	SHA-1	Derived from the shared secret in IKE exchange	Never	Stored in volatile memory.	On termination of IKE session	IKE exchange
Skeyid_d	SHA-1	Derived from skeyid via ISAKMP/IKE	Never	Stored in volatile memory.	On termination of IKE session	Deriving keying data for IPsec sa's
Skeyid_a	HAMAC SHA-1	Derived from skeyid via ISAKMP/IKE	Never	Stored in volatile memory.	On termination of IKE session	Authentication and integrity of IKE messages
Skeyid_e	3DES	Derived from skeyid via ISAKMP/Ike	Never	Stored in volatile memory	On termination of IKE session	Encryption of IKE messages
IPsec Encryption Key	3DES	IKE	Never	Stored in volatile memory.	On Re-key and termination of SA.	Encryption/decryption of IPsec ESP Packets
IPsec Authentication Key	SHA-1	IKE	Never	Stored in volatile memory	On Re-key and termination of SA	Authentication of IPsec ESP Packets
Software Integrity	16 bit CRC	Compiler	Never	Stored in Flash	Never	Verification of binary image.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
DRNG Seed	32 bit	Generated by Non-Deterministic RNG	Never	Stored in volatile memory	After seed of DRNG	Used as seed value for DRNG

1.11 Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to ensure that all components are functioning correctly. This cryptographic module performs the following self-tests:

- Power-Up Self-Tests:
  - Firmware Integrity Test
  - Known Answer Tests (KATs)
    - Triple-DES KAT
    - SHA-1 KAT
    - HMAC KAT
    - PRNG KAT

The Continuum® Network Security module performs the following conditional self-tests:

- Continuous RNG test for FIPS-Approved PRNG
- Continuous RNG test for non-FIPS approved Hardware RNG

Status output of self-tests are logged to persistent storage and are accessible via a client interface.

To view the status output of the self tests, an error log tool is provided with the Cyberstation Installation and is located at <install directory>\Continuum\bin\ControllerErrorLogTool.exe. To retrieve error log information directly from a controller, run the error log tool and provide the IP Address of the controller.

Additionally, the status output of the Known Answer Tests and the FIPS 140-2 Mode can be viewed by accessing the controller directly through the web interface. Refer to section 2.1.2 of this document for directions on how to view the status output.

If one of the KATs fails, then the ACX Series Rev 2a and NetController II Rev B will not operate in FIPS mode, and the appropriate error will be logged. To return the module to the approved mode of operation, the controller may be reset or power cycled which will re-run all of the KATs. Upon successful completion of the KATs at startup, the controller will operate in FIPS 140-2 mode.

If one of the KATs fails continuously upon restarts of the controller, this may indicate a failure of the controller and it should be returned to the factory for repair..

1.12 Design Assurance

Configuration management for all of the Schneider Electric Continuum® Network Security Module source code files are maintained in a source code versioning database.

Additionally, the Continuum® Network Security Module's FIPS 140-2 documentation are also maintained in a versioning database.

1.13 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 requirements for this validation.

2 Secure Operation

The Continuum® Network Security Module meets Level 2 requirements for FIPS 140-2. The sections below describe how to configure and maintain the module in a FIPS-approved mode of operation. Operating the module without following this guidance will remove the module from the FIPS-approved mode of operation.

2.1 Crypto-Officer Guidance

2.1.1 Initial Setup

In order to operate the NetController II Rev B or ACX Series Rev 2a on an IP network, the controller's network address information must be entered so that CyberStation can communicate with the controller. This operation is called *commissioning*.

Commissioning an NetController II Rev B or ACX Series Rev 2a requires the following:

- A laptop or other computer
- A pocket PC
- An Ethernet adapter for the above Pocket PC or computer
- Web browser software
- Cable (CAT-5, twisted pair)

You connect to the controller directly through its Ethernet port using a cable connected to the Ethernet port of your PC or you may connect the controller to an Ethernet hub/switch that your PC is connected to.

As received from the factory, the IP address settings for the controller are set to the following defaults:

Setting	**Value**
IP Address	169.254.1.1
Subnet Mask	255.255.0.0
Gateway Address	0.0.0.0

In order to communicate successfully with the controller while it is set to its default IP address, your computer or Pocket PC must be configured with an IP address in the same Network range as the controller. Setting your PC to the static IP address of 169.254.1.2 will allow successful communication to the controller with its default settings. During the commissioning process, you may enter a more permanent IP address for the controller.

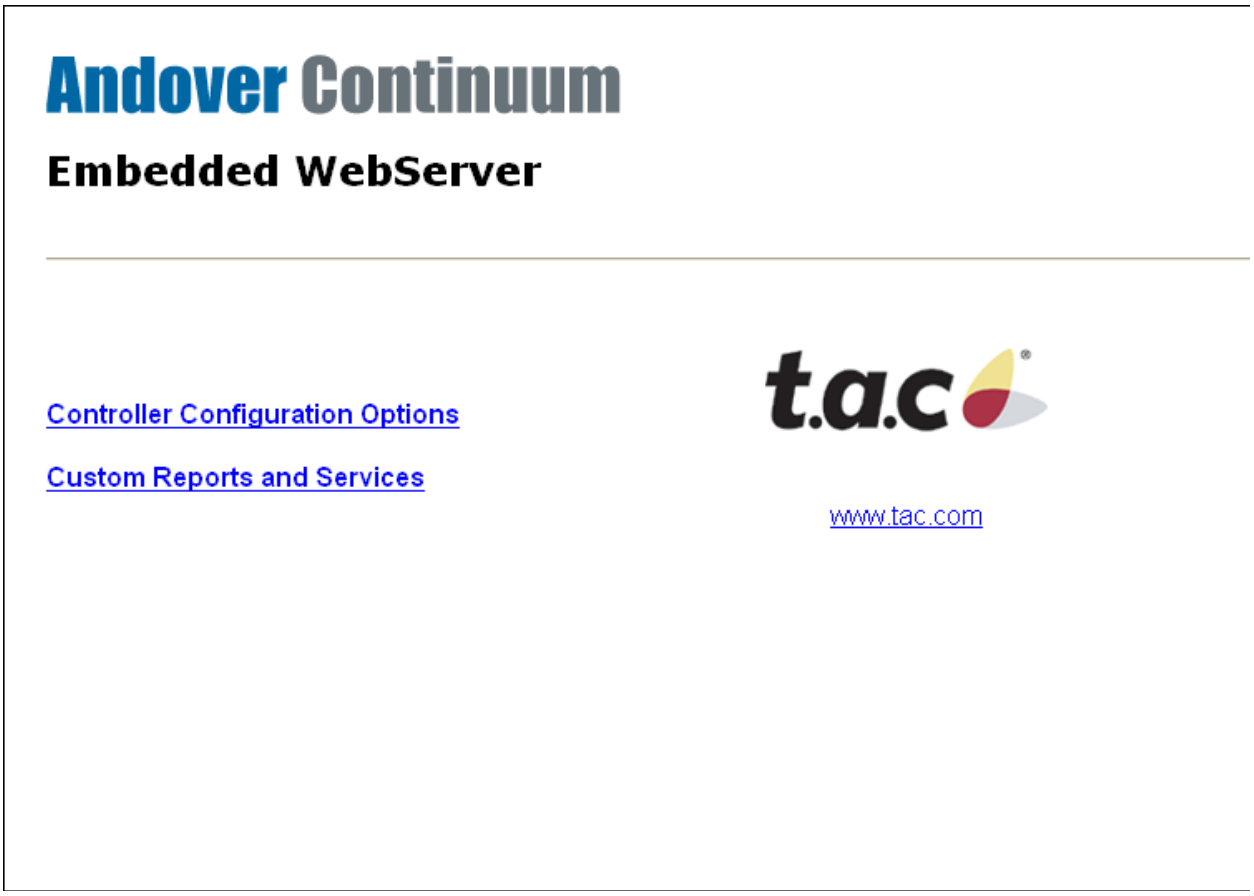
Note: Contact your system administrator for assistance with determining IP addresses, gateway addresses, and subnet masks.

