NGE, FIPS and Additional Security

Next Generation Encryption (NGE) introduces new algorithms for encryption, authentication, digital signatures, and key exchange to meet escalating security and performance requirements. The National Institute of Standards and Technology (NIST) specified a set of cryptographic algorithms that devices must support to meet U.S. federal standards for cryptographic strength. RFC 6379 defines the Suite B cryptography suites. Because the collective set of algorithms defined as NIST Suite B are becoming a standard, the AnyConnect IPsec VPN (IKEv2 only), PKI, 802.1X, and EAP subsystems now support them. AnyConnect 3.1 uses CiscoSSL 0.9.8r.1.3 FIPS certified implementation of the Suite B ciphers. (AnyConnect 3.1 does not offer support for TLS/DTLS, SRTP, and SSH Suite B.) Cisco's implementation of Suite B specifications are FIPS-certified, and throughout AnyConnect and ASDM configuration, NGE features are referred to as FIPS.

The AnyConnect VPN component can connect to one of two VPN head ends:

- ASA
- IOS

No client side configuration is required for this feature.

AnyConnect components negotiate and use NGE based on the Adaptive Security Appliance (ASA) configuration. The AnyConnect client's Statistics panel (under the Transport Information heading) shows the name of the cipher being used.

The following sections are included in this chapter:

Information About NGE and AnyConnect

Next Generation Encryption (NGE) for AnyConnect 3.1 VPN and Network Access Manager includes the following functionality:

- AES-GCM support for symmetric encryption and integrity
  - (Network Access Manager) 128-bit keys for 802.1AE (MACsec) wired traffic encryption in software (Windows 7)
  - (VPN) 128-, 192-, and 256-bit keys for IKEv2 payload encryption and authentication

  - (VPN) ESP packet encryption and authentication
- SHA-2 (SHA with 256/384/512 bits) support for hashing
  - (Network Access Manager) Ability to use certificates with SHA-2 in TLS-based EAP methods
  - (VPN) IKEv2 payload authentication (Windows Vista or later and Mac OS X 10.6 or later)
  - (VPN) ESP packet authentication (Windows Vista or later and Mac OS X 10.6 or later)
- ECDH support for key exchange
  - (Network Access Manager) Ability to use ECDHE in TLS-based EAP methods (Windows 7 and Windows XP)
  - (VPN) Groups 19, 20, and 21 IKEv2 key exchange and IKEv2 PFS
- ECDSA support (256-, 384-, 521-bit elliptic curves) for digital signature, asymmetric encryption, and authentication
  - (Network Access Manager) Ability to use certificates with ECDSA in TLS-based EAP methods (Only Windows 7 and Vista is supported for client certificates. Only Windows 7 is supported for smart cards.)
  - (VPN) IKEv2 user authentication and server certificate verification

Note On Linux, AnyConnect can use both the Firefox certificate store or the AnyConnect file certificate store. For ECDSA certificates, only the AnyConnect file store is supported. To add certificates to a file store, see Creating a PEM Certificate Store for Mac and Linux.

- New crypto algorithms for IPsecV3 VPN. AnyConnect 3.1 supports the algorithms required by IPsecV3 except for NULL encryption. IPsecV3 also specifies that Extended Sequence Numbers (ESN) must be supported, but AnyConnect 3.1 does not support ESN.
- Other cipher suite dependencies between algorithms promote support for the following in AnyConnect 3.1:
  - Diffie-Hellman Groups 14 and 24 for IKEv2.
  - RSA certificates with 4096 bit keys for DTLS and IKEv2.

Requirements

- Combined-mode encryption algorithms, where both encryption and integrity are performed in one operation, are supported only on SMP ASA gateways with hardware crypto acceleration (such as 5585 and 5515-X). AES-GCM is the combined-mode encryption algorithm that Cisco supports.

Note An IKEv2 policy can only include a normal- or a combined-mode encryption algorithm, but not both types. When a combined-mode algorithm is configured in the IKEv2 policy, all normal-mode algorithms are disabled, so the only valid integrity algorithm is NULL.

The IKEv2 IPsec proposals use a different model and can specify both normal- and combined-mode encryption algorithms in the same proposal. With this usage, you are required to configure integrity algorithms for both, which leaves a non-NULL integrity algorithm configured with AES-GCM encryption.

- NGE requires an AnyConnect premium license for IKEv2 remote access connections using NIST Suite B algorithms. Suite B algorithm usage for other connections or purposes (such as PKI) has no limitations. License checks are performed for remote access connections. If you receive a message that you are attempting to use an NIST Suite B crypto algorithm without an AnyConnect premium license, you have the option to either install the premium license or reconfigure the crypto settings to an appropriate level.
- IPSec connections require server certificates that contain Key Usage attributes of Digital Signature and Key Encipherment, as well as an Enhanced Key Usage attribute of Server Authentication or IKE Intermediate. Note that IPSec server certificates not containing a Key Usage will be considered invalid for all Key Usages, and similarly an IPSec server certificate not containing an Enhanced Key Usage will be considered invalid for all Enhanced Key Usages.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

- Suite B is available only for IKEv2/IPsec.
- No EAP methods support SHA-2 except in TLS-based EAP when validating certificates signed using SHA-2.
- TLS v1.2 handshaking is not supported in AnyConnect 3.1.
- TLS v1.2 certificate authentication is not supported in AnyConnect 3.1.
- ECDSA certificates are supported on Windows Vista or later, Mac OS X 10.6 or later, Red Hat Enterprise Linux 6.x (32-bit) or 6.4 (64-bit), and Ubuntu 9.x, 10.x, and 11.x (32-bit) and Ubuntu 12.4 and 12.10 (64-bit). ECDSA smart cards are supported only on Windows 7.
- ECDSA certificates must have a Digest strength equal or greater than the Curve strength. For example, an EC-384 key must use SHA2-384 or greater.
- Suite B profiles may require certain policy properties in the certificates; however, these requirements are enforced on the ASA and not by AnyConnect.
- Because ASA does not support ECDSA certificates for SSL VPN, you should not use such certificates for SSL VPN.
- When the ASA is configured with a different server certificate for SSL and IPsec, use trusted certificates. A Posture Assessment, WebLaunch, or Downloader failure can occur if using Suite B (ECDSA) untrusted certificates having different IPsec and SSL certificates.
- Because AES-GCM is computationally intensive algorithms, you may experience a lower overall data rate when using these algorithms. Some new Intel processors contain special instructions specifically introduced to improve the performance of AES-GCM. AnyConnect 3.1 automatically detects whether the processor on which it is running supports these new instructions. If so, AnyConnect uses the new instructions to significantly improve VPN data rates as compared to those processors that do not have the special instructions. See http://ark.intel.com/search/advanced/?s=t&AESTech=true for a list of processors that support the new instructions. For more information see http://software.intel.com/en-us/articles/intel-carry-less-multiplication-instruction-and-its-usage-for-computing-the-gcm-mode/.
- IPSec connections perform name verification on server certificates. The following rules are applied in IPSec name verification:

- If a Subject Alternative Name extension is present with relevant attributes, name verification only uses the Subject Alternative Name. Relevant attributes include DNS Name attributes for all certificates, and also include IP address attributes, if the connection is being performed to an IP address.
- If a Subject Alternative Name extension is not present, or is present but contains no relevant attributes, name verification uses any Common Name attributes found in the Subject of the certificate.
- If a certificate uses a wildcard for the purposes of name verification, the wildcard must be in the first (left-most) subdomain only, and additionally must be the last (right-most) character in the subdomain. Any wildcard entry not in compliance is ignored for the purposes of name verification.

About AnyConnect Modules with NGE

The FIPS-certified features for AnyConnect are licensed for the ASA on a per-model basis. The following AnyConnect client modules have their own FIPS configuration and requirements:

- AnyConnect core VPN client—FIPS compliance is enabled by a FIPS-mode parameter in the local policy file on the user computer. The XML file AnyConnectLocalPolicy contains security settings, but it is not deployed by the ASA. I must be installed manually, or deployed using an enterprise software deployment system. You must purchase a FIPS license for each ASA the client connects to.
- AnyConnect Network Access Manager—FIPS support in Network Access Manager is enabled by a FIPS-mode parameter in AnyConnectLocalPolicy.xml on the user computer, and a FIPS-mode parameter in a Network Access Manager group policy.

