Cisco NAC Appliance FIPS Card Field-Replaceable Unit Installation Guide

Part Number: 78-19152-01 Revised: September 23, 2011

This document contains the following sections:

- Prerequisites and Hardware Requirements, page 1
- Installing the FIPS Card Field-Replaceable Unit, page 2
- Bringing the FIPS Card Field-Replaceable Unit Online, page 7
- Verifying FIPS Card Field-Replaceable Unit Operation, page 9
- What's Next? Configuring the CAM/CAS for FIPS Compliance, page 11
- Obtaining Documentation and Submitting a Service Request, page 12

Prerequisites and Hardware Requirements

You must be running Cisco NAC Appliance Release 4.9 or 4.8 on the CAM(s) and CAS(s) in your deployment to support FIPS 140-2 compliant functions via the field-replaceable FIPS card component. For specific Release information, including FIPS compliance requirements and restrictions, see the *Release Notes for Cisco NAC Appliance* corresponding to your latest Cisco NAC Appliance release version.

You can install the field-replaceable FIPS card in the following Cisco NAC Appliance platforms:

- Cisco NAC-3310 CAM/CAS
- Cisco NAC-3350 CAM/CAS
- Cisco NAC-3390 CAM

Once you have installed the FIPS card field-replaceable unit in a Cisco NAC-3310/3350/3390 chassis, it becomes "FIPS-compliant" and to appropriately handle any problems arising with either the chassis or the FIPS card, itself, you must RMA the appliance with Cisco Systems and obtain a replacement Cisco NAC-3310/3350/3390.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Note FIPS-Compliant NAC-3310 CAS can support only 250 or 500 users.

For more information on the NAC-3310/3350/3390 as well as other Cisco NAC Appliance platforms, see the *Cisco NAC Appliance Hardware Installation Guide* corresponding to your latest Cisco NAC Appliance release version.

Installing the FIPS Card Field-Replaceable Unit

Warning **Ensure you are wearing a suitable ESD strap before touching any parts of the FIPS card field-replaceable unit or NAC-3310/3350/3390 chassis components before performing the following steps.**

Be sure to follow instructions for your particular Cisco NAC Appliance platform:

- Installing the FIPS Card in the Cisco NAC-3310, page 2
- Installing the FIPS Card in the Cisco NAC-3350/3390, page 5

Installing the FIPS Card in the Cisco NAC-3310

Before installing the field-replaceable FIPS card in any of the supported Cisco NAC Appliance platforms, be sure to disconnect all interface cables, power down the appliance, and disconnect power from the chassis.

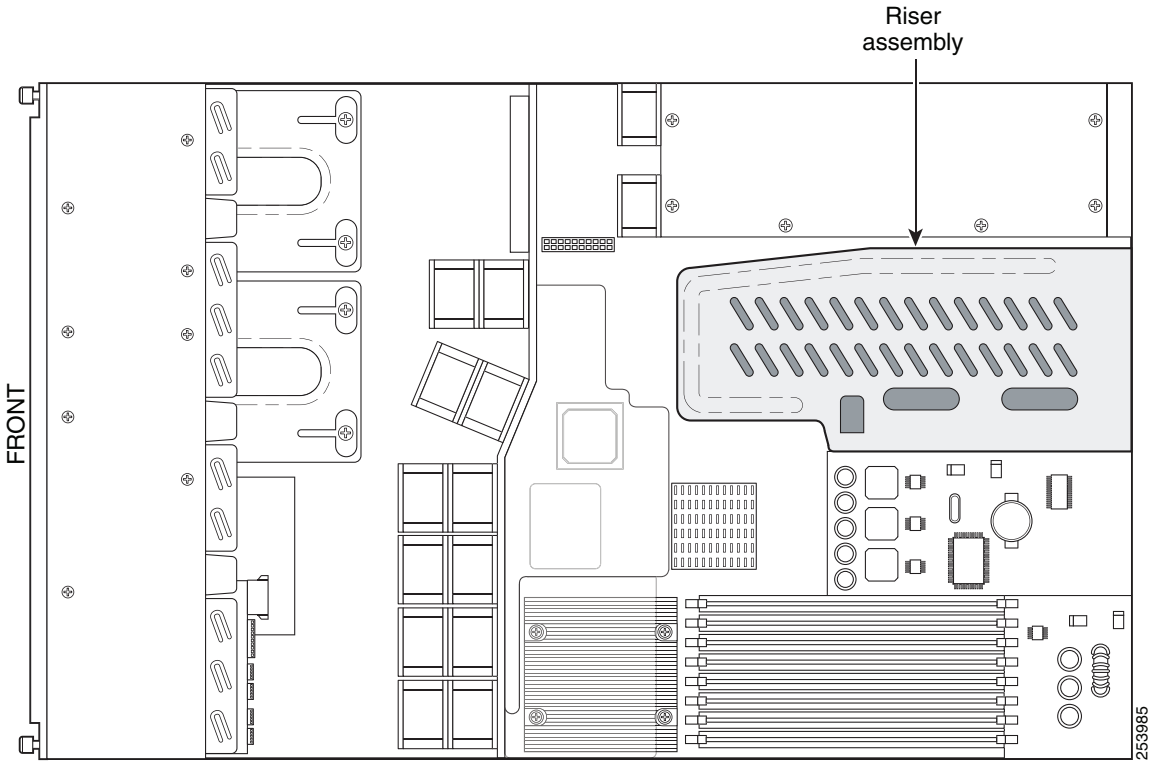
Opening the Chassis and Removing the Riser Card Assembly