There are many ways to ensure communications between the two depending upon your operating system. It is beyond the scope of this document to explain network communications. However, the following procedure is one simple method that ensures communication.

To connect from your computer to the controller, follow these steps:

1. Disable the Dynamic Host Configuration Protocol (DHCP) Services on your PC. If your PC is not configured for DHCP, record the static IP address settings that are currently configured.
2. Disconnect your computer from the network, and set your IP address to 169.254.1.2 and your subnet mask to 255.255.0.0.

3. Using a CAT5 cable (straight-through or crossover), connect your PC to the controller's Ethernet port.
4. Run your web browser and enter the URL: http://169.254.1.1 to display the following web page.

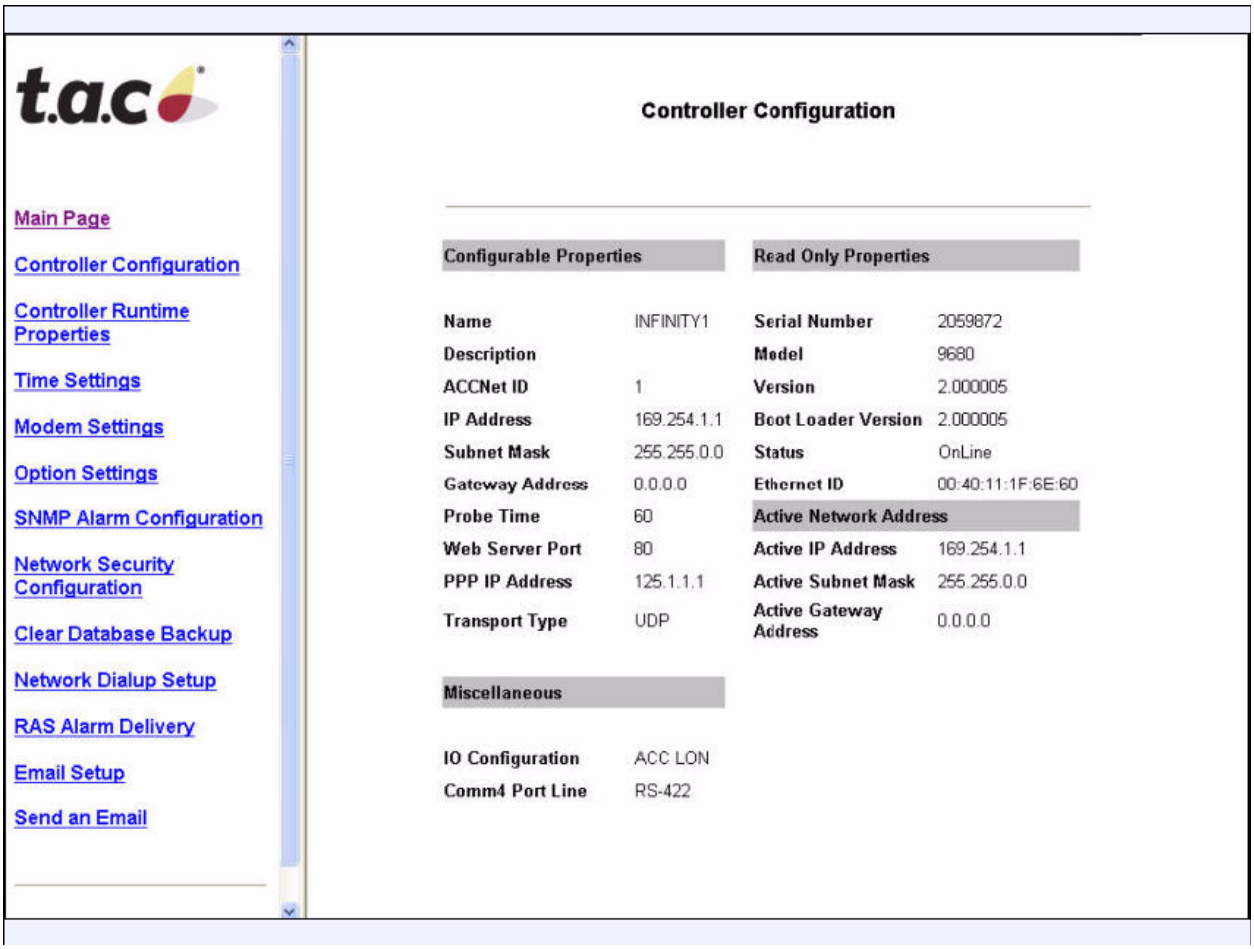


5. There are two user selections available on the displayed page:
   - Controller Configuration Options
   - Custom Reports and Services
6. Select the **Controller Configuration Options**.
7. For security reasons, the controller is password-protected. A logon dialog appears over the initial page. At the logon dialog enter the default CyberStation user name and password shown on the following illustration. (**Note:** The User Name and Password can be configured using Controller User objects.)

8. Click **OK** to logon. (**Note:** Don't forget to enable DHCP Services on your PC, and connect the NetController II Rev B to the network when it reboots after you finish the commissioning process.)

You may see the following system startup page for a few seconds while system initialization occurs.

After connecting to the IP address of the controller, the main Web Commissioning page appears.



The main page features two panes:

- A **side navigation pane** for accessing the different configuration pages. The options listed on the side navigation pane may differ based on the controller software model, the options you have enabled, or additional installed options supplied by TAC.
- The **main display pane** shows the currently active commissioning web page.

When you select **Controller Configuration** from the side navigation pane, the **Controller Configuration** page appears.

The following table describes the **Controller Configuration** fields that you can edit, as well as the action buttons. You can also access this information by clicking **Help** below the page title.

Name	Contains the name of the controller. You can enter any name you wish in this field up to a maximum of 16 characters. Spaces between name segments are not permitted. Controller device names must be unique across a network
Description	Enter a description of the controller up to 32 characters in length (optional).
ACCNet ID	Identifies each controller on an Andover Continuum® network by a unique number between 1 and 190. Each controller must have a unique ID on its particular network.
IP Address	A logical 32-bit address that identifies a TCP/IP host. Each controller requires a unique IP address. Each address has two parts: a network ID, which identifies all hosts on the same physical network, and a host ID, which identifies a host on the network.