  FIPS for Network Access Manager is supported on Windows 7/Vista and Windows XP. Windows XP requires a 3eTI FIPS validated Cryptographic Kernel Library (CKL) from 3e Technologies International, with supported drivers that integrate with the Network Access Manager. Order the FIPS 3eTI CKL supported driver installer from Cisco (shipped on a CD) using part number AIR-SSCFIPS-DRV. For information about the drivers and supported chipsets, see *Release Notes for 3eTI Cryptographic Client Software Model 3e-010F-3-IA* on the AnyConnect software download page.

Enabling FIPS for the AnyConnect Core VPN Client

You enable FIPS compliance for the core AnyConnect Security Mobility Client in the local policy file on the user computer. This file is an XML file containing security settings, and is not deployed by the ASA. The file must be installed manually or deployed to a user computer using an enterprise software deployment system. You must purchase a FIPS license for the ASA the client connects to.

AnyConnect Local Policy parameters reside in the XML file *AnyConnectLocalPolicy.xml*. This file is not deployed by the ASA. You must deploy this file using corporate software deployment systems, change the file manually on a user computer, or include it in a pre-deployed AnyConnect installer. If you do make changes to an existing local policy file on a user's system, that system should be rebooted.

Other parameters in the AnyConnect Local Policy increase security by forbidding remote updates to prevent Man-in-the-Middle attacks and by preventing non-administrator or non-root users from modifying client settings.

This section shows how to enable FIPS mode and additional security for the AnyConnect core VPN client and covers the following topics:

Enabling FIPS for Windows Clients Using an MST File

For Windows installations, you can apply the Cisco MST file to the standard MSI installation file to enable FIPS in the AnyConnect Local Policy. This MST only enables FIPS and does not change other parameters. The installation generates an AnyConnect Local Policy file with FIPS enabled. Update the user's system after running this utility.

For information about where you can download the AnyConnect MST, see the licensing information you received for the FIPS client.

Enabling FIPS and other Local Policy Parameters in an MST File

You can create an MST file to change any local policy parameters. The MST parameter names correspond to the parameters in AnyConnect Local Policy file (AnyConnectLocalPolicy.xml). See AnyConnect Local Policy Parameters and Values for the descriptions and values you can set for these parameters:

- LOCAL_POLICY_BYPASS_DOWNLOADER
- LOCAL_POLICY_FIPS_MODE
- LOCAL_POLICY_RESTRICT_PREFERENCE_CACHING
- LOCAL_POLICY_RESTRICT_TUNNEL_PROTOCOLS
- LOCAL_POLICY_RESTRICT_WEB_LAUNCH
- LOCAL_POLICY_STRICT_CERTIFICATE_TRUST

Note AnyConnect installation does not automatically overwrite an existing local policy file on the user computer. You must delete the existing policy file on user computers first, so the client installer can create a new policy file.

Any changes to the local policy file require the system to be rebooted.

Enabling FIPS and Other Parameters with the Enable FIPS Tool

For all operating systems, you can use Cisco's Enable FIPS tool to create an AnyConnect Local Policy file with FIPS enabled. The Enable FIPS tools is a command line tool that runs on Windows using administrator privileges or as a root user for Linux and Mac.

For information about where you can download the Enable FIPS tool, see the licensing information you received for the FIPS client.

Table 9-1 shows the policy settings you can specify and the arguments and syntax to use. The behavior for the argument values is the same behavior specified for the parameters in the AnyConnect Local Policy file in AnyConnect Local Policy Parameters and Values.

You run the Enable FIPS tool by entering the command **EnableFIPS** <*arguments*> from the command line of the computer. The following usage notes apply to the Enable FIPS tool:

- If you do not supply any arguments, the tool enables FIPS and restarts the vpnagent service (Windows) or the vpnagent daemon (Mac and Linux).
- Separate multiple arguments with spaces.

The following example shows the Enable FIPS tool command, run on a Windows computer:

```
EnableFIPS rwl=false sct=true bd=true fm=false
```

The next example shows the command, run on a Linux or Mac computer:

```
./EnableFIPS rwl=false sct=true bd=true fm=false
```

Table 9-1 shows the policy settings and the arguments for the Enable FIPS tool. Descriptions of the policy settings is provided in AnyConnect Local Policy Parameters and Values, page 9-11.

Table 9-1 Policy Settings and Arguments for the Enable FIPS Tool

Policy Setting	Argument and Syntax
FIPS mode	**fm=[true | false]**
Bypass downloader	**bd=[true | false]**
Restrict weblaunch	**rwl=[true | false]**
Strict certificate trust	**sct=[true | false]**
Restrict preferences caching	**rpc=[Credentials | Thumbprints | CredentialsAndThumbprints | All | false]**
Exclude FireFox NSS certificate store (Linux and Mac)	**efn=[true | false]**
Exclude PEM file certificate store (Linux and Mac)	**epf=[true | false]**
Exclude Mac native certificate store (Mac only)	**emn=[true | false]**

Changing Local Policy Parameters Manually in the Local Policy

To change AnyConnect Local Policy parameters manually, follow this procedure:

Step 1 Retrieve a copy of the AnyConnect Local Policy file (AnyConnectLocalPolicy.xml) from a client installation. The following table shows the installation path for each operating system.

Table 9-2 Operating System and AnyConnect Local Policy File Installation Path

Operating System	Installation Path
Windows 7	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Windows Vista	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Windows XP	C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client
Windows Mobile	%PROGRAMFILES%\Cisco AnyConnect VPN Client[1]
Linux	/opt/cisco/anyconnect
Mac OS X	/opt/cisco/anyconnect

1. AnyConnect 3.0+ does not support Windows Mobile. This path is of the local policy file for AnyConnect 2.5.

Step 2 Edit the parameter settings. You can either edit the AnyConnectLocalPolicy file manually, or use the VPN Local Policy editor, which is distributed with the AnyConnect Profile Editor installer. The parameters are described in AnyConnect Local Policy Parameters and Values, page 9-11.

Step 3 Save the file as *AnyConnectLocalPolicy.xml* and deploy the file to remote computers using a corporate software deployment system.

Step 4 Reboot the remote computers so the changes to the local policy file will take effect.

Avoiding Endpoint Problems from AnyConnect FIPS Registry Changes

Enabling FIPS for the core AnyConnect client has system-wide consequences on the endpoint device. AnyConnect changes Windows registry settings on the endpoint. Other components of the endpoint may detect that AnyConnect has enabled FIPS and started using cryptography. For example, the Microsoft Terminal Services client Remote Desktop Protocol (RDP) will not work, because RDP requires that servers use FIPS compliant cryptography.

To avoid these problems, you can temporarily disable FIPS encryption in the Windows Local System Cryptography settings by changing the parameter *Use FIPS compliant algorithms for encryption, hashing, and signing* to **Disabled**.

Be aware that rebooting the endpoint device changes this setting back to enabled.

Table 9-3 shows the Windows registry changes performed by AnyConnect that you should be aware of:

Table 9-3 Windows Registry Key Changes Performed When Enabling AnyConnect FIPS

Windows Version	Registry Key	Action Taken
Windows XP and Later	HKLM\System\CurrentControlSet\Control\Lsa	FIPSAlgorithmPolicy changed from 0 to 1.

Windows Version	Registry Key	Action Taken
Windows Vista and Later	HKLM\System\CurrentControlSet\Control\Lsa\ FIPSAlgorithmPolicy	Enabled changed from 0 to 1.
	HKCU\Software\Microsoft\Windows\ CurrentVersion\Internet Settings	SecureProtocols setting changed to TLSV1 by performing a bit-wise “or” of 0x080 with the original setting.
	HKLM\Software\Policies\Microsoft\Windows\ CurrentVersion\Internet	SecureProtocols setting changed to TLSV1 by performing a bit-wise “or” of 0x080 with the original setting. This sets TLSv1 for a group policy.

Configuring your Update Policy

Update Policy Overview

AnyConnect software and profile updates occur when they are available and allowed by the client upon connecting to a headend. Configuring the headend for AnyConnect updates makes them available, the Update Policy settings in the VPN Local Policy file determine if they are allowed.

