APPENDIX B

Reimaging and Configuring the CSC SSM Using the CLI

This appendix describes how to reimage and configure the CSC SSM using the CLI, and includes the following sections:

The Trend Micro InterScan for Cisco CSC SSM software is preinstalled on the adaptive adaptive security appliance. Normally, you only need to use the information in this appendix for password or system recovery procedures.

Note If installation is required, the Setup Wizard launched from the ASDM is the preferred method of installation. For more information, see the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

Installation Checklist

Before you start, be prepared to supply the following information during installation, shown in Table B-1. If you prefer, you can print a copy of this table and use it as a checklist to record the values you enter.

Table B-1 Installation Checklist

Information Requested	Information Entered	Completed
Administrator password for the CLI	Do not record your password.	—
SSM card IP address		❑
Subnet mask		❑
Hostname (1 to 63 alphanumeric characters; can include hyphens, except as the first character). For example: cisco1-ssm-csc		❑

Table B-1 Installation Checklist (continued)

Information Requested	Information Entered	Completed
Domain name		❑
Primary DNS IP address		❑
Secondary DNS IP address (optional)		❑
Gateway IP address		❑
Proxy server? (optional) If yes: Proxy server IP address Proxy server port number		❑ ❑ ❑
Domain name for incoming e-mail		❑
Administrator password for the CSC SSM console	Do not record your password.	—
Administrator e-mail address		❑
Notification e-mail server IP address		❑
Notification e-mail server port number		❑
Base License Activation Code		❑
Plus License Activation Code (optional)		❑
License Renewal Notification E-mail Address		❑
License Renewal Notification SMTP Server IP Address		❑

Preparing to Reimage the Cisco CSC SSM

You should reimage the CSC SSM under the following conditions:

- No previous image of CSC has been installed on the SSM.
- The CSC image is suspected of being corrupted beyond repair.
- The CSC card is rebooting regularly.
- The CSC card becomes unresponsive or unstable after an upgrade.

During installation, you are prompted to synchronize the date and time on the CSC SSM with the adaptive security appliance. Before you begin, make sure that the date and time settings on the adaptive security appliance are correct.

To prepare for reimaging, perform the following steps:

Step 1 Download the Trend Micro InterScan for Cisco CSC SSM software to your TFTP server.

Note The TFTP server must support files sizes greater than 60 MB. The .bin files are full binary images that are to be uploaded via a TFTP server. The .pkg files are used to upgrade image files from the CSC Admin Console, which are then uploaded through a web browser. Do not upload .bin files using the CSC Admin Console.

Step 2 Using a terminal application such as Windows HyperTerminal, log in and open a terminal session to the adaptive security appliance console by entering the following command:

```
hostname# hw module 1 recover config
```

The following is example output:

```
Image URL tftp://insidehost/csc6.2.xxxx.x.bin]:tftp://insidehost/csc6.2.xxxx.x.bin
Port IP Address [000.000.0.00]:
VLAN ID [0]:
Gateway IP Address [0.0.0.0]:
hostname# hw module 1 recover boot
The module in slot 1 will be recovered. This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

Step 3 Enter **y** to confirm.

```
Recover issued for module in slot 1
```

Step 4 Enable the **debug module-boot** command.

```
hostname# debug module-boot
debug module-boot enabled at level 1
hostname# Slot-1 199> Cisco Systems ROMMON Version (1.0(8)1) #0: Thu Jan 20 20:28:49 PST
2010
Slot-1 200> Platform SSM-IDS20
Slot-1 201> GigabitEthernet0/0
Slot-1 202> Link is UP
Slot-1 203> MAC Address: 000b.fcf8.0134
Slot-1 204> ROMMON Variable Settings:
Slot-1 205>   ADDRESS=192.168.7.20
Slot-1 206>   SERVER=192.168.7.100
Slot-1 207>   GATEWAY=0.0.0.0
Slot-1 208>   PORT=GigabitEthernet0/0
Slot-1 209>   VLAN=untagged
Slot-1 210>   IMAGE=csc6.2.xxxx.x.bin
Slot-1 211>   CONFIG=
Slot-1 212> tftp csc6.2.xxxx.x.bin@192.168.7.100
Slot-1 213> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 214> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
.
.
.
```

Note This process takes about ten minutes.

