



SSC FIPS 140-2 Level 1 Validation

This chapter contains these sections:

- Overview, page 7-1
- 3eTI FIPS Certified Crypto Kernel Library (CKL), page 7-2
- Installing the 3eTI Driver, page 7-3
- FIPS 140-2 Level I Compliant Deployment Example, page 7-14
- Obtaining SSC and 3eTI Driver Installer Software, page 7-37

Overview

U.S. Federal agencies as well as Canadian government agencies are required to comply with the Federal Information Processing Standards Publication (FIPS) 140-2 when purchasing IT products that contain cryptographic modules. This release of SSC supports a FIPS 140-2 Level 1 module (currently in process for validation with the National Institute of Standards and Technology (NIST) and provides FIPS-compliant IEEE 802.11i (WPA2) security support.



FIPS functionality is not supported by the Windows Vista version of SSC.

An administrator can choose to allow enterprise employees to perform one of these operations:

- Connect to only FIPS-compliant networks.
- Connect to other non-FIPS-compliant networks.

This can be achieved by restricting the allowed association and encryption modes and the authentication methods in the policy section of the SSC schema.

The SSC FIPS module supports FIPS approved AES encryption modes including WPA2 Personal (WPA2-PSK) and WPA2 Enterprise (802.1X). The SSC FIPS module also supports EAP methods including EAP-TLS, EAP-PEAP, and EAP-FAST. SSC 5.1.1 enables administrators 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.

The administrator is responsible for naming the profile appropriately to indicate whether the network is FIPS enabled.

Γ

A fully FIPS-compliant solution requires three components:

- SSC 5.1.1 with the FIPS module
- 3eTI FIPS certified Crypto Kernel Library (CKL) with supported NIC adapter drivers
- · A FIPS-compliant network profile configuration created by the network administrator

3eTI FIPS Certified Crypto Kernel Library (CKL)

These NIC adapter chipsets are supported by the 3eTI FIPS certified CKL:

- Intel 2100, 2200, 2915, and 3945 chipsets
- Broadcom: All BCM 43xx chipsets that support driver version 4.100.27.0 or later
- Atheros PCI chipset based NIC adapters, including Cisco AIR-CB21 wireless client adapter cards
- Atheros: 5001, 5004, 5005, AR5211, and AR5212 chipsets

FIPS Integration

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

The SSC 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 7-3.

Additional FIPS Information

For additional FIPS information, refer to the "FIPS 140-2 Level I Compliant Deployment Example" section on page 7-14 and the "Configuring a Single-User Account for FIPS" section on page C-1.

Installing the 3eTI Driver

This section provides instructions for installing the 3eTI FIPS validated Cryptographic Kernel Library (CKL) with supported drivers that integrate with SSC 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 the network administrator to specify specific installation options. Pre-installations are typically preformed by a 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 | | | | |
| | <i>Pre-installation</i> 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, 12200, 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. | | | |



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 7-1).





Step 2 Click **Next** and the license agreement appears (see Figure 7-2).

| 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-UTUE-C-2 Crypto Lilent 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 ACCEPTANCE OF ALL THE TERMS AND |
| This 3eTI single user license agreement (the "AGREEMENT") is A legal agreement |
| accept the terms of the license agreement |
| O I do not accept the terms of the license agreement |
| InstallShield |
| <pre></pre> |

Figure 7-2 License Agreement

- Step 3 Read and accept the license agreement and click Next. Figure 7-3 appears.
 - Figure 7-3 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 Browse |
| InstallShield |

- Step 4 Accept the driver software default destination folder or click Browse to locate the desired folder.
- **Step 5** Click **Next** and **Figure 7-4** appears.

| 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 Ca the wizard. | incel to exit |
| InstallShield ———————————————————————————————————— | Cancel |

Figure 7-4 Ready to Install Window

Step 6 Click Install to start the installation process. When the installation completes, Figure 7-5 appears.

Figure 7-5 Wizard Complete Window





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.

20323

Step 2 Choose the 3eTI driver software, such as 3e-010F-3 and click **Remove**. A pop-up window appears (see Figure 7-6).

Figure 7-6 Uninstall Driver Software Pop-Up

| 3e-010F-3 Driver Software Setup | | | |
|---|--|--|--|
| Do you want to uninstall 3e-010F-3 Driver Software? | | | |
| <u>Y</u> es <u>N</u> o | | | |

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

Figure 7-7 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. | | |
| | < <u>B</u> ack Finish Cancel | | |

- **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 7-4).