Update policy is sometimes referred to as software locks. When multiple headends are configured, the update policy is referred to as the multiple domain policy.

By default, the Update Policy settings allow software and profile updates from any headend. Set the Update Policy parameters to restrict this as follows:

- Allow, or authorize, specific headends to update all AnyConnect software and profiles by specifying them in the **Server Name** list.

  The headend server name can be an FQDN or an IP Address. They can also be wild cards, for example: *.example.com.

  See Authorized Server Update Behavior below for a full description of how the update occurs.
- For all other unspecified, or unauthorized headends:
  - Allow or disallow software updates of the VPN core module and other optional modules using the **Allow Software Updates From Any Server** option.
  - Allow or disallow VPN Profile updates using the **Allow VPN Profile Updates From Any Server** option.
  - Allow or disallow other service module profile updates using the **Allow Service Profile Updates From Any Server** option.

  See Unauthorized Server Update Behavior below for a full description of how the update occurs.

Authorized Server Update Behavior

When connecting to an authorized headend, one identified in the **Server Name** list, the other Update Policy parameters do not apply and the following occurs:

- The version of the AnyConnect package on the headend is compared to the version on the client to determine if the software should be updated.

  - If the version of the AnyConnect package is older than the version on the client, no software updates occur.
  - If the version of the AnyConnect package is the same as the version on the client, only software modules configured for download on the headend and not present on the client are downloaded and installed.
  - If the version of the AnyConnect package is newer than the version on the client, software modules configured for download on the headend, as well as software modules already installed on the client, are downloaded and installed.
- The VPN profile and each service profile on the headend is compared to that profile on the client to determine if it should be updated:
  - If the profile on the headend is the same as the profile on the client, it is not updated.
  - If the profile on the headend is different than the profile on the client, it is downloaded.

Unauthorized Server Update Behavior

When connecting to an unauthorized headend, the **Allow ... Updates From Any Server** options are used to determine how AnyConnect is updated as follows:

- **Allow Software Updates From Any Server:**
  - If this option is checked, software updates are allowed for this unauthorized ASA. Updates are based on version comparisons as described above for authorized headends.
  - If this option is not checked, software updates do not occur. In addition, VPN connection attempts will terminate if updates, based on version comparisons, should have occurred.
- **Allow VPN Profile Updates From Any Server:**
  - If this option is checked, the VPN profile is updated if the VPN profile on the headend is different than the one on the client.
  - If this option is not checked, the VPN profile is not updated. In addition, VPN connection attempts will terminate if the VPN profile update, based on differentiation, should have occurred.
- **Allow Service Profile Updates From Any Server:**
  - If this option is checked, each service profile is updated if the profile on the headend is different than the one on the client.
  - If this option is not checked, the service profiles are not updated.

Update Policy Guidelines

- Enable remote users to connect to a headend using its IP address by listing that server's IP address in the authorized **Server Name** list. If the user attempts to connect using the IP address but the headend is listed as an FQDN, the attempt is treated as connecting to an unauthorized domain.
- Software updates include downloading customizations, localizations, and transforms. When software updates are disallowed these items will not be downloaded.
- Downloading a VPN profile with Always-On enabled deletes all other VPN profiles on the client. Consider this when deciding whether to allow or disallow VPN profiles updates from unauthorized, or non-corporate, headends.

- If no VPN profile is downloaded to the client due to your installation and udpate policy, the following features are unavailable:

Service Disable	Untrusted Network Policy
Certificate Store Override	Trusted DNS Domains
Show Pre-connect Message	Trusted DNS Servers
Local LAN Access	Always-On
Start Before Logon	Captive Portal Remediation
Local proxy connections	Scripting
PPP Exclusion	Retain VPN on Logoff
Automatic VPN Policy	Device Lock Required
Trusted Network Policy	Automatic Server Selection

- The downloader creates a separate text log (UpdateHistory.log) that records the download history. This log includes the time of the updates, the ASA that updated the client, the modules updated, and what version was installed before and after the upgrade. This log file is stored here:

  %AllUsers%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Logs directory.

Update Policy Example

This example shows the client update behavior when the AnyConnect version on the client differs from various ASA headends.

Given the following Update Policy in the VPN Local Policy XML file:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
    xmlns=http://schemas.xmlsoap.org/encoding/
    xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
    xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
    <FipsMode>false</FipsMode>
    <BypassDownloader>false</BypassDownloader><RestrictWebLaunch>false</RestrictWebLaunch>
    <StrictCertificateTrust>false</StrictCertificateTrust>
    <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
    <RestrictTunnelProtocols>false</RestrictTunnelProtocols>
    <UpdatePolicy>
        <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
        <AllowVPNProfileUpdatesFromAnyServer>false</AllowVPNProfileUpdatesFromAnyServer>
        <AllowServiceProfileUpdatesFromAnyServer>false</AllowServiceProfileUpdatesFromAnyS
        erver>
        <AuthorizedServerList>
           <ServerName>seattle.example.com</ServerName>
           <ServerName>newyork.example.com</ServerName>
        </AuthorizedServerList>
    </UpdatePolicy>
</AnyConnectLocalPolicy>
```

With the following ASA headend configuration:

Table 9-4

ASA Headend	AnyConnect Package Loaded	Modules to Download
seattle.example.com	Version 3.0.0350	VPN, Network Access Manager, Web Security
newyork.example.com	Version 3.0.0351	VPN, Network Access Manager
raleigh.example.com	Version 3.0.0352	VPN, Posture

The following update sequence is possible when the client is currently running AnyConnect VPN and Network Access Manager modules version 3.0.0350:

- The client connects to seattle.example.com, an authorized server configured with the same version of AnyConnect. The Web Security software module will be downloaded and installed, as well as the Web Security profile if available. If the VPN and Network Access Manager profiles are available for download and different than the ones on the client they will also be downloaded.
- The client then connects to newyork.example.com, an authorized ASA configured with a newer version of AnyConnect. The VPN, Network Access Manager, and Web Security modules will be downloaded and installed. Profiles that are available for download and different than the ones on the client will also by downloaded.
- The client then connects to raleigh.example.com, an unauthorized ASA. Since software updates are allowed, the VPN, Network Access Manager, Web Security, and Posture modules are all upgraded to 3.0.0352. Because the VPN profile and service profile updates are not allowed, they are not downloaded. If the VPN profile could have been updated (based on it being different) the connection will terminate.

AnyConnect Local Policy Parameters and Values

The following parameters are elements in the VPN Local Policy Editor and in the AnyConnectLocalPolicy.xml file. XML elements are shown in brackets <>.

Note If you manually edit the file, and omit a policy parameter, that feature resorts to default behavior.

<acversion>

Specifies the minimum version of the AnyConnect client capable of interpreting all of the parameters in this file. If a client running a version of AnyConnect that is older than this version reads the file, it issues an event log warning.

The format is acversion="<version number>".

Fips Mode

<FipsMode>

Enables FIPS mode for the client. This forces the client to only use algorithms and protocols approved by the FIPS standard.

Bypass Downloader

<BypassDownloader>

When selected, disables the launch of the VPNDownloader.exe module, which is responsible for detecting the presence of and updating the local versions of dynamic content. The client does not check for dynamic content present on the ASA, including translations, customizations, optional modules, and core software updates.

When Bypass Downloader is selected, one of two things happens when that client connects to an ASA:

- If the VPN client profile on the ASA is different than the one on the client, the client aborts the connection attempt.
- If there is no VPN client profile on the ASA, the client makes the VPN connection, but it uses its hard-coded VPN client profile settings.

Note If you configure VPN client profiles on the ASA, they must be installed on the client before the client connects to an ASA with BypassDownloader set to *true*. Because the profile can contain an administrator defined policy, the BypassDownloader *true* setting is only recommended if you do not rely on the ASA to centrally manage client profiles.

Restrict Web Launch

<RestrictWebLaunch>

Prevents users from using a non-FIPS-compliant browser to initiate WebLaunch. It does this by preventing the client from obtaining the security cookie that is used to initiate an AnyConnect tunnel. The client displays an informative message to the user.

Strict Certificate Trust

<StrictCertificateTrust>

If selected, when authenticating remote security gateways, AnyConnect disallows any certificate that it cannot verify. Instead of prompting the user to accept these certificates, the client fails to connect to security gateways using self-signed certificates, and displays the following message:

```
Local policy prohibits the acceptance of untrusted server certificates. A connection
will not be established.
```

If not selected, the client prompts the user to accept the certificate, which is the default behavior, and is consistent with previous versions of AnyConnect.

Note We strongly recommend you enable Strict Certificate Trust for the AnyConnect client for the following reasons:

- With the increase in targeted exploits, enabling Strict Certificate Trust in the local policy helps prevent “man in the middle” attacks when users are connecting from untrusted networks such as public-access networks.
- Even if you use fully verifiable and trusted certificates, the AnyConnect client, by default, allows end users to accept unverifiable certificates. If your end users are subjected to a man-in-the-middle attack, they may be prompted to accept a malicious certificate. To remove this decision from your end users, enable Strict Certificate Trust.

RestrictPreferenceCaching

<RestrictPreferenceCaching>

By design, AnyConnect does not cache sensitive information to disk. Enabling this parameter extends this policy to any type of user information stored in the AnyConnect preferences.

- *Credentials*—The user name and second user name are not cached.
- *Thumbprints*—The client and server certificate thumbprints are not cached.
- *CredentialsAndThumbprints*—Certificate thumbprints and user names are not cached.
- *All*—No automatic preferences are cached.
- *false*—All preferences are written to disk (default—behavior consistent with AnyConnect 2.3 and earlier).

Exclude Pem File Cert Store (Linux and Mac)

<ExcludePemFileCertStore>

Prevents the client from using the PEM file certificate store to verify server certificates and search for client certificates.

The store uses FIPS-capable OpenSSL and has information about where to obtain certificates for client certificate authentication. Permitting the PEM file certificate store ensures remote users are using a FIPS-compliant certificate store.

Exclude Mac Native CertStore (Mac only)

<ExcludeMacNativeCertStore>

Prevents the client from using the Mac native (keychain) certificate store to verify server certificates and search for client certificates.

Exclude Firefox NSS Cert Store (Linux and Mac)

<ExcludeFirefoxNSSCertStore>

Prevents the client from using the Firefox NSS certificate store to verify server certificates and search for client certificates.

The store has information about where to obtain certificates for client certificate authentication.

Update Policy

<UpdatePolicy>

This section allows you to control which ASAs the client can get software or profile updates from.

For more information about how the software and profile update settings affect client updates, see Configuring your Update Policy, page 9-8

- Allow Software Update From Any Server

  <AllowSoftwareUpdatesFromAnyServer>

  Allow or disallow software updates of the VPN core module and other optional modules from unauthorized servers, ones not listed in the Server Name list.

- Allow VPN Policy Update From Any Server

  <AllowVPNProfileUpdatesFromAnyServer>

  Allow or disallow VPN Profile updates from unauthorized servers, ones not listed in the Server Name list.

- Allow Service Profile Updates From Any Server

  <AllowServiceProfileUpdatesFromAnyServer>

Allow or disallow other service module profile updates from unauthorized servers, ones not listed in the Server Name list.

- Server Name

  <ServerName>

  Specify authroized servers in this list. These headends are allowed full updates of all AnyConnect software and profiles upon VPN connectivity. ServerName can be an FQDN, IP address, domain name, or wildcard with domain name.

Local Policy File Example

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd"
acversion="3.0.0592">
    <FipsMode>true</FipsMode>
    <BypassDownloader>true</BypassDownloader>
    <RestrictWebLaunch>true</RestrictWebLaunch>
    <StrictCertificateTrust>true</StrictCertificateTrust>
    <RestrictTunnelProtocols>IPSec</RestrictTunnelProtocols>
    <RestrictPreferenceCaching>Credentials</RestrictPreferenceCaching>
    <ExcludePemFileCertStore>true</ExcludePemFileCertStore>
    <ExcludeWinNativeCertStore>true</ExcludeWinNativeCertStore>
    <ExcludeMacNativeCertStore>true</ExcludeMacNativeCertStore>
    <ExcludeFirefoxNSSCertStore>true</ExcludeFirefoxNSSCertStore>
    <UpdatePolicy>
        <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
        <AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer>
            <AuthorizedServerList>
                <ServerName>asa.one</ServerName>
                <ServerName>asa.two</ServerName>
            </AuthorizedServerList>
    </UpdatePolicy>
</AnyConnectLocalPolicy>
```

Enabling FIPS for the Network Access Manager

FIPS compliance for Network Access Manager is supported by enabling FIPS mode in the AnyConnect Network Access Manager client profile and enabling FIPS mode in the local policy. Windows XP also requires that you deploy the 3eTI FIPS Certified Crypto Kernel Library (CKL) to user computers connecting to FIPS networks.

With the Network Access Manager configured for FIPS compliance, users can still connect to non-FIPS networks. But when the user chooses to connect to a FIPS-compliant network, the Network Access Manager uses the 3eTI FIPS CKL and displays the FIPS compliance status (if the registry key *FIPSAlgorithmPolicy* is non-zero) in the Network Access Manager pane of the AnyConnect GUI.

This chapter describes how to enable FIPS compliance for the Network Access Manager and contains the following sections:

Enforcing FIPS Mode in the Network Access Manager

You can force enterprise employees to only connect to FIPS-compliant networks by restricting the allowed association and encryption modes, and the authentication methods, in the Network Access Manager configuration section of the AnyConnect profile.

The Network Access Manager FIPS compliance requires FIPS-approved AES encryption modes including WPA2 Personal (WPA2-PSK) and WPA2 Enterprise (802.1X).

The Network Access Manager FIPS support includes EAP methods EAP-TLS, EAP-TTLS, PEAP, EAP-FAST and LEAP.

The Network Access Manager enables you to enable both FIPS-compliant WLAN profiles as well as optional non-compliant configurations, such as access to Wi-Fi hotspots with client VPN security. As the administrator, you are responsible for naming the profile appropriately to indicate whether the network is FIPS enabled.

A fully FIPS-compliant client requires three components:

- the Network Access Manager module
- A FIPS-compliant local policy file
- For Windows XP only, 3eTI FIPS certified Crypto Kernel Library (CKL) with supported NIC adapter drivers

You enable FIPS mode in the local policy file with the Network Access Manager Profile Editor, Refer to the "Client Policy Window" section on page 4-6 for more information.

Installing the 3eTI Driver

This section provides instructions for installing the 3eTI FIPS validated Cryptographic Kernel Library (CKL) with supported drivers that integrate with Network Access Manager to provide a complete FIPS solution.

For Windows XP systems, the Network Access Manager Log Packager utility collects logs of the 3eTI packets.

Important Notes

1. The 3eTI CKL driver installer is designed to allow only one 3eTI wireless driver to be installed on a system at any given time. A previous driver must be un-installed prior to installing a different type of driver. For a driver of the same type, uninstalling the previous driver is not necessary because the next installation just updates the existing driver.
2. When the hardware is present and installed in the system, the installer updates the corresponding OEM wireless NIC adapter driver with the 3eTI modified driver that supports the 3eTI CKL.

3eTI CKL Driver Installer Overview

The 3eTI CKL driver installer can be started using one of these methods:

- Double-clicking the .exe file—can only be used for normal driver installations in which the NIC adapter is installed in the PC before the installer is run.
- Using the installer command without command-line options—can be used only for normal driver installations.

- Using the installer command with command-line options—can be used for normal and pre-installed driver installations.

When you start the driver installer by double-clicking the .exe file or using the run command without command-line options, the installer performs these operations:

- Detects and installs the 3eTI CKL with a supported NIC adapter driver for FIPS operation.
- If multiple NIC adapters are detected that support the 3eTI CKL, the installer prompts the user for adapter selection.
- If a compatible NIC adapter is not found on the PC, the installer aborts the installation and displays this error message:

  The installer cannot auto-detect a NIC chipset to provide FIPS support. To enforce a pre-installation, you are required to run the installer using the command line. For instructions or further assistance, please contact your network administrator.

Note Pre-installation scenarios are best supported with command-line options that allow you to specify specific installation options. Pre-installations are typically preformed by you, the network administrator, and not a novice user.

