



Reimaging and Configuring the CSC SSM Using the Command Line

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



Note

The setup wizard launched from the ASDM is the preferred method of installation, if installation is required. See *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* for more information.

This appendix includes the following sections:

- [Installation Checklist, page A-1](#)
- [Preparing to Reimage the Cisco CSC SSM, page A-2](#)
- [Reimaging the CSC SSM, page A-4](#)
- [Configuration via Command Line, page A-14](#)

Installation Checklist

Before you start, be prepared to supply the following information. Print a copy of this page and use it as a checklist if you prefer, to record the values you are prompted to enter during installation.

You are prompted to enter:	Your entry is:	Checkoff
Administrator password (for the CLI)	Do not record your password	
SSM card IP address		☐
Subnet mask		☐
Host name (1-63 alphanumeric characters; can include hyphens except as the first character)—for example, cisco1-ssm-csc		☐
Domain name		☐
Primary DNS IP address		☐
Secondary DNS IP address (optional)		☐

You are prompted to enter:	Your entry is:	Checkoff
Gateway IP address		☐
Proxy server? (optional) If yes:		☐
Proxy server IP		☐
Proxy server port		☐
Domain name for incoming mail		☐
Administrator password for the CSC SSM console	Do not record your password	
Administrator email address		☐
Notification email server IP		☐
Notification email server port		☐
Base License Activation Code		☐
Plus License Activation Code (optional)		☐

Preparing to Reimage the Cisco CSC SSM

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

To install via the command line, perform the following steps:

-
- Step 1** Download the Trend Micro InterScan for Cisco CSC SSM software to your TFTP server.
- Step 2** Using a terminal application such as Windows HyperTerminal, log on and open a terminal session to the ASA console. At the prompt, enter:

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

The system response is similar to the following example:

```
Image URL [tftp://insidehost/sg-6.0-1177-tftp.img]: tftp://insidehost/sg-6.0-1177-tftp.img
Port IP Address [192.168.7.20]:
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
```



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 following command to stop the module from trying to load the image.

```
hw module 1 recover stop
```

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
2005
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=sg-6.0-1177-tftp.img
Slot-1 211> CONFIG=
Slot-1 212> tftp sg-6.0-1177-tftp.img@192.168.7.100
Slot-1 213> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 214> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
.
.
.
```



Note This process takes about 10 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 2005
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...
```

Step 5 Disable the debug-module boot command:

```
hostname# no debug module-boot
```

Step 6 Show module 1 details. Sample code output is shown below:

```
JDPIX# show module 1 d
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 6.0 (Build#1345)
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: 6.0 (Build#1345)
Data plane Status: Up
Status: Up
HTTP 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 7 Open a command session:

```

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

```

Step 8 Log in to Trend Micro InterScan for Cisco CSC SSM using the default login name “cisco” and password “cisco.”

```

login: cisco
Password:

```

Step 9 You are prompted to change your password immediately. Do not use the same password that you use to access the 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

To reimaging the appliance using the command line Setup Wizard:

Step 1 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 email domain name
  4. Web console administrator password
  5. Notification settings
  6. Activation Codes
The Base License is required to activate the SSM.
Press Control-C to abort the wizard.

Press Enter to continue ...

```

Choose **1** to configure network settings and press **Enter**.

Step 2 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]

```

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

```

Network Settings
-----
IP                192.168.7.20
Netmask           255.255.255.0
Hostname          CSCSSM
Domain name       example.com

Primary DNS       10.2.200.2
Secondary DNS     10.2.203.1

Gateway           192.168.7.1
No Proxy

Are these settings correct? [y|n] y

```

Step 3 If the settings are correct, enter **y** to confirm. (If you choose **n**, the Network Settings prompts appear again; repeat Step 2.)

Step 4 After you confirm your network settings, the system responds with the following message:

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

Optionally confirm the network settings by pinging the gateway IP address. To skip pinging, enter **n**.

```

Do you want to confirm the network settings using ping? [y|n] y
Enter an IP address to ping: 192.168.7.1
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=0.2 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 ...

```

Step 5 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

```

Respond **y** to set the date and time to be synchronous with the chassis. To update the date and time, enter **n**, exit the installation wizard, update the date/time or NTP settings on the ASA chassis, and restart installation of the SSM.

Step 6 The Incoming Domain Name prompt appears.

```

Incoming Domain Name
-----

```

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

Type your highest level domain name for your organization and enter **y** to continue.

Step 7 The Administrator/Notification Settings prompts appear.