Step 1 Slide the Cisco NAC-3310 away from its position in the 4-post rack on its rack rails. If your Cisco NAC-3310 does not use rack rails, remove the chassis from the rack and place it on a suitable work surface.

Step 2 Release the captive cover anchor screw on the rear panel of the Cisco NAC-3310 chassis and slide the cover back toward the rear of the chassis to unseat it.

Step 3 Remove the cover and set it aside, exposing the inside components of the Cisco NAC-3310 chassis.

Figure 1 Cisco NAC-3310 Chassis and Riser Card Assembly



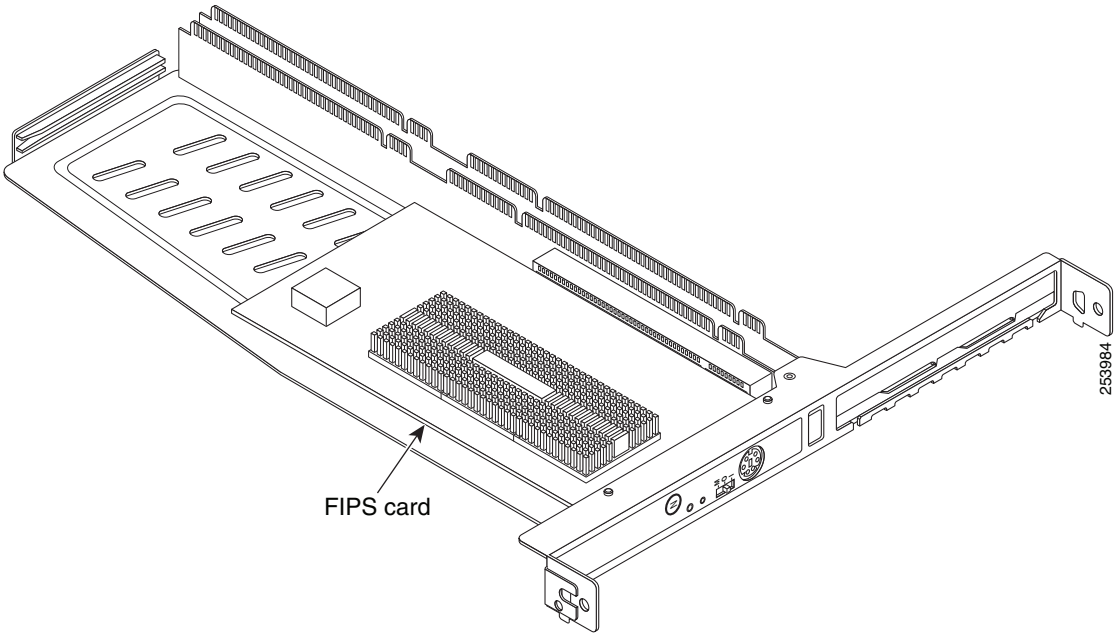
Step 4 Locate the roughly rectangular riser card assembly that comprises the upper-most portion of the back panel interfaces, release the captive riser card assembly retention screws on the rear of the chassis, and lift the assembly straight up from the chassis.