```
.
.
.
Slot-1 389>!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 390> Received 57985402 bytes
Slot-1 391> Launching TFTP Image...
Slot-1 392> Cisco Systems ROMMON Version (1.0(8)1) #0: Thu Jan 20 20:28:49 PST 2007
```

```
Slot-1 393> Platform SSM-IDS20
Slot-1 394> GigabitEthernet0/0
Slot-1 395> Link is UP
Slot-1 396> MAC Address: 000b.fcf8.0134
Slot-1 397> Launching BootLoader...
```

Caution The module recovery can loop if the image is corrupt or if the size of the image file exceeds the limitations on the TFTP server. If the module is stuck in a recovery loop, you must enter the **hw module 1 recover stop** command to stop the module from trying to load the image.

Step 5 Disable the **debug-module boot** command.

```
hostname# no debug module-boot

hostname# show module 1 details

Getting details from the Service Module, please wait...
SSM-IDS/10-K9
Model:              SSM-IDS10
Hardware version:   1.0
Serial Number:      0
Firmware version:   1.0(8)1
Software version:   CSC SSM 6.6.xxxx.x
MAC Address Range:  000b.fcf8.0159 to 000b.fcf8.0159
App. name:          CSC SSM
App. Status:        Down
App. Status Desc:   CSC SSM scan services are not available
App. version:       CSC SSM 6.6.xxxx.x
Data plane Status:  Up
Status:             Up
HTTP Service:       Down
HTTPS Service:      Down
Mail Service:       Down
FTP Service:       Down
Activated:          No
Mgmt IP addr:       <not available>
Mgmt web port:      8443
Peer IP addr:       <not enabled>
```

Step 6 Open a command session.

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 7 Log in to Trend Micro InterScan for Cisco CSC SSM using “cisco” as the default login username and password.

```
login: cisco
Password:
```

Step 8 Change your password immediately. Do not use the same password that you use to access ASDM.

```
You are required to change your password immediately (password aged)
Changing password for cisco
(current) UNIX password:
New password:
Retype new password:
```

Reimaging the CSC SSM

This section describes how to reimage the CSC SSM, and includes the following topics:

To reimage the CSC SSM using the CLI Setup Wizard, perform the following steps:

Step 1 Log in to the adaptive adaptive security appliance using the administrator username and password.

After you confirm your administrator CLI password, the Trend Micro InterScan for Cisco CSC SSM Setup Wizard appears.

```
Trend Micro InterScan for Cisco CSC SSM Setup Wizard
------------------------------------------------------------------------------
To set up the SSM, the wizard prompts for the following information:
    1. Network settings
    2. Date/time settings verification
    3. Incoming e-mail domain name
    4. Notification settings
    5. Activation Codes
The Base License is required to activate the SSM.
Press Control-C to abort the wizard.

Press Enter to continue...
```

Step 2 Enter **1** to configure network settings.

The Network Settings prompts appear.

```
Network Settings
------------------------------------------------------------------------------
Enter the SSM card IP address:
Enter subnet mask:
Enter host name:
Enter domain name:
Enter primary DNS IP address:
Enter optional secondary DNS IP address:
Enter gateway IP address:
Do you use a proxy server? [y|n] n
```

Step 3 Respond to the network settings prompts, using values from the installation checklist. When you are finished with the last network settings prompt, your entries appear for visual verification. For example:

```
Network Settings
```

```
------------------------------------------------------------------------
IP              000.000.0.00
Netmask         255.255.255.0
Hostname        CSCSSM
Domain name     example.com

Primary DNS     10.2.200.2
Secondary DNS   10.2.203.1

Gateway         000.000.0.0
No Proxy

Are these settings correct? [y|n] y
```

Step 4 If the settings are correct, retype **y** to confirm. (If you choose **n**, the Network Settings prompts reappear; repeat Step 2.)

After you confirm your network settings, the system responds with the following message:

```
Applying network settings...
```

Step 5 (Optional) Confirm the network settings by pinging the gateway IP address. To skip pinging, choose **n**.

```
Do you want to confirm the network settings using ping? [y|n] y
Enter an IP address to ping: 000.000.0.0
PING 000.000.0.0 (192.168.7.1): 56 data bytes
64 bytes from 192.168.7.1: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 192.168.7.1: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 192.168.7.1: icmp_seq=3 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=4 ttl=255 time=0.1 ms

--- 192.168.7.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.2 ms
Press Enter to continue...
```

The Date/Time Settings prompt appears.