Installer Command and Command-Line Options

The installer supports the following command and command-line options:

3eTI-drv-installer.exe *–s –auto* **Type= XXXX**

–s	**Used to perform a silent installation without prompting the user.**	
–auto	Used to perform an intelligent installation, where the installer determines the supported NIC adapter in the PC and installs the appropriate driver. This causes the installer to perform the same operations as entering the command without command line options.	
Type=*XXXX*	Used to specify the NIC adapter chipset for a pre-installation or a normal installation. *Pre-installation* means that the driver is installed before the specified NIC adapter is installed in the PC. *Normal installation* means that the NIC adapter is installed before the driver is installed.	
	XXXX Value	**Description**
	Intel3945	Specifies drivers for the Intel3945 chipset.
	Centrino	Specifies drivers for Intel 2100, l2200, and 2915 chipsets.
	Broadcom	Specifies drivers for Broadcom chipsets supported by the Installer.
	Atheros	Specifies drivers for the Atheros 5001, 5004, 5005, AR5211, and AR5212 chipsets.
	Cisco	Specifies drivers for the Cisco AIR-CB21 card with an Atheros chipset.

Note When using –s for silent installation, you must also specify –auto or Type=XXXX or both –auto and Type=XXXX.

Examples:

- Using *–auto* in conjunction with *–s*:
  - Performs an intelligent installation by automatically detecting the NIC adapter that is installed.
  - Performs a silent installation without prompting the user.
  - If multiple NIC adapters are detected, selects any supported chipset.
- Using *–auto* in conjunction with *Type=XXXX*:
  - Attempts to Install the driver for the NIC adapter chipset specified by Type=XXXX.
  - If the detected NIC adapters do not support the specified chipset, installs a driver for any NIC adapter with a supported chipset.
- **Using** *3eTI-drv-installer.exe Type=Intel3945 –auto –s*:
  - Attempts to install a driver for the Intel3945 chipset without prompting the user.
  - If a NIC adapter with the Intel3945 chipset is not detected, silently installs a driver for any other detected NIC adapter with a supported chipset.
  - If a NIC adapter with a supported chipset is not detected, does not pre-install any driver.
- **Using** *3eTI-drv-installer.exe Type=Intel3945 –s*:
  - Attempts to install a driver for the Intel3945 chipset without prompting the user.
  - If a supported NIC adapter chipset is not detected, performs a pre-install by installing the specified chipset driver.

Running the Installer without Using Command-Line Options

To perform a normal installation with the NIC adapter installed in the PC, follow these instructions:

Step 1 Start the installer by following one of these steps:

a. Use Windows Explorer to locate the **3eTI-drv-installer.exe file on your PC and double-click the filename.**

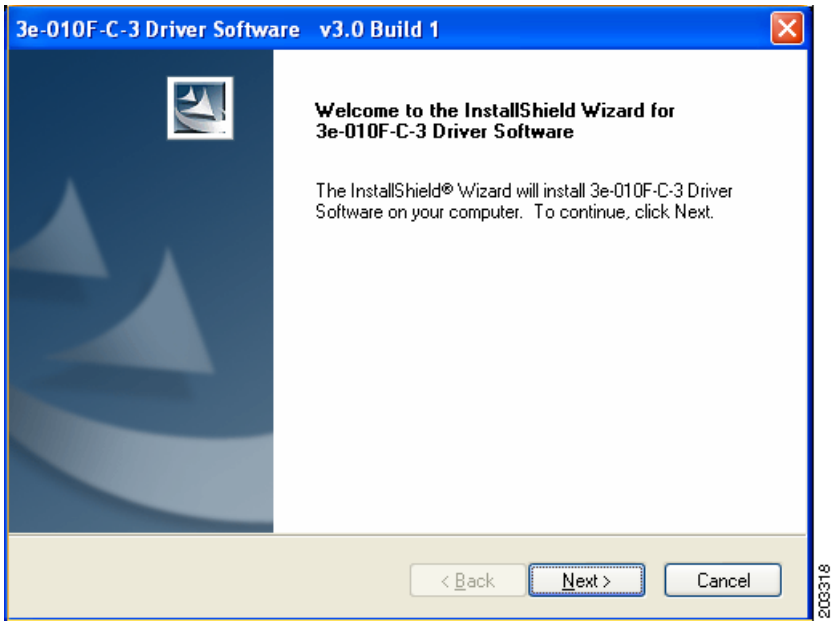
b. Click **Start > Run** and enter this installer run command:

path **/ 3eTI-drv-installer.exe**

Where *path* is the directory path to the installer file.

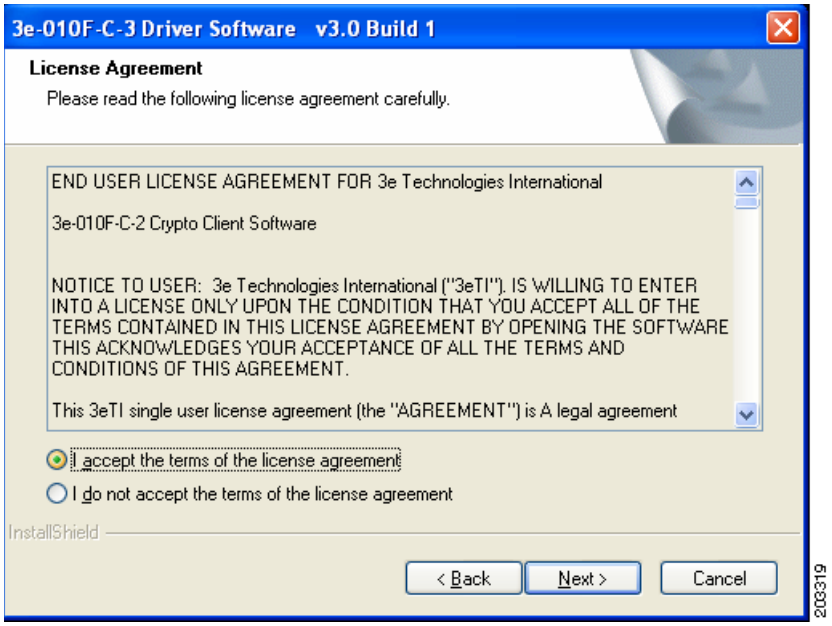
The Driver Welcome window appears (Figure 9-1).

Figure 9-1 Driver Welcome Window



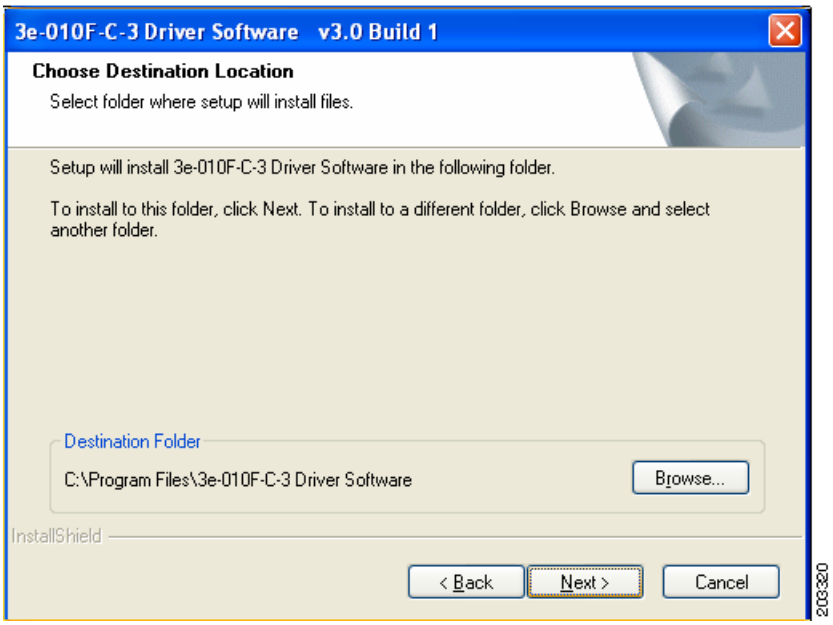
Step 2 Click **Next** and the license agreement appears (see Figure 9-2).