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 7-4).

Figure 7-1 appears.

- Step 2 Perform Step 2 through Step 7 in the "Running the Installer without Using Command-Line Options" section on page 7-5.
- **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 7-8 appears.

| 🚇 Device Manager | |
|--|------|
| Ele Action View Help | |
| | |
| E-A CGU0XP659L | ^ |
| 🕀 🍓 Batteries | |
| 🗈 😼 Computer | |
| 🐑 🥌 Disk drives | |
| 🗈 😼 Display adapters | |
| DVD/CD-ROM drives | |
| IDE ATA/ATAPI controllers | |
| 🕑 🧽 Keyboards | |
| Mice and other pointing devices | |
| Modems | 11 C |
| generations | |
| Network adapters | |
| Broadcom NetXtreme 57xx Gigabit Controller | |
| Cher devices | |
| BCI Simple Communications Controller | |
| PCI Simple Communications Controller | |
| Prote (COM & IPT) | |
| | |
| Sound, video and game controllers | |
| The Storage volumes | ~ |
| | |
| | |

Figure 7-8 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 7-9).

| Network Controller Pr | operties 🛛 🖓 🔀 | | |
|---|--|-------|--|
| General Driver Details | Resources | | |
| Network Contro | ller | | |
| Driver Provider: | Unknown | | |
| Driver Date: | Not available | | |
| Driver Version: | Not available | | |
| Digital Signer: | Not digitally signed | | |
| Driver Details | To view details about the driver files. | | |
| Ugdate Driver | To update the driver for this device. | | |
| <u>R</u> oll Back Driver | If the device fails after updating the driver, roll back to the previously installed driver. | | |
| Uninstall To uninstall the driver (Advanced). | | | |
| | Close | 20326 | |

Figure 7-9 Network Controller Properties Window

Step 4 Click **Driver > Update Driver** and **Figure 7-10** appears.



Figure 7-10 Windows Hardware Update Wizard Window

Step 5 Click **No** to prevent Windows from searching for the driver software and click **Next**. Figure 7-11 appears.





Step 6 Check Install from a list or specific location (Advanced) and click Next. Figure 7-12 appears.

| Hardware Update Wizard |
|--|
| Please choose your search and installation options. |
| ○ <u>S</u> earch 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\\ |
| ODon'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. |
| |
| |
| <pre>< Back Next > Cancel</pre> |

Figure 7-12 Search and Installation Options Window

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

Figure 7-13 Windows Hardware Type Window

| Hardware Update Wizard | |
|--|--------|
| Hardware Type. | |
| Select a hardware type, and then click Next. Common <u>h</u> ardware types: | |
| Medium Changers Mice and other pointing devices Modems Monitors Multifunction adapters Multi-port serial adapters Network adapters Network Client Network Protocol | |
| < <u>B</u> ack <u>N</u> ext | Cancel |

Step 8 Choose Network adapter and click Next. Figure 7-14 appears.

| 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! Have Disk Tell me why driver signing is important Have Disk |
| < <u>B</u> ack <u>N</u> ext > Cancel |

Figure 7-14 Select Network Adapter Window

Step 9 Choose the 3eTI network connection and click **Next**. Figure 7-15 appears.

Figure 7-15 Installation Complete Window



Step 10 The hardware driver installation is complete. Click **Finish**. The Device Manager window reappears (see Figure 7-16).



Figure 7-16 Updated Windows Device Manager Window

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.

FIPS 140-2 Level I Compliant Deployment Example

This section describes a deployment example that explains how to configure typical network authentication profiles for SSC to ensure compliance with FIPS 140-2 Level 1 requirements. SSC 5.1.0 is the first release that supports the Cisco SSC FIPS module, which is currently in process for validation with the National Institute of Standards and Technology (NIST). When the service starts up, it executes in the FIPS operating mode.

The network administrator is responsible to configure and deploy FIPS-compliant profiles for the intended user base. The SSC Management utility is used to create FIPS-compliant profiles for wired or wireless media.

- A fully FIPS-compliant solution requires three components to be installed and configured on the client:
- **1.** SSC running the SSC FIPS module (SSC 5.1.1).
- 2. A FIPS-compliant network profile configured by the network administrator.
- 3. An installed 3eTI FIPS CKL module with supported NIC adapter drivers.