```
                        Date/Time Settings
------------------------------------------------------------------------

SSM card date and time: 10/06/2005 18:14:14

The SSM card periodically synchronizes with the chassis.
Is the time correct? [y|n] y
```

Step 6 Enter **y** to set the date and time to synchronize with the chassis. Enter **n** to update the date and time, exit the Setup Wizard, update the date and time or NTP settings on the ASA chassis, and reinstall the SSM.

The Incoming Domain Name prompt appears.

```
Incoming Domain Name
------------------------------------------------------------------------

Enter the domain name that identifies incoming e-mail messages: (default:example.com)
Domain name of incoming e-mail: example.com
Is the incoming domain correct? [y|n] y
```

Step 7 Enter your highest level domain name for your organization and then **y** to continue.

The Administrator/Notification Settings prompts appear.

```
Administrator/Notification Settings
------------------------------------------------------------------------
```

```
Administrator e-mail address:
Notification e-mail server IP:
Notification e-mail server port: (default:25)
```

Step 8 Enter the correct value for each setting.

A confirmation message appears, as shown in the following example:

```
Administrator/Notification Settings
------------------------------------------------------------------------

Administrator e-mail address: tester@example.com
Notification e-mail server IP: 10.2.202.28
Notification e-mail server port: 25
Are the notification settings correct? [y|n] y
```

Step 9 Enter **y** to continue.

The Activation prompts appear.

```
                            Activation
------------------------------------------------------------------------

You must activate your Base License, which enables you to update
your virus pattern file. You may also activate your Plus License.

Activation Code example: BV-43CZ-8TYY9-D4VNM-82We9-L7722-WPX41
Enter your Base License Activation Code: PX-ABTD-L58LB-XYZ9K-JYEUY-H5AEE-LK44N
Base License activation is successful.

(Press Enter to skip activating your Plus License.)
Enter your Plus License Activation Code: PX-6WGD-PSUNB-9XBA8-FKW5L-XXSHZ-2G9MN
Plus License activation is successful.
```

The Activation Status appears.

```
Activation Status
------------------------------------------------------------------------

Your Base License is activated.
Your Plus License is activated.

Stopping services: OK
Starting services: OK

The Setup Wizard is finished.
Please use your Web browser to connect to the management console at:
https://192.168.7.20:8443
Press Enter to exit...

Remote card closed command session. Press any key to continue.
Command session with slot 1 terminated.
hostname#
```

The services starting message informs you that installation is complete.

Step 10 Use your browser to log on to the CSC SSM console by entering the URL in the following format:

```
https://<SSM IP address>:8443/
```

Confirming the Installation

When the reimaging is complete, perform the following steps:

Step 1 To view information about the CSC SSM and the services you configured during installation, enter the following command:

```
hostname# show module 1 details

Getting details from the Service Module, please wait...
SSM-IDS/20-K9
Model: SSM-IDS20
Hardware version:   1.0
Serial Number:      0
Firmware version:   1.0(8)1
Software version:   CSC SSM 6.2.xxxx.x
MAC Address Range:  000b.fcf8.0134 to 000b.fcf8.0134
App. name:          CSC SSM proxy services are not available
App. version:
App. name:          CSC SSM
App. version:       6.6.xxxx.x
Data plane Status:  Up
Status:             Up
HTTP Service:       Up
HTTPS Service:      Up
Mail Service:       Up
FTP Service:       Up
Activated:          Yes
Mgmt IP addr:       192.168.7.20
Mgmt web port:      8443
Peer IP addr:       <not enabled>
hostname#
```

Step 2 To start a command session, enter the following command:

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 3 Log in using the default login name “cisco” and the password that you configured on the Administrator/Notification Settings window during installation.

```
login: cisco
Password:
Last login: Mon Oct 10 13:24:07 from 127.0.1.1
```

The Trend Micro InterScan for Cisco CSC SSM Setup Main Menu appears.

```
     Trend Micro InterScan for Cisco CSC SSM Setup Main Menu
------------------------------------------------------------------------

1. Network Settings
2. Date/Time Settings
3. Product Information
4. Service Status
5. Password Management
6. Restore Factory Default Settings
7. Troubleshooting Tools
8. Reset Management Port Access Control List
9. Ping
10. Exit...
```

```
Enter a number from [1-10]:
```

Viewing or Modifying Network Settings

To view or modify network settings, enter **1**.

The Network Settings prompts appear.

