SSE-F3548S/SSE-F3548SR

Security

User's Guide

Revision 1.0

The information in this USER'S GUIDE has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person organization of the updates. Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

DISCLAIMER OF WARRANTY ON SOFTWARE AND MATERIALS. You expressly acknowledge and agree that use of the Software and Materials is at your sole risk. FURTHERMORE, SUPER MICRO COMPUTER INC. DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE OR MATERIALS IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SUPER MICRO COMPUTER INC. OR SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE SOFTWARE AND/OR MATERIALS PROVE DEFECTIVE, YOU (AND NOT SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICE, REPAIR, OR CORRECTION.

LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES INCLUDING NEGLIGENCE, SHALL SUPER MICRO COMPUTER INC. BE LIABLE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OR INABILITY TO USE THE SOFTWARE OR MATERIALS, EVEN IF SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Super Micro's total liability for all claims will not exceed the price paid for the hardware product.

Manual Revision 1.0
Release Date: 3/2/2020

Document Revision History

Date	Revision	Description
03/2/2020	1.0	Initial document.

Contents

1 Security Overview

Supermicro switches support four methods of user authentication:

- RADIUS – Remote Authentication Dial-In User Service (RADIUS) uses AAA service for ID verification, granting access and tracking actions of remote users.
- TACACS – *Terminal Access Controller Access Control System (TACACS)* provides accounting information and administrative control for authentication and authorization. RADIUS encrypts only password, whereas TACACS encrypts username as well, hence it is more secure.
- SSH - *Secure Shell (SSH)* is a protocol for secure remote connection to a device. SSH provides more security than telnet by encryption of messages during authentication.
- SSL –*Secure Socket Layer (SSL)* provides server authentication, encryption and message integrity as well as HTTP client authentication.

2 Login Authentication Mode

Supermicro switches allow login authentication against users in local configuration or users in RADIUS or TACACS. Switch can also be configured to fallback to local authentication if authentication with RADIUS or TACACS fails.
Follow the steps below to configure Login Authentication Mechanism.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	login authentication {local | RADIUS [local]| TACACS [local]}	Configure the login authentication mechanism to be used for switch access. Local – Use the local database in switch to authenticate users. Radius – Use RADUIS server to authenticate users. Radius local – Use RADIUS server to authenticate users and in case of failure fallback to local authentication. Tacacs – Use TACACS server to authenticate users. Tacacs local – Use TACACS server to authenticate users and in case of failure fallback to local authentication.
Step 3	End	Exits the configuration mode.
Step 4	show system information	Displays the Login Authentication mechanism.

Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The “no login authentication” command resets the login authentication to its default of ‘local’.

The example below shows the commands used to configure Login Authentication with RADIUS.

```
SMIS# configure terminal
SMIS(config)# login authentication radius
SMIS(config)# end
SMIS# show system information
Switch Name                    : SMIS
Switch Base MAC Address        : 00:30:48:e3:70:bc
SNMP EngineID                  : 80.00.08.1c.04.46.53
System Contact                 : http://www.supermicro.com/support
System Location                : Supermicro
Logging Option                 : Console Logging
Login Authentication Mode      : RADIUS
Snoop Forward Mode             : MAC based
Config Restore Status          : Not Initiated
Config Restore Option          : No restore
Config Restore Filename        : iss.conf
Config Save IP Address         : 0.0.0.0
Device Up Time                 : 0 days 0 hrs 15 mins 43 secs
Boot-up Flash Area             : Normal
NTP Broadcast Mode             : No

[NTP] ntp is disabled

   Server     Key   Prefer
=============== =====  ======
 Key #    Key
=======  ===================================
 Time zone offset not set
```

The example below shows the commands to configure RADIUS authentication with fallback to local.

```
SMIS# configure terminal
SMIS(config)# login authentication radius local
SMIS(config)# end
```

3 RADIUS

A sequence of events occurs during RADIUS client-server communication at the time of user login.

- The username and password are encrypted by the client and sent to RADIUS server.
- The client receives a response from the RADIUS server:
  - ACCEPT—User authentication is successful.
  - REJECT—User authentication failed. User is prompted to re-enter username/password, or access is denied.
  - CHALLENGE—Additional data is requested from the user.
  - CHALLENGE PASSWORD—User is prompted to select a new password.