When SSC and the management toolkit software are installed and running on the network administrator's PC, SSC scans for available wireless networks and displays the available networks.



Only the wireless network devices with their SSID's enabled for broadcast are visible.

The configured connections displayed in bold (see Figure 7-17) can be configured by the network administrator or the user. The profiles configured by the network administrator are permanent and cannot be deleted or revised by the user.

| 📵 Cisco Secure | Services Client | | | |
|---------------------------------|--|--|---------------|--|
| <u>S</u> ettings <u>G</u> roups | Help | | | |
| Available Con | nections onnections appear in bo | Idface | | |
| Connection | Signal | Security | Status | |
| wired blizzard | | WPA-Enterprise | | |
| belkin54g | | Open(non-secured) | VPN Connected | |
| NETGEAR linksys | | Open(non-secured) Open(non-secured) | | |
| | Connect | Edit | Delete | |
| VPN Connected. IP: | 192.168.2.4 | | | |

Figure 7-17 Typical Cisco SSC Window

To configure typical SSC profiles for FIPS compliance, follow these instructions:

Step 1 Navigate to the directory in which the management toolkit is installed and double-click **sscManagementUtility.exe**. Figure 7-18 appears.

| Figure 7-18 | Cisco SSC Management Utility Main Window |
|-------------------|---|
| 😩 Cisco SSC Manag | ement Utility |
| cisco | Welcome to Enterprise Deployment Configuration This Enterprise Deployment wizard for Cisco SSC enables network and desktop administrators to centrally configure, deploy, and manage the Secure Services Client in an enterprise environment. • Gives IT professionals the capability to enforce network security polices on end stations. • Provides IT professionals with the flexibility to configure various settings to support existing enterprise standards and reduce support calls. |
| | enterprise standards and reduce support calls. • Offers end users a hassle free networking experience. Create New Configuration Profile 2 |
| | Modify Existing Configuration Profile > Process Existing Configuration Profile > |
| | This Client Package Tool will only work for SSC 5.1 and higher configurations. Create Pre-Configured Client Package > |
| | SscManagementUtility © 2008 Cisco Systems, Tor. |

Step 2 To create a new configuration profile, click Create New Configuration Profile. Figure 7-19 appears.

Figure 7-19 Select Cisco SSC Version Window



Figure 7-20

Step 3 Click **Cisco SSC 5.1.1** and **Figure 7-20** appears.

Client Policy Window

| CISCO | |
|--|---------------|
| Provide License ####-####-####-####-####-####-####-## | |
| **** | |
| | -####-####-#; |
| Connection Settings | |
| Attempt connection before user logon Number of seconds to wait before allowing user to logon Attempt connection after user logon | |
| Default Connection Timeout 40 Default Association Timeout 3 | |
| - Allowed Media- | |
| ☑ Allow Wifi (wireless) Media | |
| Enable validation of WPA/WPA2 handshake | |
| Allow Wired (802.3) Media VPN Authentication | Mechanism |
| Descuerd | ~ |

You must ensure that all needed options are checked in the Allowed Media area to allow that media to be configured, such as *Allow Wired* (802.3) *Media*.

- **Step 4** follow these steps:
 - a. Check Allow Wi-Fi (wireless) Media.
 - b. Check Allow Wired (802.3) Media.
 - c. Check Provide License and enter the license if it is available.
 - **d.** If VPN is installed on the PC and supported on the enterprise network infrastructure, check **Allow VPN**. Choose the appropriate VPN Authentication Mechanism for your network.
 - e. Check Enable validation of WPA/WPA2 handshake. As a part of FIPS compliance, this option is enabled.



Some network adapter drivers might not work correctly when this option is checked.

f. Click Next and Figure 7-21 appears.

| 関 Cisco SSC 5.1 C | onfiguration Profile | |
|-------------------|--|---|
| Cisco SSC 5.1 C | Authentication Policy Allowed Association Modes Select All Open (no encryption) Open (Static WEP) Shared (WEP) WPA Personal TKIP WPA Personal AES WPA2 Personal AES Select All Open (Dynamic (802.1X) WEP) WPA Enterprise TKIP WPA2 Enterprise TKIP WPA2 Enterprise AES CCKM Enterprise TKIP CCKM Enterprise TKIP CCKM Enterprise AES | Allowed Authentication Modes Select All LEAP PEAP EAP-GTC EAP-FAST EAP-MD5 EAP-MSCHAPv2 EAP-TLS EAP-TTLS |
| | | < Back Next > Cancel |

Figure 7-21 Authentication Policy Window

Step 5 Check the appropriate association and authentication modes that are allowed on your network and click **Next.** Figure 7-22 appears.