```
Network Settings
------------------------------------------------------------------

IP              192.168.7.20
Netmask         255.255.255.0
Hostname        CSCSSM
Domain name     tester@example.com
MAC address     00:0B:FC:F8:01:34

Primary DNS     10.2.200.2
Secondary DNS   10.2.203.1

Gateway         192.168.7.1
No Proxy

Do you want to modify the network settings? [y|n] n
```

Viewing Date and Time Settings

To view the date and time settings, enter **2**.

The Date/Time Settings prompts appear:

```
Date/Time Settings
------------------------------------------------------------------

SSM card date and time: 10/10/2005 13:27:09 PDT

Press Enter to continue...
```

Note You cannot change these settings—this information is for reference only.

Viewing Product Information

To view the product version and build numbers, enter **3**.

The Product Information prompts appear:

```
                        Product Information
------------------------------------------------------------------

Trend Micro InterScan for Cisco CSC SSM 6.2.xxxx.x

Press Enter to continue...
```

Note You cannot change these settings—this information is for reference only.

Viewing or Modifying Service Status

To view or modify service status, perform the following steps:

Step 1 Enter **4**.

The Service Status prompts appear.

```
Service Status
------------------------------------------------------------------------

The CSC SSM RegServer service is running
The CSC SSM HTTP service is running
The CSC SSM HTTPS service is running
The CSC SSM FTP service is running
The CSC SSM Notification service is running
The CSC SSM Mail service is running
The CSC SSM GUI service is running
The CSC SSM SysMonitor service is running
The CSC SSM Failoverd service is running
The CSC SSM LogServer service is running
The CSC SSM SyslogAdaptor service is running
The CSC SSM Syslog-ng service is running

Do you want to restart all services? [y|n] n
```

Step 2 Enter **y** to restart scanning services. Enter **n** if everything is running smoothly.

Note If you are trying to troubleshoot a problem, restarting may return the SSM to the correct operating status. For more information about the effects of restarting services, see the "Restart Scanning Service" section on page 8-13.

Using Password Management

This section describes how to manage passwords, and includes the following topics:

- Changing the Current Password, page B-11
- Modifying the Password-Reset Policy, page B-11

To use Password Management, enter **5**.

The following prompt appears:

```
Enter a number from [1-10]: 5

                        Password Management
------------------------------------------------------------------------
```

```
1. Change Password
2. Modify Password-reset Policy
3. Return to Main Menu

Enter a number from [1-3]: 1
```

Changing the Current Password

To change the password, perform the following steps:

Step 1 Access the Change Password command, as shown in the previous procedure.

The following screen appears.

```
                          Change Password
------------------------------------------------------------------------

This option allows you to change the password for the CSC SSM that
you are currently using.
```

Step 2 Type **y** and press **Enter**.

```
Do you want to continue? [y|n] y
```

Step 3 Type the old password and press **Enter**.

```
The password will be hidden while you type.
Press Enter to return to last menu.
Enter old password:
```

Note Password characters include: ~ ! @ # $ % ^ & * ( ) _ + ` - = { } | [ ] \ : ” ; ’ < > ? , . / . The plus sign is not a valid character if you change the password through the CSC SSM console. This symbol only works through the CLI.

Step 4 Type the new password and press **Enter**. Then retype the new password and press **Enter** to confirm it.

```
Enter new password (minimum of 5, maximum of 32 characters)
Enter new password:
Re-enter new password:
Please wait...
The password has been changed.
```

Modifying the Password-Reset Policy

You can modify the password-reset policy to “Allowed” or “Denied.”

- “Allowed” means you can reset the CSC SSM password through the ASDM without verifying the old password. Under this setting, you can reset the password, even if the current password has been lost.
- “Denied” means you cannot reset the CSC SSM password through the ASDM without reimaging and reactivating the CSC SSM. However, you can still change the password to the CSC SSM if you know the current password.

Caution Setting the password-reset policy to "Allowed" compromises the security of the application.

To modify the password-reset policy, perform the following steps:

Step 1 From the Password Management menu, enter **2**. For access details, see the "Using Password Management" section on page B-10.

The following screen appears.

```
                  Modify Password-reset Policy
------------------------------------------------------------------------

Current CSC SSM password-reset policy: Allowed

"Allowed" allows the Adaptive Security Device Manager (ASDM)
to reset the CSC SSM password without verifying the old password.

"Denied" does not allow the ASDM to reset the CSC SSM password
without re-imaging and re-activating the CSC SSM.
```

Step 2 Type **y** and press **Enter** to change the password-reset policy, as shown in the following example:

```
Do you want to modify the CSC SSM password-reset policy now? [y|n] y
```

The following confirmation appears:

```
Updated CSC SSM password-reset policy: Denied
```

Restoring Factory Default Settings

To restore factory default configuration settings, enter **6**.

The Restore Factory Default Settings prompt appears.

