User Manual

Allen-Bradley

EtherNet/IP Secure Communication

Catalog Number 1756-EN2TSC

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

	**WARNING:** Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.
	**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.

Labels may also be on or inside the equipment to provide specific precautions.

	**SHOCK HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.
	**BURN HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.
	ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

This manual contains new and updated information. Changes throughout this revision are marked by change bars, as shown to the right of this paragraph.

New and Updated Information

This table contains the changes made to this revision.

Topic	Page
Clearer information on configuring an L2TP connection for a secure tunnel between the 1756-EN2TSC module and a Windows client	Chapter 3

Notes:

The 1756-EN2TSC is a security-enhanced version of the 1756-EN2T EtherNet/IP communication module. This module is designed for applications that need to limit network access to a control system from within the plant network. This module is not intended to connect any devices in the local 1756 backplane to devices outside of the plant firewall.

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

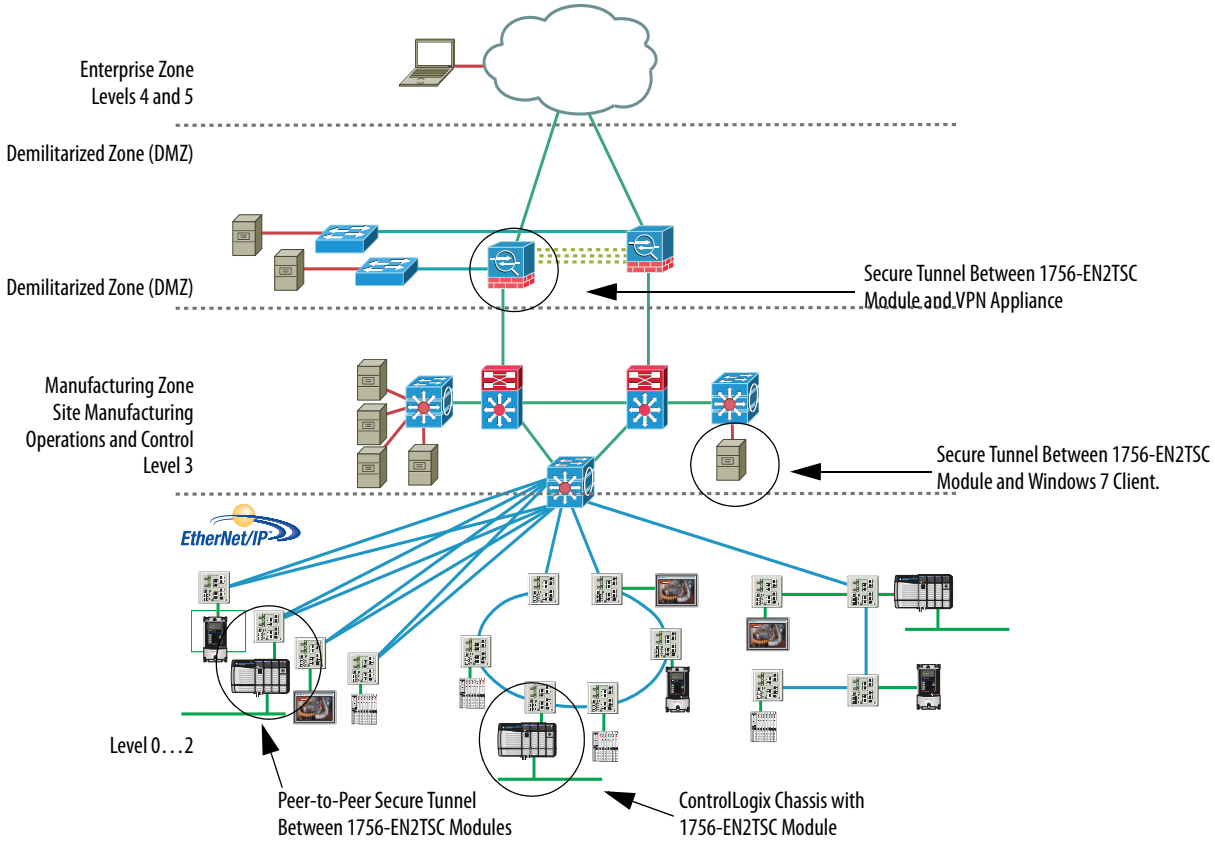
Resource	Description
1756 ControlLogix Communication Modules Specifications Technical Data, publication 1756-TD003	Specifications for ControlLogix communication modules
EtherNet/IP Network Configuration User Manual, publication ENET-UM001	Guidelines for configuring EtherNet/IP network parameters
EtherNet/IP Modules Installation Instructions, publication ENET-IN002	Guidelines for installing EtherNet/IP modules
Ethernet Design Considerations Reference Manual, publication ENET-RM002	Guidelines for Ethernet networks
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Guidelines for installing a Rockwell Automation industrial system
Product Certifications website, http://www.ab.com	Declarations of conformity, certificates, and other certification details

You can view or download publications at http:/www.rockwellautomation.com/literature/. To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

Notes:

Secure Communication Architecture

Many control systems currently use 1756-EN2T and 1756-ENBT modules to connect ControlLogix® systems to plant-level systems. A 1756-EN2TSC module offers the same connectivity, as well as additional security options to protect access to resources on the local backplane from the plant network Use the 1756-EN2TSC module to establish secure tunnels with peer modules, Windows 7 clients, and VPN appliances.



The 1756-EN2TSC module provides a level of protection against unauthorized network access, either malicious or accidental, to a ControlLogix controller via an EtherNet/IP connection. The 1756-EN2TSC module uses the IPsec protocol suite to provide a secure communication tunnel.

The 1756-EN2TSC module is intended for use behind an existing firewall/DMZ that protects the plant network from outside access. This module is not intended to be connected directly to the public Internet or to provide a mechanism by which remote access is provided to a network. The module does not provide the ability to expose a private network address range via IPsec; only the module's IP address is available.

Considerations

Out-of-the-box, the module functions just like a 1756-EN2T module, except that the module does **not** support the following:

- Integrated motion on EtherNet/IP networks
- ControlLogix redundancy systems
- SIL 2 applications
- Email capabilities
- EtherNet/IP socket interface

Once security is enabled, modules like POINT I/O™ adapters, FLEX™ I/O adapters, and PowerFlex® drives are not able to establish a secure connection because they do not support secure tunnels.

When security is enabled, the module connects with:

- Upper level systems and user workstations with Windows 7 operating systems
- Cisco ASA security appliances
- Other 1756-EN2TSC modules

The module supports the current versions of common web browsers, such as Internet Explorer (8 and 9). For security reasons, Secure Sockets Layer (SSL) 2.0 is disabled in the module. Browsers must enable support for cryptographic protocols SSL 3.0 or Transport Layer Security (TLS) 1.0.

The 1756-EN2TSC module lets only those devices with proper credentials access the module. This module is intended for use behind an existing firewall/DMZ that protects the plant network from outside access.

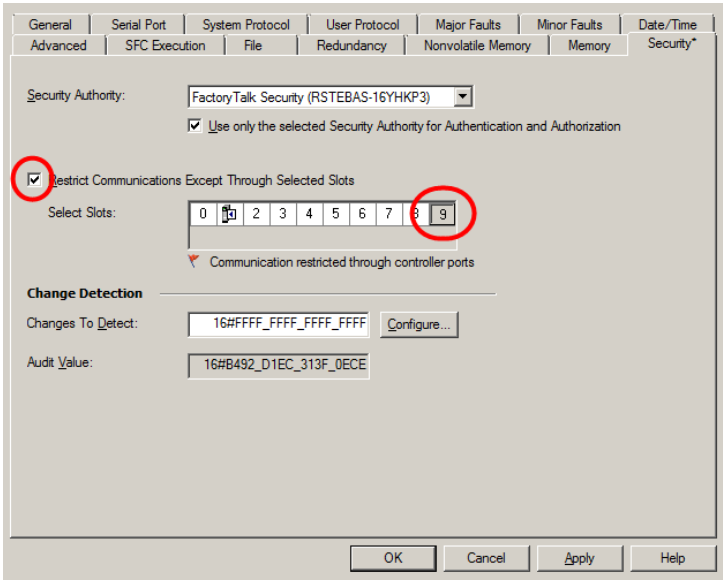
To minimize complexity, the module supports the following authentication and encryption methods.

- IPsec technology with as many as 8 VPN tunnels (only one of which can be a Cisco ASA connection)
- Pre-shared key authentication
- AES encryption (128, 192, and 256 bit)'

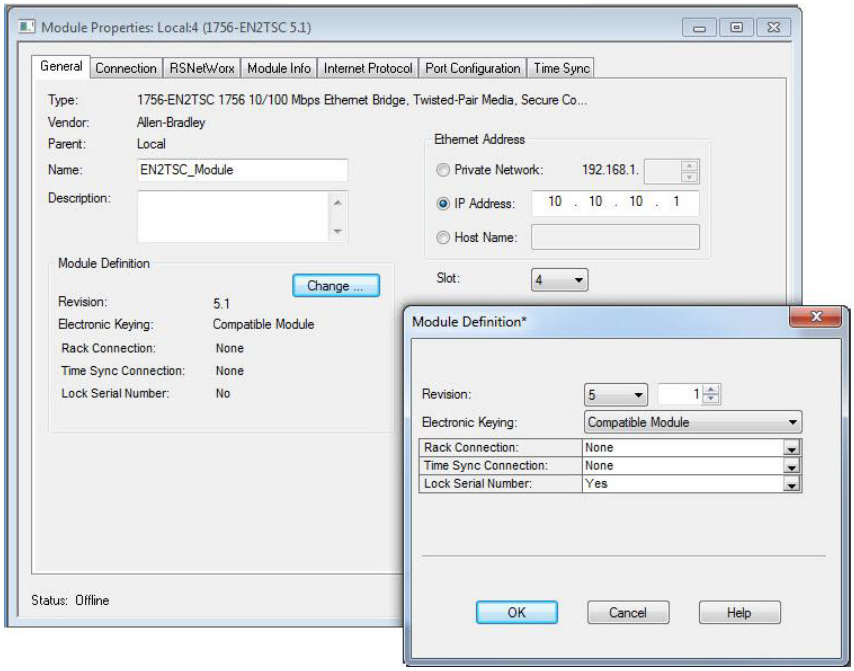
Local Chassis Security

You can use the 1756-EN2TSC module with the following features to prevent unauthorized access to a controller in the local chassis.

- The trusted slot feature (in the controller properties) designates slots in the local chassis as trusted. When the trusted slot feature is enabled, the controller denies communication through paths that are not trusted. This requires authentication to the module for anyone to access the controller with programming software.



- The serial number lock feature (in the 1756-EN2TSC module properties) in conjunction with the trusted slot features restricts communication through a module in the trusted slot with the specific serial number.



The trusted slot and serial number lock features are for applications that have concern with physical access to and tampering with the controller.

IMPORTANT Use caution with these features and make sure you have the controller project backed up in a secure location. If the module becomes disabled for any reason, you have to download to the controller to recover.

Network Access Security

The 1756-EN2TSC module uses the Internet Protocol Security (IPsec) technology to provide secure communication over the Ethernet network. IPsec is widely-deployed, and is often used to create Virtual Private Networks (VPN). IPsec provides the following security features:

- Authentication of the communication end points (both client and server)
- Data authenticity and integrity (via message integrity checks)
- Data confidentiality (via encryption algorithms)

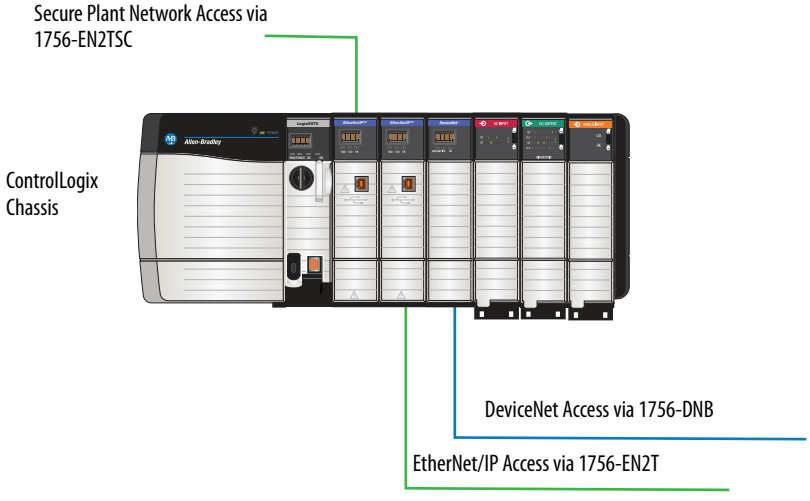
Use of the IPsec protocol suite lets you use the Microsoft Windows VPN client to connect securely to the module. IPsec also lets the module create secure tunnels with other 1756-EN2TSC modules and with off-the-shelf, VPN appliances.

IMPORTANT The module does **not** provide access to a private network.

While the module supports secure communication, the module is not intended to be connected directly to the public Internet and provide a VPN function, or be the mechanism by which remote access is provided to a network. The module does not provide the ability to expose a private network address range via IPsec—only the module's IP address is available.

The module does the following:

- Secures access to the controller and I/O modules in the local chassis
- Secures bridge access to other networks accessible within the local chassis



As part of establishing the secure tunnel, both endpoints must authenticate with each other and exchange information to ensure secure data transfer. When security is enabled, the module is able to connect only with the following:

- Upper level systems and user workstations with Windows 7 operating systems
- Cisco ASA security appliances
- Other 1756-EN2TSC modules

IPsec Association

Once the IPsec association is established, data between the two endpoints is fully encrypted (except for produced/consumed tags) or optionally sent unencrypted, but with a cryptographic message integrity code.

Capability	Description
Authentication Method	Pre-shared key (PSK). Configure a secret key on each of the endpoints.
Header Format	Encapsulating Security Payload (ESP)
Mode	Tunnel mode, default Transport mode if the module cannot negotiate tunnel mode (such as a Microsoft Windows 7 client)
Internet Key Exchange	• IKE version 1 • IKE version 2
Lifetime(s)	IKE and IPsec lifetimes user-configurable
PFS Group	None
DH Key Group	Group 2 = modp1024, default Groups 5,14,15,16,17, and 18 supported
IKE Encryption Algorithm	• AES(128 bit) • AES(192 bit) • AES(256 bit)
IKE Authentication Algorithm	SHA-1
IPsec Encryption Algorithm	• AES(128 bit) • AES(192 bit) • AES(256 bit) • None
IPsec Authentication Algorithm	SHA-1

As long as the IPsec traffic is received, the connection is considered alive. Your VPN connection can recover without having to re-authenticate if you lose your connection for a very short period of time (few seconds). However, if the time since the last received packet is greater than the timeout interval, the connection times out. This interval is common to all IPsec connections and is not configurable. The default keepalive-timeout is 30 seconds.

Performance

The basic communication capability of the module is the same as the 1756-EN2T module.

- The module supports the same number of TCP and CIP connections as the 1756-EN2T module (256 CIP connections and 128 TCP/IP connections).
- The module supports configuration of IPsec associations with as many as 8 IP addresses (devices); only 1 of which can be a Cisco ASA connection.
- The module supports CIP Sync communication.

Traffic Filtering

When IPsec is enabled, the module blocks traffic that is not received via a VPN client, another peer with an IPsec connection, or an appliance with an IPsec connection, with these exceptions:

- BOOTP/DHCP traffic (to let the module obtain an IP address)
- HTTPS traffic (needed to configure the module)
- CIP Sync packets (you have the option to disable CIP Sync)
- Logix produced/consumed tags (the establishment of the produced/consumed connection occurs over via IPsec)
- 1756 I/O connections in a remote chassis

If the 1756-EN2TSC module is the trusted slot for a ControlLogix chassis, the following traffic to the controller must go through the 1756-EN2TSC module.