SSC can be configured to support both FIPS-compliant and non-compliant profiles. FIPS-compliant profiles include WPA2 Personal AES and WPA2 Enterprise AES. Supported EAP types with WPA2 Enterprise AES include: EAP TLS, PEAP, and EAP Fast.

| cisco | | | | |
|-------|-----------------|-------------------|----------------|--|
| | Group / Network | Media | Security Level | |
| | Default | in Groupsj | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Add | Group Add Network | Modify Remove | |

Figure 7-22 Networks Window

Step 6 Click **Add Network**. The first network to create is a wired network. This causes SSC to limit the connections to only one at a time. Figure 7-23 appears.

I

| 🔋 Cisco SSC 5.1 C | onfiguration Profile |
|-------------------|--|
| a a a | Network Media |
| CISCO | Choose Your Network Media |
| | Wired (802.3) Network |
| | Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable, |
| | 🔘 WiFi (wireless) Network |
| | Select a WiFi network, if the endstations will be connecting to the network via a wireless radio connection to an Access Point. |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | < Back Next > Cancel |

Figure 7-23 Network Media Window

Step 7 Check Wired (802/3) Network and click Next. Figure 7-24 appears.

| | Wired Network Settings |
|-------|---|
| cisco | Network Settings |
| | Display Name: Wired |
| | Connection Timeout: 40 |
| | Security Level |
| | Open Network Open networks have no security, and are open to anybody with physical access. This is the least secure type of network. Authenticating Network Authentication networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure. |
| | |
| | |
| | |
| | |

Figure 7-24 Wired Network Settings Window

- **Step 8** Enter **Wired** in the Display Name field and check **Open Network**.
- **Step 9** Click **Next** and **Figure 7-25** appears.

| 1111111 | Network Connection Type |
|---------|---|
| CISCO | Network Connection Type |
| | O Machine Connection |
| | Machine connection should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access. |
| | User Connection |
| | User connection should be used when a machine connection is not necessary. A user connection will make the network available after the user has logged on. |
| | |
| | |

Figure 7-25 Network Connection Type Window

Step 10 Check **User Connection** and click **Finish**. You have configured your wired non-authentication port. The next operation is necessary to configure a FIPS-compliant wireless authentication profile.

Figure 7-26 appears.

| cisco | - Networks | | | |
|-------|--|------------------|----------------|---|
| | Group / Network | Media | Security Level | |
| | E - [Networks Available to All Group Wired Default | s] Wired (802.3) | | 4 |
| | Add Group | Add Network | Modify Remove | |

Figure 7-26 Networks Window

In Figure 7-26, the wired network is shown configured.

Step 11 Click Add Network and Figure 7-27 appears.

| 🕄 Cisco SSC 5.1 C | onfiguration Profile |
|-------------------|--|
| ahaha | Network Media |
| CISCO | Choose Your Network Media |
| | O Wired (802.3) Network |
| | Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. |
| | WiFi (wireless) Network |
| | Select a WiFi network, if the endstations will be connecting to the network via a wireless radio connection to an Access Point. |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | < Back Next > Cancel |

Figure 7-27 Network Media Window

Step 12 Check Wi-Fi (wireless) Network and click Next. Figure 7-28 appears.

L

| 📵 Cisco SSC 5.1 Co | onfiguration Pro | file | | | | × |
|--|-----------------------|--|----------|--------|-----------|---------------------------------|
| ahaha | Wifi Netwo | rk S | Settings | | | |
| cisco | -Network Setting: | - Network Settings | | | | |
| | Display Name: | Display Name: Enterprise-ssid (FIPS Compliant Profile) | | | | |
| | SSID: Enterprise-ssid | | | | | |
| | Association Time | out: | 8 | 0 | | |
| | Connection Time | out: | 40 | 0 | | |
| Security Level Open Network Open networks have no security, and are open to anybody within range. This is th least secure type of network. Shared Key Networks, use a shared key to encrypt data between end stations and network access points. This is a medium security level, suitable for small offices, or home offices. Authenticating Network Authentication networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and oth network infrastructure. | | | | | | the and or vr other |
| | | | | | | |
| | | | | < Back | Next > Ca | ancel |

Figure 7-28 Wi-Fi Network Settings Window



Some smartcard authentication systems require almost 60 seconds to complete an authentication. When using a smartcard, it might be necessary to increase the Connection Timeout value.