```
Restore Factory Default Settings
------------------------------------------------------------------------

Are you sure you want to restore the factory default settings? [y|n] n
```

Caution If you enter **y**, all your configuration settings are returned to the preinstallation default settings. For a description of the default settings, see the "Default Mail Scanning Settings" section on page 3-1 and the "Default Web and FTP Scanning Settings" section on page 4-1. Additional configuration changes you have made since installation, such as registration or activation, licensing, enabling spyware or grayware detection, file blocking, file blocking exceptions, and other settings are lost.

Although this option is available from the CLI, a better alternative for restoring configuration settings is available from the CSC SSM console. Choose **Administration > Configuration Backup** to view the Configuration Backup window, which allows you to export your configuration settings to a configuration file that you can import at a later time.

Note Choose the Restore Factory Default Settings option only if you must reinstall the CSC SSM.

Troubleshooting Tools

This section describes the troubleshooting tools, and includes the following topics:

Enter **7** to display a menu of troubleshooting tools. These tools are available to help you or Cisco TAC obtain information to troubleshoot a problem.

```
Troubleshooting Tools
------------------------------------------------------------------------

1. Enable Root Account
2. Show System Information
3. Gather Logs
4. Gather Packet Trace
5. Modify Upload Settings
6. Modify Management Port Console Access Settings
7. Return to Main Menu

Enter a number from [1-7]:
```

Enabling Root Account

To enable root account access, perform the following steps:

Step 1 Enter **1**.

The following warning appears:

```
********************** WARNING ************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and
troubleshooting purposes only. Unauthorized modifications
are not supported and will require this device to be
re-imaged to guarantee proper operation.
*******************************************************
Do you want to accept the warning and enable the root account? [y|n] y
```

Step 2 Enter **y** to enable the root account.

This warning only appears the first time you enable the root account. After the root account is enabled, you cannot disable it.

Caution This option is not intended for use by system administrators; it is provided for use by Cisco service personnel only. Do not choose this option unless directed to do so by Cisco TAC.

Showing System Information

This section describes how to show system information, and includes the following topics:

To view system information directly on the screen, enter **2**. Alternatively, you can save the data to a file and transfer the information using FTP or TFTP. The Troubleshooting Tools - Show System Information menu appears.

```
Troubleshooting Tools - Show System Information
------------------------------------------------------------------------

1. Show System Information on Screen
2. Upload System Information
3. Return to Troubleshooting Tools Menu
```

Showing System Information on Screen

To show system information on screen, perform the following steps:

Step 1 Enter **1** from the Troubleshooting Tools - Show System Information menu. System information is available from various locations on the ASDM and CSC SSM interfaces; however, this CLI makes the information available in one place, as shown in the following example:

```
++++++++++++++++++++++
Mon Jul 24 18:38:01 PST 2007 (-8)

System is: Up

# Product Information
Trend Micro InterScan for Cisco CSC SSM
Version: 6.02.xxxx.x
SSM Model: SSM-10

# Scan Engine and Pattern Information
Virus Scan Engine: 8.500.1002 (Updated: 2007-07-24 14:10:07)
Virus Pattern: 4.613.00 (Updated: 2007-07-23 14:10:39)
Grayware Pattern: 0.527.00 (Updated: 2007-07-23 14:13:11)
PhishTrap Pattern: 392 (Updated: 2007-07-23 14:13:28)
AntiSpam Engine: 15320 (Updated: 2007-07-24 14:11:04)
AntiSpam Rule: 3.8.1029 (Updated: 2007-07-24 14:12:53)
IntelliTrap Pattern: 0.527.00 (Updated: 2007-07-23 14:13:11)
IntelliTrap Exception Pattern: 0.527.00 (Updated: 2007-07-23 14:13:11)

# License Information
Product: Base License
Version: Standard
Activation Code:BX-9YWQ-3685S-X39PZ-H96NW-MAJR7-CWBXR
Seats:000250
Status:Expired within grace period
Expiration date:12/31/2007
Product:Plus License
```

```
Version: Standard
Activation Code:PX-P67G-WCJ6G-M6XJS-2U77W-NM37Y-EZVKJ
Status: Expired within grace period
Expiration date:12/31/2007