- RSLinx® Classic traffic (such as Studio 5000™ and ControlFLASH communication)
- RSLinx Enterprise traffic (such as FactoryTalk View® SE and FactoryTalk View ME communication)

Get Started

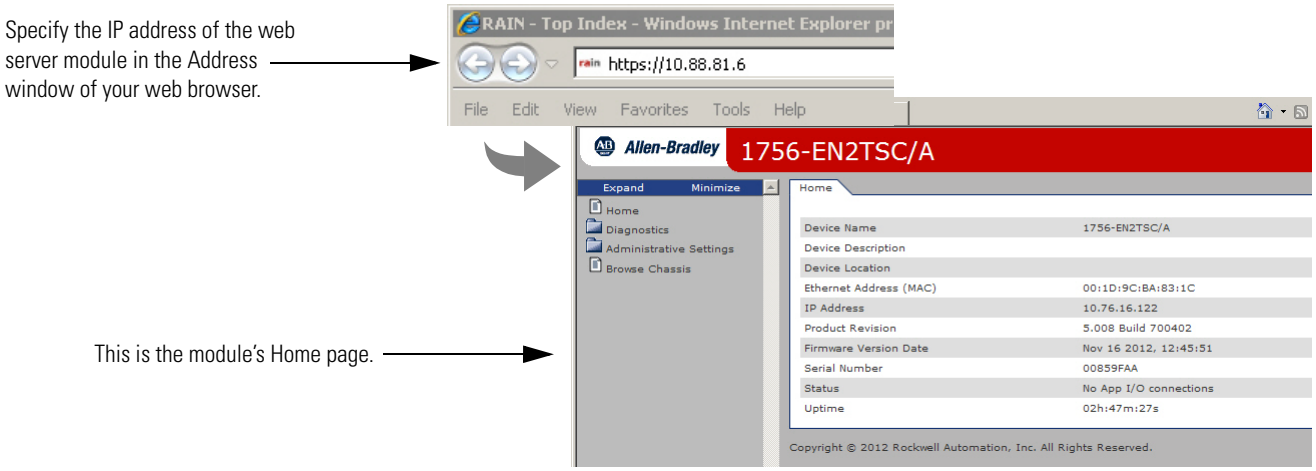
This chapter describes the initial configuration settings required for the module. After setting up the module, see the next chapters for security configuration examples.

For information on installing the module, see EtherNet/IP Network Modules Installation Instructions, publication ENET-IN002.

Add the module to a controller project the same as you add a 1756-EN2T module. All security-related configuration is via the module web pages.

IMPORTANT When you finish using the web pages, close the web browser. This prevents any user on a shared computer from accessing the web pages.

Configure all security parameters via the web server. In the Address field of your web browser, enter the IP address that displays on the front of the module.



'The 1756-EN2TSC module has an embedded HTTPS server that it uses to provide secure web communication. An HTTPS server uses a certificate so that the client can verify server authenticity. For web sites connected to the Internet, certificates are normally signed by a trusted certificate authority. Web browsers are then able to verify the authenticity of the web server by virtue of its certificate.

The module comes with a self-signed certificate because the module is not directly connections to the Internet. Self-signed certificates are not signed by a known, trusted authority, so they must explicitly be accepted by the user when connecting via the web browser.

Initial Powerup

On initial powerup, the module generates a new certificate for the embedded HTTPS server. This can take up to several minutes. During this process, the message 'SSL certificate generation in progress' is shown on the module display. Wait until the module is fully booted and 'OK' is shown on the display before accessing the module by using a web browser.

1. In the Address field of your web browser, enter the IP address that displays on the front of the module.

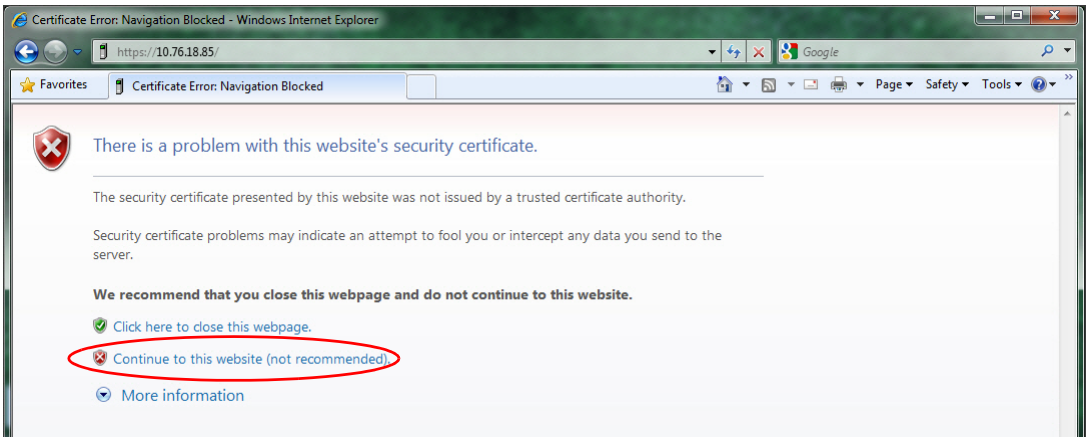
IMPORTANT	When you enter the IP address, you must enter the prefix https:// in the address. If you enter an http:// prefix, the module redirects to the https:// prefix.

2. After the web browser connects to the server, a warning message is shown about the certificate not being signed by a trusted authority.

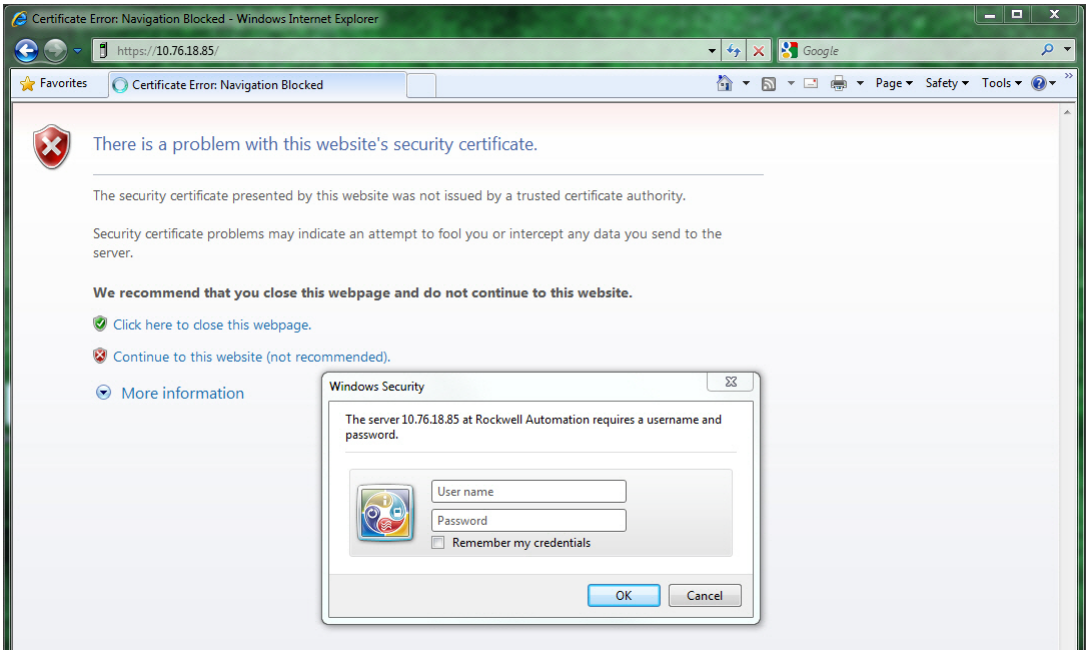
   Accept this message and continue to the web page.

IMPORTANT In general, do not accept the certificate not being signed by a trusted authority. But in the case of initial powerup, the module has a self-signed certificate, so continue to the website even though the message says this option is not recommended.

The self-signed certificate warning continues to display unless you add the certificate to the list of exceptions for the web browser.



3. After accepting the self-signed certificate, enter the user name and password.



Default Credentials

Default credentials are case sensitive and are as follows:

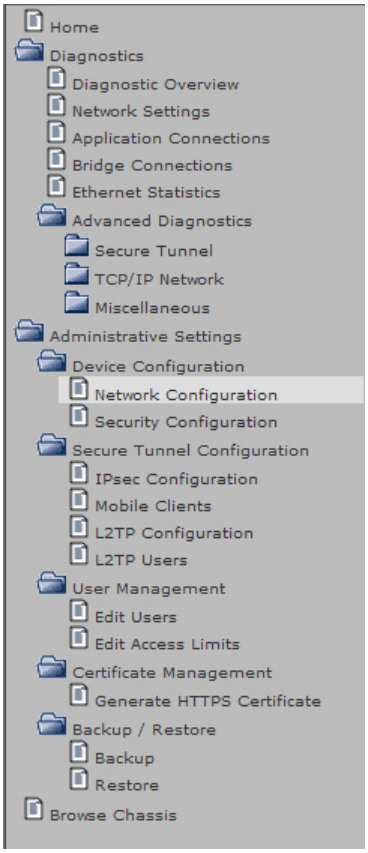
- User name: Administrator
- Password: admin

You are prompted to change the password on the Administrator account. Enter the new password and click Change.

The browser prompts you to authenticate again. Use the Administrator user name and new password.

Configuration Overview

The left pane of the web browser is a navigation tree to configure and maintain the module.



See the next chapters in this manual for different security configurations.

Assign Network Settings

By default, the module is BOOTP enabled.

IMPORTANT Do not simply configure the initial address assigned to the module as a static IP address. Contact your network administrator for an appropriate static IP address.

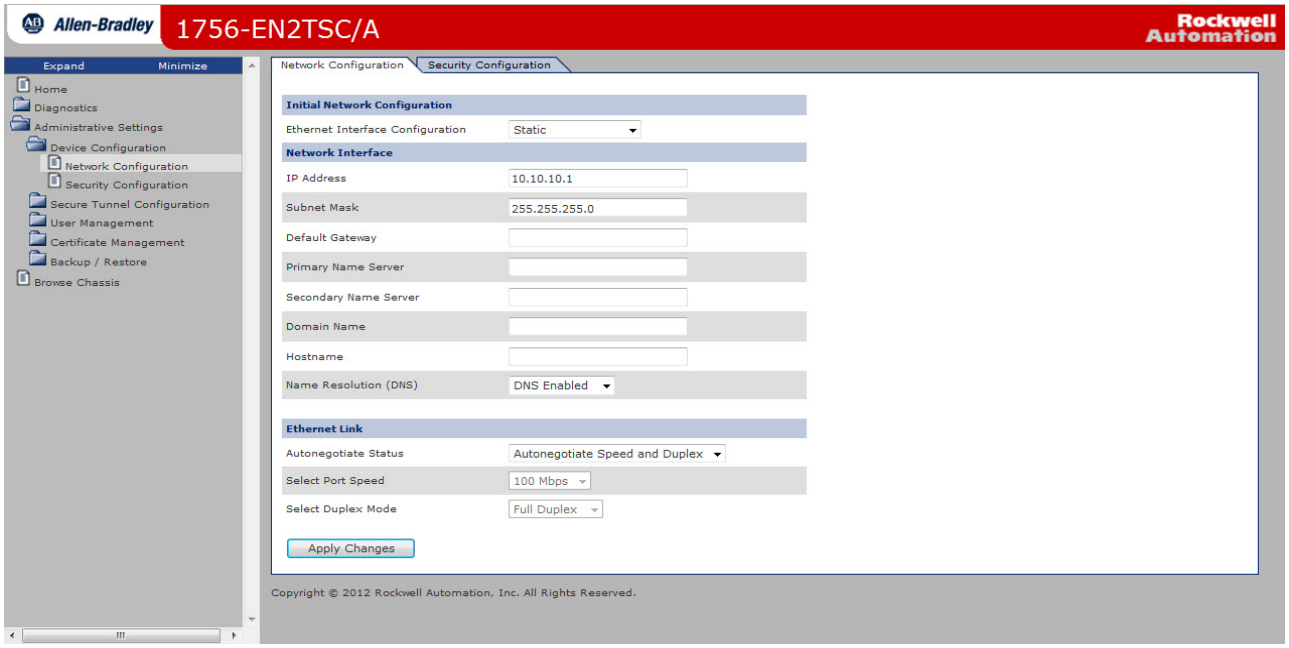
Choose one of the following methods to assign an IP address.

- Rotary switches on the module (before you install the module)
- Rockwell BOOTP/DHCP utility (available with RSLinx and Studio 5000 software)
- RSLinx software
- Studio 5000 software

For information on assigning network parameters, see EtherNet/IP Network Configuration User Manual, publication ENET-UM001.

Change Network Settings via the Module Web Page

Choose Administrative Settings > Device Configuration > Network Configuration. An authenticated user can modify network parameters.



In This Field	Specify
Ethernet Interface Configuration	The network configuration scheme: • Dynamic BOOTP (default) • Dynamic DHCP • Static
IP Address	IP address for the module: If you want to specify a static IP address for the module, you must also choose Static for the Ethernet Interface Configuration field.
Subnet Mask	Subnet mask for the module.
Default Gateway	Gateway address for the module.
Primary Server Name Secondary Server Name	DNS server addresses, if you are using DNS addressing within your Logix program.
Domain Name	Domain name for the web server module, if you are using DNS addressing within your Logix program.
Host Name	Host name for the module.
Name Resolution (DNS)	Whether the module uses DNS addressing within your Logix program.
Autonegotiate Status	How to determine port speed and duplex: • Autonegotiate speed and duplex (recommended) • Force speed and duplex
Select Port Speed	Port speed (10 Mbps or 100 Mbps), if you chose to force speed and duplex.
Select Duplex Mode	Duplex (full or half), if you chose to force speed and duplex.

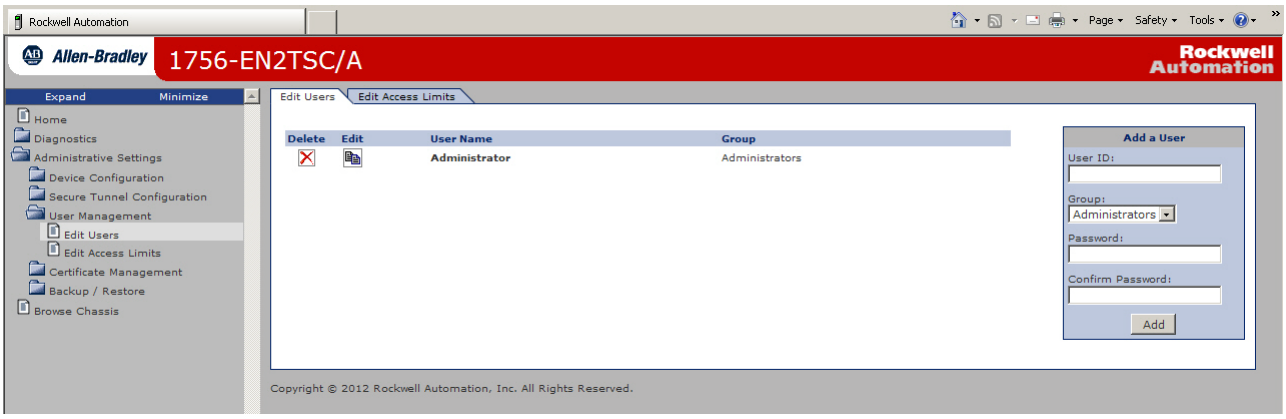
Create User Accounts

You can define user accounts for the web interface to the module. These accounts are typically for administrators or others who need to access the module's diagnostic information.