Step 13 follow these steps:

- **a.** Enter the Display Name for the profile. It is recommended that the display name set by the network administrator to indicate that it is a FIPS-compliant profile, such as adding *FIPS* in addition to the display name (see Figure 7-28). This profile identification indicates that when connected using this administrator-deployed profile, the network authentication profile conforms to FIPS requirements.
- **b.** Enter the SSID value in the SSID field. The SSID should be set to a valid enterprise SSID. The SSID value is case sensitive.
- c. Change the Association Timeout from the default of 3 to value of 8 to 10 seconds.



The Cisco AIR-CB21client adapter is not sensitive to this value; however, other wireless client adapters, such as the Intel 3945 client adapter require the increased association timeout value.

- d. Click Next.
- **Step 14** When the CCX Settings window appears, ignore the settings and click Next. Figure 7-29 appears.

Note

The CCX Setting window options are not applicable to Windows XP or Windows 2000 environments.

Figure 7-29 Connection Settings Window

| 🖲 Cisco SSC 5.1 Co | onfiguration l | Profile | |
|--------------------|----------------|---------------------|--------|
| ahaha | Connecti | ion Settings | |
| CISCO | -802.1X Setti | ngs | |
| | authPeriod | 30 | |
| | heldPeriod | 60 | |
| | startPeriod | 30 | |
| | maxStart | 3 | |
| | Association | Mode | |
| | Mode: WP4 | A2 Enterprise (AES) | ~ |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | < Back Next > | Cancel |

- Step 15 Click the Association Mode drop-down arrow and choose WPA2 Enterprise (AES).
- Step 16 When configuring the 802.1X settings, Cisco recommends that you use the 802.1X default settings.These settings are optimized for several different wireless environments and for a wired authenticating profile. Other setting values can be used, but they might not produce optimized operation.
- **Step 17** Click **Next** and Figure 7-30 appears.



Figure 7-30 Network Connection Type Window

Any of the three options can be selected and will be FIPS-compliant.

Step 18 For this example, check User Connection and click Next. Figure 7-31 appears.

| 😫 Cisco SSC 5.1 C | onfiguration Profile | |
|-------------------|---------------------------|-------------------------------------|
| ahaha | Machine Authentication (B | EAP) Method |
| CISCO | - EAP Methods | |
| | C LEAP | |
| | O EAP-TLS | Configure |
| | O EAP-TTLS | Configure |
| | O PEAP | Configure |
| | C EAP-FAST | Configure |
| | | |
| | | <pre>Seck Next > Cancel 88</pre> |

Figure 7-31 User Authentication (EAP) Method Window

Step 19 Follow one of these steps with the following EAP methods:

- Check EAP-TLS and click Next. Go to Step 20.
- Check **PEAP** and click **Next**. Go to Step 21.
- Check EAP-Fast and click Next. Go to Step 22.

Step 20 If you checked EAP-TLS, Figure 7-32 appears.

When using smartcards, there are two typical usage scenarios:

- The smartcard must be inserted for every smartcard re-authentication.
- The smartcard must be inserted for the first authentication, then the smartcard can be removed and only needs to be reinserted when the user logs out.

Both usage scenarios are acceptable for a FIPS-compliant profile.

Follow these steps:

| Figure 7-32 | EAP-TLS Settings | Window |
|-------------|------------------|--------|
|-------------|------------------|--------|

| EAP TLS Settings |
|---------------------------------|
| EAP TLS Settings |
| ✓ Validate Server Certificate |
| Enable Fast Reconnect |
| Disable when using a Smart Card |
| |
| |
| |
| |
| |
| |
| OK Cancel |
| |

- a. In a FIPS-compliant profile, check Validate Server Certificate.
- b. Click OK. The User Authentication (EAP) Method window reappears.
- c. Click Next on the User Authentication (EAP) Method window and go to Step 23.