Subnet Mask	Subnets divide a large network into multiple physical networks connected with routers. A subnet mask blocks out part of the IP address so that TCP/IP can distinguish the network ID from the host ID. When TCP/IP hosts try to communicate, the subnet mask determines whether the destination host is on a local or remote network. To communicate within a local network, computers and controllers must have the same subnet mask.
Gateway Address	The Gateway is the intermediate device on a local network that stores network IDs of other networks in the enterprise or on the Internet. To communicate with a host of another network, configure an IP address for the default Gateway. TCP/IP sends packets for remote networks to the default gateway (if no other route is configured), which forwards the packets to other gateways until the packet is delivered to a gateway connected to the specific destination. If you are using a proxy server, you must define a default router here.
Probe Time	Displays the time, in seconds, between controller probes. A probe is a message that the device sends out to its controllers to check their COMM status. Controllers respond to probe messages to let the device know they are online. When a device does not receive a response from a controller, it changes the controller's COMM status to Offline.

Web Server Port	The standard port for Web communications. The default setting is 80. The Web Server Port can be set to any number from 1 to 65,534. If changed, browser requests must specify the port number in the URL, for example, http://<IP Address>:<Web Server Port>.
PPP IP Address	Point-to-Point Protocol Address of the controller.
Transport Type	UDP - This controller will communicate with other controllers and Workstations primarily using the UDP protocol. TCP - This controller will communicate with other controllers and Workstations primarily using the TCP protocol. TCP/UDP - This controller will communicate with other controllers and Workstations primarily using the TCP protocol, but can also speak to controllers and Workstations that communicate primarily using the UDP protocol.
IO Configuration	Allows the IO bus configuration to be either ACC LON or L-BUS.
Comm4 Port Line	Allows Comm4 to be configured as either RS422 or RS485.
Action Buttons	
Submit to Controller	Submit all form data to the controller. After submitting data, navigate to the Commit Changes page to write the changes to flash memory and restart the controller.
Reset Form	Undo any changes that were previously submitted.

2.1.2 Management

The communication between the controller and workstation is secured using Internet Protocol Security (IPsec) and the Internet Key Exchange Protocol (IKE).

IPsec, a set of extensions to the IP protocol family, ensures data authentication, integrity, and encryption or authentication and integrity only of IP packets.

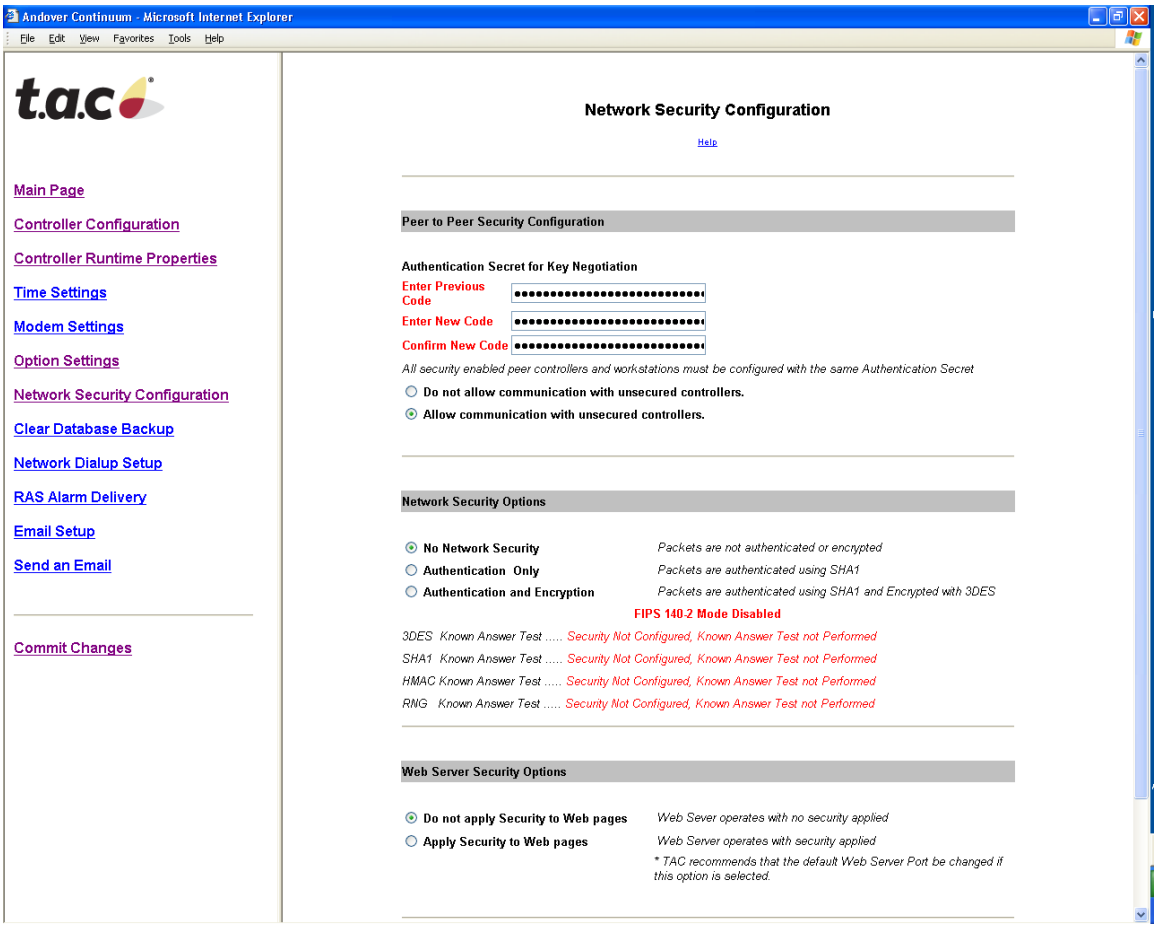
IKE securely negotiates the properties of the security associations of IPsec enabled peers, such as Andover Continuum® controllers and workstations, once all of the following tasks have been addressed.

Configuring Network security for the newest generation of TAC controllers includes the following steps:

Task 1: Configure controller for secure communication
Task 2: Configure network security on the workstation

Task 1: Configure controller for secure communication

To access the controller's web configuration page, login as an administrative user and navigate to the **Network Security Configuration** web page.



When you are configuring the controller on the **Network Security Configuration** web page, you can set the following security options:

- **Peer to Peer Security Configuration** -- These options allow each workstation and controller to communication with each other and authenticate each other's identity using the same Shared Authorization Secret.
- **Network Security Options** -- These options allow for different levels of network security, including no security (the factory default), a network security policy requiring that all TAC Andover Continuum® traffic be authenticated, or a network security policy requiring that all TAC Andover Continuum® traffic be authenticated and encrypted.
- **Web Server Security Options** -- This option allows for applying the network security level selected under Network Security Options to the controllers Web Server. The network security level will be applied to all of the Web Configuration and Plain English Web pages if this option is turned on.

To configure **Peer to Peer Security**, complete this procedure:

Step 1: In the **Enter Code Previous Code** field, enter the previously configured Authentication **Secret for Key Negotiation**. The secret may be any ASCII string up to 32 characters. (**Note:** The default secret from the factory is “itsasecret”. You must remember the secret that you enter here for later use. All controllers and CyberStations that need to communicate securely must be configured with the same secret.)

Step 2: You may enter a new secret in the **Enter New Code** field to if you wish to change the Authentication Secret, or enter the previous secret.