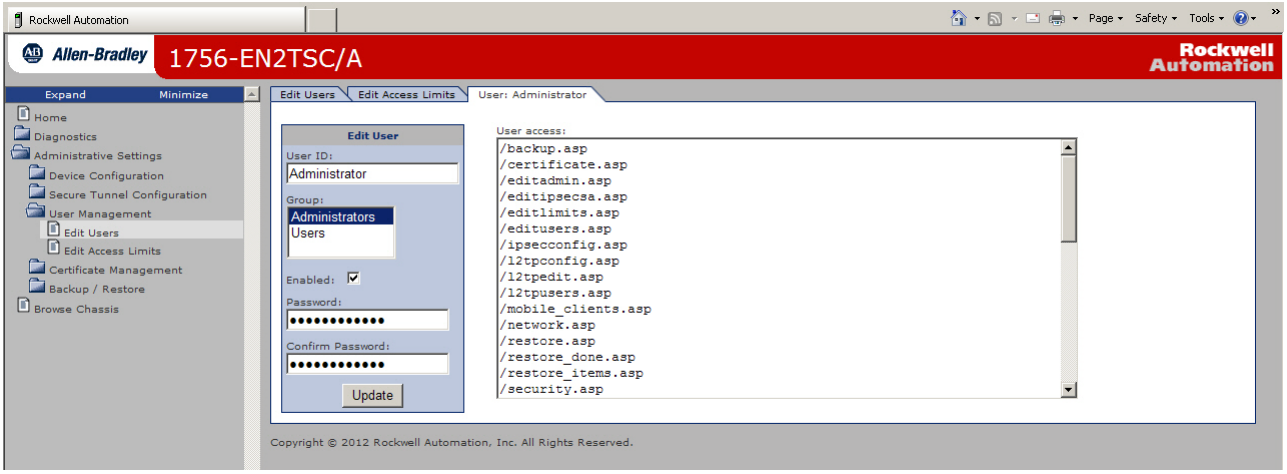
Assign user accounts with access levels to manage who has access to change configuration or to view module information. Define each user as a member of the Users group or the Administrators group. Members of the Administrators group have all access rights to the module. Administrators can limit access of members in the Users group by editing their access limits.

Every user is authenticated by a user name and a password.

To add or remove a user, access Administrative Settings > User Management > Edit Users.



To edit an existing user, click the Edit icon.



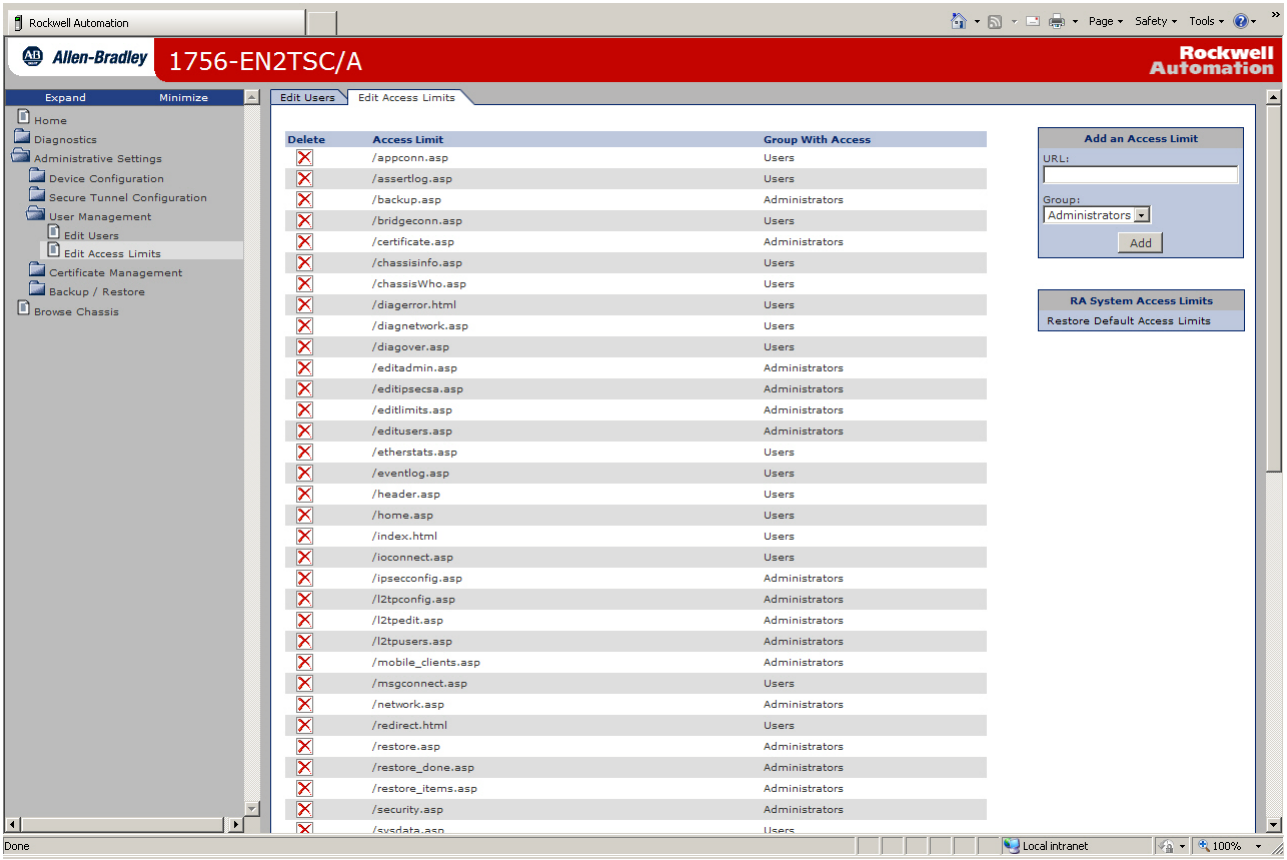
From this form, you can change the following:

- Password
- Group membership
- Status (enabled or disabled)

You cannot change the user name.

Edit Access Limits

To add or remove access rights for a user to web pages, access Administrative Settings > User Management > Edit Access Limits.



Default access limits allow members of the Users group to access status and diagnostic pages and diagnostics, but limit configuration pages to members of the Administrators group.

IMPORTANT Do not remove default access limits because that makes them available without authentication.

Some web pages use both .asp, form, and URL elements. In such cases, each element is represented by a separate access limit. For example, the 'Edit Access Limits' web page is composed of the following:

- editlimits.asp to generate a list of access limits
- /rokform/AddAccessLimits to add or update an existing limit
- /rokform/DeleteAccessLimit to delete an existing limit

IMPORTANT Limiting access to the .asp file is not enough to limit its functionality. If unsecured, a form handler could be used with externally prepared request.

Generate HTTPS Certificate

You can generate a new HTTPS certificate if needed. This is optional as the module automatically generates a certificate when the module is turned on for the first time after factory reset.

- The certificate generated at first powerup of the module is not bound to any specific IP address. This can cause the browser to report a certificate error and you can decide whether to generate a new certificate.
- If you generate a new certificate and then later change the IP address of the module, the current certificate becomes invalid. Generate a new certificate that uses the new IP address; otherwise the browser reports a certificate error.

A newly-generated certificate has an advantage that the module uses the current IP address. This can limit web browser certificate warnings, even though the browser can still report an error due to a self-signed certificate.

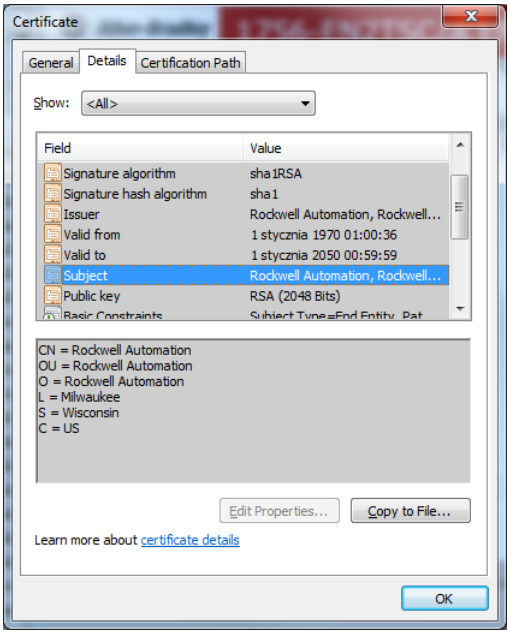
You can specify the validity period of the certificate you generate. The period is set from the current time on the module to a specified end time. Synchronize the real-time clock on the Logix5000 controller with the current time. Generating a short-validity period without the clock being synchronized can generate an outdated certificate.

To generate a new certificate, choose Administrative Settings > Certificate Management > Generate HTTPS Certificate.

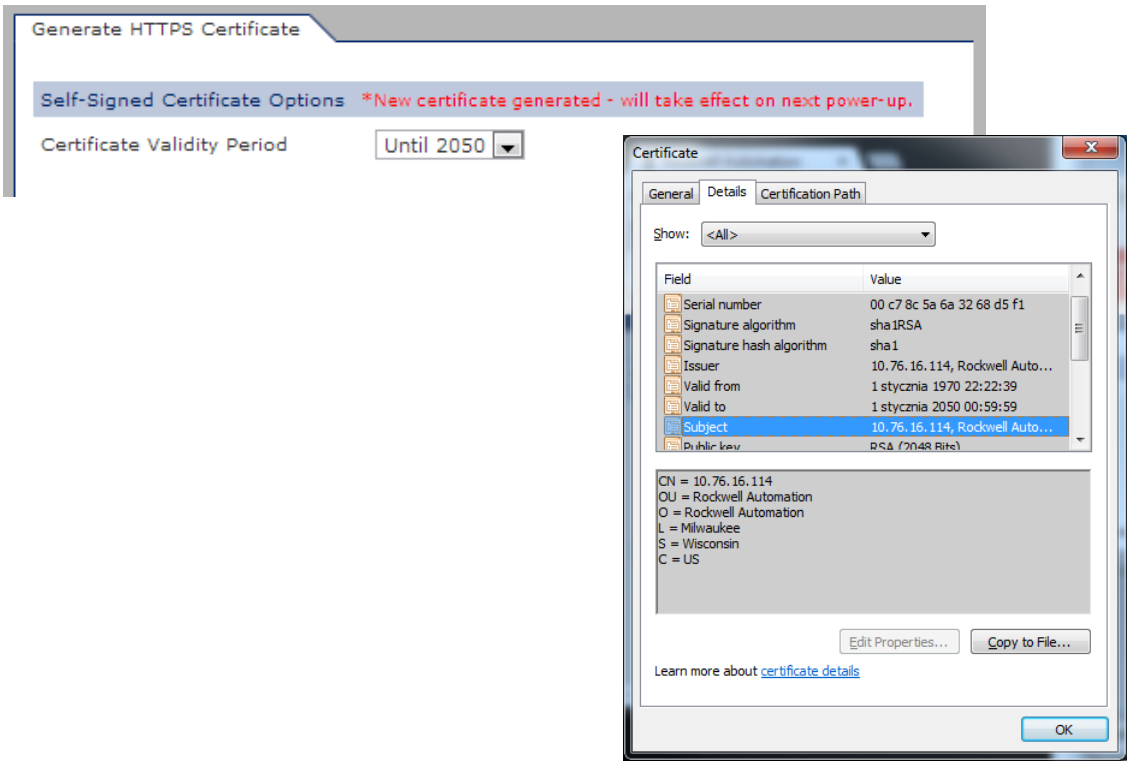
Use the pull-down menu to choose a valid length of time for the certificate to be enabled.

Certificates

On initial powerup, the subject common name (CN) of the self-generated certificate is set to Rockwell Automation.

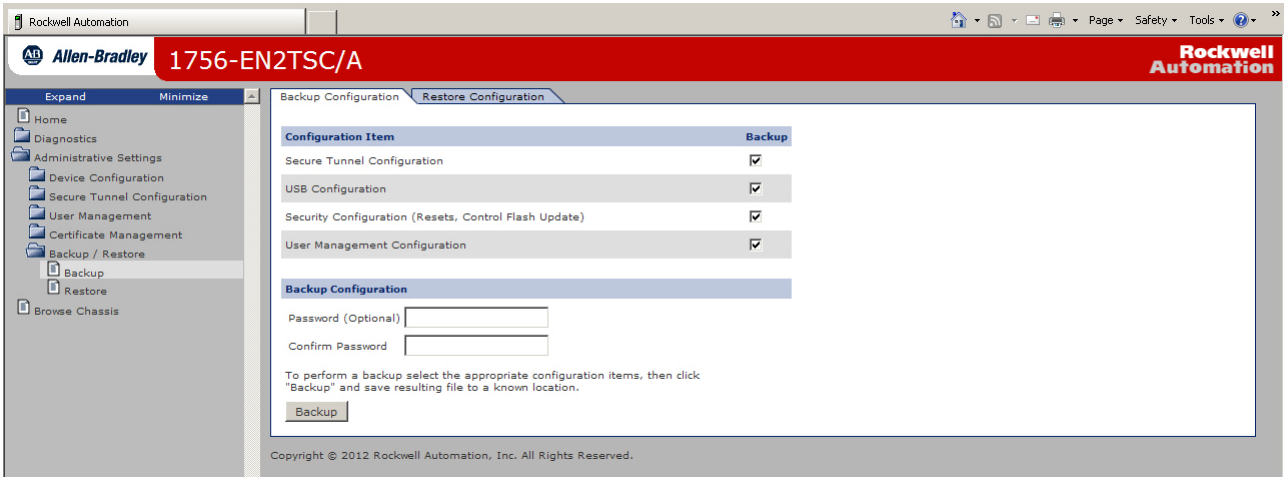


When you generate a new certificate, the CN is changed to the IP address of the module and the new certificate is applied at the next restart of the module.



Backup / Restore

To back up module configuration, choose Administrative Settings > Backup / Restore > Backup.



Choose which items to include in the back-up configuration.

Configuration Item	Description
Secure Tunnel Configuration	Secure tunnel settings: • IPsec Configuration • Mobile Clients • L2TP Configuration • L2TP Users
USB Configuration	USB port enable/disable status
Security Configuration	Security settings: • 888 Factory Reset • Remote Factory Reset • Remote Reset • Control Flash Update
User Management Configuration	User management settings • Users, passwords, groups • Access limits

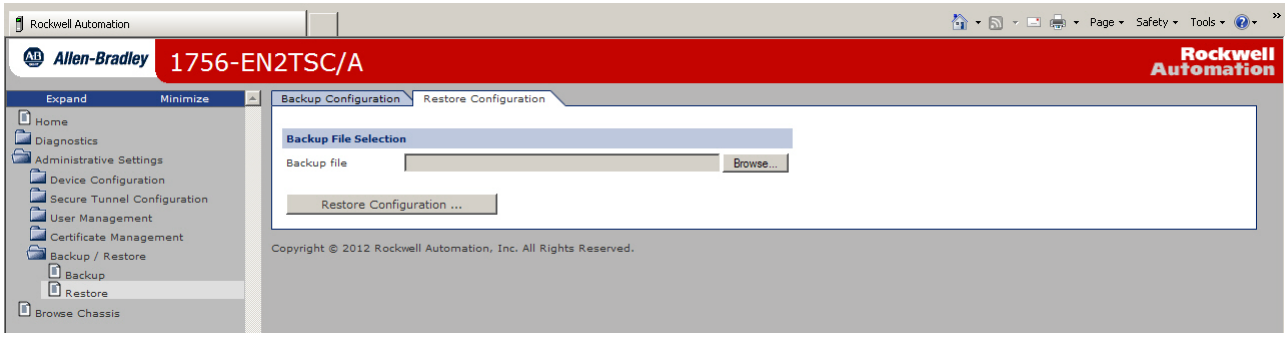
You can also enter a password if you need to protect the back-up file.