Step 21 If you checked PEAP, Figure 7-33 appears.

| 😫 PEAP Settings 🛛 🔀 | |
|---|-------|
| PEAP Settings | |
| Validate Server Identity | |
| Enable Fast Reconnect | |
| Disable when using a Smart Card | |
| Inner Methods based on Credentials Source | |
| Authenticate using a Password | |
| EAP-MSCHAPv2 | |
| EAP-GTC | |
| O Authenticate using a Token and EAP-GTC | |
| EAP-TLS, using a Certificate | |
| | |
| | |
| OK Cancel | 01010 |

Figure 7-33 PEAP Settings Window

For a FIPS-compliant profile, follow these steps:

- a. Check Validate Server Identity.
- b. Click OK and the User Authentication (EAP) Method window reappears.
- c. Click Next on the User Authentication (EAP) Method window and go to Step 23.

Step 22 If you checked EAP-Fast, Figure 7-34 appears.

Figure 7-34 EAP-Fast Settings Window

| EAP FAST Settings |
|---|
| EAP Fast Settings |
| Validate Server Identity |
| Enable Fast Reconnect |
| Disable when using a Smart Card |
| Allow Posture |
| Inner Methods based on Credentials Source |
| Authenticate using a Password |
| EAP MSCHAPv2 If using PACs, allow unauthenticated PAC provisioning |
| ✓ EAP GTC |
| O Authenticate using a Token and EAP GTC |
| Authenticate using a Certificate |
| When requested send the client certificate in the clear Definite distribute and the distribute and the send of the burged |
| Send the client certificate requests in the dear, only send when protected inside the tanker Send the client certificate using EAP TLS in the tunnel |
| Use PACs |
| Filename |
| |
| |
| |
| |
| |
| |
| Add PAC File |
| OK Cancel |

For a FIPS-compliant profile, follow these steps:

- a. Check Validate Server Identity.
- **b.** Click **OK** the User Authentication (EAP) Method window reappears.
- c. Click Next on the User Authentication (EAP) Method window and go to Step 23.

Step 23 If you previously checked Validate Server Identity, Figure 7-35 appears.

| ahaha | User Server \ | /alidation | | | |
|-------|------------------------|------------------|-------|--------|----------|
| cisco | -Certificate Trusted S | ierver Rules | | | |
| | Certificate Field | Match | Value | Remove | |
| | Subject Alt. Nar 🚩 | exactly matche 💙 | | F | Remove |
| | Common Name | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | Add Rule |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Figure 7-35 Certificate Trusted Server Validation Rules Window

Step 24 Optional, define server validation rules by following these steps:

- a. Click Add Rule.
- **b.** Click the drop-down arrows and highlight the desired options.
- c. Enter a value in the Value field.



Click **Remove** to remove the rule.

d. When complete, click Next and Figure 7-36 appears.

Even when certificate rules are not created, these validations occur implicitly to satisfy FIPS:

- The received server certificate has not expired.
- The server certificate chain is valid.
- The root node of the server certificate chain is trusted.

| () Cisco SSC 5.1 C | onfiguration Profile |
|--------------------|---|
| a a a a | User Server Validation |
| CISCO | Trusted Certificate Authority |
| | Trust any Root Certificate Authority (CA) Installed on the OS |
| | Include Root Certificate Authority (CA) Certificates |
| | Certificate File |
| | |
| | |
| | |
| | |
| | |
| | Add Certificate |
| | |
| | |
| | |
| | |
| | < Back Next > Cancel |

Step 25 Accept the default setting or check the desired option. Click **Next** and Figure 7-37 appears.

I

| 🕲 Cisco SSC 5.1 Co | nfiguration Profile |
|--------------------|--|
| alada | User Credentials |
| CISCO | User Identity Unprotected Identity Pattern: [username] |
| | User Credentials |
| | Use Single Sign On Credentials Prompt for Credentials |
| | Remember Forever Remember while the User is Logged On Never Remember |
| | Certificates sources — Remember Smart Card Pin — |
| | Smart Card or OS certificates Remember Forever Remember while the User is Logged Smart Card certificates only Never remember |
| | O Use Static Credentials |
| | Certificate: Browse |
| | < Back Finish Cancel |

Figure 7-37 Credentials Window

Step 26 Follow these steps:

- **a**. Enter a username the Unprotected Identity Pattern field.
- **b.** Check one of these options:
 - Single Sign On Credentials
 - Prompt for Credentials
 - Use Static Credentials
- c. If using Prompt for Credentials, check one of these options:
 - Never Remember
 - Remember while the User is Logged On

For FIPS-compliance, Never Remember and Remember while the User is Logged On are the only acceptable selections. All relevant security critical parameters are handled securely and cleared when no longer needed.



