CHAPTER 8

Enabling FIPS and Additional Security

The Cisco AnyConnect Secure Mobility client VPN functionality and the optional Network Access Manager and telemetry modules support Level 1 of the Federal Information Processing Standard (FIPS), 140-2, a U.S. government standard for specific security requirements for cryptographic modules. The FIPS 140-2 standard applies to all federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems.

The FIPS feature is 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. This file is an XML file containing security settings, and is not deployed by the ASA, but must be installed manually or deployed using an enterprise software deployment system. You must purchase a FIPS license for the ASA the client connects to.
- AnyConnect Network Access Manager—Supported on Windows XP computers only, and enabled in the AnyConnect client profile. FIPS support for the Network Access Manager requires that you deploy 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.

This section contains the following sections:

- Enabling FIPS for the AnyConnect Core VPN Client, page 8-2
- Enabling Software and Profile Locks, page 8-6
- AnyConnect Local Policy Parameters and Values, page 8-11
- Enabling FIPS for the Network Access Manager, page 8-15

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 or change the file manually on a user computer.

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.

You must also ensure the list of SSL encryption types configured on the ASA has a FIPS-compliant cipher configured as the top position in the list. Otherwise, the DTLS connection fails.

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 our MST File, page 8-2
- Enabling FIPS and other Local Policy Parameters with your own MST File, page 8-2
- Enabling FIPS and Other Parameters with our Enable FIPS Tool, page 8-3
- Changing Local Policy Parameters Manually in the Local Policy, page 8-4
- Configuring the ASA to use FIPS-Compliant SSL Encryption, page 8-5
- Avoiding Endpoint Problems from AnyConnect FIPS Registry Changes, page 8-5
- AnyConnect Local Policy Parameters and Values, page 8-11

Enabling FIPS for Windows Clients using our MST File

For Windows installations, you can apply the MST file we provide to the standard MSI installation file to enable FIPS in the AnyConnect Local Policy. The MST only enables FIPS and does not change other parameters. The installation generates an AnyConnect Local Policy file with FIPS enabled.

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

Enabling FIPS and other Local Policy Parameters with your own MST File

You can create your own MST file to change any local policy parameters. Create your own MST file using the following parameters. The names correspond to the parameters in AnyConnect Local Policy file (AnyConnectLocalPolicy.xml). See Table 8-9 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, then the client installer can create the new policy file.

Enabling FIPS and Other Parameters with our Enable FIPS Tool

For all operating systems, you can use our 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 8-1 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 Table 8-9.

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 8-1 shows the policy settings and the arguments for the Enable FIPS tool.

Table 8-1 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.

Table 8-2 shows the installation path for each operating system.

Table 8-2 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 for the local policy file for AnyConnect 2.5.

Step 2 Edit the parameter settings. The example below shows the contents of the AnyConnect Local Policy file for Windows:

```
<?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>
</AnyConnectLocalPolicy>
```

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

Configuring the ASA to use FIPS-Compliant SSL Encryption

By default, AnyConnect SSL connections to the ASA use Datagram Transport Layer Security (DTLS), which improves the performance of real-time applications that are sensitive to packet delays. The cipher specified in the list of SSL encryptions configured on the ASA is the one specified for the connection.

By default, the SSL encryption list on the ASA contains these ciphers in the following order:

- RC4-SHA1
- AES128-SHA1 (FIPS-compliant)
- AES256-SHA1 (FIPS-compliant)
- 3DES-SHA1 (FIPS-compliant)

Therefore, by default, the ASA specifies the *non-FIPS-compliant* RC4-SHA1 for the connection. To be FIPS-compliant, you must ensure a FIPS-compliant cipher is the first one specified in the list of SSL encryptions. Otherwise, the DTLS connection fails. Furthermore, we recommend you remove all non-FIPS ciphers from the list to ensure the connection failure doesn't occur.

In ASDM, go to **Configuration** > **Remote Access VPN** > **Advanced** > **SSL Settings** to specify the SSL encryption types. In the Encryption area, move a FIPS-compliant cipher to the top position in the list.

If you are using CLI, use the **ssl encryption** command from global configuration mode to order the list.

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 AnyConnect has enabled FIPS and start using cryptography also. For example, the Microsoft Terminal Services client Remote Desktop Protocol (RDP) will not work because RDP will require 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 8-3 shows the Windows registry changes performed by AnyConnect that you should be aware of:

Table 8-3 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 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.

Enabling Software and Profile Locks

You can restrict the client to obtaining software or client profile updates only from ASAs that you allow by using the software lock or profile lock. By default, the locks are disabled. The AnyConnect client can receive software or client profile updates from any ASA.

With the software lock enabled, the client checks that the ASA is on the list of authorized servers before updating the core VPN client and any optional client modules (such as the Network Access Manager, telemetry, Web Security, and so on). If the client version loaded on the ASA is newer than the client on the endpoint, but the ASA is not in the list of servers in the software lock, the endpoint client cannot connect. If the client versions are the same, the endpoint client can connect to the ASA.

With the profile lock enabled, the client checks the same list before updating the client profiles for VPN or the other modules. If the ASA is not on the list, the client connects to the ASA but doesn't update the profile(s). If this occurs, the following features are unavailable:

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

AnyConnect Upgrades

When the client connects to the ASA, and a new AnyConnect client package is available, it first determines if the ASA is an authorized server by comparing the ASA name with the server name in the *Authorized Server list* in the local policy file or the *default domain* from the global preferences file. If the ASA is authorized, the client downloads all modules and launches the upgrade of the core VPN client, deleting and recreating the plugins directory, which disables all the optional modules currently installed.

After the core VPN client upgrade, optional modules specified at the ASA are upgraded. Those modules already installed but not specified at the ASA are not upgraded and remain disabled. The client also downloads all the profiles, including the VPN profile and other service profiles supported on the endpoint computer.

If the ASA is not an authorized one, the client checks for the software lock and VPN profile lock. If unauthorized, the only client profile downloaded is the VPN profile. Profiles for the optional modules are not downloaded, irrespective of the lock.

Note If the ASA is not authorized, the Network Access Manager, telemetry, and Web Security profiles are not downloaded to the ASA, regardless of the profile lock.

Connecting to an Unauthorized ASA

If the software lock is on, the client does not upgrade anything and disconnects. If the software lock is off, the client ignores the list of optional modules at the ASA and gets the list of all modules currently installed on the system from the *VPNmanifest.dat* file and upgrades only those modules from the ASA. Therefore, any new modules specified at this unauthorized ASA are not installed, and any modules not enabled at the ASA but currently installed on the endpoint computer are not disabled.

The software lock also controls downloading customizations, localizations, scripts and transforms—they are not downloaded from an unauthorized ASA if the software lock is on. Therefore, you must make sure that policy enforcement is not done through scripts for non-corporate assets.

Note If both corporate and non-corporate assets connect to a specific ASA, and that ASA deploys scripts for policy enforcement, those scripts will not run on non-corporate assets that have the software lock on. To remedy this, separate the users of these non-corporate assets into a different group policy on the ASA.