Step 3: You must re-enter the same secret in the **Confirm New Code** field to confirm your new secret.

Step 4: If this controller will be required to communicate with legacy controllers that do not support network security or controllers that have network security disabled on the same logical network, select **Allow communication with unsecured controllers**.

Step 4: If this controller will only communicate with secure peers, select **do not allow communication with unsecured controllers**.

To configure the **Network Security Options**, complete this procedure:

Step 1: Keeping the default selection, **No Network Security**, allows this controller to communicate unsecurely, without network security. With this configuration, the controller will NOT operate in FIPS 140-2 Mode.

Step 2: Selecting **Authentication Only** authenticates packets only. Choosing this option will allow packet snooping of the TAC Andover Continuum® Protocol on the wire. However, packets may not be replayed to the controller and the controller will disregard any packets that have had their data altered by an intrusive third party. With this configuration the controller will operate in FIPS 140-2 Mode.

Step 3: Selecting **Authentication and Encryption** authenticates and encrypts packets. Choosing this option does not allow snooping of the TAC Andover Continuum® Protocol on the wire, as the data are encrypted. Packets may not be replayed to the controller and the controller will disregard any packets that have had their data altered by an intrusive third party. With this configuration the controller will operate in FIPS 140-2 Mode. (**Note:** You must remember the option you selected for later use. All controllers and CyberStations that will communicate securely MUST be configured with the same option.)

Note: In order to operate in FIPS 140-2 Mode, the controller must be configured to operate in either **Authentication Only** or **Authentication and Encryption** mode.

To configure the Web Server Security Options, complete this procedure:

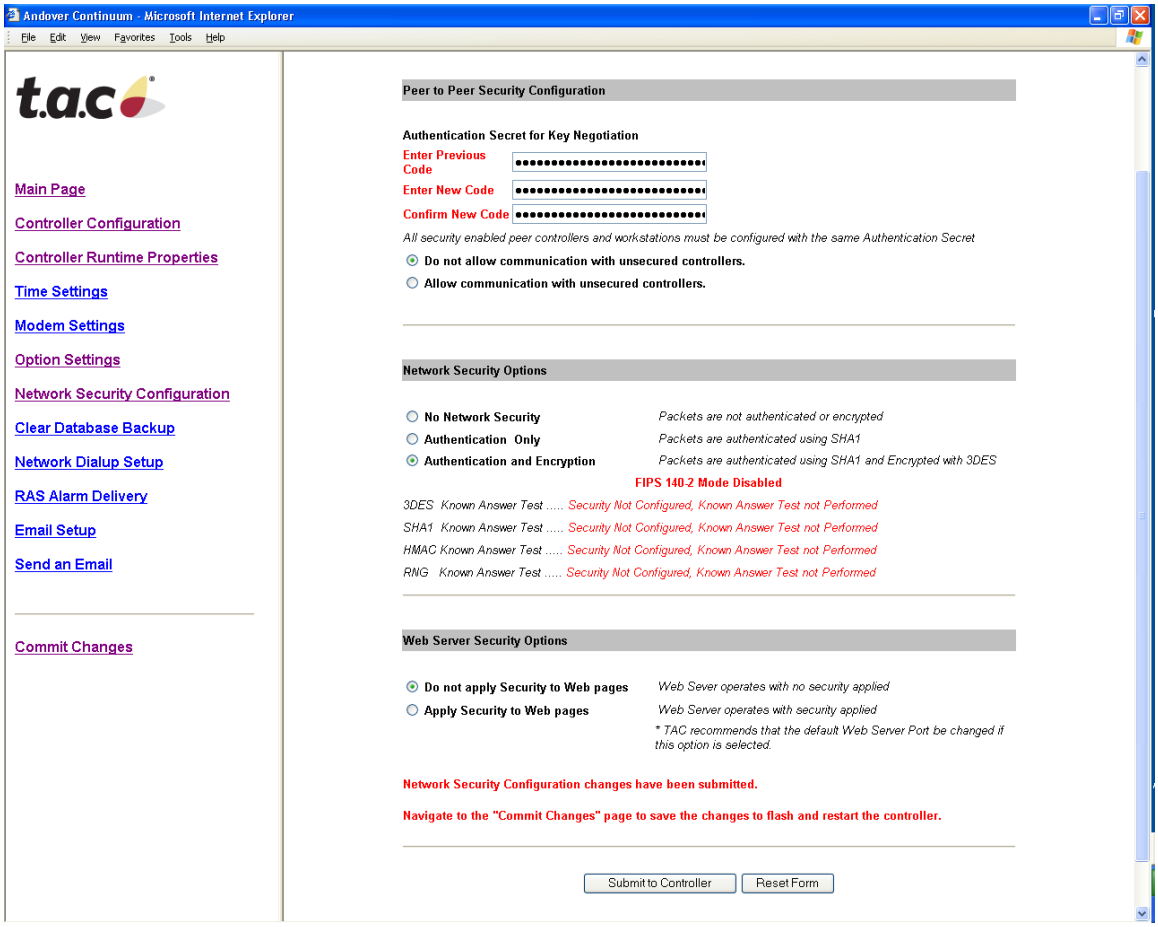
Step 1: Selecting **do not apply Security to Web pages** will allow all web communication to be unsecured and allows sniffing of the http protocol.

With this configuration the controller will operate in FIPS 140-2 Mode, however TAC highly recommends securing the web communication to the controller.

Step 2: Selecting **Apply Security to Web Pages** secures the web communication with the selected **Network Security Option**. (**Note:** If this option is selected, it is recommended that the default web port be changed from TCP Port 80, to Port 33920. You can make this change on the controller's **Controller Network Configuration** web page.)

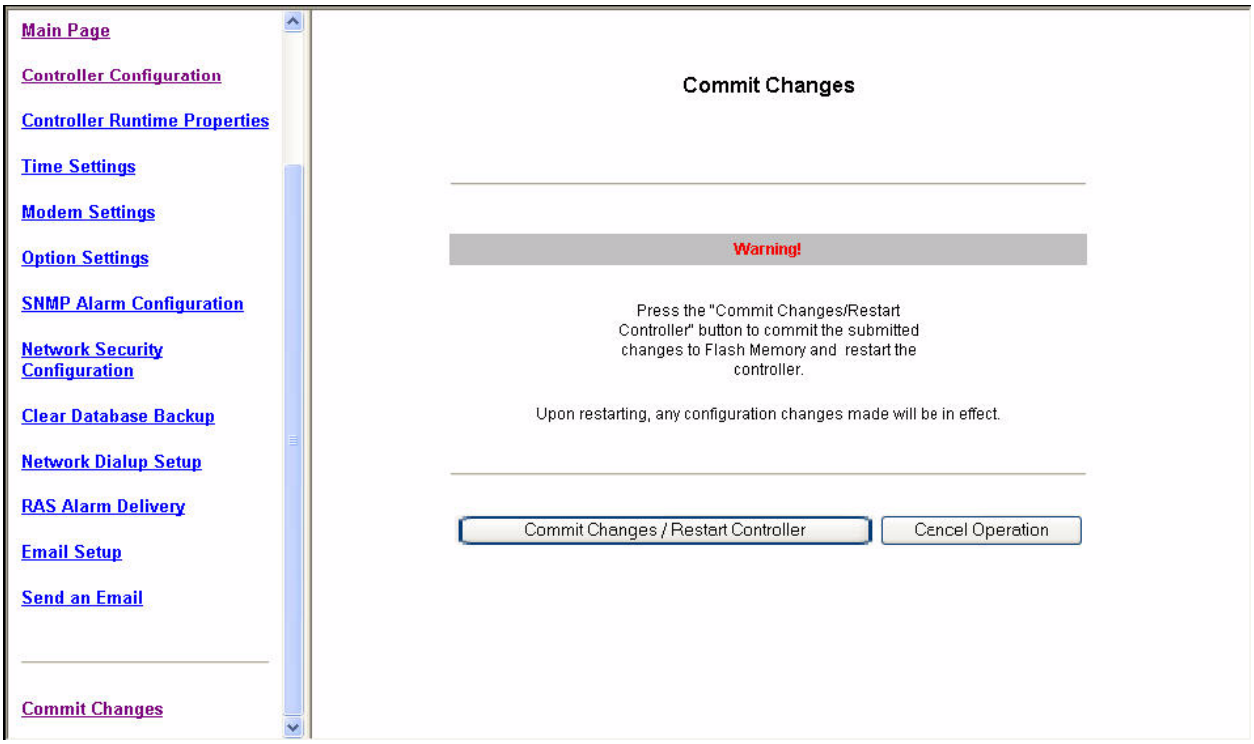
To submit changes, follow this procedure:

Step 1: Review all changes.



Note: After submitting changes, informational messages that signify the configuration changes are displayed on the bottom of the page.

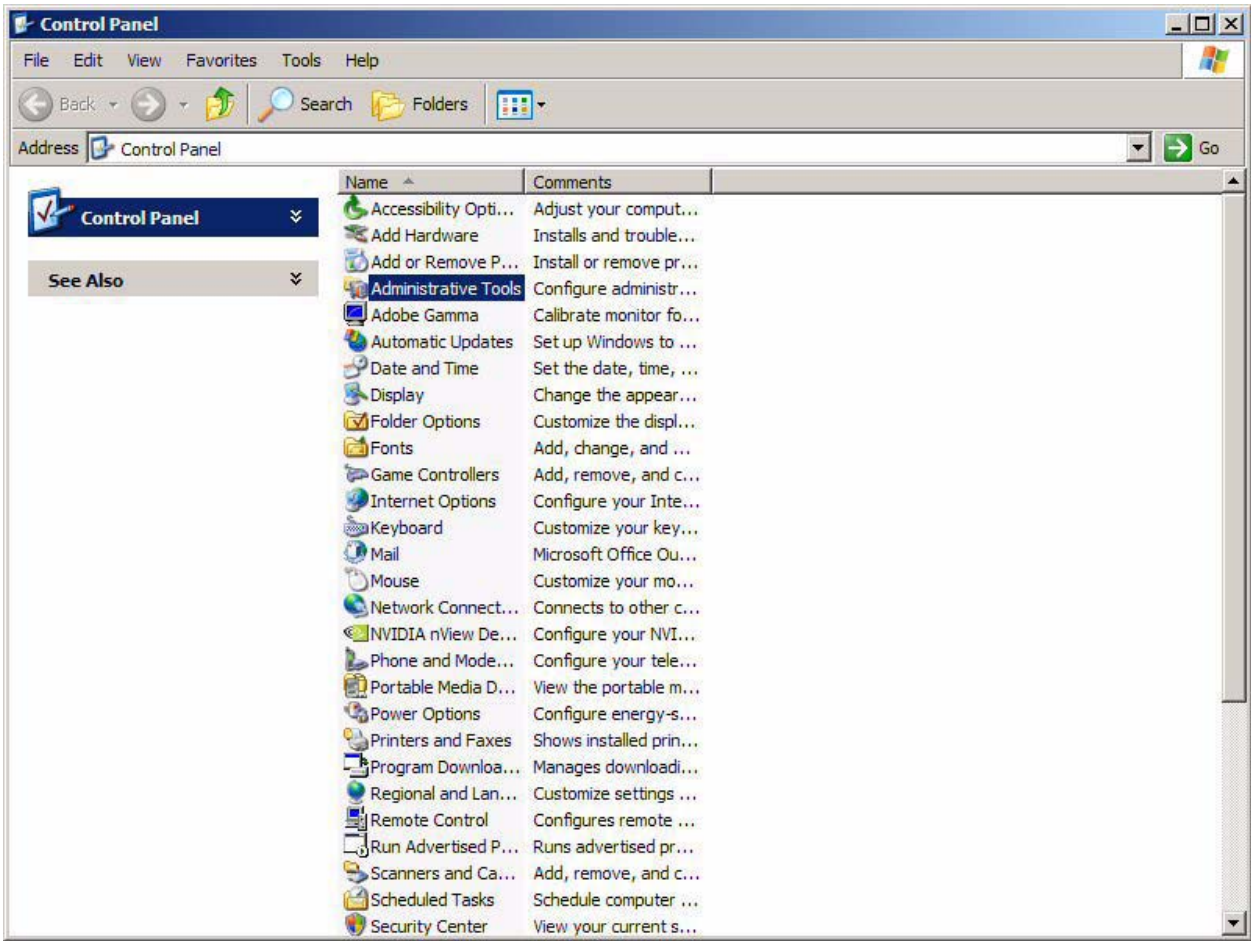
Step 2: To commit the changes and restart the controller, navigate to the **Commit Changes** page and then click **Commit Changes/Restart Controller**. Changes take effect when the controller restarts.



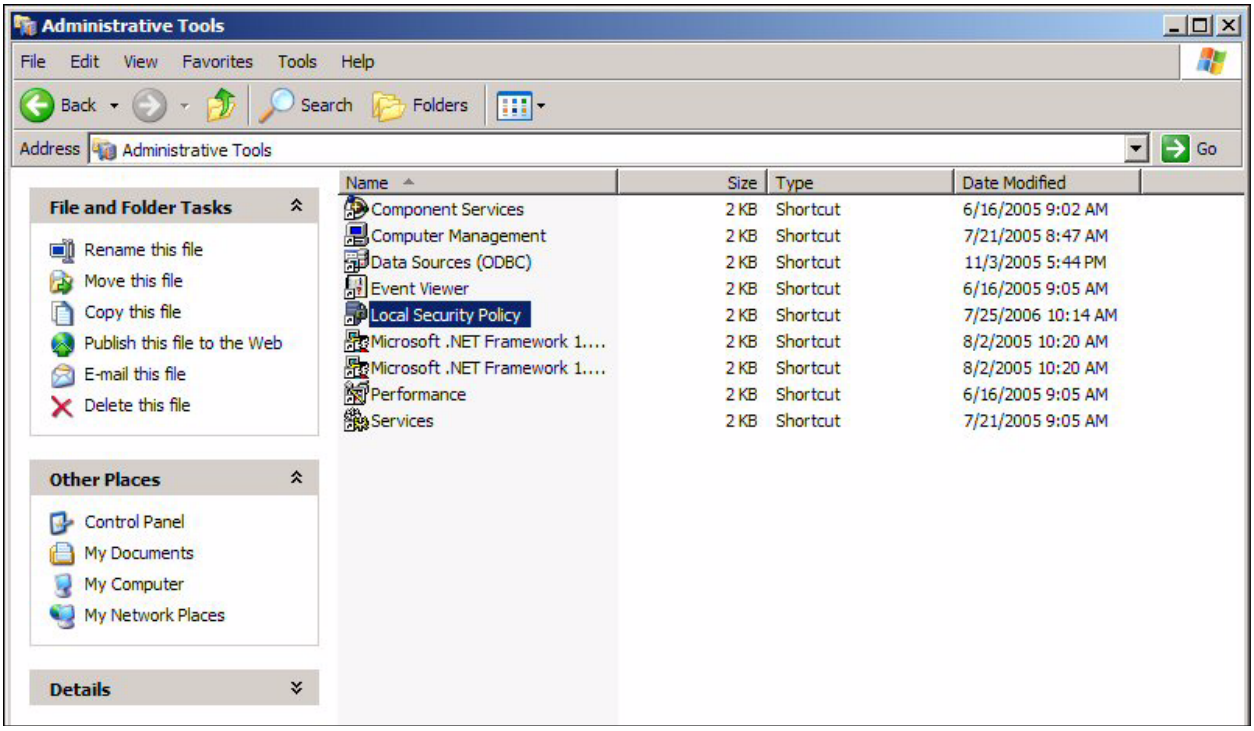
Task 2: Configure network security on the workstation