The Single Sign On and Use Static Credentials can be used in FIPS enabled mode.

d. Click Finish and Figure 7-38 appears.

| Cisco SSC 5.1 Co | nfiguration Profile Networks | | | |
|------------------|--|----------------------------------|-----------------|--------|
| cisco | Networks | | | |
| | Group / Network | Media | Security Level | |
| | [Networks Available to All Groups] Wired Enterprise-ssid (FFIPS Compli Default | Wired (802.3) Wifi (wireless) | Authentication | |
| | | | | |
| | | | | |
| | Add Group | Add Network | Modify Remove | |
| | | | < Back Next > C | iancel |

Figure 7-38 Configured Networks Window

This window lists the networks that have been created for this profile.

- **Step 27** Click **Next** and Figure 7-39 appears.
 - Figure 7-39 Validation Window

| 📵 Cisco SSC 5.1 C | onfiguration Profile 🛛 🔀 |
|-------------------|---|
| ahaha | Validation |
| cisco | The configuration has been validated. |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | Save Processed and Signed Configuration File |
| | sers\Application Data\Cisco\Cisco Secure Services Client\newConfigFiles\configuration.xml |
| | |
| | Sack Finish Cancel |

This window allows the administrator to view the configuration XML and save the configuration in an encrypted file for deployment. The administrator can also save an un-encrypted file for review, but this file must never be deployed.

Step 28 Follow these steps:

- **a**. Accept the default location for storage of the encrypted configuration file or click **Browse** to browse to a different folder.
- b. Optional, uncheck Save Original Configuration File.
- c. Click Finish.

The configuration is now complete. If you open the SSC main window (see Figure 7-40), the new Enterprise-ssid (FIPS-compliant profile) have been added to the list of connections.

Figure 7-40 Available Connections Window

| Cisco Secure Services Client | | | | |
|--|-------------------|--|-----------|---|
| ettings <u>G</u> roups <u>H</u> elp | | | | |
| Available Connections Configured connections appear in boldf | ace | | | |
| Connection | Signal | Security | Status | ^ |
| wired Office Enterprise-ssid(FIPS compliant profile) belkin54g | | WPA-Enterprise WPA2-Enterprise Open(non-secured) | Connected | = |
| 11n-open guest static-open web-auth static-wpa static-wep10 | | Open(non-secured) Open(non-secured) Open(non-secured) Open(non-secured) WPA2-Personal WEP | | - |
| Connect | <u>E</u> dit | <u>D</u> elete | | × |
| <u>A</u> dd SSID | Connection Status | VPN Connect |) | |

In Figure 7-40 the Enterprise-ssid profile is easily identified as a FIPS-compliant profile. For this profile, the delete button is disabled so that the user cannot delete the profile. Also, all the administrator configured credential settings are unavailable, when the Edit button is clicked. The only option that can be user-configured is to automatically initiate VPN connections on the FIPS-compliant network connection between the access point and the client PC.

Obtaining SSC and 3eTI Driver Installer Software

SSC 5.1.0 software is available from the Cisco Software Center:

- SSCMgmtToolKit—Contains the sscManagementUtility and support files.
- Cisco_SSC-XP2K_5.1.0.zip—Contains the SSC files. For SSC license information, refer to the "SSC License Information" section on page 2-5.
- CiscoClientUtilities_5.1.0.zip—Contains the Log Packager.

The SSC software can be obtained from the Cisco Software Center at this URL:

http://www.cisco.com/public/sw-center/index.shtml

Click Wireless Software > Client Adapters and Client Software > Cisco Secure Services Client and follow the prompts to 5.1.0 under Latest Releases.



You must register with Cisco.com or be a registered user to download 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 SSC software can be ordered from Cisco using these product numbers:

- AIR-SC5.0-XP2K—Cisco SSC Release 5.1 software license.
- AIR-SSCFIPS-DRV—3eTI CKL supported driver installer

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



The SSCMgmtToolKit (SSC Management Utility) and the Cisco Client Utilities are only available for download from the Cisco Software Center.