If VPN profile lock is off, the client fetches only the VPN profile and saves it. If on, the VPN profile is not downloaded. The client continues to connect without the profile, resulting in many features being unavailable.

Same Version With Different Modules Enabled

When the client connects to an authorized ASA and determines the modules have changed, it downloads and installs any new modules specified on the ASA. In the case where the core VPN client is not updated, the plugins directory is not deleted. Therefore, modules that have been installed but not specified at the ASA remain enabled.

In case of an unauthorized ASA, the client does not install any new modules or disable any modules not specified at the ASA.

Uninstalling the Core VPN Client

If you uninstall the core VPN client manually (using Windows Add or Remove Programs), all optional client modules also uninstall regardless of the version of the installed core VPN client.

Default Authorized Domain

When the client connects for the first time to a ASA, the global preferences file does not have a value for the default domain. Without a value, if the authorized server list is empty, the current ASA domain name (the ASA name minus the host name) is added as a default domain in the global preferences file. For example, if the ASA is vpn.newyork.example.com, the following lines are added to the global preferences file:

```
<DefaultDomain>example.com</DefaultDomain>
```

The default domain is treated as an authorized ASA, as if it appeared in the list of authorized servers in the local policy file. Be aware that the settings defined in the local policy take precedence over the default domain. Therefore, if you deploy a new local policy file which contains an authorized server list using a software management system (or some other method), the default domain is ignored.

Connecting to an Unauthorized ASA with the Profile Lock Off

If a client connects to an unauthorized ASA that has the Always-on feature enabled and the VPN profile lock is off in the local policy, the old profiles are deleted and the client cannot reconnect to that ASA. Therefore, if you are using Host Scan to detect corporate assets, or you have the right group partitions enabled, be careful that you do not force the Always-on feature to the non-corporate assets and guests.

Logging

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.

XML Tags for the Software and Profile Locks

The following text is an example local policy file. The XML tags for the software and profile locks appear between the UpdatePolicy tags. These tags appear in bold in this example.

You list the authorized servers between the <AuthorizedServerList> tags. The servers can contain either an FQDN or an IP Address. They can have also contain wild cards. For example: newyork.example.com, *.example.com, or 1.2.3.*

Note If you want remote users to connect using the IP address of the server, be sure so list the IP address in the authorized server list. If the user attempts to connect using the IP address but the server is listed as an FQDN, the attempt is treated as connecting to an unauthorized domain.

The example server names *seattle.example.com* and *newyork.example.com* are FQDNs of authorized servers:

```
<?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>true</AllowVPNProfileUpdatesFromAnyServer>
        <AuthorizedServerList>
            <ServerName>seattle.example.com</ServerName>
            <ServerName>newyork.example.com</ServerName>
        </AuthorizedServerList>
    </UpdatePolicy>
</AnyConnectLocalPolicy>
```

Software Lock Use Cases

Table 8-4, Table 8-5, Table 8-6, and Table 8-7 provide use cases for the client connecting to authorized and unauthorized ASAs with client package versions that are the same, and different:

Table 8-4 Connecting to an Authorized ASA Having a Newer AnyConnect Package

Client Modules Initially Installed	ASA with Modules A, B, C, D enabled	ASA with modules A, B, X, Y enabled	ASA with modules A, B enabled
A, B, C installed and enabled.	A, B, and C are updated with the version loaded on the ASA. The version of D loaded on the ASA is installed.	A and B are updated with the version loaded on the ASA. The versions of X and Y loaded on the ASA are installed. C is disabled but remains installed and is not upgraded.	A and B are updated with the version loaded on the ASA. C is disabled but remains installed and is not upgraded.
A, B, C installed. C is disabled due to previous update.	A, B, and C are updated. C is enabled. D is installed.	A and B are updated. X and Y are installed. C remains disabled and is not updated.	A and B are updated. C remains disabled and is not updated.

Table 8-5 Connecting to an Unauthorized ASA Having a Newer AnyConnect Package

Client Modules Initially Installed	ASA with Modules A, B, C, D Enabled	ASA with Modules A, B, X, Y Enabled	ASA with Modules A, B Enabled
A, B, C installed and enabled. Software lock OFF.	A, B and C are updated with the version loaded on the ASA. D is not downloaded.	A and B are updated with the version loaded on the ASA. C is updated even though it is not specified at this ASA. X and Y are not downloaded.	A and B are updated with the version loaded on the ASA. C is updated even though it is not specified at this ASA.
A, B, C installed. C is disabled due to previous update. Software lock OFF.	A and B are updated with the version loaded on the ASA. C is not updated and remains disabled.	A and B are updated with the version loaded on the ASA. C is not updated and remains disabled.	A and B are updated with the version loaded on the ASA. C is not updated and remains disabled.
A, B, C installed and enabled. Software lock ON.	No modules are downloaded or updated, and the client disconnects.	No modules are downloaded or updated, and the client disconnects.	No modules are downloaded or updated, and the client disconnects.
A, B, C installed. C is disabled due to previous update. Software lock ON.	No modules are downloaded or updated, and the client disconnects.	No modules are downloaded or updated, and the client disconnects.	No modules are downloaded or updated, and the client disconnects.

Table 8-6 Connecting to an Authorized ASA with the Same Version AnyConnect Package but Different Modules

Client Modules Initially Installed	ASA with Modules A, B, C, D Enabled	ASA with Modules A, B, D Enabled	ASA with Modules A, B Enabled
A, B, C installed and enabled.	D is downloaded and installed. A, B, C and D are installed and enabled.	D is downloaded and installed. C is not disabled. A, B, C, and D are installed and enabled.[1]	No modules are downloaded. A, B, and C remain enabled.
A, B, C installed. C is disabled due to previous update.	D is downloaded and installed. A, B, and D are installed and enabled. C remains disabled.[2]	D is downloaded and installed. A, B, and D are installed and enabled. C remains disabled.	No modules are downloaded. A and B remain enabled. C remains disabled.

[1] If you want to disable C, you must deploy a client VPN profile with a *Disable Service* enabled.

[2] You can only enable C if you load an AnyConnect package that is newer and C is enabled.

Table 8-7 Connecting to an Unauthorized ASA with the Same Version AnyConnect Package but Different Modules

Client Modules Initially Installed	ASA with Modules A, B, C, D Enabled	ASA with Modules A, B, D Enabled	ASA with Modules A, B Enabled
A, B, C installed and enabled. Software lock OFF or ON.	No modules are downloaded. A, B, and C remain enabled.	No modules are downloaded or disabled. A, B, and C remain enabled.	No modules are disabled. A, B, and C remain enabled.

Software and Profile Lock Example

The following example scenario describes the client upgrading behavior with differing versions of AnyConnect package on the client PC and the ASA. Table 8-8 lists the AnyConnect package versions for three ASAs:

Table 8-8 Example ASA and AnyConnect Client Information

ASA	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, telemetry

Continuing with this example, the local policy XML file has the following contents:

```
<UpdatePolicy>
    <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
    <AllowVPNProfileUpdatesFromAnyServer>false</AllowVPNProfileUpdatesFromAnyServer>
    <AuthorizedServerList>
        <ServerName>seattle.example.com</ServerName>
        <ServerName>newyork.example.com</ServerName>
    </AuthorizedServerList>
</UpdatePolicy>
```

According to this local policy, the software lock is *off* and the VPN profile lock is *on*.