To restore module configuration, choose Administrative Settings > Backup / Restore > Restore.

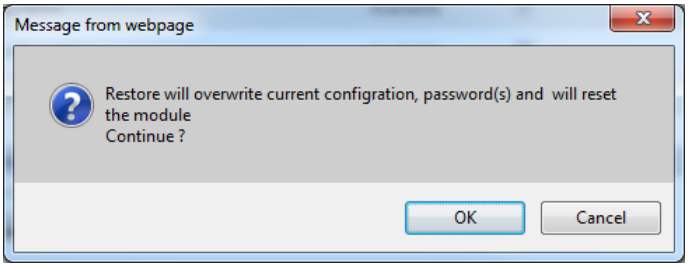
IMPORTANT Restoring a configuration overwrites the current configuration settings in the module, including user names and passwords. The restore operation can result in changes that do not allow further web access to the device.

To reduce this risk, the 888 Factory Reset feature is enabled after every restore. If you want to disable this feature, you must do so manually.

1. Specify the back-up file to use.



2. If the back-up file is password protected, enter the password when prompted.
3. When prompted that the restore overwrites the module, click OK.

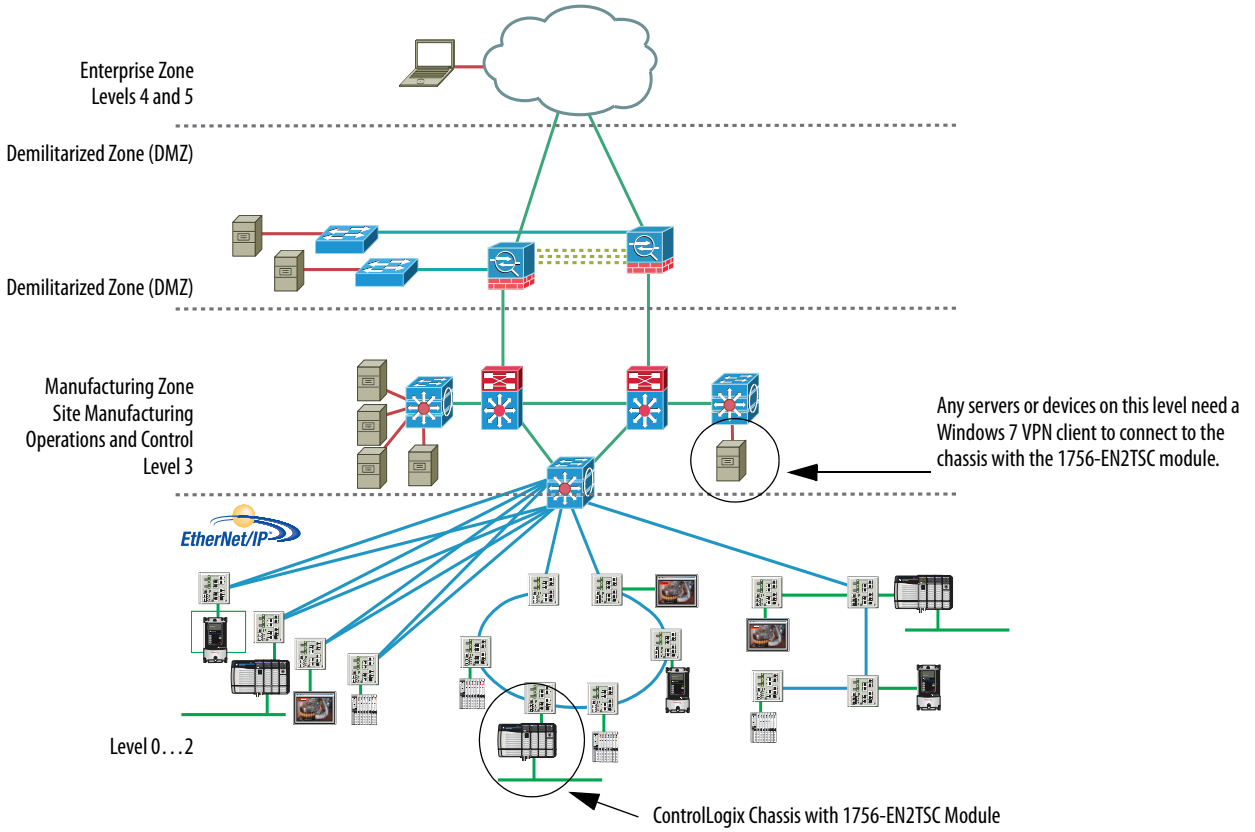


When the restore is complete, the module displays a status message.

The module is now configured so that the 888 Factory Reset feature is enabled in case you need to reset the module to factory settings.

Configure a Secure Connection to a Microsoft Windows Client

In this scenario a Microsoft Windows 7 client establishes an IPsec association with the 1756-EN2TSC module.



An example of a Windows 7 client is a personal computer running Studio 5000, FactoryTalk View, or RSLinx software.

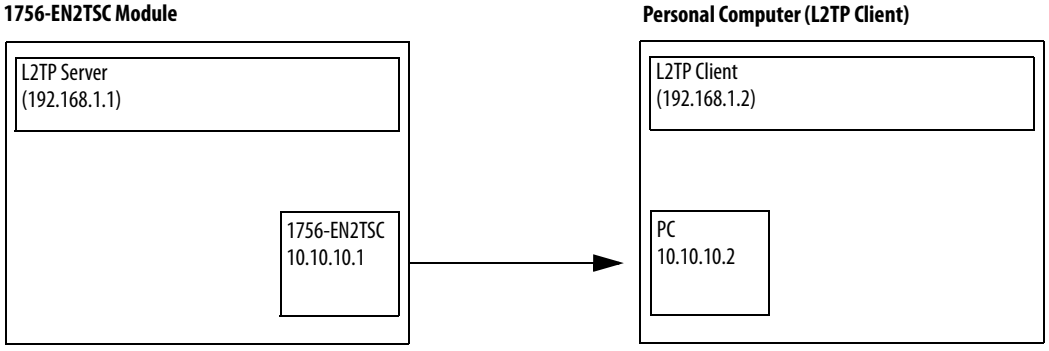
To configure this secure connection, do the following.

1. Configure the 1756-EN2TSC module to support a connection to a mobile client.
2. Configure a connection to the Microsoft Windows client.
3. Open the connection.

L2TP Connections

The 1756-EN2TSC module uses Layer 2 Tunneling Protocol (L2TP) connections for Windows clients. Communication occurs within an L2TP tunnel (after VPN is already running). The server IP address is used to communicate with the module. The client IP address is assigned from the client address pool.

All communication generated by software products, such as RSLinx software, to an L2TP server address of a 1756-EN2TSC module is sent via an IPsec connection. This diagram shows how the physical and L2TP IP addresses differ.



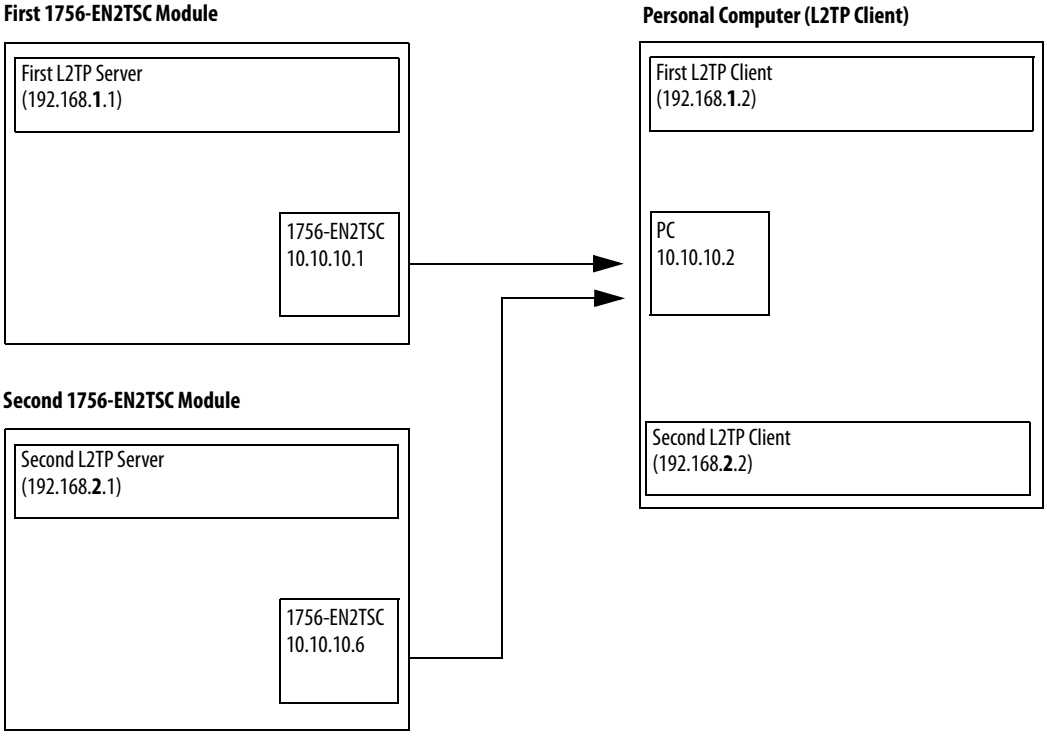
- Client, physical IP address 10.10.10.2
- 1756-EN2TSC module, physical IP address 10.10.10.1
- L2TP server, virtual IP address 192.168.1.1
- L2TP client, pool of virtual IP addresses start 192.168.1.2 and end 192.168.1.100

The client uses IP address 10.10.10.2 to establish a connection with the 1756-EN2TSC module at IP address 10.10.10.1. The L2TP server on the 1756-EN2TSC module at IP address 192.168.1.1 establishes a secure connection with the L2TP client on the client at an IP address from the pool 192.168.1.2 through 192.168.1.100.

Once the pool of addresses is configured, that pool is reserved for that specific 1756-EN2TSC module. If you have a second 1756-EN2TSC module in the same controller chassis, you must use a separate subnet (such as 192.168.2.1), even though the pool from the first address is not completely used.

The Microsoft IPSec client uses classful network-addressing architecture.

- The traffic from a Windows client is directed to a specific VPN based on the class of the IP address set in the L2TP configuration.
- Class C addresses (192.168.0.0 through 192.168.255.255) provide the fewest addresses and supports as many as 256 non-overlapping subnets. Class C addresses also ensure that no IP address is masked by the active VPN connection.
- Two 1756-EN2TSC modules connected to the same Windows client at the same time must be assigned to non-overlapping subnets. Once the secure tunnel exists, RSLinx software uses the L2TP server IP addresses to communicate with the controllers through the 1756-EN2TSC modules.

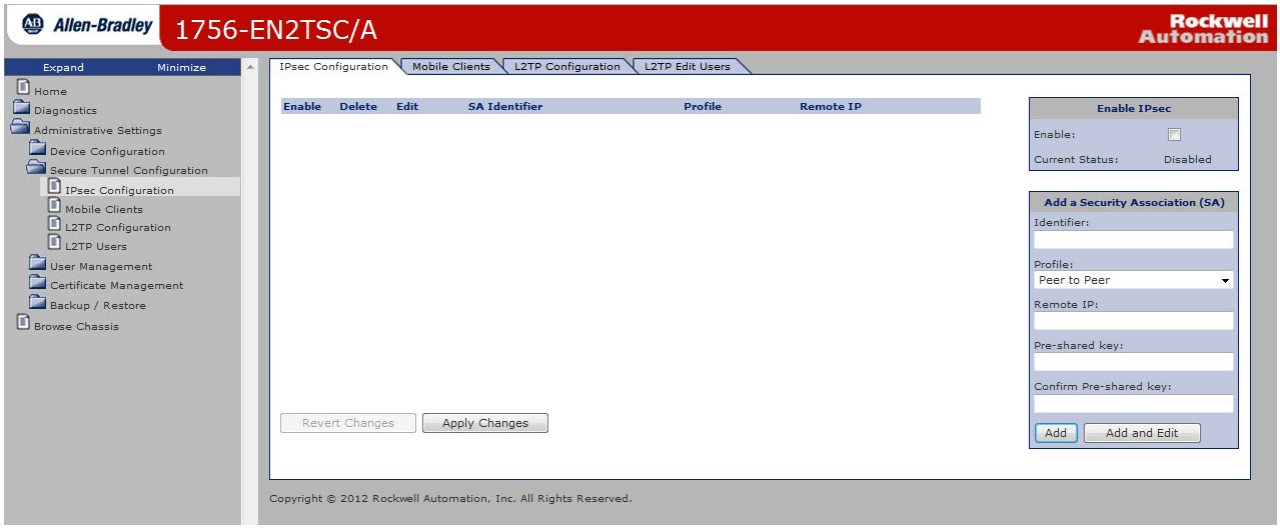


Configure a Mobile Client

A mobile client does not have a predetermined IP address explicitly configured in the module. For example, a personal computer configured for DHCP connects to the module. If the IP address of the personal computer changes, no configuration changes are required on the module.

If the Windows client is a mobile client, make the following configurations on the module.

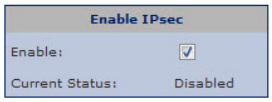
1. Log in to the 1756-EN2TSC module and choose Administrative Settings > Secure Tunnel Configuration> IPsec Configuration.

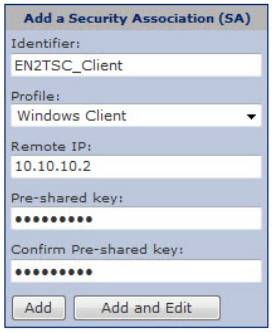


2. On the right side of the screen, check Enable to enable IPsec connections.
3. In the Add a Security Association (SA) area, do the following.
   a. Enter the Identifier as a text description of the connection.
   b. Choose the Windows Client profile.
   c. Enter the Remote IP address.

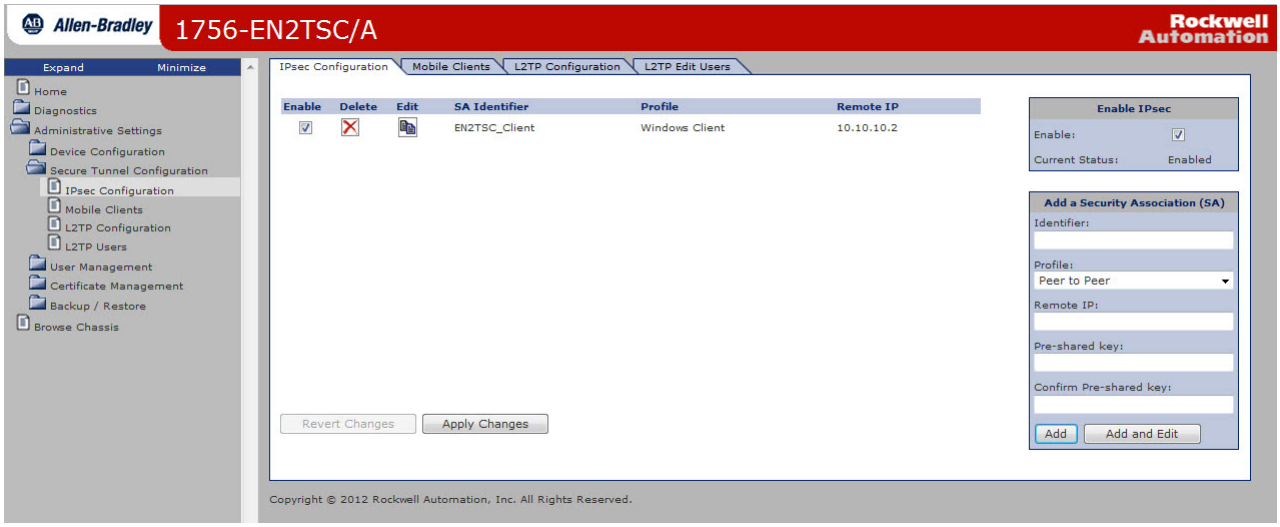
      The Windows client does not use this field but you must enter a value to complete the configuration. Enter the physical IP address of the client (10.10.10.2 in the above examples) to help identify the secure tunnel and the client. This address is for display purposes only and does not affect configuration.
   d. Enter the pre-shared key and confirm the pre-shared key.