Installing the FIPS Card in the Riser Card Assembly

There is only one way you can install the FIPS card and simultaneously have enough room to fit the card inside the chassis.

Step 1 Place the riser card assembly upside-down on a suitable work surface.

Figure 2 Cisco NAC-3310 Riser Card Assembly



Step 2 Plug the field-replaceable FIPS card into the wider left-hand slot, ensuring that the FIPS card faceplate seats flush with the frame of the riser card assembly.

Reinstalling the Riser Card Assembly and Closing the Chassis

Step 1 Flip the riser card right-side-up and position it over the respective empty slots in the Cisco NAC-3310 chassis.

Step 2 Press down gently on both the front and rear of the riser card assembly until it seats properly into the chassis.

Step 3 Tighten the captive riser card assembly retention screws to ensure the riser assembly does not shift within the chassis when you replace the chassis cover.

Step 4 Place the chassis cover back on the chassis about 1 inch from the forward seated position, slide the chassis cover forward, and tighten the captive cover anchor screw to completely close the Cisco NAC-3310 chassis.

Step 5 Return the Cisco NAC-3310 to its position in the 4-post rack.

Installing the FIPS Card in the Cisco NAC-3350/3390

Note Cisco ships both the field-replaceable FIPS card and the required Cisco NAC-3350/3390 riser card assembly replacement for this particular installation.

Before installing the field-replaceable FIPS card in any of the supported Cisco NAC Appliance platforms, be sure to disconnect all interface cables, power down the appliance, and disconnect power from the chassis.

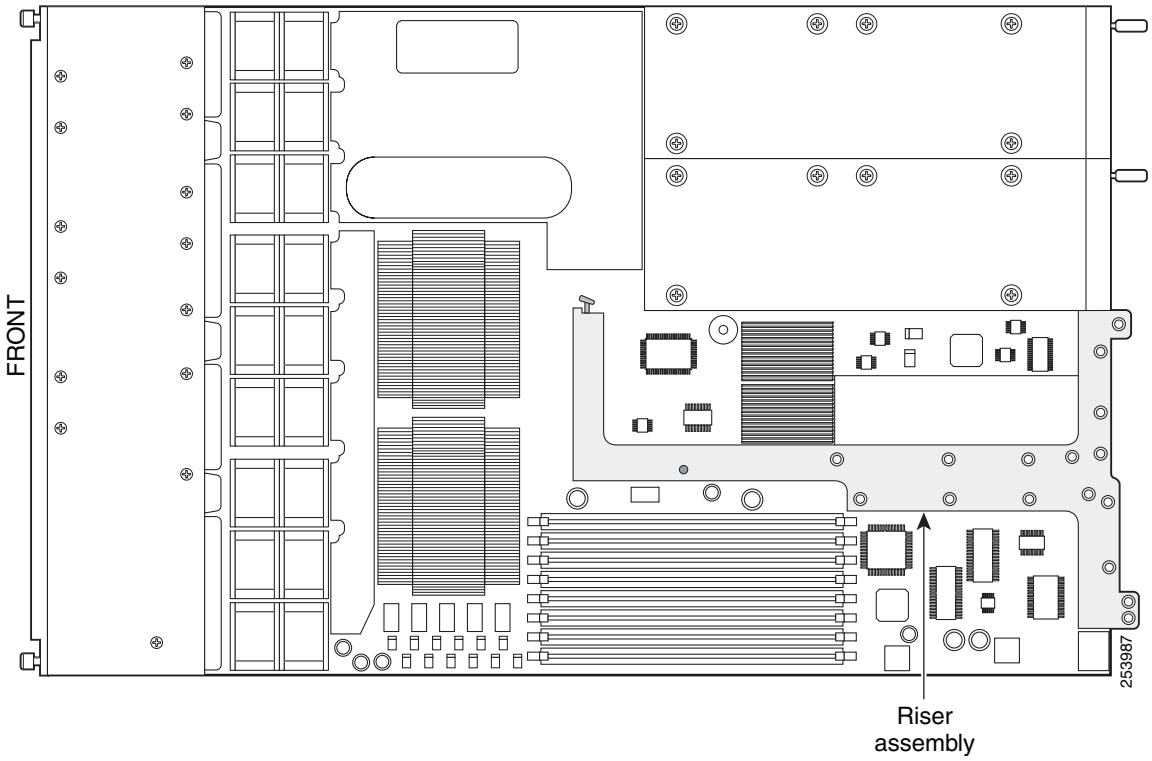
Opening the Chassis and Removing the Existing Riser Card Assembly