Figure 9-2 License Agreement



Step 3 Read and accept the license agreement and click **Next**. The Destination Location Window opens Figure 9-3.

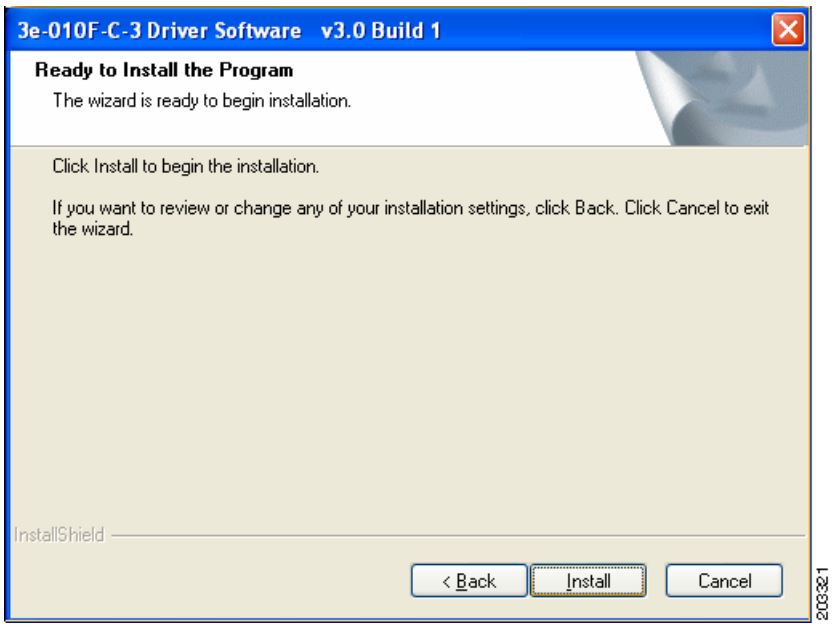
Figure 9-3 Destination Location Window



Step 4 Accept the driver software default destination folder or click **Browse** to locate the desired folder.

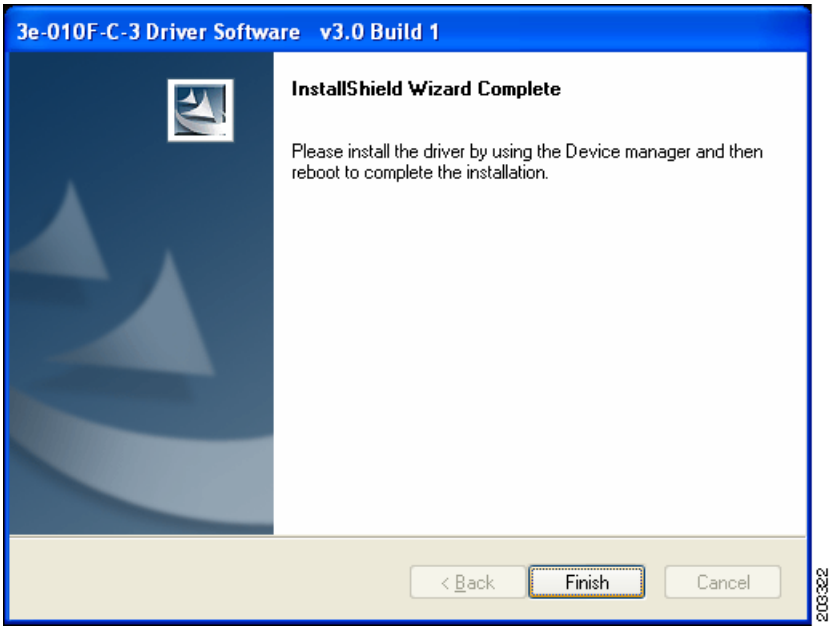
Step 5 Click **Next.** The Ready to Install window opens (Figure 9-4).

Figure 9-4 Ready to Install Window



Step 6 Click **Install** to start the installation process. When the installation completes, the Wizard Complete window opens, (Figure 9-5).

Figure 9-5 Wizard Complete Window



Step 7 Click **Finish**.

Uninstalling Previous 3eTI Driver Software

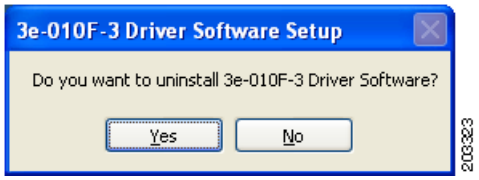
To uninstall previous 3eTI driver software, follow these steps:

Step 1 To uninstall the previous 3eTI driver software, click **Start > Settings > Control Panel > Add or Remove Programs**.

Step 2 Choose the 3eTI driver software, such as 3e-010F-3 and click **Remove**.

The Uninstall Driver Software window opens (see Figure 9-6).

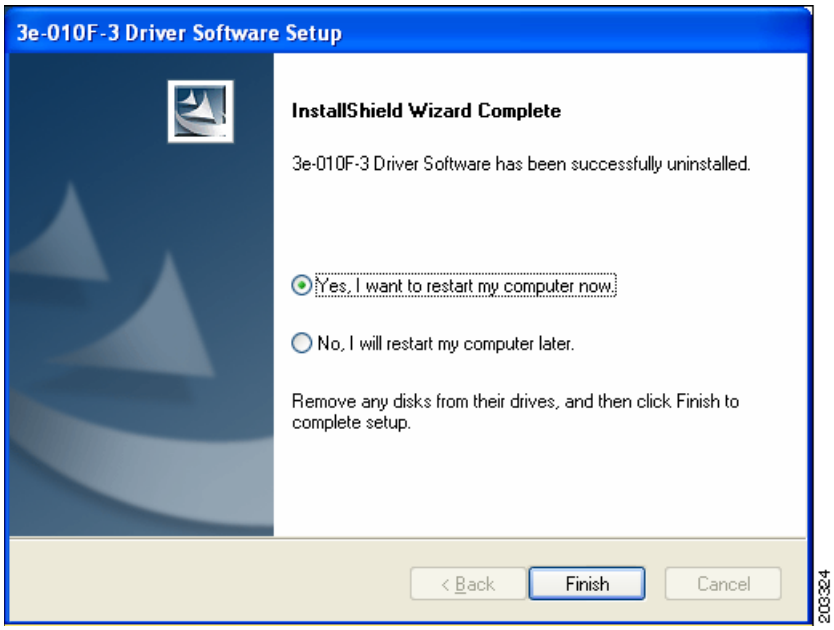
Figure 9-6 Uninstall Driver Software Pop-Up



Step 3 Click **Yes** to uninstall the driver software.

The Restart Computer window opens, Figure 9-7.

Figure 9-7 Restart Computer Now Window



Step 4 Check **Yes** to restart your computer.

Step 5 Click **Finish**.

Your PC reboots to completely remove the driver software.

Silent Driver Installation for Enterprise Deployment

To run the installer using a silent mode, follow these steps:

Step 1 Run the installer by entering this command:

path **/ 3eTI-drv-installer.exe -s Type=***XXXX*

Where:

path is the directory path to the installer file.

-s indicates silent installation.

Type= *XXXX specifies the chipset, such as Centrino, Intel3945, or Cisco (see the* "Installer Command and Command-Line Options" section on page 9-16*).*

A pop-up status window appears indicating that the driver installation is in progress and then disappears when the installation completes.

Installing the Driver without a Previously Installed Network Adapter

To install the 3eTI driver on a PC without an installed NIC adapter, follow these steps:

Step 1 Start the installer by clicking **Start** > **Run** and enter this installer run command:

path **/ 3eTI-drv-installer.exe Type =** *XXXX*

Where:

path is the directory path to the installer file.

Type=*XXXX specifies the chipset, such as Centrino, Intel3945, or Cisco (see the* "Installer Command and Command-Line Options" section on page 9-16*).*

Figure 9-1 appears.

Step 2 Perform Step 2 through Step 7 in the "Running the Installer without Using Command-Line Options" section on page 9-17.

Step 3 When the driver installation is complete, insert or install the NIC adapter in the PC.

Manually Upgrading the 3eTI Driver Software

Manual upgrade instructions are provided to help troubleshoot driver installation problems. This is not expected to be a part of an enterprise-wide deployment.