      A pre-shared key is similar to a password. Enter a phrase or set of characters. For example, you could enter 'rockwell' as a pre-shared key. Remember the pre-shared key. You enter the same value when you configure the Windows connection (see page 39).

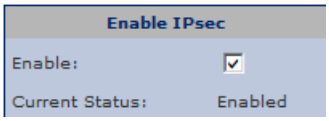




4. Click Add.
5. Click Apply Changes.



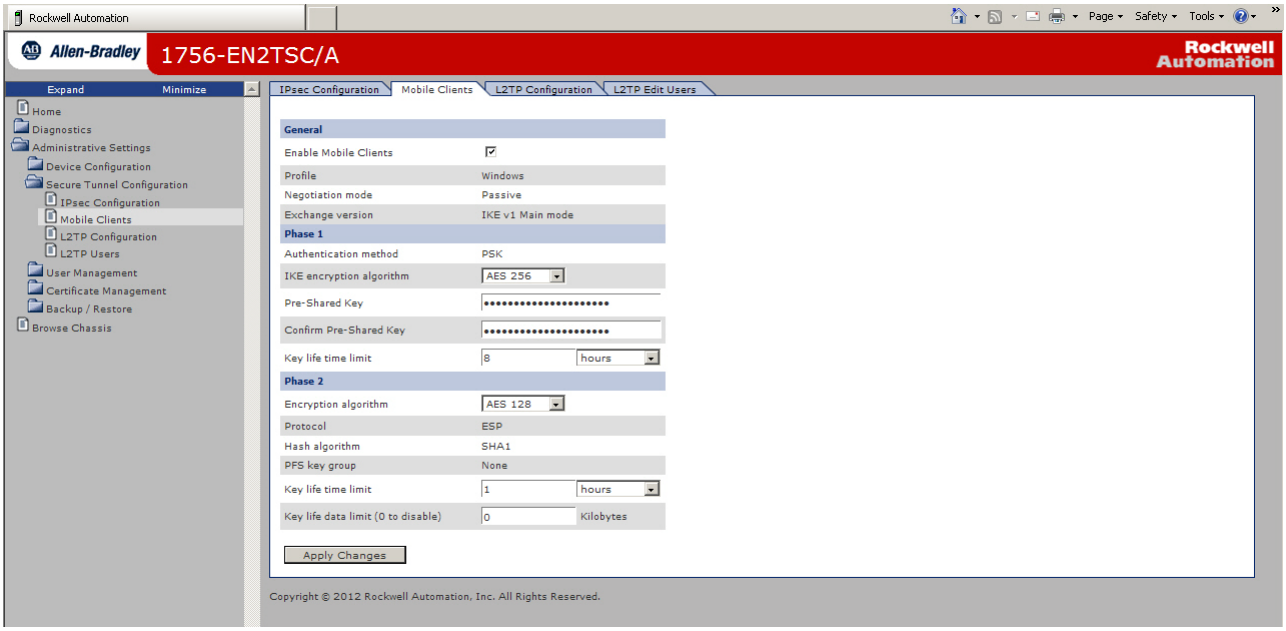
6. Verify IPsec connections are enabled.



7. Choose Administrative Settings > Secure Tunnel Configuration> Mobile Clients.

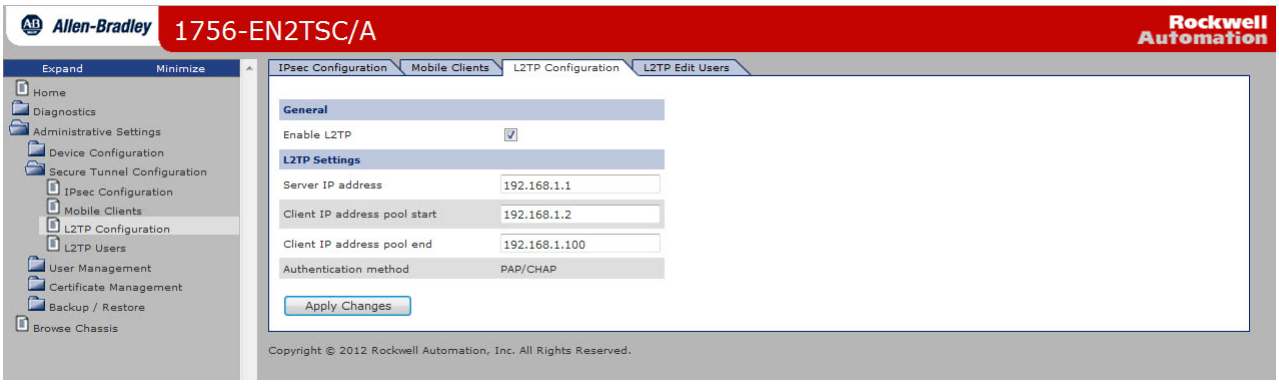
8. Make the following configuration selections.
   a. Check Enable Mobile Clients.
   b. Enter the pre-shared key and confirm the pre-shared key.

      If there are already characters in the pre-shared key field, delete those characters and re-enter the same pre-shared key you entered on the IPsec Configuration tab.
   c. Choose an encryption algorithm.



9. Click Apply Changes.
10. Choose Administrative Settings > Secure Tunnel Configuration> L2TP Configuration.

    Make sure L2TP is enabled.



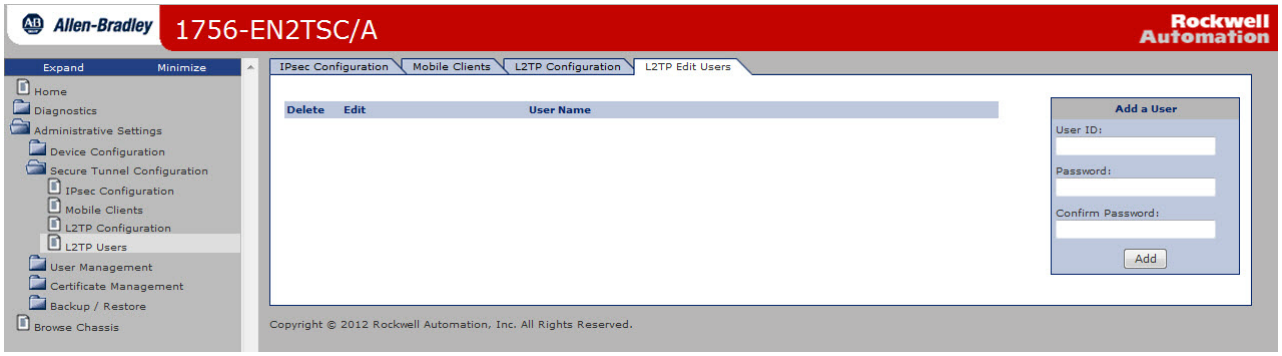
11. If needed, change the range of available client IP addresses

The IP addresses on this screen are the virtual IP addresses for the L2TP server (in the 1756-EN2TSC module) and the pool of virtual IP addresses (for Windows clients).

Once the secure tunnel is established, use the L2TP server IP address to identify the 1756-EN2TSC module. The Windows client will use an IP address from the L2TP pool.

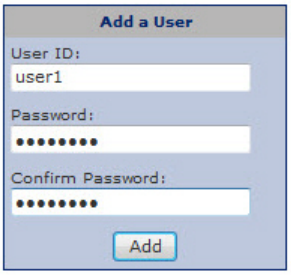
12. Click Apply Changes.

13. Choose Administrative Settings > Secure Tunnel Configuration> L2TP Users.

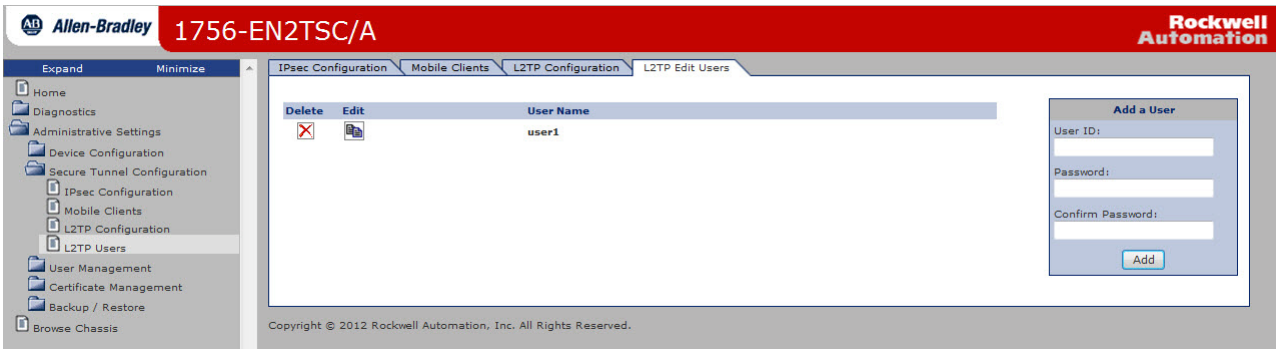


14. For each user, define a user ID and password.

Each L2TP user must authenticate when establishing a tunnel to the module. Configure a user name and password for each LT2P user. Remember the user names and passwords. You enter the same values when you configure the Windows connection (see page 30).



15. Click Add.

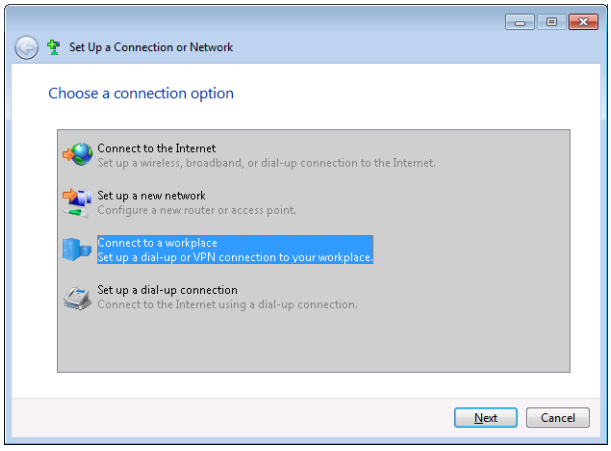


Configure a Connection to a Microsoft Windows Client

An IPsec client is required to make a secure connection to the module. Without an active IPsec association, the module drops packets, which appear as message timeouts. The IPsec client comes pre-installed in the Windows 7 operating system.

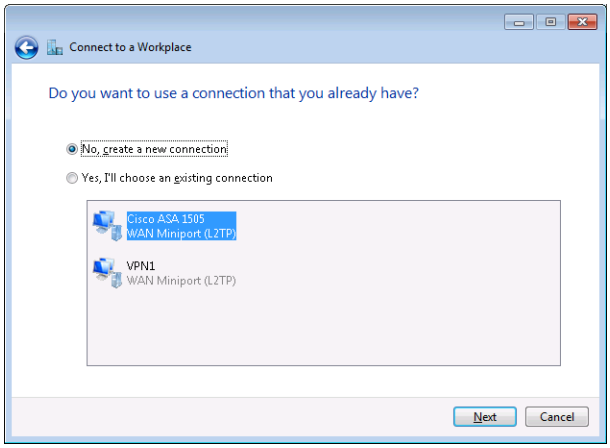
To configure a Microsoft Windows client, do the following.

1. From the Control Panel, open the Network and Sharing Center.
2. Click Setup a new connection or network.
3. Select Connect to a workplace and click Next.

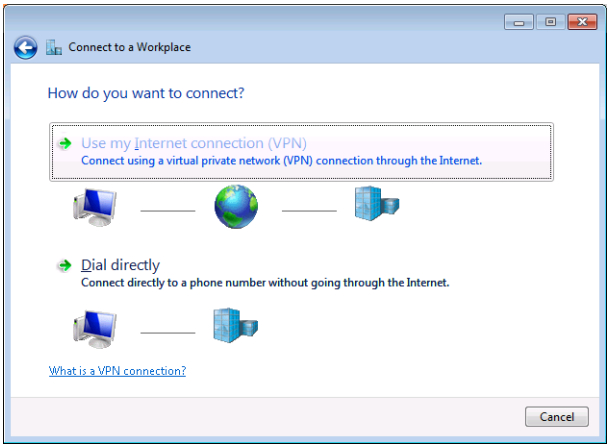


4. Select No, create a new connection and click Next.

   You do not see this screen if there are no connections set.

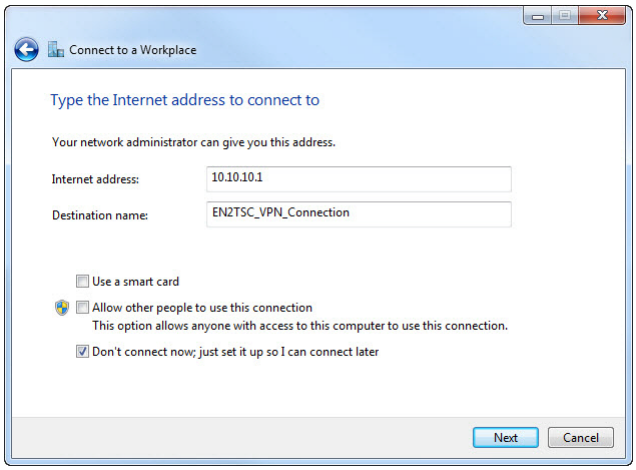


5. Choose Connect using a virtual private network (VPN) connection through the internet.



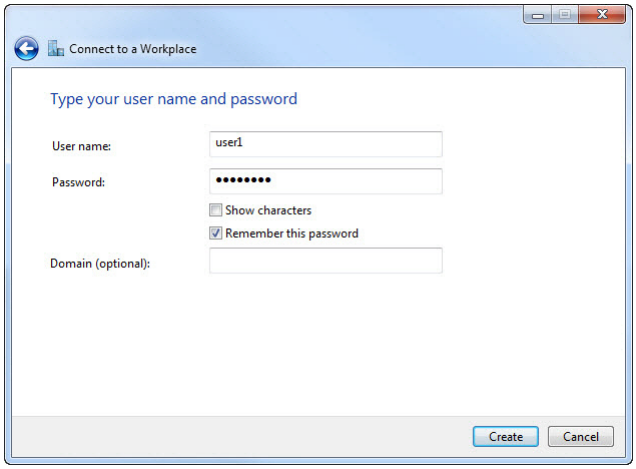
6. If prompted, choose I'll set up an Internet connection later.

7. Enter the physical IP address of the 1756-EN2TSC module and a name for the connection.
8. Select Don't connect now; just set it up so I can connect later and click Next.