Daily Node Count: 0
Current Node Count: 0

# Kernel Information
Linux csc 2.4.26-cscssm #2 SMP Mon Mar 19 11:53:05 PST 2007 (1.0.6) i686
unknn

ASDP Driver 1.0(0) is UP:
    Total Connection Records: 169600
    Connection Records in Use: 0
    Free Connection Records: 169600
```

The information continues to scroll.

Step 2 Enter **q** to quit.

Uploading System Information

To upload system information, perform the following steps:

Step 1 From the Troubleshooting Tools - Show System Information menu, enter **2**.

The following prompts appear:

```
Gathering System Information...
Creating temporary file CSCSSM-SYSINFO-20060109-184511.txt
Uploading temporary file CSCSSM-SYSINFO-20060109-184511.txt
Uploading file...
Deleting temporary file CSCSSM-SYSINFO-20060109-184511.txt
Press Enter to continue...
```

Step 2 Respond to these prompts to upload the system information. The system information is sent using the upload settings created by entering **5**, **Modify Upload Settings**. For more information, see the "Modifying Upload Settings" section on page B-16.

If you did not configure the upload settings, the following prompts precede those appearing in the previous step:

```
Choose a protocol [1=FTP 2=TFTP]: 1
Enter FTP server IP: 10.2.15.235
Enter FTP server port: (default:21)
Enter FTP user name: ftp
The password will be hidden while you type.
Enter FTP password:
Retype FTP server password:
Saving Upload Settings: OK
```

Step 3 When you are finished, enter **3** from the Show System Information menu.

Collecting Logs

To collect all logs, perform the following steps:

Step 1 To collect all logs on the CSC SSM, enter **3**. Upload them via FTP or TFTP to your server, so that Cisco TAC can then obtain them through a pre-arranged method. The logs are sent using the upload settings created by entering **5**, **Modify Upload Settings**. For more information, see the "Modifying Upload Settings" section on page B-16.

```
Troubleshooting Tools - Gather Logs
-------------------------------------------------------------------

Gather logs now? [y|n] y
Gathering logs...
Creating temporary file CSCSSM-LOG-20060109-184525.tar.gz
Uploading temporary file CSCSSM-LOG-20060109-184525.tar.gz
Uploading file...
Deleting temporary file CSCSSM-LOG-20060109-184525.tar.gz
```

Step 2 Enter **y** to gather logs.

Note Logs are automatically named using the following convention: CSCSSM-LOG-<date-time>.tar.gz.

Enabling Packet Tracing

If you attempt to use the packet tracing command in CSC SSM, the following message appears:

```
"This function is now obsolete. Please use the 'capture' command in the ASA CLI for the
'asa_dataplane' interface."
```

To enable packet tracing between the CSC SSM and adaptive security appliance, use the **packet capture** command shown in the "Performing a Packet Capture" procedure on page 8-7.

Modifying Upload Settings

To modify upload settings, perform the following steps:

Step 1 To set the uploading method to either FTP or TFTP, enter **5**.

Note Your FTP or TFTP server must be set up to enable uploading.

When you enter **5**, the following prompts appear:

```
Troubleshooting Tools - Upload Settings
-------------------------------------------------------------------

Choose a protocol [1=FTP 2=TFTP]: (default:1) 2
Enter TFTP server IP: (default:10.2.42.134)
Enter TFTP server port: (default:69)
Saving Upload Settings: OK
```

```
Press Enter to continue...
```

Step 2 Respond to the prompts to configure the upload settings. The settings are saved for future use.

Step 3 When you are finished, enter **7**, **Return to Main Menu**.

Changing the Management Port Console Access Settings

If the ASDM is unable to communicate with the CSC SSM, try resetting port access by performing the following steps:

Step 1 To reset the management port access control, enter **6.**

When you enter **6**, the following appears:

```
Troubleshooting Tools - Management Port Console Access Settings
----------------------------------------------------------------------

Current Telnet Access: Disabled
Current SSH Access: Disabled
Modify Telnet Setting [1=Enable 2=Disable]: (default:2) 1
Modify SSH Setting [1=Enable 2=Disable]: (default:2) 1
Saving Management Port Console Access Settings: OK
Press Enter to continue ...
```

Step 2 Respond to the prompts to configure the port access. The settings are saved for future use.

Step 3 When you are finished, enter **7**, **Return to Main Menu**.

Resetting the Management Port Access Control

To reset the management port access control, enter **8** from the main menu.

The following appears:

```
Resetting management port access control list: OK
Press Enter to continue ...
```

If the ASDM is unable to communicate with the CSC SSM, try resetting port access via this option.

Pinging an IP Address

To ping an IP address, perform the following steps:

Step 1 Enter **9**. The ping option is available for diagnostic purposes.

The following appears:

```
Enter an IP address to ping:
```

Step 2 Enter an IP address.

The system responds as follows:

```
PING 192.168.7.1 (192.168.7.1): 56 data bytes
64 bytes from 192.168.7.1: icmp_seq=0 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=2 ttl=255 time=0.1 ms
64 bytes from 192.168.7.1: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 192.168.7.1: icmp_seq=4 ttl=255 time=0.1 ms

--- 192.168.7.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.2 ms
Press Enter to continue...
```

Exiting the Setup Wizard

To exit the Setup Wizard, perform the following steps:

Step 1 To exit the Setup Wizard, enter **10**.

The Exit Options menu appears.

```
Exit Options
-----------------------------------------------------------------------

1. Logout
2. Reboot
3. Return to Main Menu

Enter a number from [1-3]: 1
Remote card closed command session. Press any key to continue.
Command session with slot 1 terminated.
hostname#
```

Step 2 From the Exit Options menu, choose **1** to log out, **2** to reboot the system, or **3** to return to the Setup menu.

Resetting the Configuration via the CLI

This section describes some alternatives that are available for users who want to use the CLI instead of the CSC SSM console. Not all features have an available alternative.

After you have installed Trend Micro InterScan for Cisco CSC SSM, if you have used TFTP to reimage the SSM, the following prompt may appear for the first time when you access the CLI:

```
Trend Micro InterScan for Cisco CSC SSM Setup Wizard
-----------------------------------------------------------------------

To set up the SSM, the wizard prompts for the following information:
1. Network settings
2. Date/time settings verification
3. Incoming e-mail domain name
4. Notification settings
5. Activation Codes
The Base License is required to activate the SSM.
Press Control-C to abort the wizard.
```

```
Press Enter to continue...
```

Enter **y** to restore the SSM configuration settings to the state they were in the last time you saved the configuration. This is a CLI alternative to the functionality available on the Administration > Configuration Backup window on the CSC SSM console.

Improving CSC SSM Performance

This section provides information about how to improve CSC SSM performance, and includes the following topics:

When users initially connect to the Internet through the CSC SSM, the CSC SSM contacts the Trend Micro web server using an HTTP request to determine the URL category for URL filtering and blocking. The CSC SSM scans this HTTP request again, which results in two HTTP connections for one initial request.

Note This additional scan is unnecessary. HTTP performance may improve when you prevent CSC SSM packets from being scanned unnecessarily.

Depending on your topology and configuration, you may be able to improve HTTP performance through the CSC SSM by configuring the adaptive security appliance to skip the scanning of management traffic.

To improve HTTP performance, perform the following steps:

Step 1 Collect the following information:

a. Determine the management IP address by executing the **show module 1 details** command on the adaptive security appliance or from the CSC SSM Home pane in ASDM.

```
hostname# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-10
Model: ASA-SSM-10
Hardware version: 1.0
Serial Number: JAB093102KY
Firmware version: 1.0(10)0
Software version: CSC SSM 6.2.xxxx.x
MAC Address Range: 0013.c480.b183 to 0013.c480.b183
App. name: CSC SSM
App. Status: Up
App. Status Desc: CSC SSM scan services are available
App. version: 6.2.xxxx.x
Data plane Status: Up
Status: Up
HTTP Service: Up
HTTPS Service: Up
Mail Service: Up
FTP Service: Up
Activated: Yes
Mgmt IP addr: 10.132.84.251
Mgmt web port: 8443
Peer IP addr: <not enabled>
```