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

The password will be hidden while you type.
Web console administrator password:
Retype Web console administrator password:
Administrator email address:
Notification email server IP:
Notification email server port: (default:25)
```

When you have made your entries, a confirmation appears as shown in the following example:

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

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

Enter **y** to continue.

Step 8 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-8TY9-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.
```

Step 9 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 lets you know that installation is complete. As suggested in the prompt at the end of the Setup Wizard, use your browser to log on to the CSC SSM console. Enter 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** Enter the following command to view information about the SSM and the services you configured during installation:

```
hostname# show module 1 details
```

The system responds as follows:

```
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 6.0 (Build#1177)  
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: 6.0 (Build#1177)  
Data plane Status: Up  
Status: Up  
HTTP 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** Open a command session as follows:

```
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. Change Password for Command Line Interface
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]:
```

## View/Change Network Settings

Choose option **1** to view and/or modify your network settings configuration. The following appears:

```
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
```

Any of these settings can be changed via the command-line interface.

## View Date/Time Settings

Choose option **2** to view the SSM date and time settings. 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 ...
```

The settings cannot be changed, this information is for reference only.

## View Product Information

Choose option **3** to view the component (version and build) settings. The Product Information prompts appear:

```
Product Information

Main version 6.0 build 1177
Mail component version 5.5 build 1064
Web component version 2.1 build 1103

Press Enter to continue ...
```

The settings cannot be changed, this information is for reference only.

## View Service Status

Choose option **4** to view the component (version and build) settings. The following appears:

```
Service Status

The CSC SSM RegServer service is running
The CSC SSM HTTP 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
```

The **Do you want to restart all services prompt** allows you to restart scanning services. If everything is running smoothly, there is no need to restart. If you are trying to troubleshoot a problem, restarting may get you back in a proper operating status. See the [“Restart Scanning Service” section on page 8-12](#) for more information about the impact of restarting services.

## Change Password for Command Line Interface

Choose option **5** to display the Set Password for Command Line Interface prompts. The following appears:

```
Set Password for Command Line Interface

This option allows you to change the password for the Command Line Interface
that you are currently using.
Do you want to continue? [y|n]

The password will be hidden while you type.
Changing password for cisco
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
```

```
Re-enter new password:
Password changed.
```

Follow the prompts to update your password.

## Restore Factory Defaults

Choose option **6** to restore the pre-installation configuration settings. 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 choose **y**, all your configuration settings are returned to the pre-installation 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](#) for a description of the default settings. Additional configurations you have made since installation, such as registration/activation, licensing, enabling spyware/grayware detection, file blocking, file blocking exceptions, and so on are lost.

While this option is available from the command line, a better alternative for restoring configuration settings is available from the CSC SSM console. Click **Administration > Configuration Backup** to view the Configuration Backup window. The Configuration Backup window allows you to save (export) your configuration settings into a configuration file that can be imported (restored) at a later time.

Choose the Restore Factory Default Settings option only if you need to start over and re-install the CSC SSM.

## Troubleshooting Tools

Choose option **7** to display a menu of troubleshooting tools.

```
Troubleshooting Tools

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

Enter a number from [1-6]:
```

These tools are available to help you or Cisco TAC get information from the system to troubleshoot a problem.

## Enable Root Account

Option **1** enables the root account. 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]

This warning appears only the first time you enable the root account. Once the root account is enabled, it cannot be disabled.

**Caution**

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

## Show System Information

Option 2 allows you to view helpful system information, either directly on the screen, or you can save the data to a file and transfer the information using FTP or TFTP. When you select option 2, Show System Information menu displays:

```
Troubleshooting Tools - Show System Information

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

### Show System Information on Screen

Here is an example of system information displayed on the screen when you select option 1 from the Show System Information menu. This information is available from various locations on the ASDM and CSC SSM interfaces, but this CLI version makes it quickly available all in one place:

```
+++++++
Mon Jan 9 18:38:01 PST 2006 (-8)

System is : Up

Product Information
Trend Micro InterScan for Cisco CSC SSM
Version: 6.0 (Build#1340)
SSM Model: SSM-10

Scan Engine and Pattern Information
Virus Scan Engine: 8.100.1002 (Updated: 2006-01-09 14:10:07)
Virus Pattern: 3.149.00 (Updated: 2006-01-09 14:10:39)
Garyware Pattern: 0.327.00 (Updated: 2006-01-09 14:13:11)
PhishTrap Pattern: 223 (Updated: 2006-01-09 14:13:28)
AntiSpam Engine: 14196 (Updated: 2006-01-09 14:11:04)
AntiSpam Rule: 3.51.1033 (Updated: 2006-01-09 14:12:53)