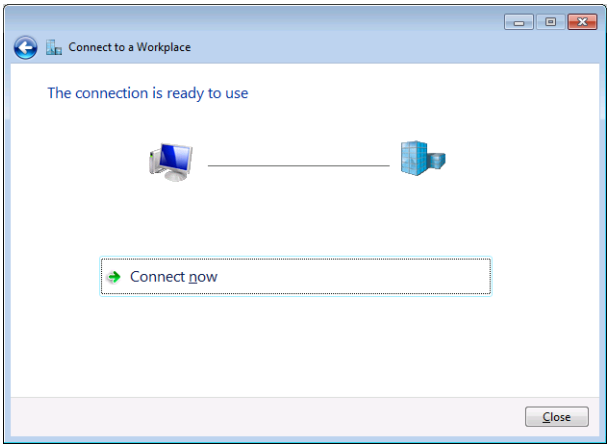
9. Enter the appropriate user name and password.

   The user name and password must have already been configured as an L2TP user on the 1756-EN2TSC module. See the L2TP Edit Users tab as part of configuring the 1756-EN2TSC module (page 33).



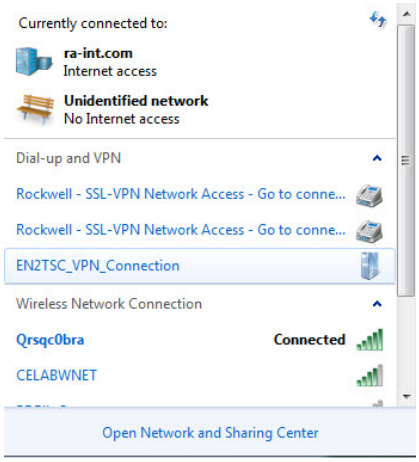
10. Check Remember this password.
11. Click Create.

12. Once the connection is created, click Close.

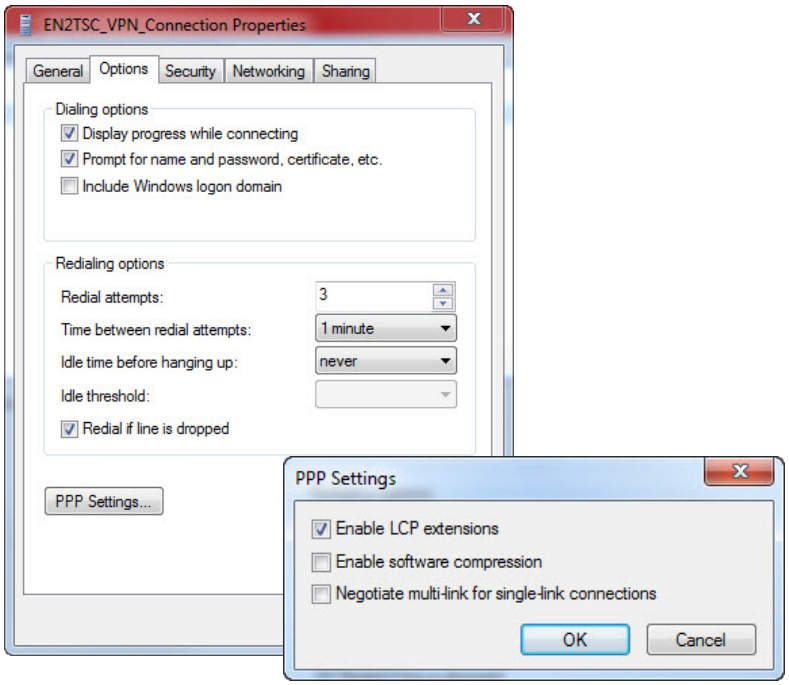


13. Click the network icon in the right, bottom corner of the Windows taskbar.

14. Select the created connection, right-click, and choose Properties.



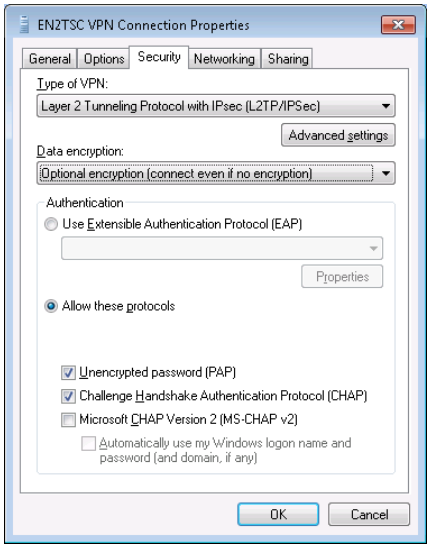
15. On the Options tab, do the following.
    a. Check Display progress while connecting.
    b. Check Prompt for name and password, certificate, etc.
    c. Clear Include Windows logon domain.
    d. Accept the defaults for PPP settings.



16. On the Security tab, do the following.
    a. Choose Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec) as the type of VPN.
    b. Choose Optional encryption (connect even if no encryption) as the type of data encryption.

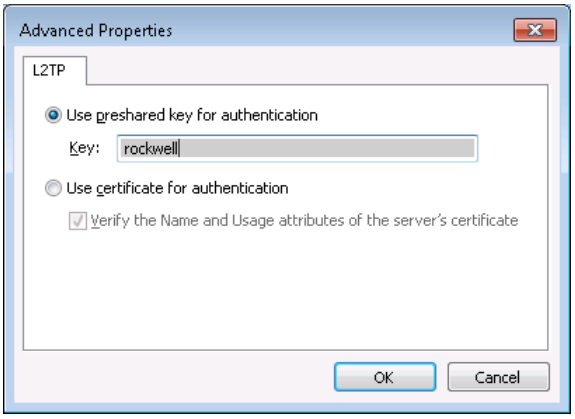
> **IMPORTANT** This setting means that the L2TP configuration does not enforce encryption, but there still is IPsec encryption.

    c. Click Allow these protocols.
    d. Check Unencrypted password (PAP).
    e. Check Challenge Handshake Authentication Protocol (CHAP).
    f. Clear the Microsoft CHAP version 2 (MS-CHAP v2) checkbox.

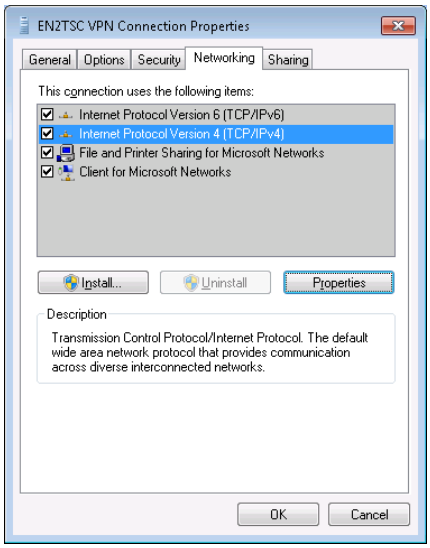


17. On the Security tab, click Advanced Settings and enter the pre-shared key.

    The pre-shared key must be same as defined for the mobile client as part of configuring the 1756-EN2TSC module (page 29).



18. On the Networking tab, check Internet Protocol Version 4 (TCP/IPv4).



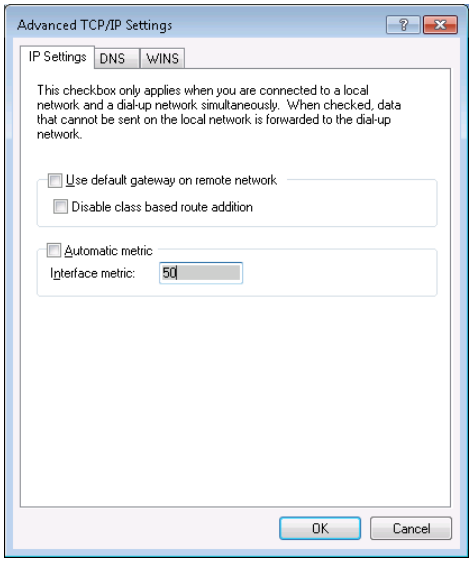
19. On the Networking tab, click Properties and then click Advanced.

    By default all the traffic is forwarded through the established VPN tunnel. To have both the VPN tunnel to the 1756-EN2TSC module and preserve access to the local network (such as Internet or corporate mail server), do the following.

    a. Clear the Use default gateway on remote network checkbox.

    b. Clear the Automatic metric checkbox.

    c. In the Interface metric field, enter a value larger than the metric of the default gateway route in the routing table.



20. Click OK until you exit the configuration tabs.

Interface Metric

The interface metric specifies an integer cost metric (1...9999) for the route. This metric is used when choosing among multiple routes in the routing table that most closely match the destination address of a packet being forwarded.

- Use the ipconfig command to identify the IP address of the default gateway.
- Use the route print command to identify the metric of the default gateway.