The AnyConnect client user connects to seattle.example.com first. Then VPN, the Network Access Manager and Web Security are installed (all the modules supported by version 3.0.0350). The user then decides to connect to newyork.example.com, an authorized ASA running a newer version (version 3.0.0351). The ASA deletes the plugins directory, and VPN and the Network Access Manager are upgraded to version 3.0.0351. Web Security remains at version 3.0.0350 and disabled.

The user then connects to raleigh.example.com which is not in the authorized server list. Since the software lock is not on, VPN and the Network Access Manager are upgraded to 3.0.0352. However, the other modules specified (posture and telemetry) are not installed. Web Security remains at version 3.0.0350 and disabled.

Because the VPN profile lock is on, the VPN client profile is not downloaded. Because raleigh-example.com is not an authorized server, other service profiles are also not downloaded.

AnyConnect Local Policy Parameters and Values

Note If you omit a policy parameter in the profile file, the feature resorts to default behavior.

Table 8-9 describes the parameters in the AnyConnect Local Policy file and their values:

Table 8-9 AnyConnect Local Policy File and their Values

Parameter and Description	Values and Value Formats
acversion Specifies the minimum version of the AnyConnect client capable of interpreting all of the parameters in the file. If a client older than the version specified reads the file, it issues an event log warning.	The format is acversion="<version number>".
xmlns The XML namespace specifier. Most administrators do not change this parameter.	The format is a URL, for example: xmlns=http://schemas.xmlsoap.org/encoding/
xsi:schemaLocation The XML specifier for the schema location. Most administrators do not change this parameter.	The format is a URL, for example: xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectLocalPolicy.xsd">
xmlns:xsi The XML schema instance specifier. Most administrators do not change this parameter.	The format is a URL, for example: xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance

Table 8-9 AnyConnect Local Policy File and their Values (continued)

Parameter and Description	Values and Value Formats
FipsMode Enables FIPS mode for the client. The client uses only algorithms and protocols approved by the FIPS standard.	*true*—Enables FIPS mode. *false*—Disables FIPS mode (default).
BypassDownloader Disables the launch of the VPNDownloader.exe module, which is responsible for detecting the presence of and updating the local versions of the dynamic content.	*true*—The client does not check for dynamic content present on the ASA, including translations, customization, optional modules, and core software updates; however, the client will attempt to compare its VPN client profile to the one associated with its group policy on the ASA. *false*—The client checks for dynamic content present on the ASA (default). When the client attempts to connect to the ASA, both the client and the ASA must have the same VPN client profile installed. If they do not have the same VPN client profile, the client attempts to download the VPN client profile assigned to the selected ASA AnyConnect Connection Profile. If **BypassDownloader** is set to **true**, the client will not download the VPN client profile. If the client does not download the VPN client profile, one of two things happens: • If the VPN client profile on the ASA is different than the one on the client, the client aborts the connection attempt because the policy defined by the VPN client profile on the ASA will not be enforced. • 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 prior to the client connecting to the 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.
RestrictWebLaunch Prevents users from using a non-FIPS-compliant browser to obtain the security cookie used to initiate an AnyConnect tunnel by forbidding the use of WebLaunch and forcing users to connect using the AnyConnect FIPS-compliant stand-alone connection mode.	*true*—WebLaunch attempts fail, and the client displays an informative message to the user. *false*—Permits WebLaunch (default—behavior consistent with AnyConnect 2.3 and earlier).

Table 8-9 AnyConnect Local Policy File and their Values (continued)

Parameter and Description	Values and Value Formats
StrictCertificateTrust 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. **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 were 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.	*true*—The client fails to connect to security gateways that use self-signed certificates and displays this message: `Local policy prohibits the acceptance of untrusted server certificates. A connection will not be established.` *false*—The client prompts the user to accept the certificate (default—behavior consistent with AnyConnect 2.3 and earlier).
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).
RestrictTunnelProtocols (currently not supported) Forbids the use of certain tunnel protocol families to establish a connection to the ASA.	*TLS*—The client only uses IKEv2 and ESP to establish the tunnel and will not use TLS/DTLS to communicate information to the secure gateway. *IPSec*—The client only uses TLS/DTLS for authentication and tunneling. *false*—Any encrypted protocol may be used in connection establishment (default). **Note** If you forbid the use of TLS or other protocols, certain advanced features, such as the automatic upgrading of Secure Desktop, may not work.

Table 8-9 AnyConnect Local Policy File and their Values (continued)

Parameter and Description	Values and Value Formats
ExcludeFirefoxNSSCertStore (Linux and Mac) Permits or excludes the client from using the Firefox NSS certificate store to verify server certificates. The store has information about where to obtain certificates for client certificate authentication.	*true*—Excludes the Firefox NSS certificate store. *false*—Permits the Firefox NSS certificate store (default).
ExcludePemFileCertStore (Linux and Mac) Permits or excludes the client from using the PEM file certificate store to verify server 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.	*true*—Excludes the PEM file certificate store. *false*—Permits the PEM file certificate store (default).
ExcludeMacNativeCertStore (Mac only) Permits or excludes the client from using the Mac native (keychain) certificate store to verify server certificates.	*true*—Excludes the Mac native certificate store. *false*—Permits the Mac native certificate store (default).
ExcludeWinNativeCertStore (Windows only, currently not supported) Permits or excludes the client from using the Windows Internet Explorer native certificate store to verify server certificates.	*true*—Excludes the Windows Internet Explorer certificate store. *false*—Permits the Windows Internet Explorer certificate store (default).
AllowSoftwareUpdateFromAnyServer Allows software updates from any ASA, or restricts the client to obtaining software only from ASAs that you allow.	*true*—Software updates for the AnyConnect client are allowed from any ASA (default). *false*—Software updates for the AnyConnect client are allowed only from ASAs specifed in the AuthorizedServerList section.
AllowVPNPolicyUpdateFromAnyServer Allows updates to the VPN local policy file from any ASA, or restricts the client to obtaining updates only from ASAs that you allow.	*true*—VPN local policy file updates for the AnyConnect client are allowed from any ASA (default). *false*—VPN local policy file updates for the AnyConnect client are allowed only from ASAs specifed in the AuthorizedServerList section.
AuthorizedServerList A list of servers allowed to update the AnyConnect client software or VPN local policy file.	Server names listed with ServerName.
ServerName A server name for the software of local policy lock.	The name of a server from which the AnyConnect client can receive software or VPN local policy file updates. ServerName can be an FQDN, IP address, domain name, or wildcard with domain name.