```
hostname#
```

b. Determine which adaptive security appliance interface the SSM management port is connected to in the network.

Step 2 Configure service policies.

- To exclude SSM management traffic for scanning, you must use access list-based class maps in service policies. For more information, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*, at the following URL:

  http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html

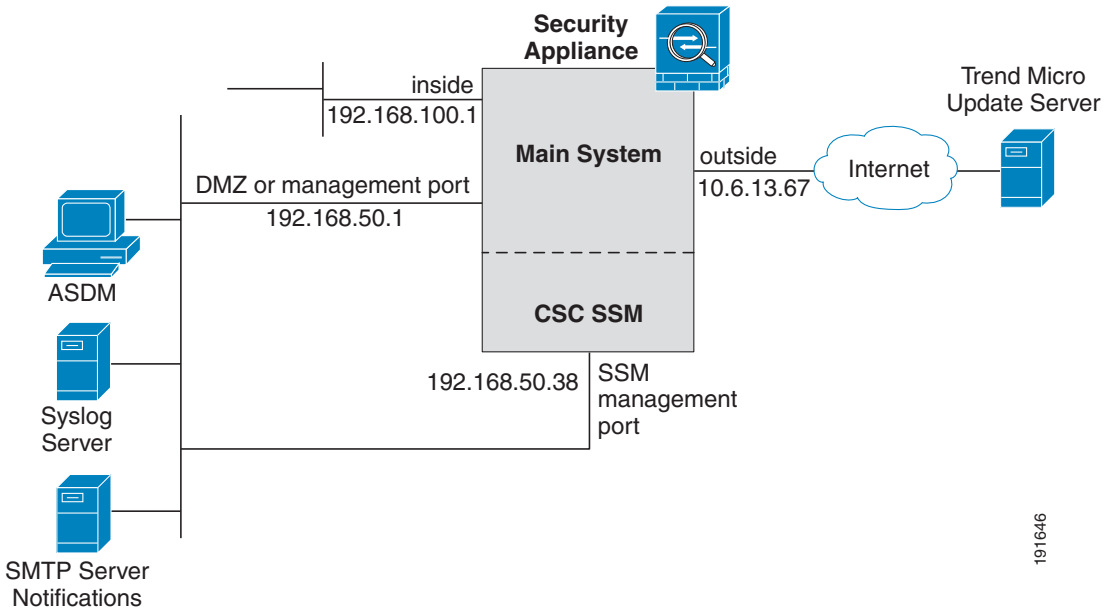
- Do not configure a class map matched with a port.

Note If a NAT device exists between the SSM management port and the adaptive security appliance interface, be sure you use the applicable NAT device address.

Using the CSC SSM with a Management Network

Figure B-1 shows an example of a CSC SSM deployment with a management network. The SSM IP address is 192.168.50.38, and management traffic goes through the DMZ or management interface before reaching the Trend Micro web server on the Internet.

Figure B-1 CSC SSM Deployment with a Management Network



Example 1: CSC Scanning from All Interfaces

To perform CSC scanning from all interfaces, perform the following steps:

Step 1 Create an access list that matches all traffic, except traffic for the SSM management IP address, using the following commands:

```
access-list csc-scan line 1 extended deny tcp host 192.168.50.38 any
access-list csc-scan line 2 extended permit tcp any any
```

Note You may have different entries instead of "**any any**."

Step 2 Create the class map, global-class, with the access list that was created in Step 1, and apply this class map to a global policy for CSC scanning, using the following commands:

```
class-map global-class
   match access-list csc-scan
policy-map global-policy
   class global-class
      csc fail-open
service-policy global-policy global
```

Example 2: CSC Scanning on Specific Ports

To perform CSC scanning on specific ports for SMTP, POP3, HTTP, and FTP traffic from a specific interface (for example, DMZ) and to exclude the SSM management IP address, perform the following steps:

Step 1 Create an access list, using the following commands:

```
access-list csc-scan line 1 extended deny tcp host 192.168.50.38 any
access-list csc-scan line 2 extended permit tcp any any eq smtp
access-list csc-scan line 3 extended permit tcp any any eq pop3
access-list csc-scan line 4 extended permit tcp any any eq http
access-list csc-scan line 5 extended permit tcp any any eq ftp
```

Step 2 Create the class map, dmz-class, with the access list that was created in Step 1, and apply this class-map to an interface (DMZ) for CSC scanning, using the following commands:

```
class-map dmz-class
   match access-list csc-scan
policy-map dmz-policy
    class dmz-class
        csc fail-open
service-policy dmz-policy interface dmz
```

Note Your configuration may have an access list with different sources and destinations than the examples shown in this document. If the access list has **deny ACE** for the SSM management IP address, the configuration will still work.

If you have both global and interface-specific service policies, you must add an access list to exempt the SSM management port IP address from scanning. For any service policy or class map, if the configuration includes URL categorization (HTTP) traffic, you must add an access list with **deny ACE** that exempts the SSM IP address from scanning.

If the class-map on the SSM-connected interface uses port-matching criteria by means of the **match** command, you must convert these criteria into access list-based matching criteria to ensure that SSM management traffic is not scanned.