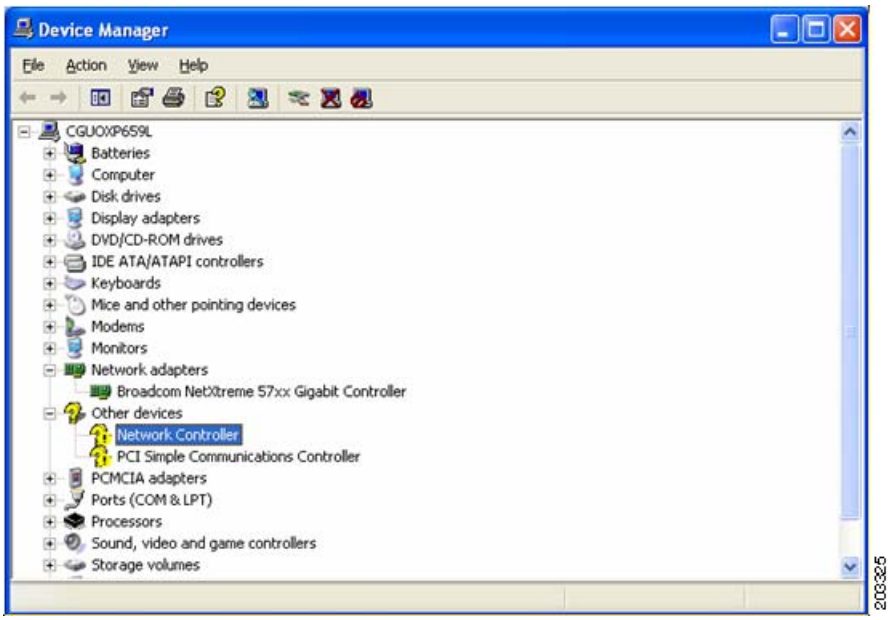
Follow these steps to manually upgrade the 3eTI driver software using the Windows Device Manager:

Step 1 Right-click the **My Computer** icon on your desktop and choose **Properties**.

Step 2 Click **Hardware** on the System Properties window, click **Device Manager**.

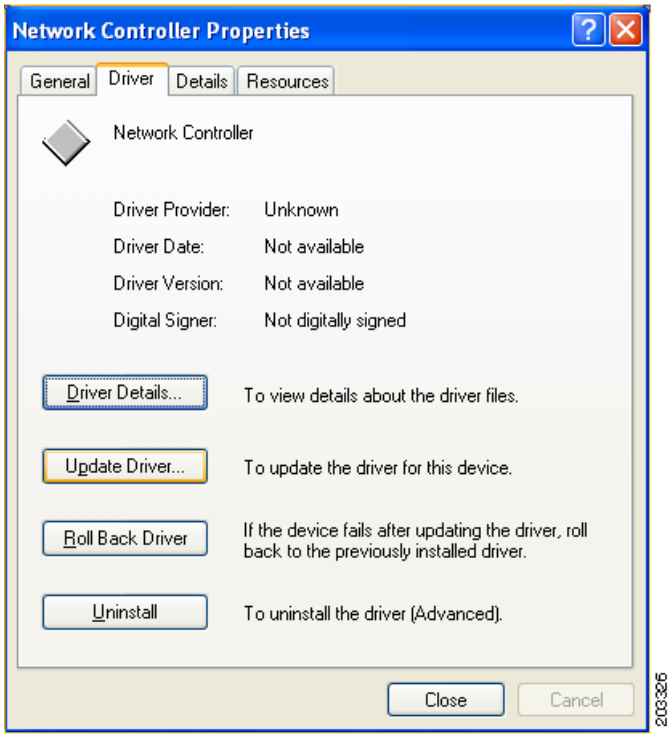
The Windows Device Manager window opens, Figure 9-8.

Figure 9-8 Windows Device Manager Window



Step 3 If your Network Adapter is installed or inserted and the driver software is not installed, the device will be listed under Other devices and shown with a yellow question mark. Right-click on your network adapter and choose **Properties**. The Network Controller Properties window opens, Figure 9-9.

Figure 9-9 Network Controller Properties Window



Step 4 Click **Driver > Update Driver.**

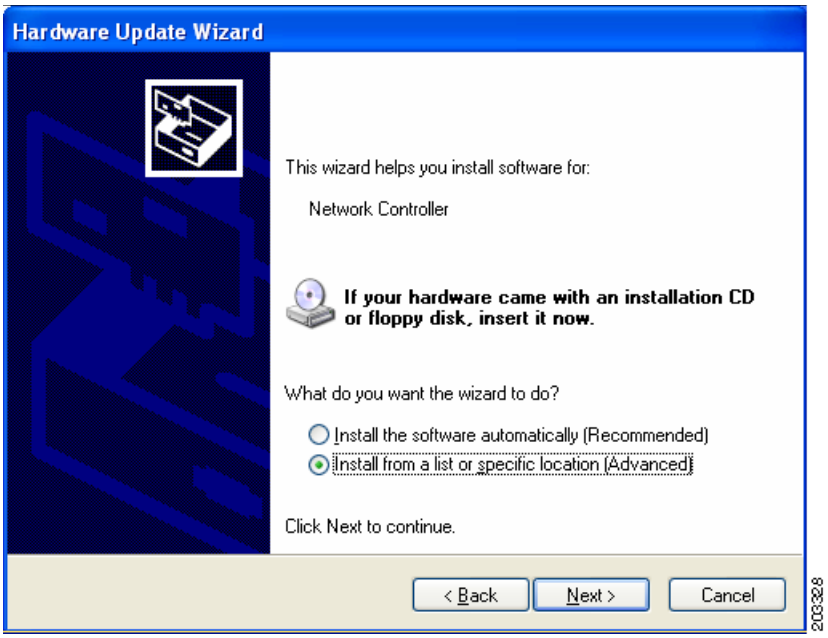
The Windows Hardware Update Wizard window opens, Figure 9-10.

Figure 9-10 Windows Hardware Update Wizard Window

Step 5 Click **No** to prevent Windows from searching for the driver software and click **Next**.

The Hardware Update wizard continues, Figure 9-11.

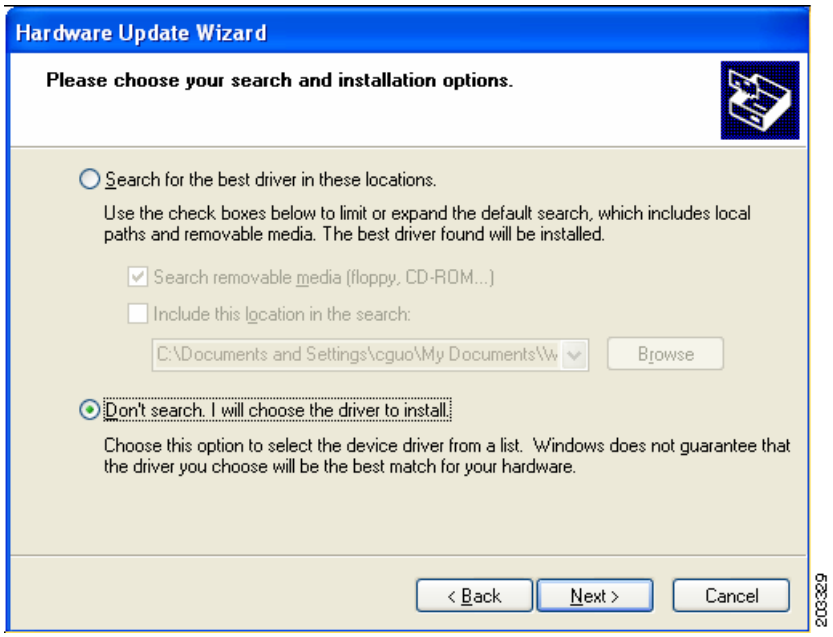
Figure 9-11 Installation CD or Floppy Disk Option Window



Step 6 Check **Install from a list or specific location (Advanced)** and click **Next**.

The Search and Installation Options window opens, Figure 9-12.