Importing the IPsec Security Policy

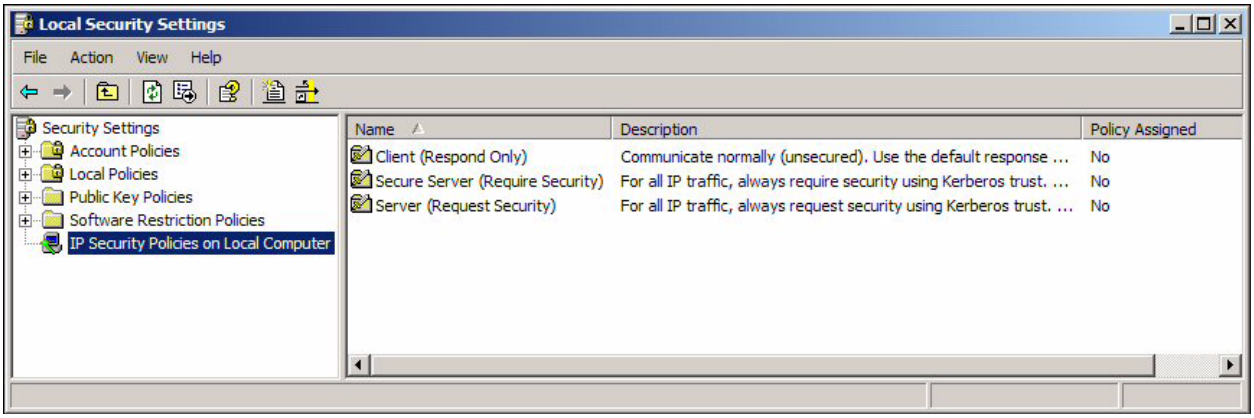
To import IPsec Security Policies, complete this procedure:
Step 1: From the Windows Control Panel, double click on “Administrative Tools.”



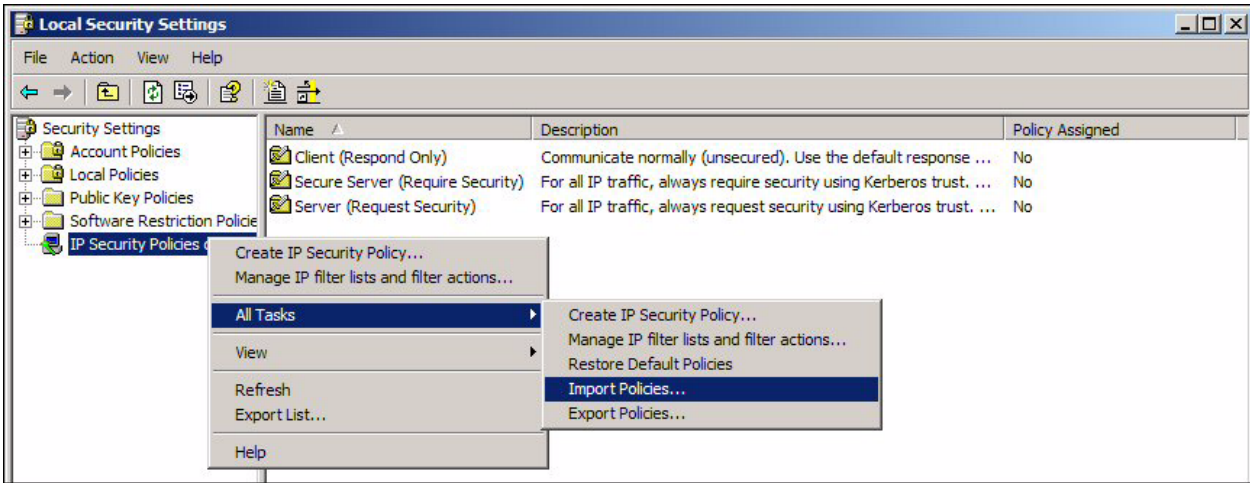
Step 2: From the **Administrative Tools** display, double click **Local Security Policy**.



Step 3: From the **Local Security Settings** dialog, right click on **IP Security Policies on Local Computer**.

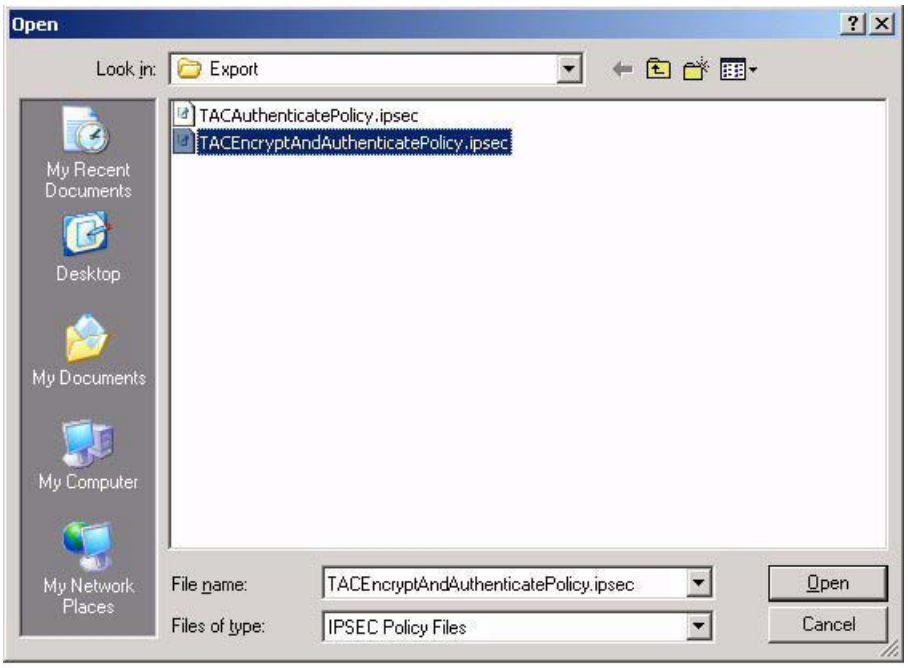


Step 4: Select **All Tasks** from the popup menu, and then select **Import Policies** from the submenu.



