Initial Configurations

This chapter describes how to initially configure the SSL Services Module and has these sections:

Using the CLI

The software interface for the SSL Services Module is the Cisco IOS CLI. To understand the Cisco IOS CLI and Cisco IOS command modes, refer to Chapter 2, "Command-Line Interfaces," in the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*.

Unless your switch is located in a fully trusted environment, we recommend that you configure the SSL Services Module through a direct connection to the module's console port or through an encrypted session using Secure Shell (SSH). See the "Configuring SSH" section on page 2-4 for information on configuring SSH on the module.

Note The initial SSL Services Module configuration must be made through a direct connection to the console port on the module.

Initial SSL Services Module Configuration

Note You are required to make the following initial SSL Services Module configurations through a direct connection to the SSL Services Module console port. After the initial configurations, you can make an SSH or Telnet connection to the module to further configure the module.

The initial SSL Services Module configuration consists of the following tasks:

Configuring VLANs on the SSL Services Module

When you configure VLANs on the SSL Services Module, configure one of the VLANs as an administrative VLAN. The administrative VLAN is used for all management traffic, including SSH, public key infrastructure (PKI), secure file transfer (SCP), and TFTP operations. The system adds the default route through the gateway of the administrative VLAN.

Note Configure only one VLAN on the SSL Services Module as the admin VLAN.

Note VLAN IDs must be the same for the switch and the module. Refer to the "Configuring VLANs" chapter in the *Catalyst 6500 Series Switch Software Configuration Guide* for details.

Note The SSL software supports only the normal-range VLANs (2 through 1005). Limit the SSL Services Module configuration to the normal-range VLANs.

To configure VLANs on the SSL Services Module, perform this task:

	Command	Purpose
Step 1	`ssl-proxy(config)# ssl-proxy vlan vlan`	Configures the VLANs and enters VLAN mode.
Step 2	`ssl-proxy(config-vlan)# ipaddr ip_addr netmask`	Configures an IP address for the VLAN.
Step 3	`ssl-proxy(config-vlan)# gateway gateway_addr`	Configures the client-side gateway IP address. **Note** Configure the gateway IP address in the same subnet as the VLAN IP address.

	Command	Purpose
Step 4	`ssl-proxy(config-vlan)# route ip_addr netmask gateway ip_addr`	(Optional) Configures a static route for servers that are one or more Layer 3 hops away from the SSL Services Module.
Step 5	`ssl-proxy(config-vlan)# admin`	(Optional) Configures the VLAN as the administrative VLAN[1].

1. The administrative VLAN is for management traffic (PKI, SSH, SCP and TFTP). Specify only one VLAN as the admin VLAN.

This example shows how to configure the VLAN and specify the IP address, the subnet mask, and the global gateway, and also specifies the VLAN as the administrative VLAN:

```
ssl-proxy(config)# ssl-proxy vlan 100
ssl-proxy(config-vlan)# ipaddr 10.1.0.20 255.255.255.0
ssl-proxy(config-vlan)# gateway 10.1.0.1
ssl-proxy(config-vlan)# admin
ssl-proxy(config-vlan)# ^Z
ssl-proxy#
```

Configuring Telnet Remote Access

To configure the SSL Services Module for Telnet remote access, perform this task:

	Command	Purpose
Step 1	`ssl-proxy(config)# enable password password`	Specifies a local enable password.
Step 2	`ssl-proxy(config)# line vty starting-line-number ending-line-number`	Identifies a range of lines for configuration and enters line configuration mode.
Step 3	`ssl-proxy(config-line)# login`	Enables password checking at login.
Step 4	`ssl-proxy(config-line)# password password`	Specifies a password on the line.

This example shows how to configure the SSL Services Module for remote access:

```
ssl-proxy(config)# enable password cisco
ssl-proxy(config)#line vty 0 4
ssl-proxy(config-line)#login
ssl-proxy(config-line)#password cisco
ssl-proxy(config-line)#end
ssl-proxy#
```

Note In addition to the standard Telnet TCP port 23, other legacy Telnet variant ports will appear as open, but are only used for VTS debugging. These ports are TCP/2001-2003 (VTY virtual terminal), TCP/4001-4003 (raw TCP), and TCP/6001-6003 (binary mode Telnet).

Configuring the Fully Qualified Domain Name

If you are using the SSL Services Module to enroll for certificates from a certificate authority, you must configure the Fully Qualified Domain Name (FQFDN) on the module. The FQDN is the hostname and domain name of the module.