Local Policy File Example

The following is an example of the AnyConnect Local Policy 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>
</AnyConnectLocalPolicy>
```

Enabling FIPS for the Network Access Manager

FIPS compliance for Network Access Manager is supported for Windows XP only and requires that you enable FIPS mode in the AnyConnect client Network Access Manager profile and 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 these sections:

- Enforcing FIPS Mode in the Network Access Manager, page 8-15
- Enabling FIPS Status Reporting on the AnyConnect GUI, page 8-16
- Installing the 3eTI Driver, page 8-16
- Obtaining the 3eTI Driver Installer Software, page 8-29

Note FIPS compliance for the Network Access Manager is only supported on user computers running Windows XP.

Enforcing FIPS Mode in the Network Access Manager

You can allow 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 supports 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, EAP-PEAP, and EAP-FAST.

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

A fully FIPS-compliant solution requires three components:

- the Network Access Manager
- 3eTI FIPS certified Crypto Kernel Library (CKL) with supported NIC adapter drivers
- A FIPS-compliant network profile configuration

Within the Network Access Manager Profile Editor, you can enable FIPS mode. Refer to the "Configuring a Client Policy" section on page 4-4 for more information.

Enabling FIPS Status Reporting on the AnyConnect GUI

The AnyConnect GUI provides a FIPS status indicator on the Network Access Manager pane of the GUI. You must set the following registry key on the endpoint computer to a non-zero value to enable the FIPS status indicator:

```
HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy
```

FIPS Integration

To ensure a FIPS-compliant solution, you must set up network profiles that allow only WPA2 handshakes with AES encryption with FIPS-compliant EAP types or WPA2-Personal (Pre-shared key).

The Network Access Manager Log Packager utility collects logs of the 3eTI packets.

3eTI CKL Driver Installer

For instructions on how to install the 3eTI FIPS validated CKL with supported drivers, see the "Installing the 3eTI Driver" section on page 8-16.

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.

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.

<table>
<tr><td rowspan="7"><b>Type=</b><i>XXXX</i></td><td colspan="2">Used to specify the NIC adapter chipset for a pre-installation or a normal installation.
<i>Pre-installation</i> means that the driver is installed before the specified NIC adapter is installed in the PC.
<i>Normal installation</i> means that the NIC adapter is installed before the driver is installed.</td></tr>
<tr><td><b>XXXX Value</b></td><td><b>Description</b></td></tr>
<tr><td>Intel3945</td><td>Specifies drivers for the Intel3945 chipset.</td></tr>
<tr><td>Centrino</td><td>Specifies drivers for Intel 2100, l2200, and 2915 chipsets.</td></tr>
<tr><td>Broadcom</td><td>Specifies drivers for Broadcom chipsets supported by the Installer.</td></tr>
<tr><td>Atheros</td><td>Specifies drivers for the Atheros 5001, 5004, 5005, AR5211, and AR5212 chipsets.</td></tr>
<tr><td>Cisco</td><td>Specifies drivers for the Cisco AIR-CB21 card with an Atheros chipset.</td></tr>
</table>

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.

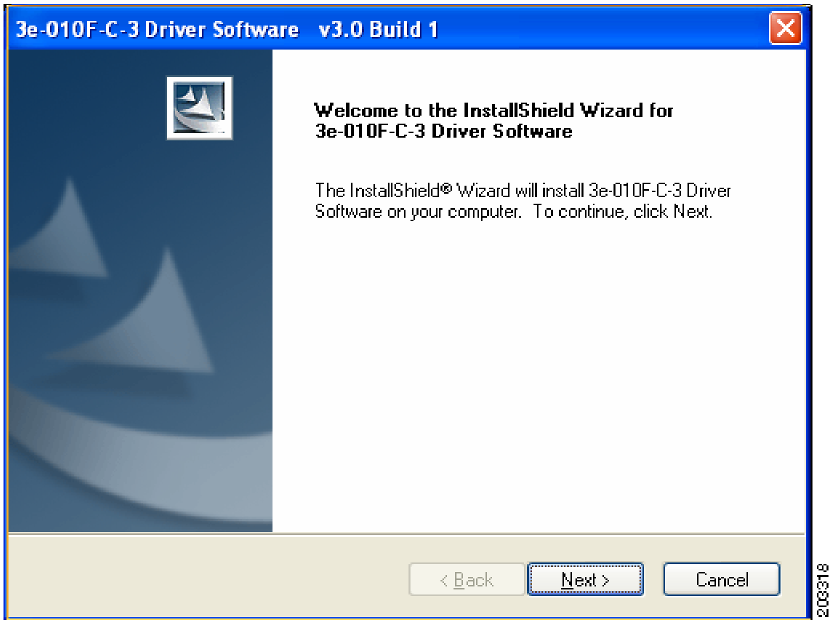
b. Click **Start** > **Run** and enter this installer run command:

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

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

The Driver Welcome window appears (Figure 8-1).

Figure 8-1 Driver Welcome Window



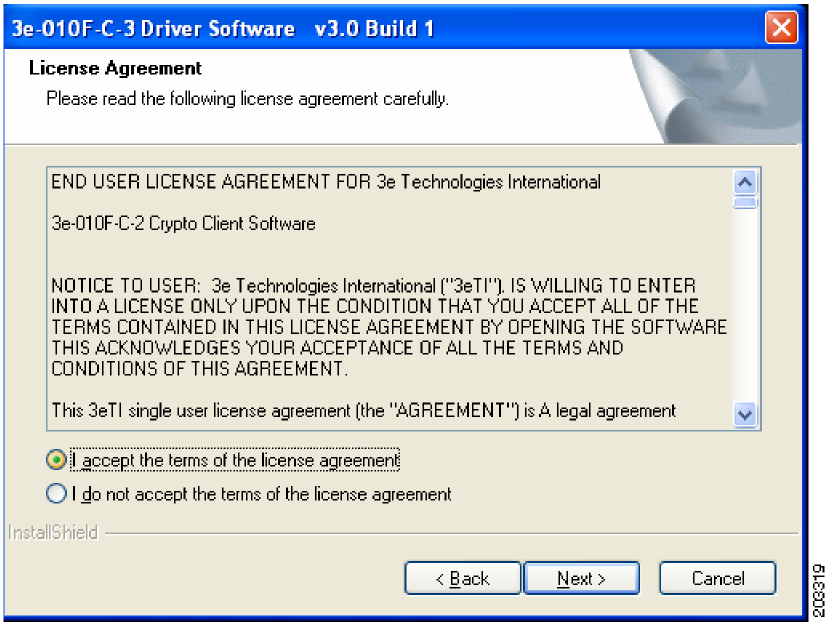
3e-010F-C-3 Driver Software v3.0 Build 1

Welcome to the InstallShield Wizard for 3e-010F-C-3 Driver Software

The InstallShield® Wizard will install 3e-010F-C-3 Driver Software on your computer. To continue, click Next.

Step 2 Click **Next** and the license agreement appears (see Figure 8-2).

Figure 8-2 License Agreement



3e-010F-C-3 Driver Software v3.0 Build 1

License Agreement