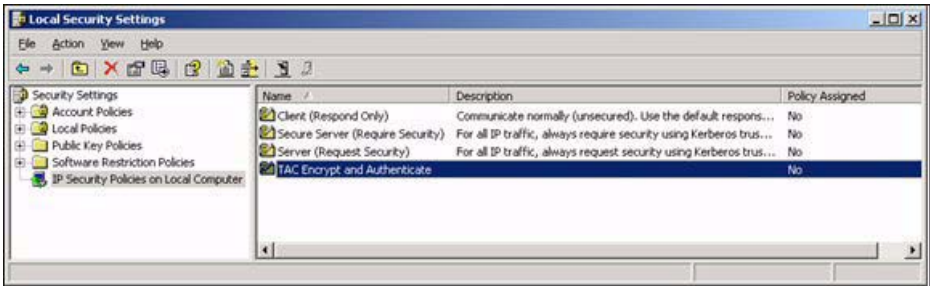
Step 5: From the **Open** dialog, navigate to the **Network Security Policy** folder: <install drive>:\Program Files\Continuum\Network Security. If you installed Continuum® to another directory other than the default, the files will reside at: <install path>\Network Security.

Step 6: If you configured the controller for **Authentication Only**, select the TACAuthenticatePolicy.IPsec file. If you configured the controller for **Authentication and Encryption**, select the TACEncryptAndAuthenticatePolicy.IPsec file.



Step 7: Click **Open** to import the policy.

Step 8: Verify that the appropriate policy--**TAC Encrypt and Authenticate** or **TAC Authenticate**--is now available under **Local Security Settings**.

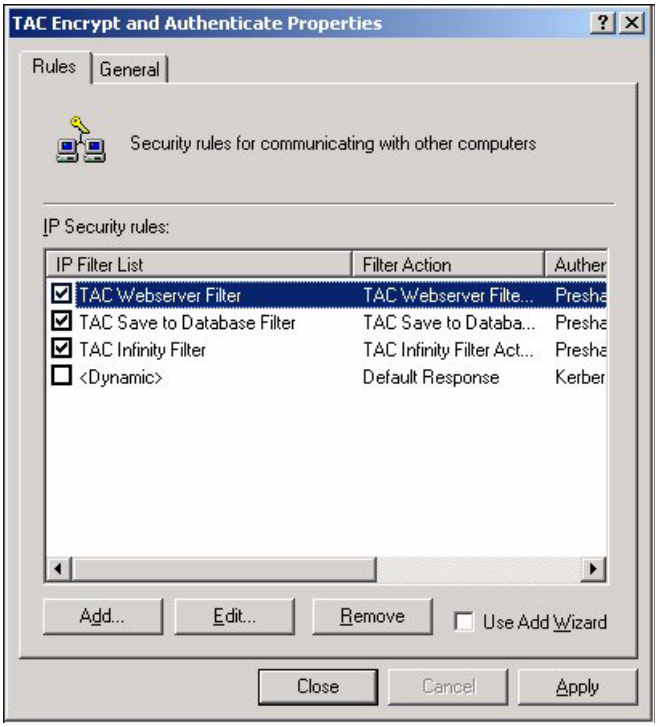


Editing the Imported Security Policy

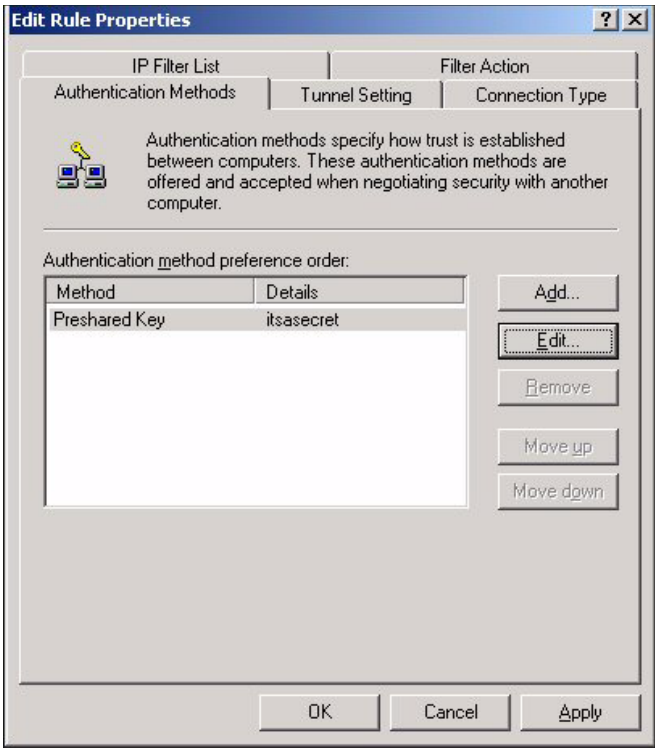
To edit imported security policies, complete this procedure:

Step 1: Double click the name of the imported security policy. The **TAC Encrypt and Authenticate Properties dialog** appears.

Step 2: If you configured the controller for Web Security, enable the **TAC Web Server Filter** in the **IP Security rules** list by checking the check box on the **Rules** tab. If you did not configure the controller for Web Security, leave the check box unchecked.

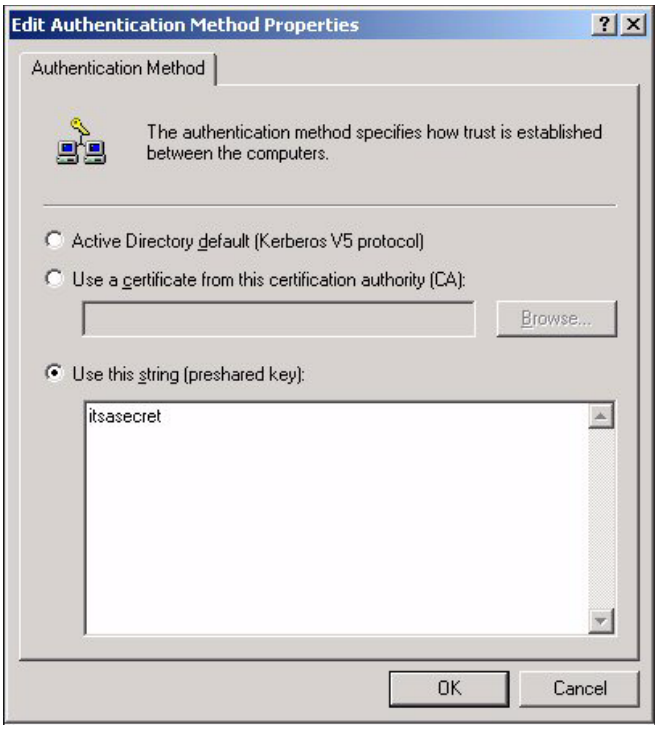


Step 3: For each TAC rule in the list, click **Edit**. For each, the **Edit Rule Properties** dialog appears.