If you do not want all network traffic to go through the VPN tunnel, set the metric of the route though the VPN connection to be larger than the metric of the route through the default gateway. In the example below, the metric is 10; the interface field metric must be 11 or greater.

```
C:\>route print
===========================================================================
Interface List
 34.........................1.EN2TSC VPN Connection
 11...f0 4d a2 20 ee d7 ......Broadcom NetXtreme 57xx Gigabit Controller
 18...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 20...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1
 12...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 13...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 19...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 21...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
 22...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
===========================================================================
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.76.16.1     10.76.16.127     10 <- metric of default gateway
       10.76.16.0    255.255.252.0         On-link      10.76.16.127    266
     10.76.16.127  255.255.255.255         On-link      10.76.16.127    266
     10.76.18.110  255.255.255.255         On-link      10.76.16.127     11
     10.76.19.255  255.255.255.255         On-link      10.76.16.127    266
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.1.0    255.255.255.0      192.168.1.1      192.168.1.2     11 <- interface field metric for client
      - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Open the VPN Connection to the 1756-EN2TSC Module

Once the Windows client and 1756-EN2TSC module are configured, you must establish the VPN connection.

1. From the Windows notification area, select the network icon.
2. Right-click the EN2TSC VPN Connection and click Connect.
3. Log on with your 1756-EN2TSC user name and password.

It can take 30 seconds or more to connect.

TIP If you want to delete a VPN connection on the Windows client (for example, it does not work and you want to create a new one).

1. Choose Control Panel > Network and Sharing Center > Change Adapter Settings.
2. Right-click the connection and choose Delete.

Communicate to the Module via an RSLinx Driver

If you communicate to the module through an RSLinx driver, you must use an L2TP connection and the Ethernet devices (AB_ETH-1) driver.

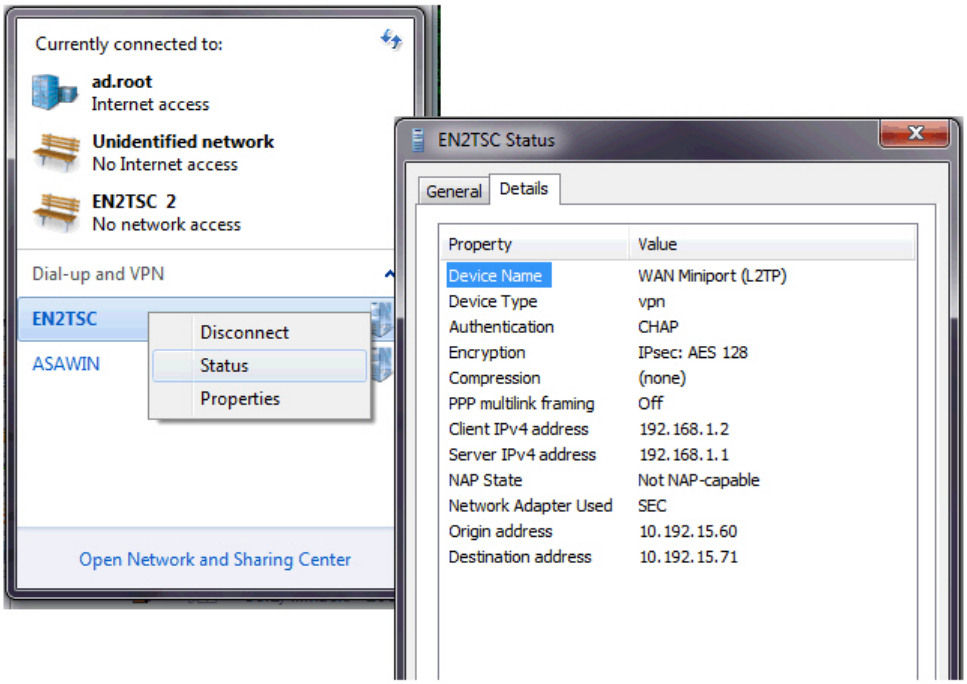
Once the secure tunnel exists to the 1756-EN2TSC module, RSLinx software uses the L2TP server IP addresses to communicate with the controller through the 1756-EN2TSC module.

IMPORTANT The Microsoft Windows client must use the module IP address specified (predetermined) on the L2TP configuration tab for all communication to the module, including RSLinx and Studio 5000 connections. The original IP address for the module is not in the VPN tunnel and cannot be used.

In the AB_ETH driver configuration, enter the L2TP server IP address (virtual IP address) of the 1756-EN2TSC module to the Station Mapping dialog box.

If you connect to the 1756-EN2TSC module without knowing the L2TP server IP address, you can find that after the connection is established.

1. Click the network icon in the right, bottom of the Windows taskbar.
2. Choose Status.
3. Click the Details tab.

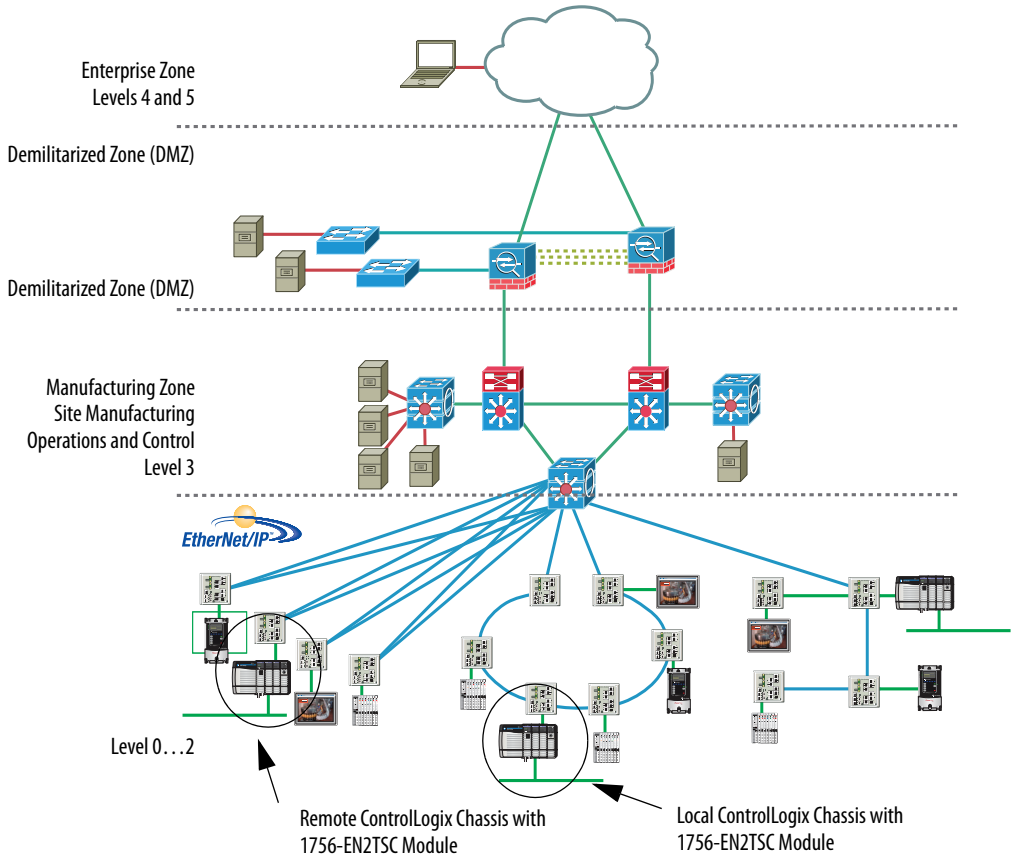


RSLinx software uses the L2TP server IP address to communicate with the 1756-EN2TSC module inside the secure tunnel.

Configure Secure Communication Between Two 1756-EN2TSC Modules

In this scenario an IPsec association is established between two 1756-EN2TSC modules (peer-to-peer). In this case, there are remote and local IP networks serviced by a VPN tunnel. There is one IP address at either end of the IPsec association.

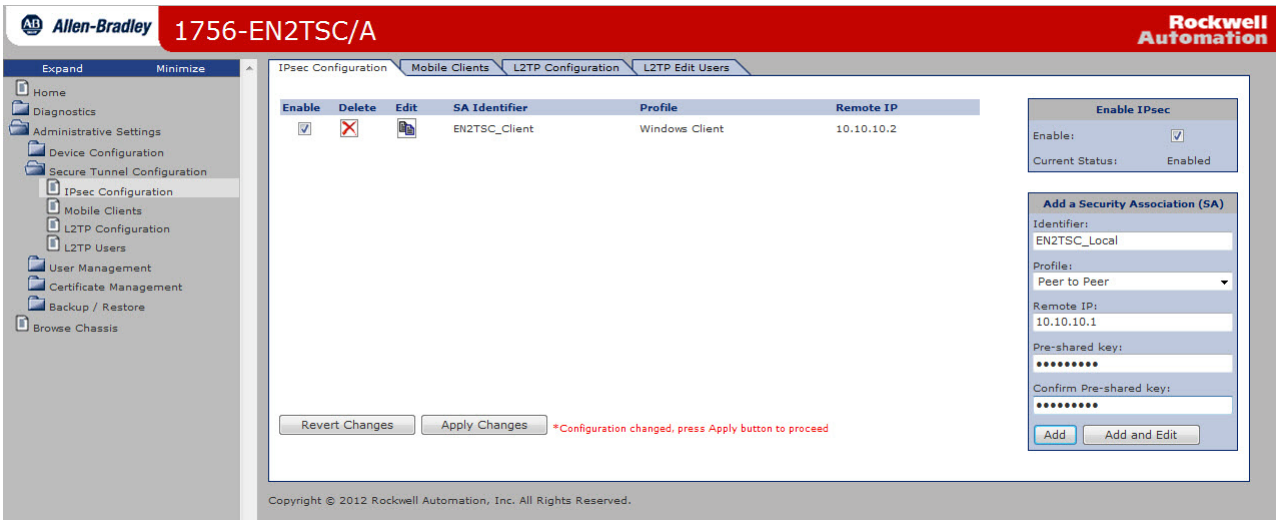
To create a security association with another module, each module must be configured with the pre-shared key of the other module.



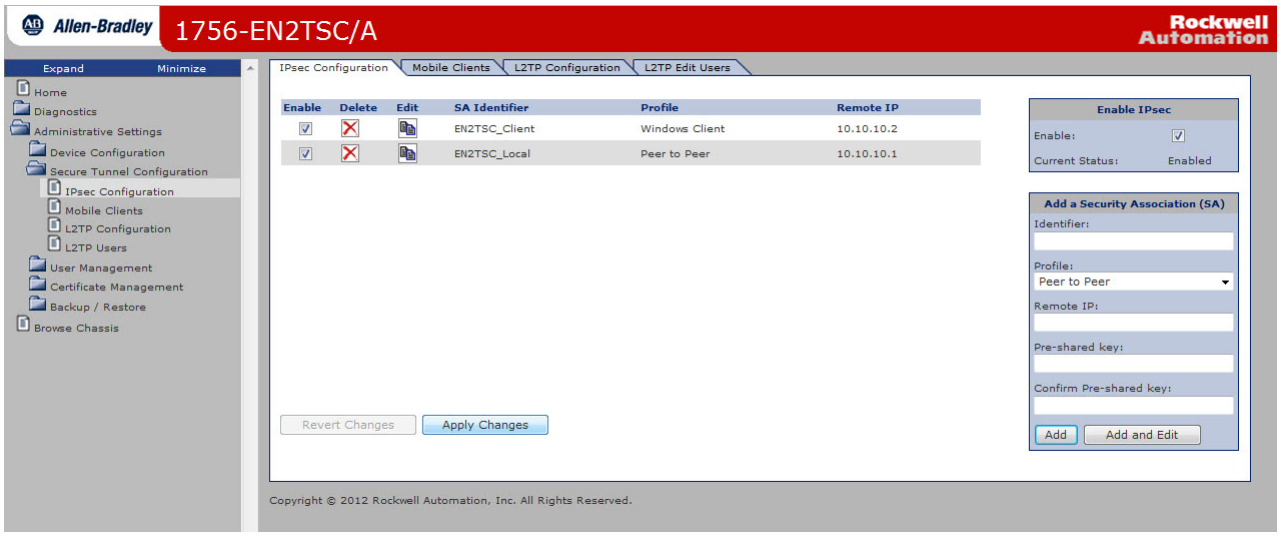
IMPORTANT This peer-to-peer configuration does not maintain the security features of the module if you use produced/consumed tags, CIP Sync packets, or multicast communication. Use MSG instructions rather than produced/consumed tags to share data.

Configure the First (Local) Module

1. Choose Administrative Settings > Secure Tunnel Configuration > IPsec Configuration and make sure that Enable IPsec is enabled.

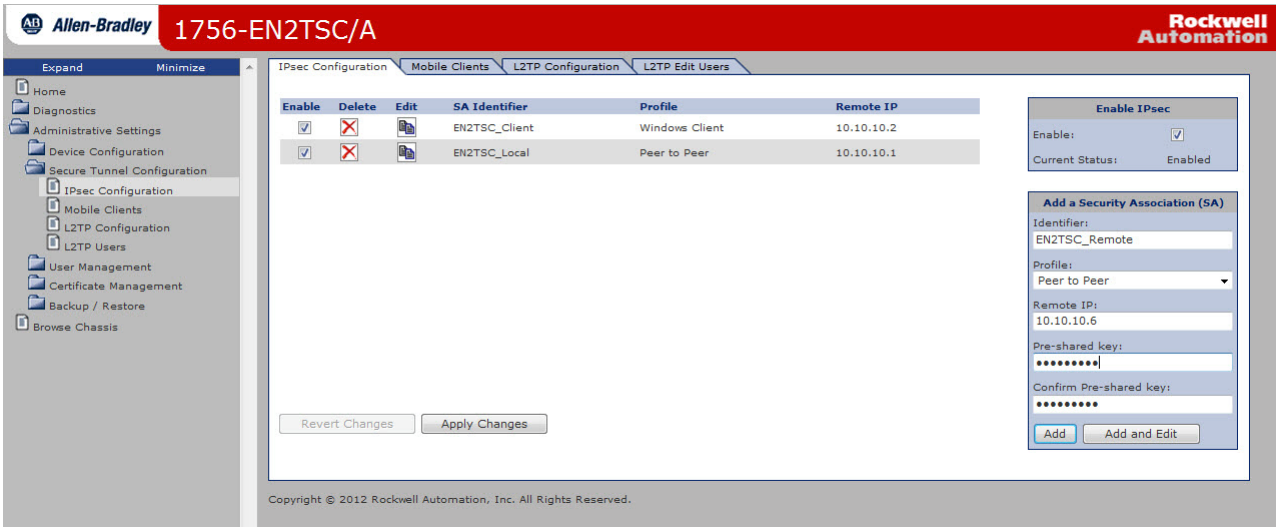


2. To create a new secure association, do the following.
   a. Enter the Identifier as a text description of the connection.
   b. Choose the Peer to Peer as the Profile.
   c. Enter the IP address of the second (remote) module.
   d. Enter the pre-shared key and confirm the pre-shared key.
3. Click Add.
4. Click Apply Changes after entering all configurations.

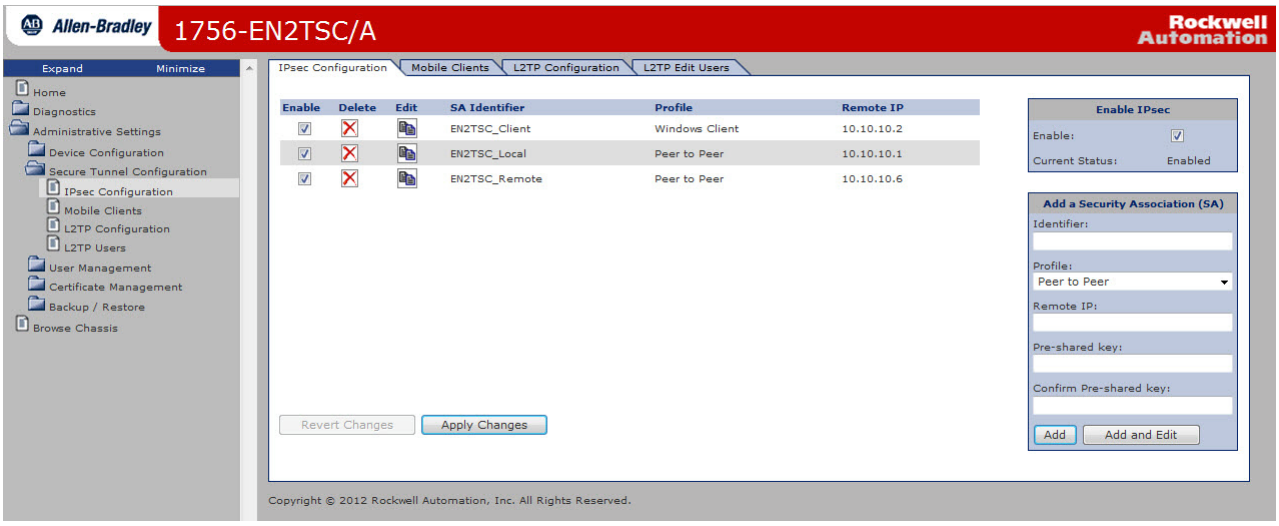


Configure the Second (Remote) Module

1. Choose Administrative Settings > Secure Tunnel Configuration > IPsec Configuration and make sure that Enable IPsec is enabled.

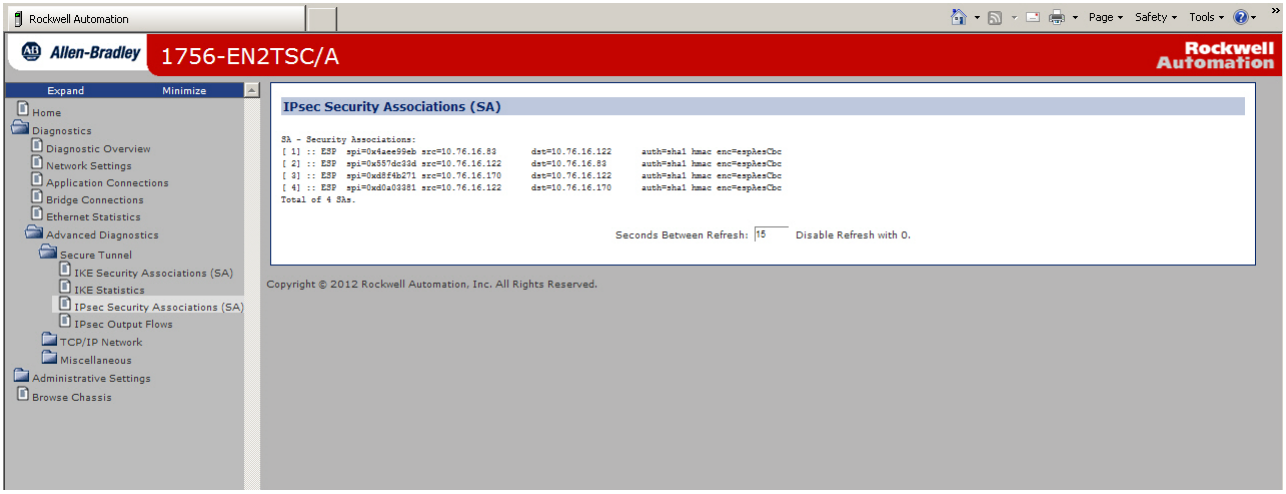


2. To create a new secure association, do the following.
   a. Enter the Identifier as a text description of the connection.
   b. Choose the Peer to Peer as the Profile.
   c. Enter the IP address of the first (local) module.
   d. Enter the pre-shared key and confirm the pre-shared key.
3. Click Add.
4. Click Apply Changes after entering all configurations.



Test the Connection

When the security association is added on both sides of connection, the modules take a few seconds to establish the IPsec tunnel between the modules. To verify that the connection is established, access Diagnostics > Advanced Diagnostics > Secure Tunnel > IPsec Security Associations.



Edit the Security Association

If you want to edit the settings for the association you just created, click the Edit button next to the association in the list.

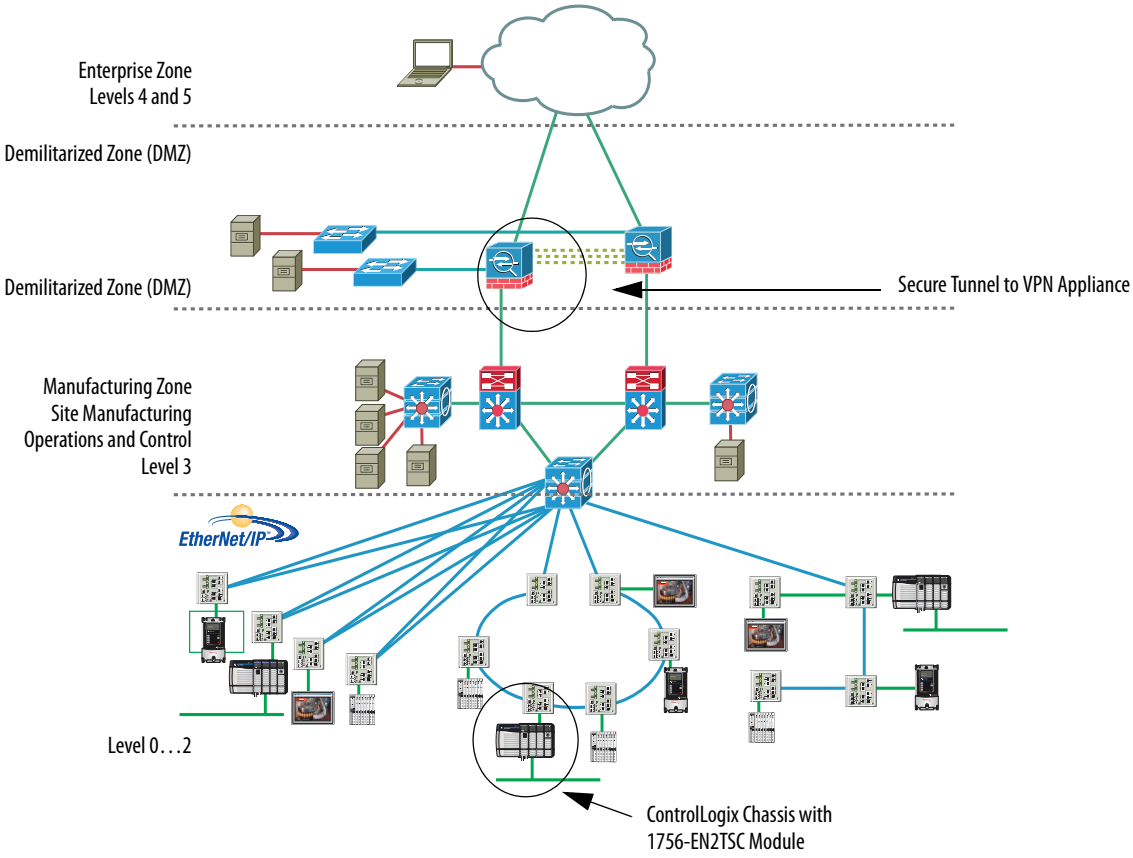
Notes:

Configure a Secure Connection to a VPN Appliance

In this scenario, a VPN appliance (such as a firewall) establishes the IPsec association with the 1756-EN2TSC module. Client workstations or other modules then establish IPsec associations with the VPN appliance. The VPN appliance then routes packets between the IPsec associations.

The IPsec association between the VPN appliance and module services multiple remote (from the module's point of view) devices and networks. You configure the module to know which remote networks are routed via the VPN appliance.

This configuration lets you consolidate multiple VPN clients through a single location (the VPN appliance). This limits the need for multiple secure tunnels to each VPN client as you need only one secure tunnel between the 1756-EN2TSC module and the VPN appliance.



An appliance like the Cisco ASA supports multiple methods for authentication, multiple encryption algorithms, and multiple types of VPN technology (such as SSL VPN.

Configure the Module to Connect to a VPN Appliance

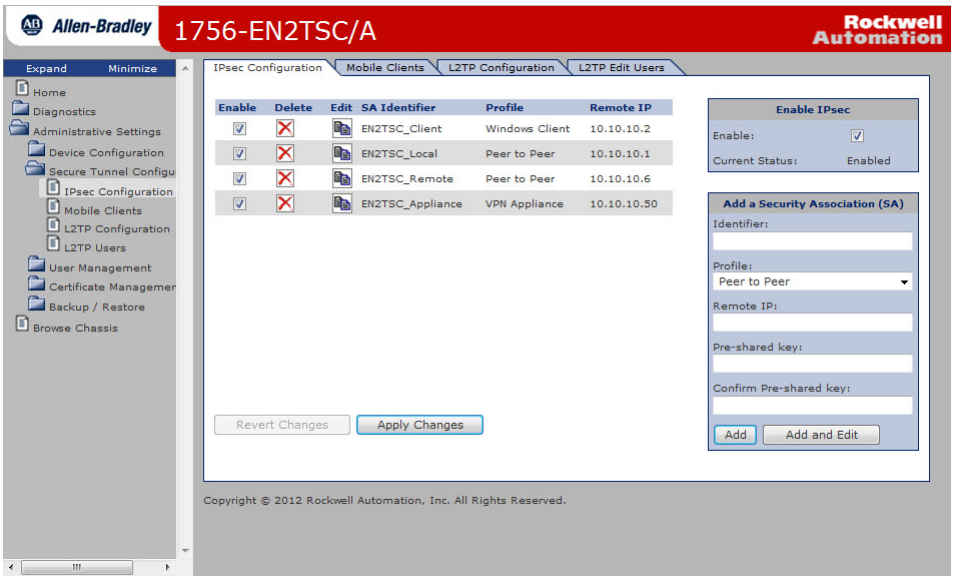
1. Choose Administrative Settings > Secure Tunnel Configuration > IPsec Configuration and make sure that Enable IPsec is enabled.