Please read the following license agreement carefully.

END USER LICENSE AGREEMENT FOR 3e Technologies International

3e-010F-C-2 Crypto Client Software

NOTICE TO USER: 3e Technologies International ("3eTI"). IS WILLING TO ENTER INTO A LICENSE ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT BY OPENING THE SOFTWARE THIS ACKNOWLEDGES YOUR ACCEPTANCE OF ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT.

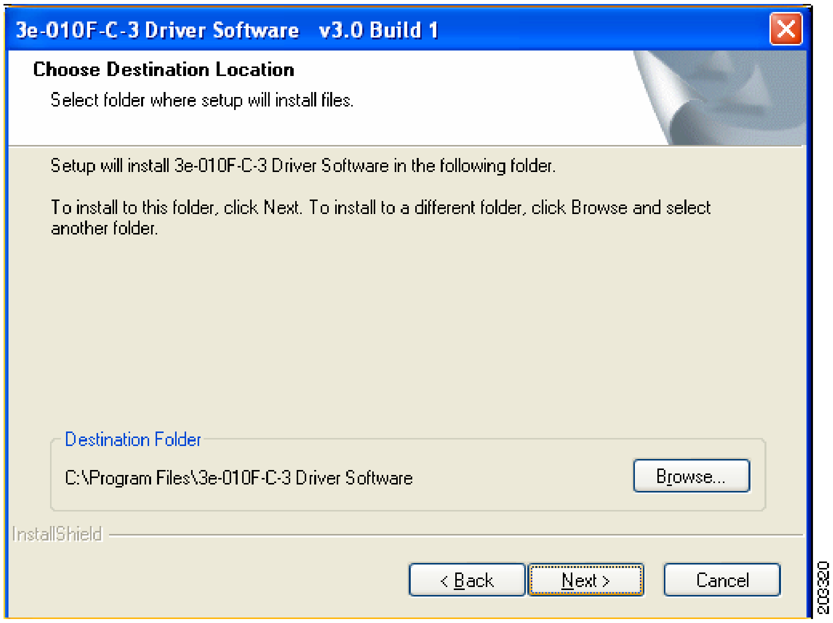
This 3eTI single user license agreement (the "AGREEMENT") is A legal agreement

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

Step 3 Read and accept the license agreement and click **Next**. Figure 8-3 appears.

Figure 8-3 Destination Location Window



3e-010F-C-3 Driver Software v3.0 Build 1

Choose Destination Location

Select folder where setup will install files.

Setup will install 3e-010F-C-3 Driver Software in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

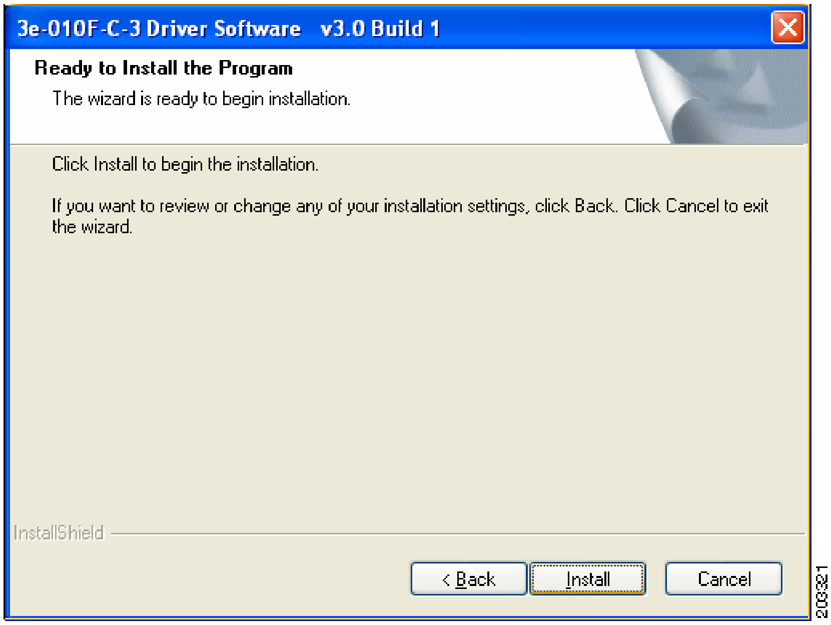
Destination Folder

C:\Program Files\3e-010F-C-3 Driver Software

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

Step 5 Click **Next** and Figure 8-4 appears.

Figure 8-4 Ready to Install Window



3e-010F-C-3 Driver Software v3.0 Build 1

Ready to Install the Program

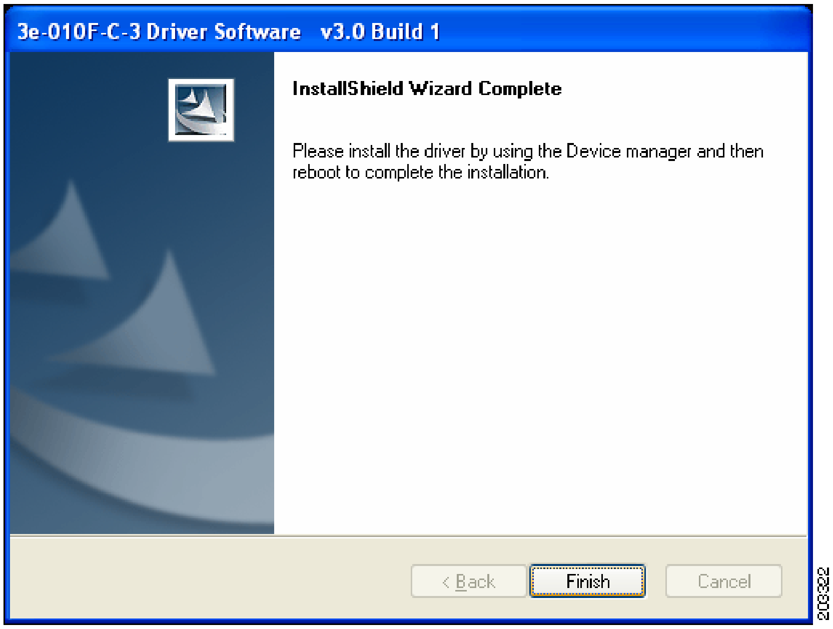
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Step 6 Click **Install** to start the installation process. When the installation completes, Figure 8-5 appears.

Figure 8-5 Wizard Complete Window



3e-010F-C-3 Driver Software v3.0 Build 1

InstallShield Wizard Complete

Please install the driver by using the Device manager and then reboot to complete the installation.

Step 7 Click **Finish**.

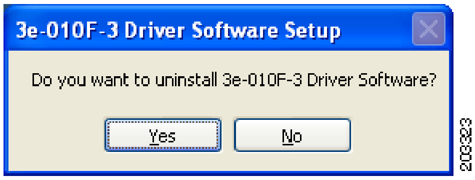
Uninstalling Previous 3eTI Driver Software

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**. A pop-up window appears (see Figure 8-6).

Figure 8-6 Uninstall Driver Software Pop-Up

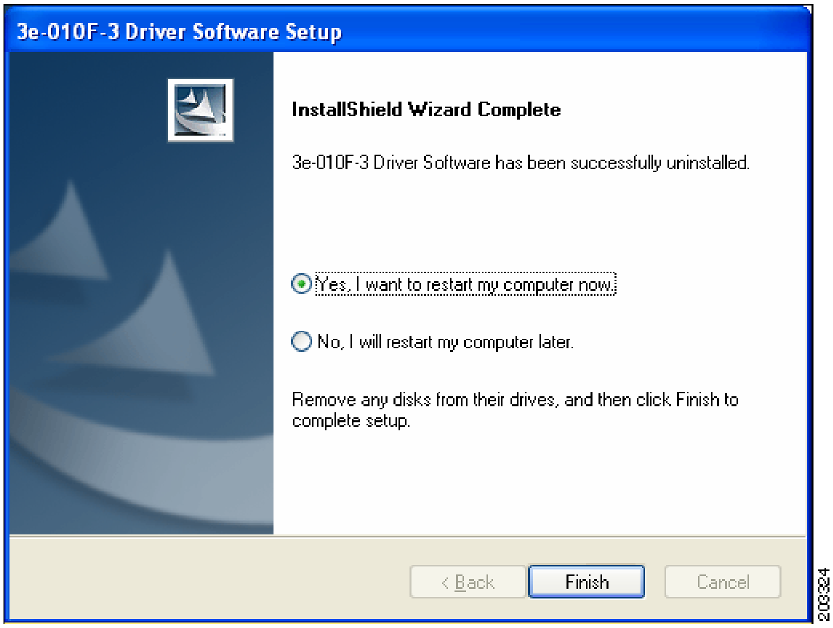


3e-010F-3 Driver Software Setup

Do you want to uninstall 3e-010F-3 Driver Software?

Step 3 Click **Yes** to uninstall the driver software. Figure 8-7 appears.

Figure 8-7 Restart Computer Now Window



3e-010F-3 Driver Software Setup

InstallShield Wizard Complete

3e-010F-3 Driver Software has been successfully uninstalled.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

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 8-17).