To configure the FQDN, perform this task:

	Command	Purpose
Step 1	`ssl-proxy(config)# hostname name`	Configures the hostname.
Step 2	`ssl-proxy(config)# ip domain-name name`	Configures the domain name.

This example shows how to configure the FQDN on the SSL Services Module:

```
ssl-proxy(config)# hostname ssl-proxy2
ssl-proxy2(config)# ip domain-name example.com
ssl-proxy2(config)# end
ssl-proxy2(config)#
```

Configuring SSH

After you complete the initial configuration for the module, enable SSH on the module, and then configure the user name and password for the SSH connection using either a simple user name and password or using an authentication, authorization, and accounting (AAA) server.

These sections describe how to enable and configure SSH:

- Enabling SSH on the Module, page 2-4
- Configuring the User Name and Password for SSH, page 2-5
- Configuring Authentication, Authorization, and Accounting for SSH, page 2-6

Enabling SSH on the Module

SSH uses the first key pair generated on the module. In the following task, you generate a key pair used specifically for SSH.

Note If you generate a general-purpose key pair (as described in the "Generating RSA Key Pairs" section on page 3-5) without specifying the SSH key pair first, SSH is enabled and uses the general-purpose key pair. If this key pair is later removed, SSH is disabled. To reenable SSH, generate a new SSH key pair.

To generate an SSH key pair and enable SSH, perform this task:

	Command	Purpose
Step 1	`ssl-proxy# configure terminal`	Enters configuration mode, selecting the terminal option.
Step 2	`ssl-proxy(config)# ip ssh rsa keypair-name` *ssh_key_name*	Assigns the key pair name to SSH.
Step 3	`ssl-proxy(config)# crypto key generate rsa general-keys label` *ssh_key_name*	Generates the SSH key pair. SSH is now enabled.
Step 4	`ssl-proxy(config)# end`	Exits configuration mode.
Step 5	`ssl-proxy# show ip ssh`	Shows the current state of SSH.

This example shows how to enable SSH on the module, and how to verify that SSH is enabled:

```
ssl-proxy(config)# ip ssh rsa keypair-name ssh-key
Please create RSA keys to enable SSH.
ssl-proxy(config)# crypto key generate rsa general-keys label ssh-key
The name for the keys will be: ssh-key
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]

ssl-proxy(config)#
*Aug 28 11:07:54.051: %SSH-5-ENABLED: SSH 1.5 has been enabled
ssl-proxy(config)# end

ssl-proxy# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
ssl-proxy#
```

Configuring the User Name and Password for SSH

To configure the user name and password for the SSH connection, perform this task:

	Command	Purpose
Step 1	`ssl-proxy# configure terminal`	Enters configuration mode, selecting the terminal option.
Step 2	`ssl-proxy(config)# enable password` *password*	Specifies a local enable password, if not already specified.
Step 3	`ssl-proxy(config)# username` *username* {**password** | **secret**} *password*	Specifies the user name and password.
Step 4	`ssl-proxy(config)# line vty` *line-number ending-line-number*	Identifies a range of lines for configuration and enters line configuration mode.
Step 5	`ssl-proxy(config-line)# login local`	Enables local username authentication.

This example shows how to configure the user name and password for the SSH connection to the SSL Services Module:

```
ssl-proxy# configure terminal
ssl-proxy(config)# enable password cisco
ssl-proxy(config)# username admin password admin-pass
ssl-proxy(config)# line vty 0 4
ssl-proxy(config-line)# login local
ssl-proxy(config-line)# end
```

After you configure the user name and password, see the "Initial Catalyst 6500 Series Switch Configuration" section on page 2-7 to configure the switch.

Configuring Authentication, Authorization, and Accounting for SSH

To configure authentication, authorization, and accounting (AAA) for SSH, perform this task:

	Command	Purpose
Step 1	`ssl-proxy# configure terminal`	Enters configuration mode, selecting the terminal option.
Step 2	`ssl-proxy(config)# username` *username* `secret {0 | 5}` *password*	Enables enhanced password security for the specified, unretrievable username.
Step 3	`ssl-proxy(config)# enable password` *password*	Specifies a local enable password, if not already specified.
Step 4	`ssl-proxy(config)# aaa new-model`	Enables authentication, authorization, and accounting (AAA).
Step 5	`ssl-proxy(config)# aaa authentication login default local`	Specifies the module to use the local username database for authentication.
Step 6	`ssl-proxy(config)# line vty` *line-number ending-line-number*	Identifies a range of lines for configuration and enters line configuration mode.
Step 7	`ssl-proxy(config-line)# transport input ssh`	Configures SSH as the only protocol used on a specific line (to prevent non-SSH connections).