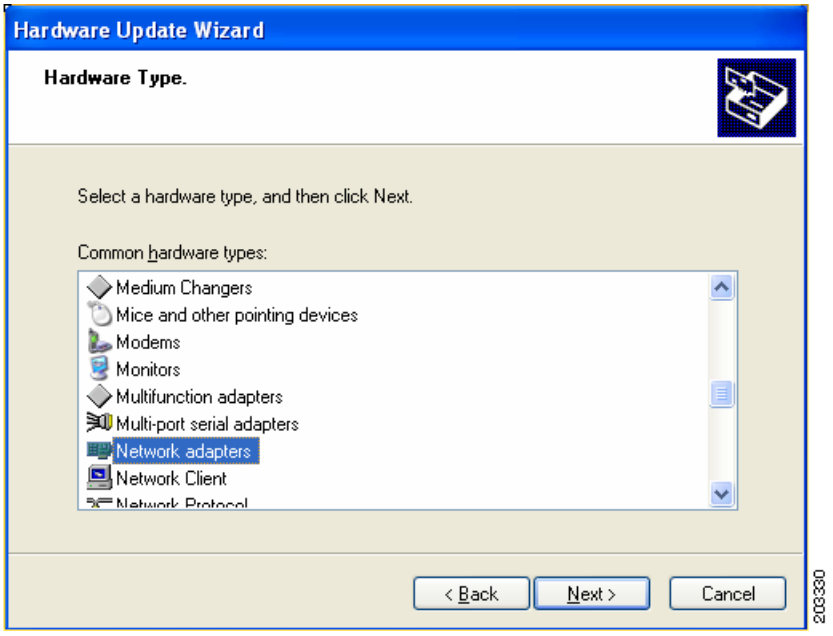
Figure 9-12 Search and Installation Options Window



Step 7 Check **Don't search. I will choose the driver to install** and click **Next**.

The Windows Hardware Type window opens, Figure 9-13.

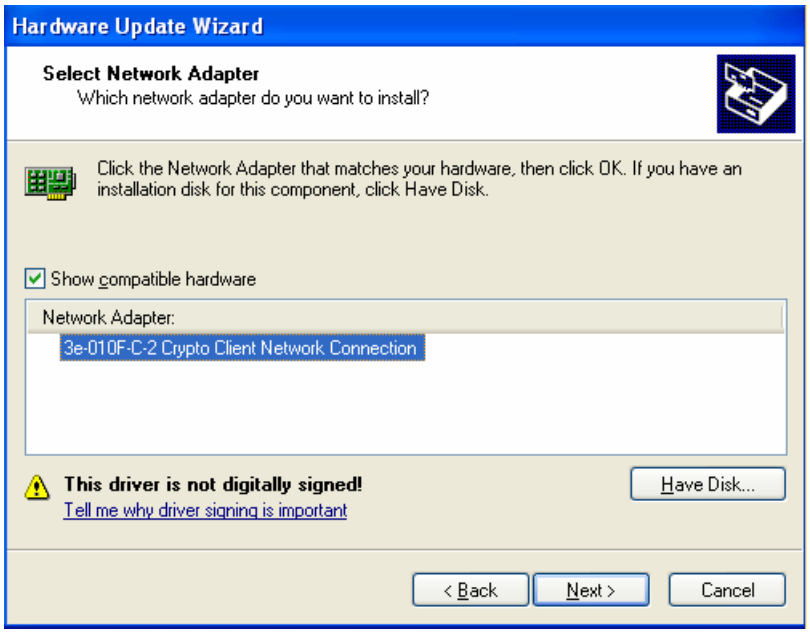
Figure 9-13 Windows Hardware Type Window



Step 8 Choose **Network adapter and** click **Next.**

Step 9 The Select Network Adapter window opens, Figure 9-14.

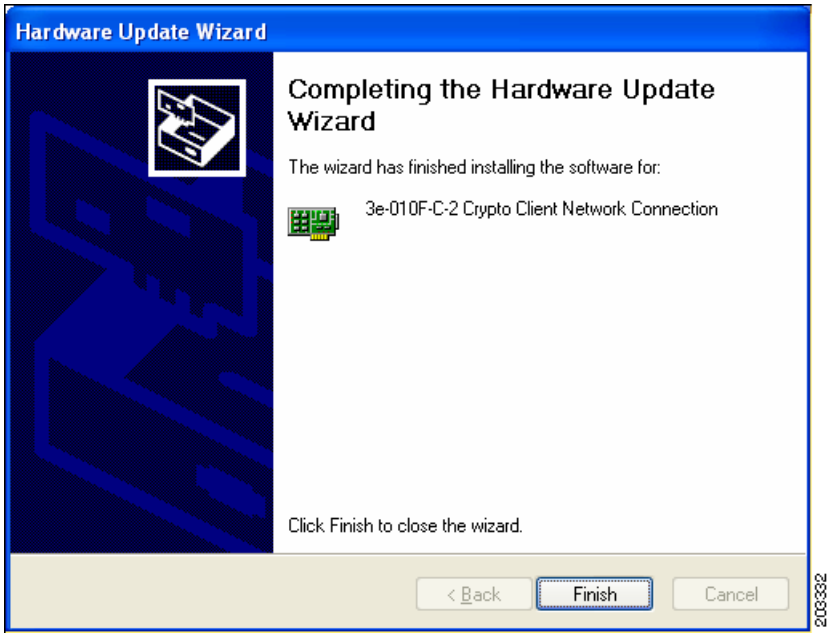
Figure 9-14 Select Network Adapter Window



Step 10 Choose the 3eTI network connection and click **Next**.

The Installation Complete window opens, Figure 9-15.

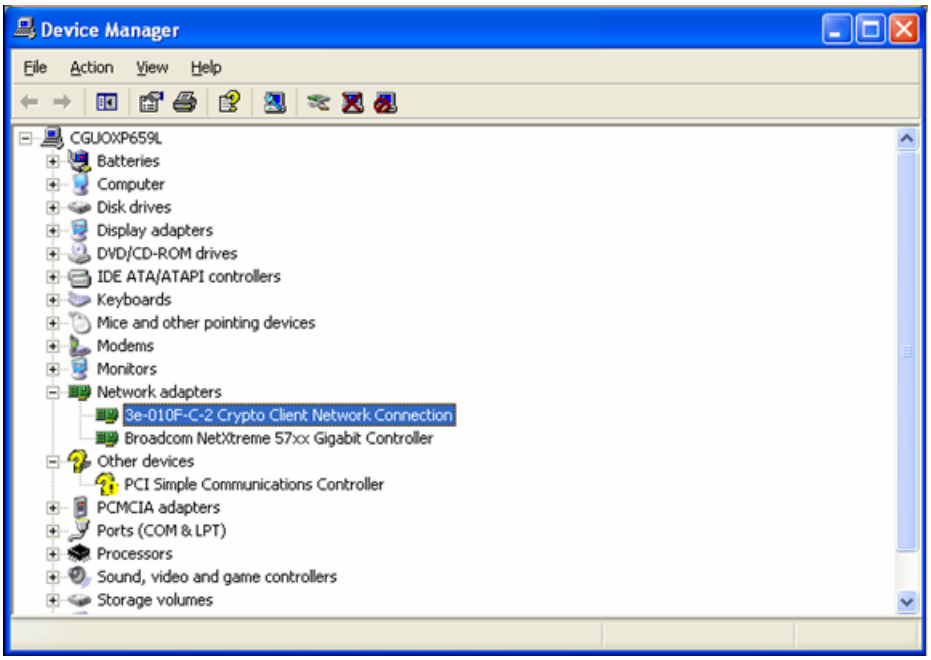
Figure 9-15 Installation Complete Window



Step 11 The hardware driver installation is complete. Click **Finish**.

The Device Manager window reappears (see Figure 9-16).

Figure 9-16 Updated Windows Device Manager Window



Step 12 To verify that the driver is installed properly, right click on the 3eTI network connection and choose **Properties**. Ensure that the adapter properties window indicates **This device is working properly** under the Device status.

Obtaining the 3eTI Driver Installer Software

The FIPS 3eTI CKL supported driver installer cannot be downloaded from the Cisco Software Center and must be ordered from Cisco. A non-expiring license for the driver installer can be ordered from Cisco using this product number: AIR-SSCFIPS-DRV

The ordered 3eTI CKL supported driver installer software is shipped to you on a product CD.