Step 1 Slide the Cisco NAC-3350/3390 away from its position in the 4-post rack on its rack rails. If your Cisco NAC-3350/3390 does not use rack rails, remove the chassis from the rack and place it on a suitable work surface.

Step 2 Use the recessed grips on the Cisco NAC-3350/3390 chassis cover to slide the cover back toward the rear of the chassis and unseat it.

Step 3 Remove the cover and set it aside, exposing the inside components of the Cisco NAC-3350/3390 chassis.

Figure 3 Cisco NAC-3350/3390 Chassis and Riser Card Assembly



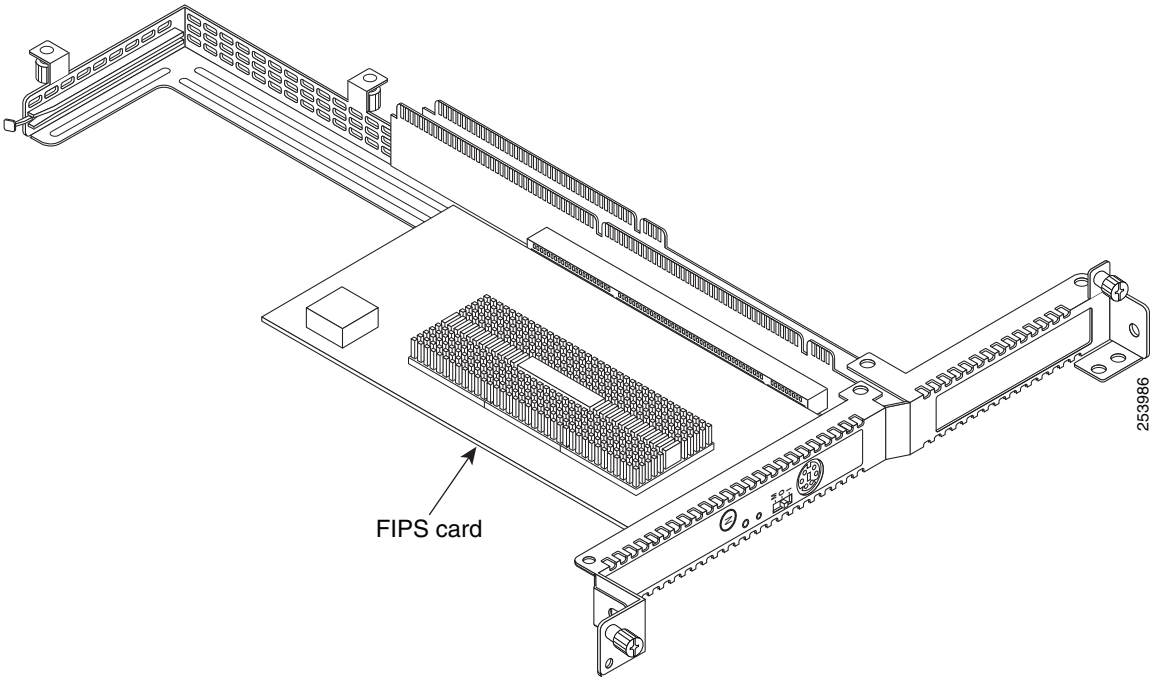
Step 4 Locate the large "T-shaped" riser card assembly that comprises the upper-most portion of the back panel interfaces, release the captive riser card assembly retention screws on the rear of the chassis and near the front of the riser card within the chassis, and lift the assembly straight up from the chassis.

Installing the FIPS Card in the New Riser Card Assembly

There is only one way you can install the FIPS card and simultaneously have enough room to fit the card inside the chassis.

Step 1 Place the new Cisco-supplied riser card assembly upside-down on a suitable work surface.