Step 4: Select the **Authentication Methods** tab, select the **Preshared Key** method, and click **Edit**.

Step 5: In the **Edit Authentication Method Properties** dialog, enter the same secret here that was entered in the controller.



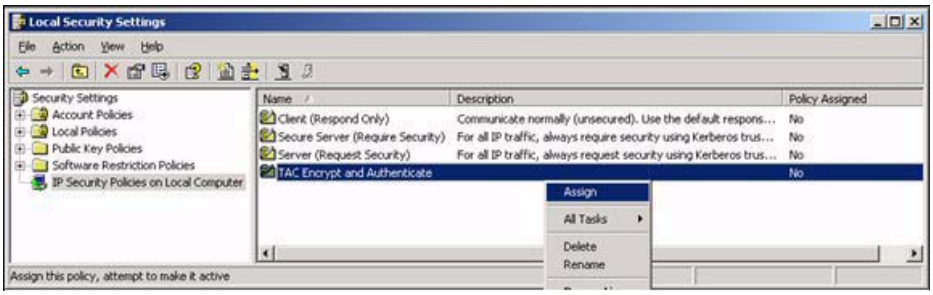
Step 6: Repeat setting the Authentication Secret for each rule in the List.

Note: The secret entered here is not a hidden field. Access to the Local Security Policy tool is restricted to users with administrative privileges on the machine. In order to protect access to the shared secret, all other users of the machine that will run CyberStation should be restricted to Windows "Power Users."

Assigning the Imported Security Policy

To assign imported security policies, complete this procedure:

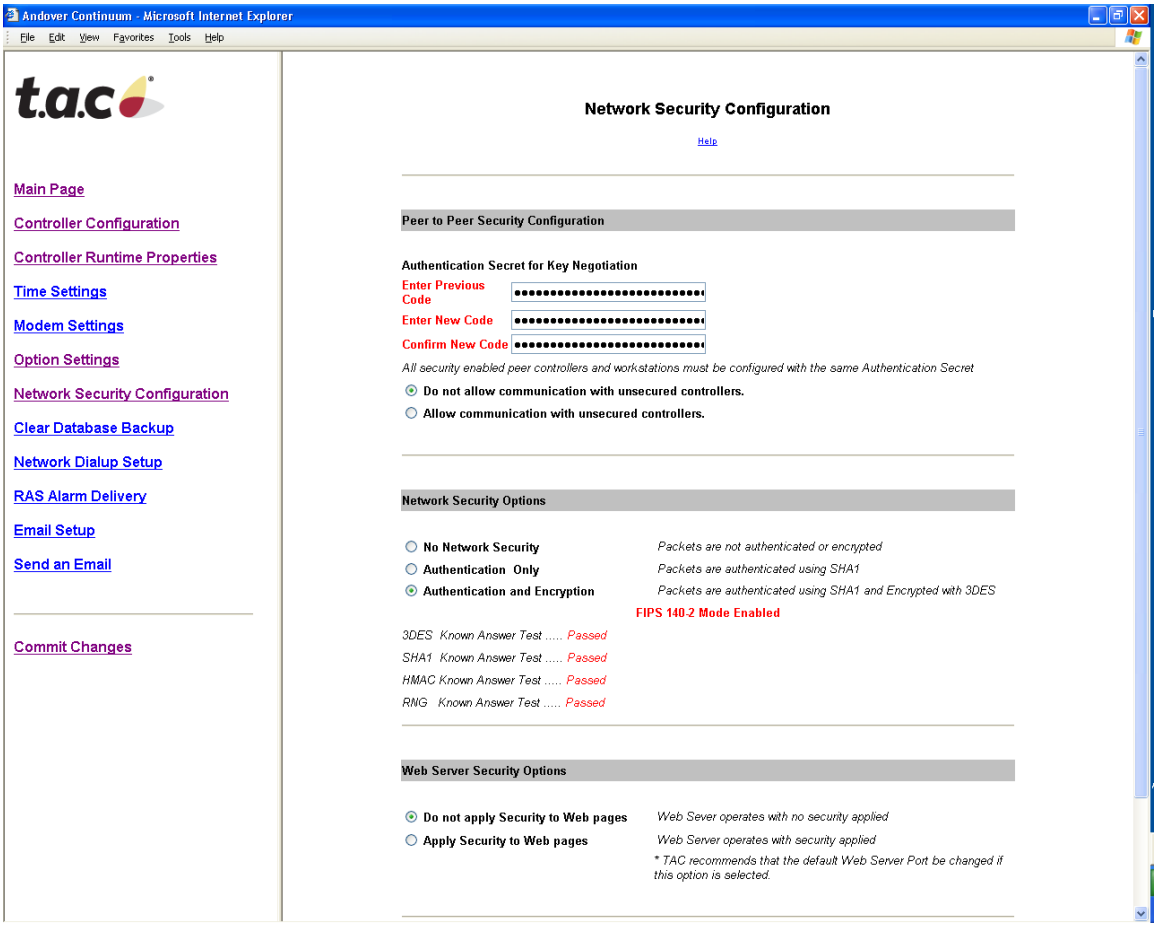
Step 1: Right click on **TAC Encrypt and Authenticate** or TAC Authenticate, depending on which Security Policy you imported, and select **Assign**.



Step 2: IPsec Security Policy is now enabled, and the workstation can communicate to security enabled controllers.

Step 3: To verify the changes made to the controller and to insure that communication settings have been configured properly, navigate to the controller Network Security Configuration Page after it has restarted. Verify that FIPS 140-2 Mode is enabled and that all Known Answer Tests have passed.

To run the Known Answer Tests at any time, restart the controller and navigate to the Network Security Configuration page to view the Known Answer Test results.



2.2 User Guidance

2.2.1 Setup/Operation

The Continuum® Network Security Module is configured by the Crypt-Officer. The User role is assumed by application processes running in the controller. There is no other setup required by the user.

Operation is assumed by the application processes that access the module's cryptographic services for the establishment of IPsec and IKE security associations.

3 Acronyms

Table 6 - Acronyms

Acronym	Definition
FIPS	Federal Information and Processing Standard
IPsec	Internet Protocol Security
IKE	Internet Key Exchange
ISAKMP	Internet Security And Key Messaging Protocol
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
IP	Internet Protocol
PUB	Publication
CPU	Central Processing Unit
HVAC	Heating, Ventilation, and Cooling
RAM	Random Access Memory
DB	Database
MB	Mega Bytes
GCM	General Control Module
DC	Direct Current
AC	Alternating Current
PHY	Physical Transceiver
MHz	Megahertz
DDR	Double Data Rate
SDRAM	Synchronous Dynamic Random Access Memory
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
LED	Light Emitting Diode
SA	Security Association
KAT	Known Answer Test
DES	Data Encryption Standard
HMAC	Hashed Message Authentication Code
RNG	Random Number Generator
SHA	Secure Hashing Algorithm

Acronym	Definition
CBC	Cipher block chaining
DRNG	Deterministic random number generator
SNMP	Simple network management protocol
SMTP	Simple mail transfer protocol
PCB	Printed circuit board
CRC	Cyclical redundancy check
ESP	Encapsulated security payload
PRNG	Pseudo-random number generator