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 8-17).

Figure 8-1 appears.

Step 2 Perform Step 2 through Step 7 in the "Running the Installer without Using Command-Line Options" section on page 8-18.

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

Manually Upgrading the 3eTI Driver Software

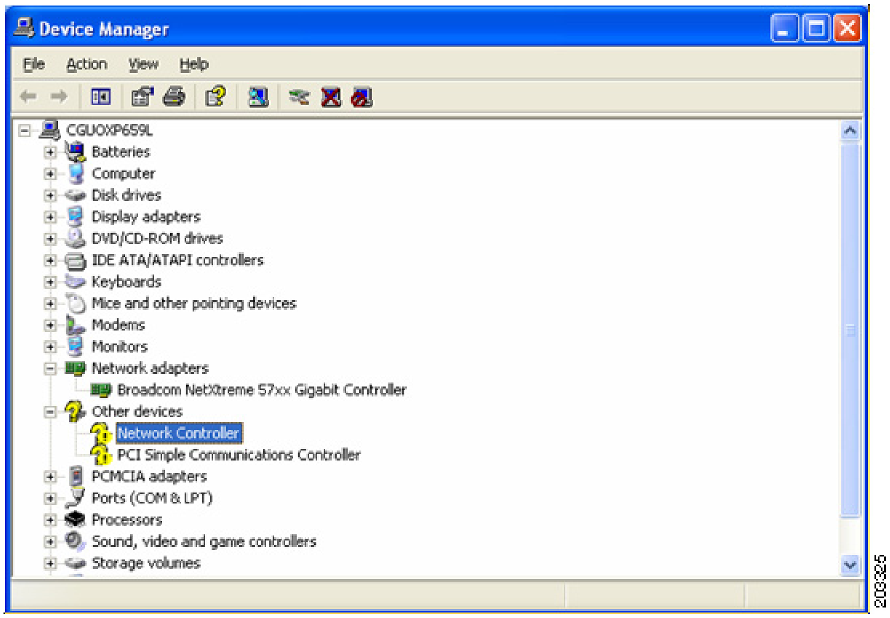
Manual upgrade instructions are provided to help troubleshoot driver installation problems. This is not expected to be a part of an enterprise-wide deployment.

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**.

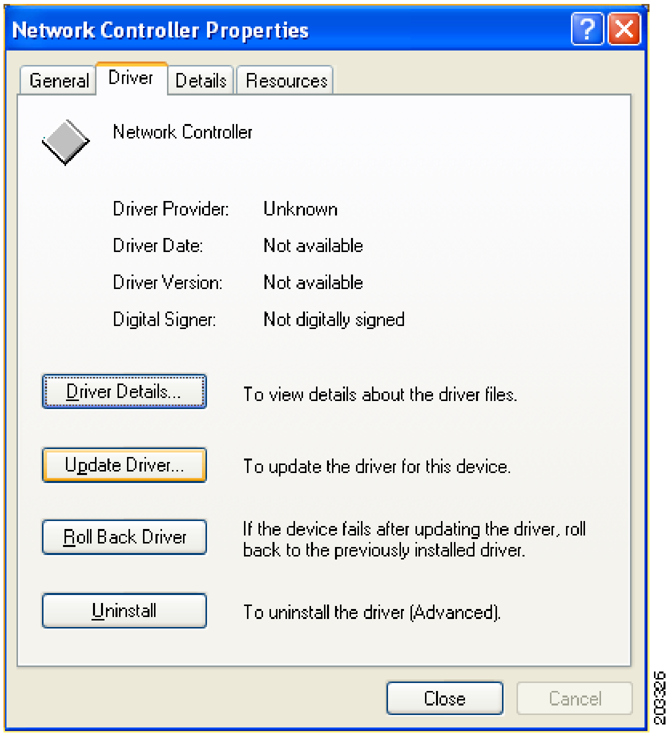
Step 2 Click **Hardware** on the System Properties window, click **Device Manager**. Figure 8-8 appears.

Figure 8-8 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 appears (see Figure 8-9).

Figure 8-9 Network Controller Properties Window



Network Controller Properties

Network Controller

Driver Provider: Unknown

Driver Date: Not available

Driver Version: Not available

Digital Signer: Not digitally signed

To view details about the driver files.

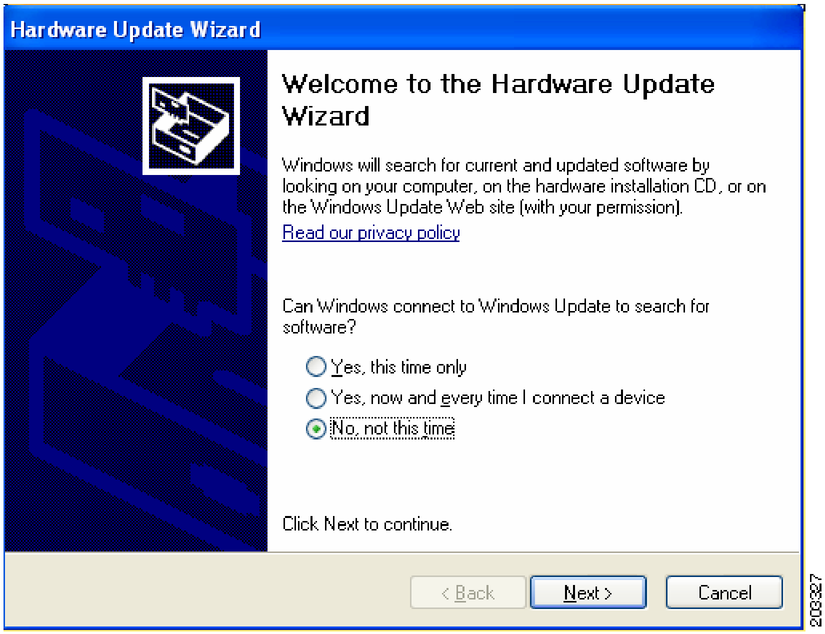
To update the driver for this device.

If the device fails after updating the driver, roll back to the previously installed driver.

To uninstall the driver (Advanced).

Step 4 Click **Driver** > **Update Driver** and Figure 8-10 appears.

Figure 8-10 Windows Hardware Update Wizard Window



Hardware Update Wizard

Welcome to the Hardware Update Wizard

Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).

Read our privacy policy

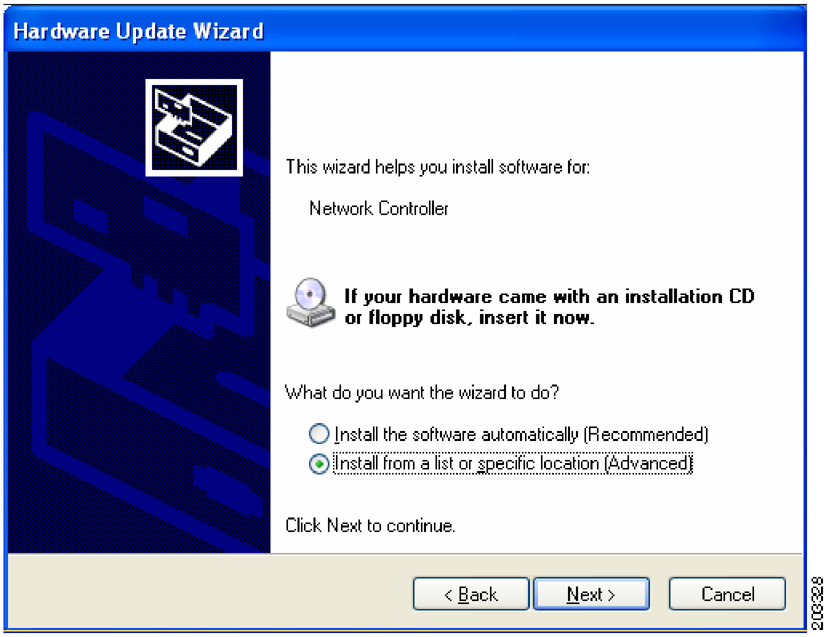
Can Windows connect to Windows Update to search for software?

○ Yes, this time only
○ Yes, now and every time I connect a device
● No, not this time

Click Next to continue.

Step 5 Click **No** to prevent Windows from searching for the driver software and click **Next**. Figure 8-11 appears.

Figure 8-11 Installation CD or Floppy Disk Option Window



Hardware Update Wizard

This wizard helps you install software for:

Network Controller

If your hardware came with an installation CD or floppy disk, insert it now.

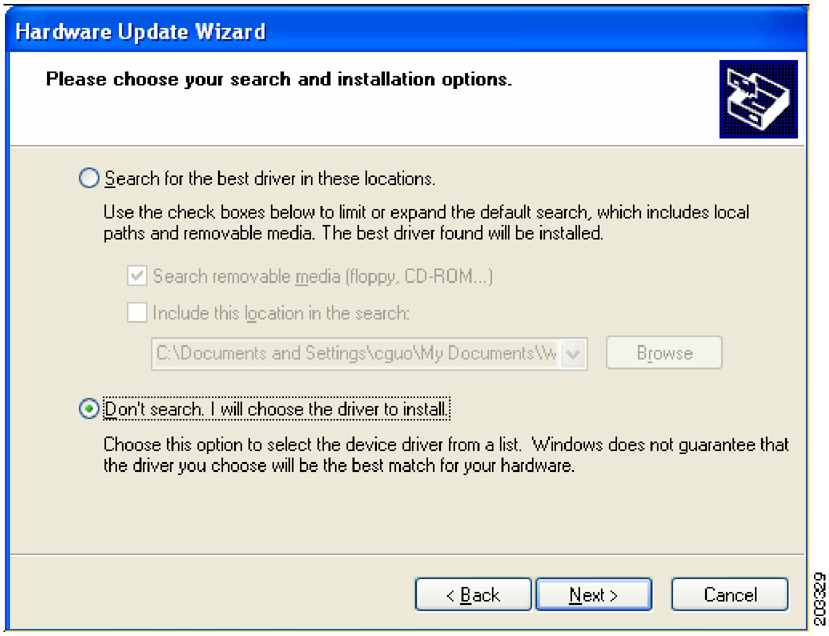
What do you want the wizard to do?

○ Install the software automatically (Recommended)
● Install from a list or specific location (Advanced)

Click Next to continue.

Step 6 Check **Install from a list or specific location** (**Advanced**) and click **Next**. Figure 8-12 appears.