Figure 4 Cisco NAC-3350/3390 Riser Card Assembly



Step 2 Plug the field-replaceable FIPS card into the wider left-hand slot, ensuring that the FIPS card faceplate seats flush with the frame of the riser card assembly.

Step 3 Transfer any existing interface card from the right-hand slot in the old riser card assembly to the new one.

Installing the Completed Riser Card Assembly and Closing the Chassis

Step 1 Flip the riser card right-side-up and position it over the respective empty slot in the Cisco NAC-3350/3390 chassis.

Step 2 Press down gently on both the front and rear of the riser card assembly until it seats properly into the chassis.

Step 3 Tighten the four captive riser card assembly retention screws to ensure the riser assembly does not shift within the chassis when you replace the chassis cover.

Step 4 Place the chassis cover back on the chassis about 1 inch from the forward seated position and slide the chassis cover forward to completely close the Cisco NAC-3350/3390 chassis.

Step 5 Return the Cisco NAC-3350/3390 to its position in the 4-post rack.

Bringing the FIPS Card Field-Replaceable Unit Online

Once the FIPS card is installed and you have reconnected interfaces and power to the chassis, access the CAM/CAS console CLI and log in as **`root`** , enter the **`service perfigo config`** command, and accept the existing values for all configuration settings except the items specific to FIPS configuration.

Step 1 Connect the external FIPS Smart card reader module by plugging the Smart card reader mini-DIN cable into the female mini-DIN port on your newly installed FIPS card. (Ensure you also have a Smart card inserted into the reader.)

Step 2 In the CAM/CAS CLI, enter **`service perfigo config`** to launch the initial configuration dialog. The configuration prompts guide you through verifying existing configuration values and then asks if you want to enable FIPS mode on the appliance. Choose **`y`** to enable FIPS on your appliance.

```
Would you like to turn on fips mode? (y/n)? [y]
 ---- Stopping any nCipher servers ----

No nCipher init scripts installed.

 ---- Cleaning up any old install ----

No nCipher components requiring cleanup found.

 ---- Installing ----

-- Running install fragment 10nfastug

Checking for user 'nfast' in group 'nfast'
User 'nfast' or group 'nfast' do not exist.  To create the 'nfast' user,
in group 'nfast', with home directory /opt/nfast please select one of the
following options, based on the current linux distribution:
  1) Run 'useradd -r nfast' (this should work with Red Hat, SuSE, and
      Fedora-based distributions).
  2) Run 'adduser --group --system nfast' (this should work with Debian
      and Ubuntu-based distributions).
  3) Edit /etc/passwd and /etc/group (this should work with most
      distributions that do not use shadow passwords).
  4) Exit the script so you can create the user and group manually.
      Rerun the install script when this is complete.
  5) Abort the installation process.
Please select a number from 1 to 5:

-- Running install fragment 15makefiles
Setting up directories.
Making default config file.

-- Running install fragment 45drivers
Unloading old nCipher PCI nfp driver.
Checking for PCI nfp hardware.
```

```
Found: /dev/nfastpci0
Installing startup scripts for 'drivers'.
Linking in init scripts
Loading nCipher PCI nfp driver.

-- Running install fragment 46exard
Remove old nCipher PCI miniHSM devices.
Checking for nCipher PCI miniHSM hardware.
No nCipher PCI miniHSM devices found.
Installing startup scripts for 'exard'.
Not linking in init scripts or loading drivers.

-- Running install fragment 50hardserver
Making privconn setuid and root.
Installing startup scripts for 'hardserver'.
Linking in init scripts
Starting nCipher 'hardserver' server process.
waiting for nCipher server to become operational ...
waiting for nCipher server to become operational ...
waiting for nCipher server to become operational ...
nCipher server now running

 -- Running install fragment 60cmdadp

 ---- Installation complete ----
 -- Running shutdown script 50hardserver

 -- Running shutdown script 46exard

 -- Running shutdown script 45drivers

 -- Running startup script 45drivers

 -- Running startup script 46exard

 -- Running startup script 50hardserver

Security world not found
Creating the security world and initializing the smart cards
How many cards do you want to initialize (1-6)? [1] 1
Set ncipher card switch in i mode and press Return to continue
```