2. To create a new secure association, do the following.
   a. Enter the Identifier as a text description of the connection.
   b. Choose the VPN Appliance as the Profile.
   c. Enter the IP address of the VPN appliance.
   d. Enter the pre-shared key and confirm the pre-shared key.

In This Field	Specify
Identifier	Name for the security association, such as VPN_connection
Profile	VPN Appliance
Remote IP	IP address of the VPN appliance
Pre-shared key	Pre-shared key for the connection
Confirm Pre-shared key	Same pre-shared key for the connection, as entered above

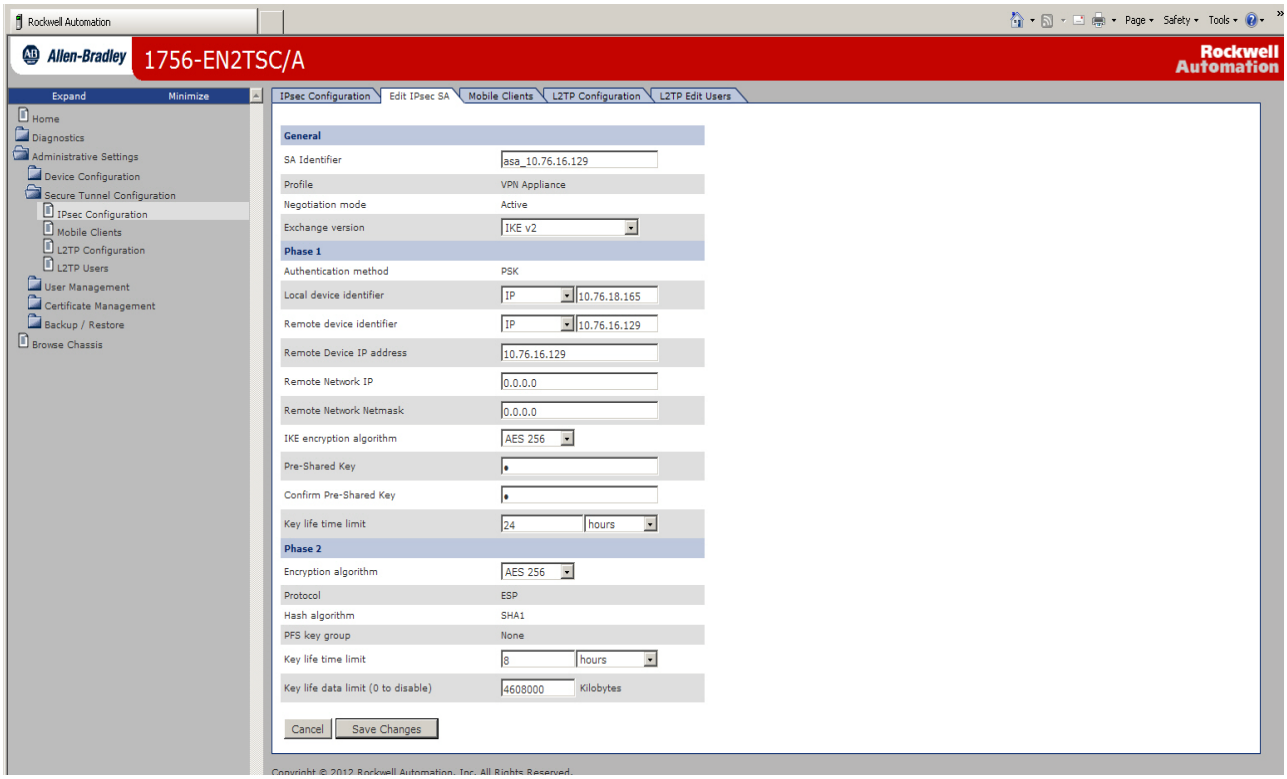
3. Click Add.

4. Click Apply Changes.



Edit the Security Association

If you want to edit the settings for the association you just created, click the Edit button next to the association in the list.



Set the key life time (10 min...8 hr) and key life data (1000...10000000 KB) values to the same value as on the VPN appliance. If these values differ, there can be issues with rekeying, even though the initial connection is successful.

You must specify a value for key life time. If key life data is not used, set the value to 0.

You can specify a subnetwork accessible via the VPN appliance by specifying addresses for Remote Network IP and Remote Network Netmask.

Default values of all zeroes direct all of the VPN network traffic to the VPN appliance. However, other security associations, such as peer to peer connections, still work as narrower address ranges take precedence over the wider range specified for VPN appliance.

Notes:

Diagnostics

Diagnostic Web Pages

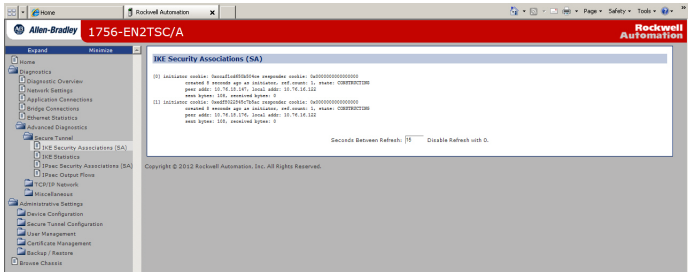
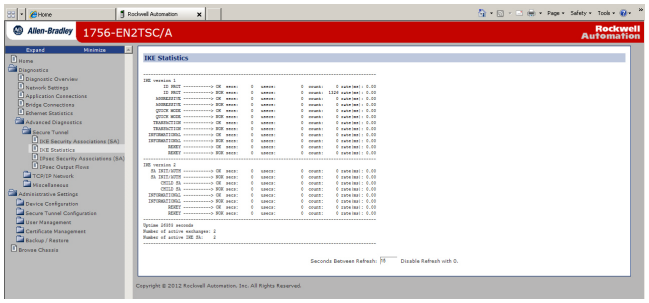
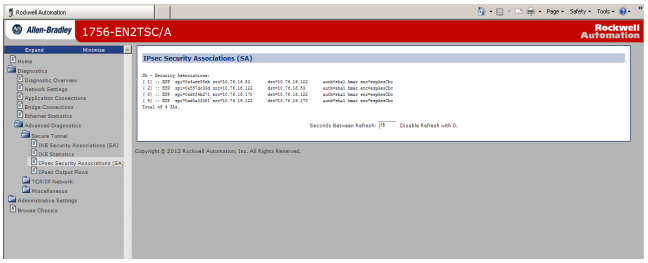
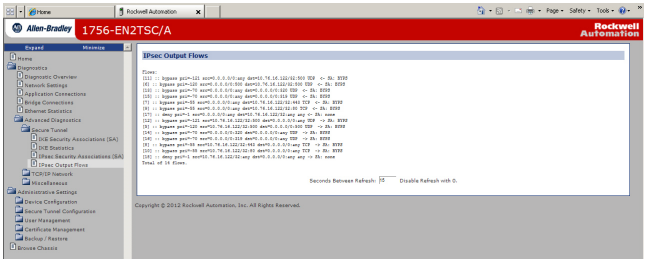
The 1756-EN2TSC module supports the same diagnostic web pages as the 1756-EN2T modules, including these pages.

- Diagnostic Overview for a summary of the configuration and overall status of the module
- Network Settings for the Ethernet configuration parameters of the module
- Ethernet Statistics for a summary of the status of communication activity on the Ethernet network

For information on these standard diagnostic web pages, see EtherNet/IP Network Configuration User Manual, publication ENET-UM001.

Secure Tunnel Diagnostics Web Page

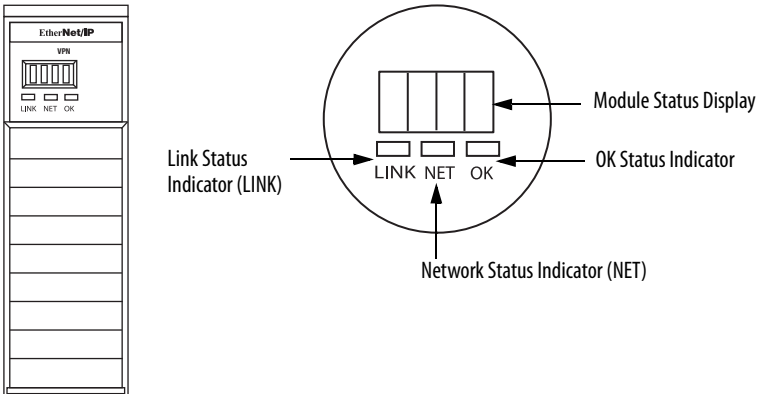
For specific diagnostics regarding secure connections, choose Diagnostics > Advanced Diagnostics > Secure Tunnel.

This Diagnostic Web Page	Displays
IKE Security Associations (SA)	Active IKE security associations 
IKE Statistics	Statistics of active exchanges and IKE security associations 
IPsec Security Associations (SA)	Active IPsec security associations 
IPsec Output Flows	Defined IPsec output flow rules 

Status Indicators

The 1756-EN2TSC module uses the same status indicators as the 1756-EN2T module:

- Module Status Display
- Link Status Indicator (LINK)
- Network Status Indicator (NET)
- OK Status Indicator (OK)



Link (LINK) Status Indicator

Status	Description
Off	One of these conditions exists: • The module is not powered. – Verify there is chassis power. – Verify that the module is completely inserted into the chassis and backplane. • No link exists on the port. – Verify the RJ45 connector in the Ethernet port is completely inserted and the other end of the cable is connected to a device in your network
Flashing green	Activity exists on the port.
Green	A link exists on the port.

Network (NET) Status Indicator

Status	Description
Off	One of these conditions exists: • The module is not powered. – Verify there is chassis power. – Verify that the module is completely inserted into the chassis and backplane. – Make sure the module has been configured. • The module is powered but does not have an IP address. Assign an IP address to the module.
Flashing green	The controller has an IP address and one of these conditions exists: • The module has not established any CIP connections. If connections are configured for this module, check the connection originator for the connection error code. • One or more connections have timed out. For example, an HMI or I/O connection has timed out. Reestablish the connection.
Green	The module has established at least 1 CIP connection and is operating properly. The module's IP address scrolls across the Module Status display.
Red	The module is in conflict mode. The module shares an IP address with another device on the network. The module's current IP address scrolls across the Module Status display. The display scrolls: OK <IP_address_of_this_module> Duplicate IP <Mac_address_of_duplicate_node_detected> For example: OK 10.88.60.196 Duplicate IP - 00:00:BC:02:34:B4 Change the module's IP address.
Flashing green/flashing red	The module is performing its power-up testing.

OK Status Indicator

Status	Description
Off	The module is not powered. • Verify there is chassis power. • Verify that the module is completely inserted into the chassis and backplane. • Make sure the module has been configured.
Flashing green	The module is not configured. The Module Status display scrolls: BOOTP or DHCP<Mac_address_of_module> For example: BOOTP 00:0b:db:14:55:35 Configure the module.
Green	The module is operating correctly. The module's IP address scrolls across the Module Status display.
Flashing red	The module detected a recoverable minor fault. Check the module configuration. If necessary, reconfigure the module.
Red	The module detected an unrecoverable major fault. Cycle power to the module. If this does not clear the fault, replace the module.
Flashing red/ flashing green	The module is performing its power-up testing.

T

U

V

W

Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products. At http://www.rockwellautomation.com/support you can find technical and application notes, sample code, and links to software service packs. You can also visit our Support Center at https://rockwellautomation.custhelp.com/ for software updates, support chats and forums, technical information, FAQs, and to sign up for product notification updates.

In addition, we offer multiple support programs for installation, configuration, and troubleshooting. For more information, contact your local distributor or Rockwell Automation representative, or visit http://www.rockwellautomation.com/services/online-phone.

Installation Assistance

If you experience a problem within the first 24 hours of installation, review the information that is contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the Worldwide Locator at http://www.rockwellautomation.com/rockwellautomation/support/overview.page, or contact your local Rockwell Automation representative.

New Product Satisfaction Return

Rockwell Automation tests all of its products to help ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

United States	Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for the return procedure.

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete this form, publication RA-DU002, available at http://www.rockwellautomation.com/literature/.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication ENET-UM003B-EN-P - September 2013
Supersedes ENET-UM003A-EN-P – February 2013