License Information
Product:Base License
Version:Full
Activation Code:BX-9YWQ-3685S-X39PZ-H96NW-MAJR7-CWBXR
Seats:000250
Status:Expired within grace period
Expiration date:12/31/2005
Product:Plus License
```

```

Version:Full
Activation Code:PX-P67G-WCJ6G-M6XJS-2U77W-NM37Y-EZVKJ
Seats:000250
Status:Expired within grace period
Expiration date:12/31/2005

Daily Node Count: 0
Current Node Count: 0

Kernel Information
Linux csc 2.4.26-cscssm #2 SMP Mon Dec 19 11:53:05 PST 2005 (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. Enter **q** to quit.

## Upload System Information

When you select option **2** from the Show System Information menu, the following prompts display:

```

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 ...

```

Follow and respond to the prompts to upload the system information. The system information is sent using the upload settings created using option **5**, Modify Upload Settings. See [Modify Upload Settings, page A-13](#) for more information. If you did not configure the upload settings, the prompts are preceded by the following:

```

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

```

Select option **3**, Return to Troubleshooting Tools menu, when you are finished on the Show System Information menu.

## Gather Logs

Option **3** allows you to collect all logs on the CSC SSM and send them out via FTP or TFTP, for example, to Cisco TAC. The logs are sent using the upload settings created using option **5**, Modify Upload Settings. See [Modify Upload Settings, page A-13](#) for more information.

```

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
```

**Note**

Logs are automatically named using the following convention: CSCSSM-LOG-<date-time>.tar.gz. A similar convention for packets (described below) is used: CSCSSM-PACKET-<date-time>.gz.

## Gather Packet Trace

Option **4** allows you to capture packets passing between the CSC SSM and ASA. This information is typically used by Cisco TAC.

The following prompts display:

```
Troubleshooting Tools - Gather Packet Trace

Gather packet trace now? [y|n] y
Press Control-C to stop.
Gathering packet trace ...
Creating temporary file CSCSSM-PACKET-20060109-184529.gz
Upload the packet trace now? [y|n] y
Uploading temporary file CSCSSM-PACKET-20060109-184529.gz
Uploading file ...
```

To enable packet tracing:

- Step 1** Select **y** when prompted to gather packet traces.
- Step 2** Press Control-C to stop.
- Step 3** Select **y** to when prompted to upload packet traces.

The packets are uploaded using the protocol defined using option **5**, Modify Upload Settings. See [Modify Upload Settings, page A-13](#) for more information.

## Modify Upload Settings

Option **5** allows you to set the uploading method to either FTP or TFTP, as used by features described previously in this chapter.

**Note**

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

When you select option **5**, the following prompts display:

```
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 ...
```

Follow and respond to the prompts to configure the upload settings. The settings are saved for future use.

Select option **6**, Return to Main menu, when you are finished on the Troubleshooting Tools menu.

## Reset Management Port Access Control

Choose option **8** to reset the management port access control list. The following appears:

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

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

## Ping IP

The ping option is available for diagnostic purposes. Choose option **9** to ping an IP address. The following appears:

```
Enter an IP address to ping:
After you enter the 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 ...
```

## Exit Options

Choose option **10**, Exit, to exit the setup options. 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#
```

From the Exit Options menu, you can log out. Alternatively, you can reboot the system, or return to the Setup menu.

## Configuration via Command Line

This section describes some command-line alternatives that are available for users who prefer command line over use of the CSC SSM console. Not all features have an alternative available.

## Re-set Configuration

After you have installed Trend Micro InterScan for Cisco CSC SSM, if you have used TFTP to re-image the SSM, you may see this prompt for the first time when you access the CLI:

“Do you want to restore the previous configuration? [y/n]”

The question appears in the Setup Wizard menu, as shown below.

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

Do you want to restore the previous configuration? [y|n] n
To set up the SSM, the wizard prompts for the following information:
1. Network settings
2. Date/time settings verification
3. Incoming email domain name
4. Web console administrator password
5. Notification settings
6. Activation Codes
The Base License is required to activate the SSM.
Press Control-C to abort the wizard.

Press Enter to continue ...
```

If you choose **y**, the SSM configuration settings are restored to the state they were in the last time you saved configuration. This is a command-line alternative to the functionality on the **Administration > Configuration Backup** window in the CSC SSM console.