Figure 8-12 Search and Installation Options Window


Hardware Update Wizard

Please choose your search and installation options.

○ Search for the best driver in these locations.

Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.

☑ Search removable media (floppy, CD-ROM...)

□ Include this location in the search:

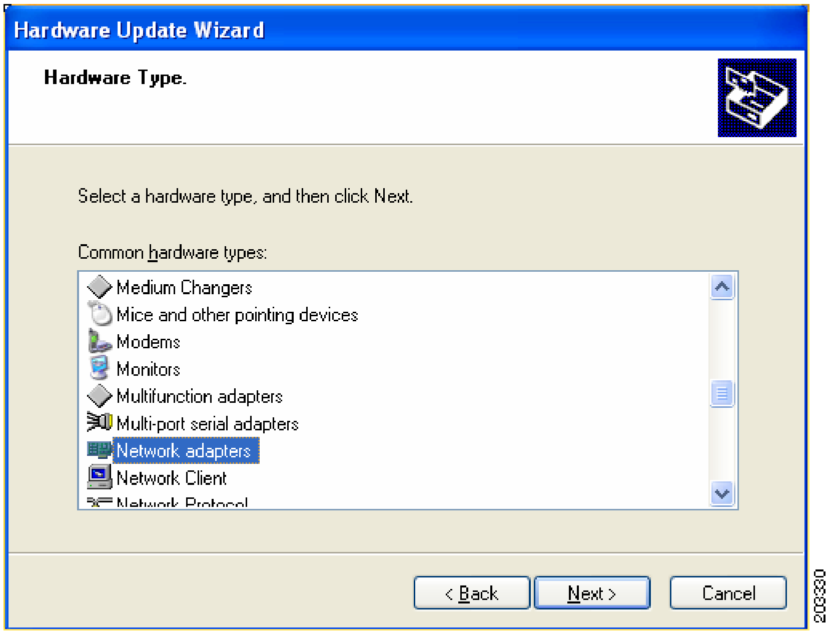
C:\Documents and Settings\cguo\My Documents\W

● Don't search. I will choose the driver to install.

Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.

Step 7 Check **Don't search. I will choose the driver to install** and click **Next**. Figure 8-13 appears.

Figure 8-13 Windows Hardware Type Window


Hardware Update Wizard

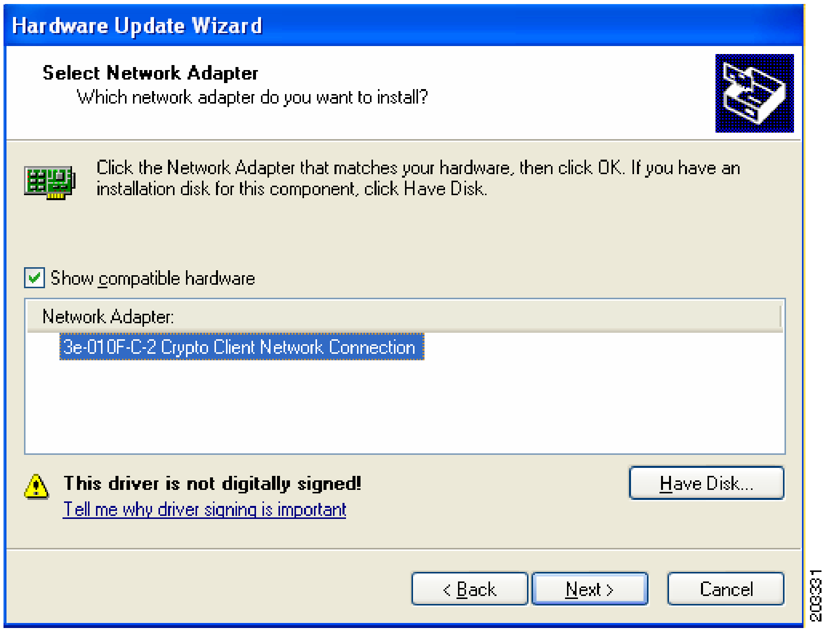
Hardware Type.

Select a hardware type, and then click Next.

Common hardware types:

Step 8 Choose **Network adapter** and click **Next**. Figure 8-14 appears.

Figure 8-14 Select Network Adapter Window



Hardware Update Wizard

Select Network Adapter
Which network adapter do you want to install?

Click the Network Adapter that matches your hardware, then click OK. If you have an installation disk for this component, click Have Disk.

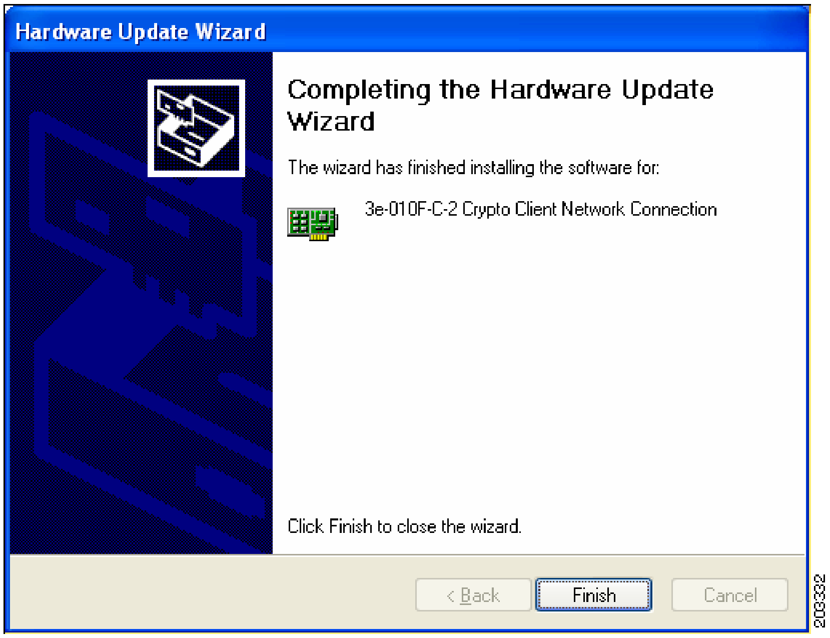
☑ Show compatible hardware

Network Adapter:
3e-010F-C-2 Crypto Client Network Connection

This driver is not digitally signed!
Tell me why driver signing is important

Step 9 Choose the 3eTI network connection and click **Next**. Figure 8-15 appears.

Figure 8-15 Installation Complete Window



Hardware Update Wizard

Completing the Hardware Update Wizard

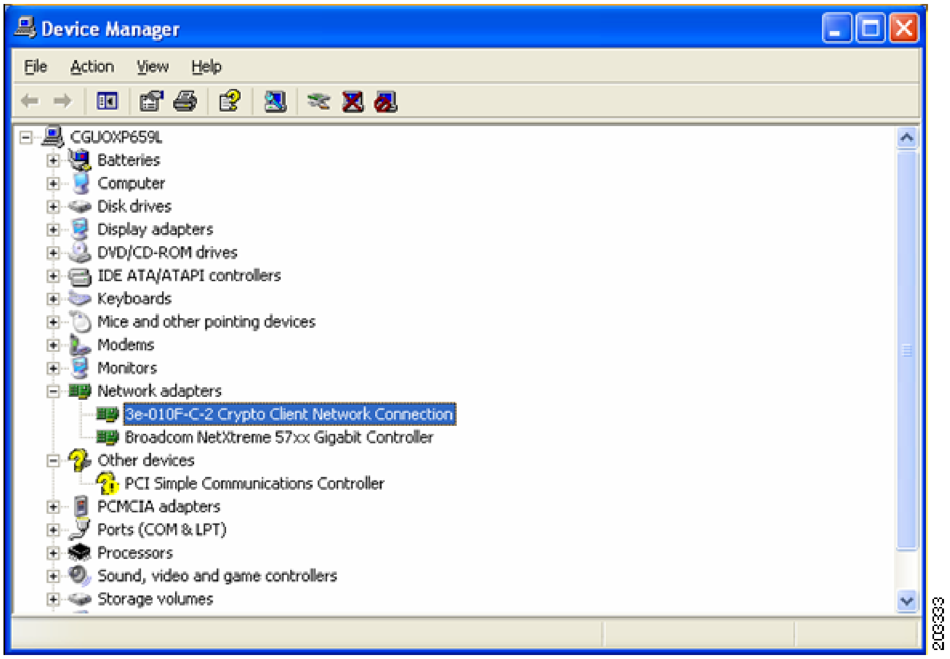
The wizard has finished installing the software for:

3e-010F-C-2 Crypto Client Network Connection

Click Finish to close the wizard.

Step 10 The hardware driver installation is complete. Click **Finish**. The Device Manager window reappears (see Figure 8-16).

Figure 8-16 Updated Windows Device Manager Window



- CGUOXP659L
  - Batteries
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Modems
  - Monitors
  - Network adapters
    - 3e-010F-C-2 Crypto Client Network Connection
    - Broadcom NetXtreme 57xx Gigabit Controller
  - Other devices
    - PCI Simple Communications Controller
  - PCMCIA adapters
  - Ports (COM & LPT)
  - Processors
  - Sound, video and game controllers
  - Storage volumes

Step 11 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.