Step 3 Enter the number of Smart Cards you want to initialize, ensure that the FIPS card operation switch on the back of the CAM/CAS is switched to “I” (for “initialize”), and press Return. You will also need to enter a passphrase to enable FIPS functions on the appliance.

```
Module 1, command ClearUnit: OK

Create Security World:
 Module 1: 0 cards of 1 written
 Module 1 slot 0: unformatted card
 Module 1 slot 0:- passphrase specified - writing card
Card writing complete.

security world generated on module #1; hknso = 32f3a58da27cd15cd2a7fda08526f1d0ca96ac63
Set ncipher card switch in o mode and press Return to continue
```

Step 4 Switch the FIPS card switch back to “O” (for “operational”) and press Return.

```
Module 1, command ClearUnit: OK
writing RSA key
Card(s) check passed
```

Step 5 Continue through the CAM/CAS initial configuration dialog session, accepting current values for any existing configuration settings and enter the following command to reboot the CAM/CAS after configuration is complete:

```
Configuration is complete.
Changes require a REBOOT of Clean Access Server.

# reboot
```

Step 6 After the CAM/CAS reboots, repeat Step 2 through Step 5.

The initial configuration is now complete.

Verifying FIPS Card Field-Replaceable Unit Operation

There are two methods you can use to verify proper installation and FIPS operation on the CAM/CAS:

- Command Line Interface Method
- CAM/CAS Web Console Method

Command Line Interface Method

Verify FIPS functionality on the CAM/CAS as follows:

- Ensure the FIPS card operation switch is set to “O” (for operational mode).
- Log into the CAM console interface as **root**.
- Navigate to the **/perfigo/common/bin/** directory.
- Enter **./test_fips.sh info** and verify the following output:

```
Installed FIPS card is nCipher
Info-FIPS file exists
Info-card is in operational mode
Info-httpd worker is in FIPS mode
Info-sshd up
```

CAM/CAS Web Console Method

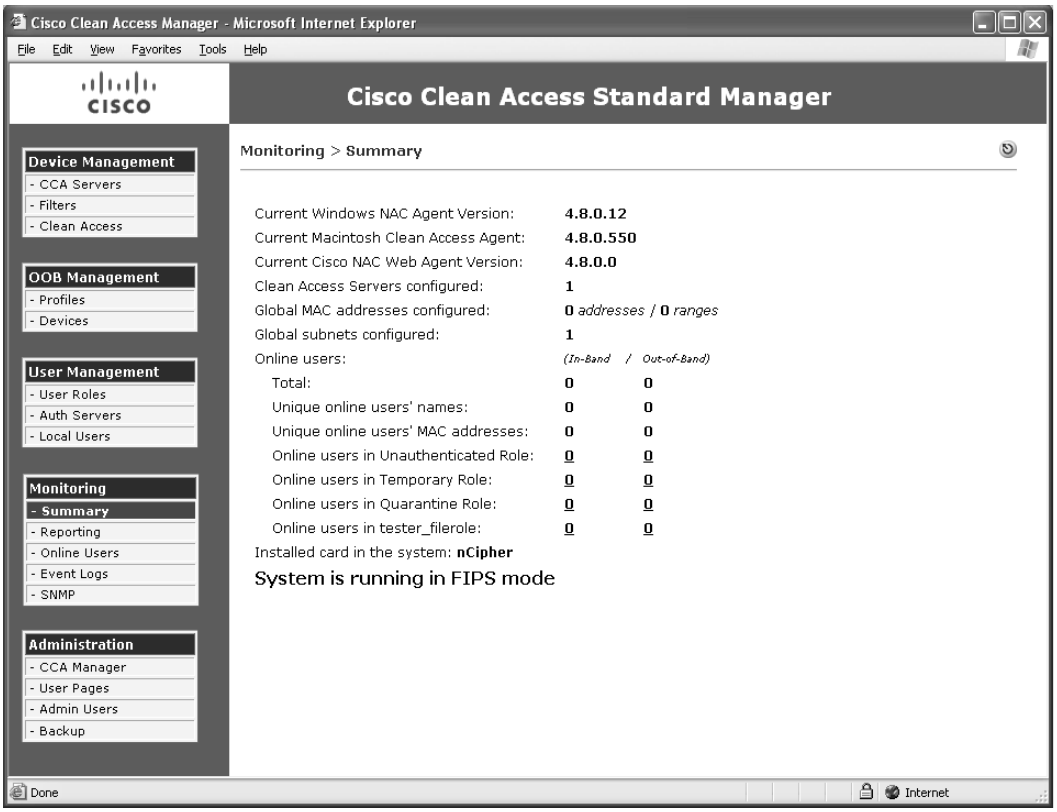
To verify FIPS operation on the CAM:

Step 1 On your local machine, launch a browser session, and log into the CAM web console,

Step 2 View the status messages in the CAM **Monitoring > Summary** page (Figure 5). The page should read:

```
Installed card in the system: nCipher
System is running in FIPS mode
```

Figure 5 CAM Monitoring > Summary Page



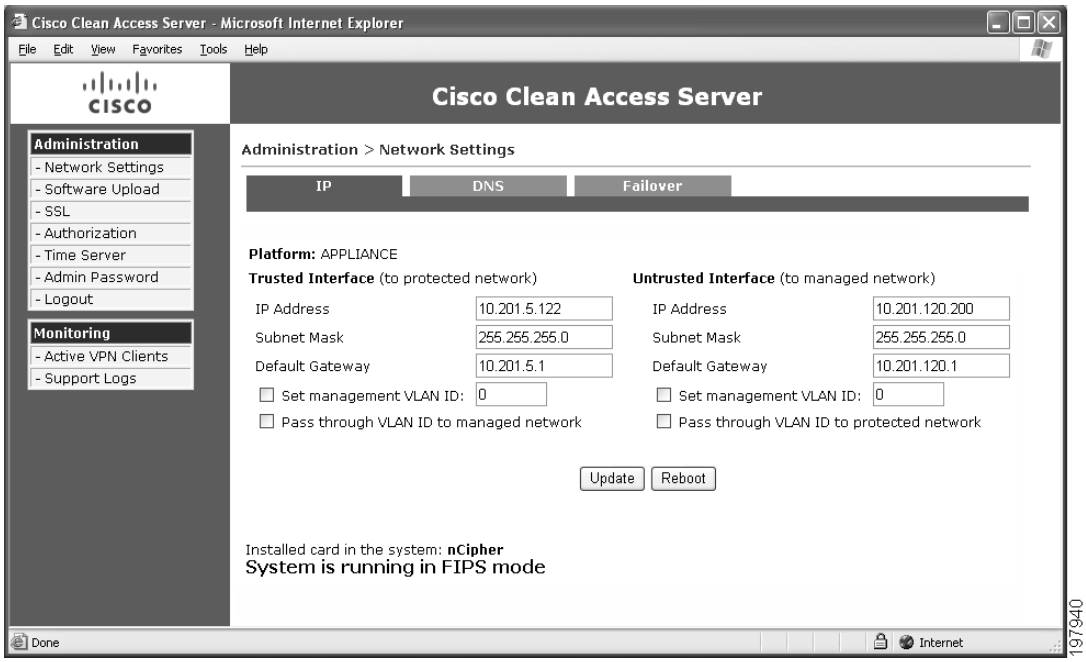
To verify FIPS operation on the CAS:

Step 1 On your local machine, launch a browser session, and log into the CAS web console,

View the status messages in the CAS **Administration > Network Settings > IP** page (Figure 6). The page should read:

```
Installed card in the system: nCipher
System is running in FIPS mode
```

Figure 6 CAS Administration > Network Settings > IP Page



What's Next? Configuring the CAM/CAS for FIPS Compliance

After you install and enable field-replaceable FIPS cards in your NAC-3310/33/50/3390s, connectivity with external components like RADIUS servers, Wireless LAN Controllers, and VPN Concentrators will likely fail. This field-replaceable unit installation guide does not address configuring and enabling FIPS functionality on your CAMs/CASs to ensure connectivity with such external components. Refer to the following documents for complete information on configuring your CAMs/CASs to operate and maintain connectivity with other external components in a FIPS-compliant environment:

- See the "FIPS 140-2 Compliance" section of the *Release Notes for Cisco NAC Appliance* corresponding to your latest Cisco NAC Appliance release version.
- See the "FIPS Compliance in the Cisco NAC Appliance Network" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide* corresponding to your latest Cisco NAC Appliance release version.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.