This example shows how to configure AAA for the SSH connection to the SSL Services Module:

```
ssl-proxy# configure terminal
ssl-proxy(config)# username admin secret admin-pass
ssl-proxy(config)# enable password enable-pass
ssl-proxy(config)# aaa new-model
ssl-proxy(config)# aaa authentication login default local
ssl-proxy(config)# line vty 0 4
ssl-proxy(config-line)# transport input ssh
ssl-proxy(config-line)# end
ssl-proxy#
```

After you configure AAA, see the "Initial Catalyst 6500 Series Switch Configuration" section on page 2-7 to configure the switch.

Initial Catalyst 6500 Series Switch Configuration

How you configure the Catalyst 6500 series switch depends on whether you are using Cisco IOS software or the Catalyst operating system software.

The following sections describe how to configure the switch from the CLI for each switch operating system:

Cisco IOS Software

The initial Catalyst 6500 series switch configuration consists of the following:

Configuring VLANs on the Switch

Note VLAN IDs must be the same for the switch and the module. Refer to the "Configuring VLANs" chapter in the *Catalyst 6500 Series Switch Software Configuration Guide* for details.

Note The SSL software supports only the normal-range VLANs (2 through 1005). Limit the SSL Services Module configuration to the normal-range VLANs.

To configure VLANs on the switch, perform this task:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters configuration mode, selecting the terminal option.
Step 2	`Router(config)# vlan vlan_ID`	Enters VLAN configuration mode and adds a VLAN. The valid range is 2 through 1001. **Note** Do not add an external VLAN.
Step 3	`Router(config-vlan)# end`	Updates the VLAN database and returns to privileged EXEC mode.

This example shows how to configure VLANs on the switch:

```
Router> enable
Router# configure terminal
Router(config)# vlan 100
VLAN 100 added:
     Name: VLAN100

Router(config-vlan)# end
```

Configuring Layer 3 Interfaces

To configure the corresponding Layer 3 VLAN interface, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface vlan vlan_ID`	Selects an interface to configure.
Step 2	`Router(config-if)# ip address ip_address subnet_mask`	Configures the IP address and IP subnet.
Step 3	`Router(config-if)# no shutdown`	Enables the interface.
Step 4	`Router(config-if)# exit`	Exits configuration mode.

This example shows how to configure the Layer 3 VLAN interface:

```
Router# configure terminal
Router(config)# interface vlan 100
Router(config-if)# ip address 10.10.1.10 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

Configuring a LAN Port for Layer 2 Switching

To place physical interfaces that connect to the servers or the clients in the corresponding VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface type[1] mod/port`	Selects the LAN port to configure.
Step 2	`Router(config-if)# switchport`	Configures the LAN port for Layer 2 switching. **Note** You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 port before you can enter additional **switchport** commands with keywords.
Step 3	`Router(config-if)# switchport mode access`	Puts the LAN port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The LAN port becomes a nontrunk port even if the neighboring LAN port does not agree to the change.

	Command	Purpose
Step 4	`Router(config-if)# switchport access vlan vlan_ID`	Configures the default VLAN, which is used if the interface stops trunking.
Step 5	`Router(config-if)# no shutdown`	Activates the interface.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure a physical interface as a Layer 2 interface and assign it to a VLAN:

```
Router(config)# interface gigabitethernet 1/1
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 100
Router(config-if)# no shutdown
Router(config-if)# exit
```

Adding the SSL Services Module to the Corresponding VLAN

Note By default, the SSL Services Module is in trunking mode with native VLAN 1.

To add the SSL Services Module to the corresponding VLAN, enter this command:

Command	Purpose
`Router (config)# ssl-proxy module mod allowed-vlan vlan_ID`	Configures the VLANs allowed over the trunk to the SSL Services Module. **Note** One of the allowed VLANs must be the admin VLAN.

This example shows how to add an SSL Services Module installed in slot 6 to a specific VLAN:

```
Router>
Router> enable
Router# configure terminal
Router (config)# ssl-proxy module 6 allowed-vlan 100
Router (config)# end
```

Verifying the Initial Configuration

To verify the configuration, enter these commands:

Command	Purpose
`Router# show spanning-tree vlan vlan_ID`	Displays the spanning tree state for the specified VLAN.
`Router# show ssl-proxy mod mod state`	Displays the trunk configuration.

Note In the following examples, the SSL Services Module is installed in slot 4 (Gi4/1).

This example shows how to verify that the module is in forwarding (FWD) state:

```
Router# show spanning-tree vlan 100

VLAN0100
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0009.e9b2.b864
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768
             Address     0009.e9b2.b864
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi3/1            Desg FWD 4         128.129  P2p
Gi4/1            Desg FWD 4         128.193  P2p
Po261            Desg FWD 3         128.833  P2p
Router
```

This example shows how to verify that the VLAN information displayed matches the VLAN configuration:

```
Router# show ssl-proxy mod 6 state
SSL-services module 6 data-port:
 Switchport:Enabled
Administrative Mode:trunk
Operational Mode:trunk
Administrative Trunking Encapsulation:dot1q
Operational Trunking Encapsulation:dot1q
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Trunking VLANs Enabled:100
Pruning VLANs Enabled:2-1001
Vlans allowed on trunk:100
Vlans allowed and active in management domain:100
Vlans in spanning tree forwarding state and not pruned:
100
Allowed-vlan :100
```

Catalyst Operating System Software

The initial Catalyst 6500 series switch configuration consists of the following:

- Configuring VLANs on the Switch, page 2-11
- Configuring Layer 3 Interfaces on the MSFC, page 2-11
- Adding the SSL Services Module to the Corresponding VLAN, page 2-12
- Verifying the Initial Configuration, page 2-12

Configuring VLANs on the Switch

Note VLAN IDs must be the same for the switch and the module. Refer to the "Configuring VLANs" chapter in the *Catalyst 6500 Switch Series Software Configuration Guide* for details.

Note The SSL software supports only the normal-range VLANs (2 through 1005). Limit the SSL Services Module configuration to the normal-range VLANs.

To configure VLANs on the switch, perform this task:

	Command	Purpose
Step 1	`Console> enable`	Enters privileged mode.
Step 2	`Console> (enable) set vlan vlan_id`	Adds a VLAN. The valid range is 2 through 1001. **Note** Do not add an external VLAN.

This example shows how to configure VLANs on the switch:

```
Console> enable
Enter Password: <password>
Console> (enable) set vlan 100
Vlan 100 configuration successful
Console> (enable)
```

Configuring Layer 3 Interfaces on the MSFC

To configure the corresponding Layer 3 VLAN interface on the multilayer switch feature card (MSFC), perform this task:

	Command	Purpose
Step 1	`Console> (enable) session [mod]`[1]	Accesses the MSFC from the switch CLI using a Telnet session[2].
Step 2	`Router> enable`	Enters enable mode.
Step 3	`Router# configure terminal`	Enters global configuration mode.
Step 4	`Router(config)# interface vlan vlan_id`	Specifies a VLAN interface on the MSFC.
Step 5	`Router(config-if)# ip address ip_address subnet_mask`	Assigns an IP address to the VLAN.
Step 6	`Router(config-if)# no shutdown`	Enables the interface.
Step 7	`Router(config-if)# exit`	Exits the MSFC CLI and returns to the switch CLI.

1. The *mod* keyword specifies the module number of the MSFC; either 15 (if the MSFC is installed on the supervisor engine in slot 1) or 16 (if the MSFC is installed on the supervisor engine in slot 2). If no module number is specified, the console will switch to the MSFC on the active supervisor engine.
2. To access the MSFC from the switch CLI directly connected to the supervisor engine console port, enter the **switch console** *mod* command. To exit from the MSFC CLI and return to the switch CLI, press **Ctrl-C** three times at the Router> prompt.

This example shows how to configure the Layer 3 VLAN interface on the MSFC:

```
Console> (enable) session 15
Trying Router-15...
Connected to Router-15.
Type ^C^C^C to switch back...
Router> config t
Router(config)# interface vlan 100
Router(config-if)# ip address 10.10.1.10 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Console> (enable)
```

Adding the SSL Services Module to the Corresponding VLAN

Note By default, the SSL Services Module is in trunking mode with native VLAN 1.

To add the SSL Services Module to the corresponding VLAN, enter this command:

Command	Purpose
`Console> (enable) set trunk mod/port vlan_id`	Configures the VLANs allowed over the trunk to the SSL Services Module. **Note** One of the allowed VLANs must be the admin VLAN.

This example shows how to add an SSL Services Module installed in slot 6 to a specific VLAN:

```
Console> (enable) set trunk 6/1 100
Adding vlans 100 to allowed list.
Console> (enable)
```

Verifying the Initial Configuration

To verify the configuration, enter one of these commands:

Command	Purpose
`Console> show spanntree vlan_ID`	Displays the spanning tree state for the specified VLAN.
`Console> show trunk mod/port`	Displays the trunk configuration.

Note In the following examples, the SSL Services Module is installed in slot 6.

This example shows how to verify that the module is in forwarding (FWD) state:

```
Console> show spantree 100
VLAN 100
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled
```

```
Designated Root             00-06-2a-db-a5-01
Designated Root Priority    32768
Designated Root Cost        0
Designated Root Port        1/0
Root Max Age   20 sec   Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-06-2a-db-a5-01
Bridge ID Priority          32768
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 6/1                      100  forwarding          100   32 enabled  033
Console>
```

This example shows how to verify that the VLAN information displayed matches the VLAN configuration:

```
Console> show trunk 6/1
* - indicates vtp domain mismatch
# - indicates dot1q-all-tagged enabled on the port
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 6/1      nonegotiate  dot1q          trunking      1

Port      Vlans allowed on trunk
--------  --------------------------------------------------------------------
 6/1      100

Port      Vlans allowed and active in management domain
--------  --------------------------------------------------------------------
 6/1      100

Port      Vlans in spanning tree forwarding state and not pruned
--------  --------------------------------------------------------------------
 6/1      100
```

Recovering a Lost Password

Note You can download the password recovery script from the Cisco.com software center.

Note You must have access to the supervisor engine to perform the SSL module password recovery procedures. To recover the enable password on the supervisor engine, refer to the software configuration guide for your software platform.

Note To run the password recovery script, the SSL module must be in the application partition (AP).

Note The password recovery script is not compatible with SSL software release 1.x.

Caution For security reasons, all private keys are unusable after password recovery.

To recover a lost password on the SSL module, perform this task:

	Command	Purpose
Step 1	`Console>(enable) session mod`	Sessions to the MSFC. This step is required if you are running Catalyst operating system software.
Step 2	`Router> enable`	Initiates enable mode enable.
Step 3	`Router# copy tftp: pclc#mod-fs:`	Downloads the script to the specified module.
Step 4	`ssl-proxy# copy startup-config running-config`	Saves the startup configuration into the running configuration.
Step 5	`ssl-proxy(config)# enable password password`	Specifies a local enable password.
Step 6	`ssl-proxy(config)# line vty starting-line-number ending-line-number`	Identifies a range of lines for configuration and enters line configuration mode.
Step 7	`ssl-proxy(config-line)# login`	Enables password checking at login.
Step 8	`ssl-proxy(config-line)# password password`	Specifies a password on the line.
Step 9	`ssl-proxy(config-line)# end`	Exits line configuration mode.
Step 10	`ssl-proxy# copy system:running-config nvram:startup-config`	Saves the configuration to NVRAM.
Step 11	`Router# hw-module module mod reset`	Resets the module.

The following example shows how to recover a lost password on the SSL module installed in slot 4:

- From the supervisor engine:

```
Console> (enable) session 15
Trying Router-15...
Connected to Router-15.
Type ^C^C^C to switch back...
Router>
Router> enable
Password:
Router# copy tftp: pclc#4-fs:
Address or name of remote host []? 10.1.1.100
Source filename []? images/c6svc-ssl-pwr.2-1-1.bin
Destination filename [images/c6svc-ssl-pwr.2-1-1.bin]?
Accessing tftp://10.1.1.100/images/c6svc-ssl-pwr.2-1-1.bin...
Loading images/c6svc-ssl-pwr.2-1-1.bin from 10.1.1.100(via Vlan999): !
[OK - 435 bytes]

435 bytes copied in 0.092 secs (4728 bytes/sec)
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:MP upgrade/Password Recovery started.
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:Uncompress of the file succeeded.
Continuing upgrade/recovery.
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:This file appears to be a
PasswordRecovery image. Continuing.
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:Extraction of password recovery image
succeeded.
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:Continuing with password recovery.

2003 Nov 10 21:55:03 %SYS-3-SUP_ERRMSGFROMPC:System in password recovery mode.
2003 Nov 10 21:55:03 %SYS-3-SUP_ERRMSGFROMPC:Please recover configuration and reset
board.

Router#
```

- From the SSL module console port:

```
ssl-proxy# copy system:startup-config nvram:running-config

ssl-proxy(config)# enable password cisco
ssl-proxy(config)# line vty 0 4
ssl-proxy(config-line)# login
ssl-proxy(config-line)# password cisco
ssl-proxy(config-line)# end
ssl-proxy# copy system:running-config nvram:startup-config
```

- From the supervisor engine:

```
Router# hw-module module 4 reset
```

- From the SSL module console port, import the keys from backup or regenerate the keys.

  See the "Configuring Keys and Certificates" section on page 3-3 for information on generating keys and importing keys.