Along with ACCEPT or REJECT packets, service options (Telnet, SSH, rlogin, or privileged EXEC services) and connection parameters like user timeouts are sent by RADIUS server.

Defaults – RADIUS

Parameter	Default Value
Server	None
Timeout	3 seconds
Re-transmit	3
Key	None

3.1 RADIUS Server

Supermicro switches function as a RADIUS client. The RADIUS server to be contacted for authentication can be configured in the switch.

Follow the steps below to configure RADIUSserver Parameters.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	radius-server host <ip-address> [timeout <1-120>] [retransmit <1-254>] key <secret-key-string> [type {authenticating | accounting | both}]	Configure RADIUS server for purpose of authenticating or accounting or both. *ip-address* – serverIP address. *timeout* – Specify RADIUS server timeout in range 1-120 *retransmit* – Specify number of retries to attempt to connect to RADIUS server in range 1-254 *key* –Specify authentication key
Step 3	End	Exits the configuration mode.

Step 4	show radius server show radius statistics	Displays the RADIUS configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The “no radius-server host <ip-address>” command deletes the RADIUS client.

The example below shows the commands used to configure RADIUS server.

```
SMIS# configure terminal
SMIS(config)#radius-server host 200.200.200.1 timeout 50 retransmit 250 key key1
SMIS(config)# end
SMIS# show radius server
Radius Server Host Information
------------------------------
Index                : 1
Server address       : 200.200.200.1
Shared secret        : key1
Radius Server Status : Enabled
Response Time        : 50
Maximum Retransmission  : 250
------------------------------------------

SMIS# show radius statistics
Radius Server Statistics
-------------------------
Index                       : 1
Radius Server Address       : 200.200.200.1
UDP port number             : 1812
Round trip time             : 0
No of request packets       : 0
No of retransmitted packets : 0
No of access-accept packets : 0
No of access-reject packets : 0
No of access-challenge packets  : 0
No of malformed access responses : 0
No of bad authenticators    : 0
No of pending requests      : 0
No of time outs             : 0
No of unknown types         : 0
------------------------------------------
```

4 TACACS

TACACS provides access control to switch through a client-server model, similar to RADIUS except that it provides enhanced security by encryption of all messages and reliability via TCP.
Defaults – TACACS

Parameter	Default Value
TACACS server	None
TACACS server re-tries	2
TACACS TCP port	49
TACACS Authentication Mode	PAP
TACACS Authorization status	Diabled
Privilege	1

4.1 TACACS Server

Supermicro switches allow configuration of multiple TACACS servers. One of these servers provides the authentication support.
Follow the steps below to configure TACACS server.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	tacacs-server host <ip-address> [single-connection] [port <tcp port (1-65535)>] [timeout <time out in seconds>] key <secret key>	Configure TACACS server. *ip-address* – TACACS Server IP-address *single-connection* – When this option is specified,only one connection to one of the configured TACACS servers is permitted. *port* – Specify TCP port in range 1-65535 *timeout* - Specify TACACS server timeout in range 0 – 255 seconds *key* – Authentication key of maximum length 64 characters.
Step 3	End	Exits the configuration mode.
Step 4	show tacacs	Displays the TACACS configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The “no tacacs-server host <ip-address>” command deletes the TACACS server.

The example below shows the commands used to configure TACACS server.

```
SMIS# configure terminal
SMIS(config)# tacacs-server host 10.10.10.1 port 500 timeout 200 key key123
SMIS(config)# end
SMIS# show tacacs
Server : 1
    Address         : 10.10.10.1
    Single Connection : no
    TCP port        : 500
    Timeout         : 200
    Secret Key      : key123
Client uses server: 0.0.0.0
Authen. Starts sent    : 0
Authen. Continues sent : 0
Authen. Enables sent   : 0
Authen. Aborts sent    : 0
Authen. Pass rvcd.     : 0
Authen. Fails rcvd.    : 0
Authen. Get User rcvd. : 0
Authen. Get Pass rcvd. : 0
Authen. Get Data rcvd. : 0
Authen. Errors rcvd.   : 0
Authen. Follows rcvd.  : 0
Authen. Restart rcvd.  : 0
Authen. Sess. timeouts : 0
Author. Requests sent  : 0
Author. Pass Add rcvd. : 0
Author. Pass Repl rcvd : 0
Author. Fails rcvd.    : 0
Author. Errors rcvd.   : 0
Author Follows rcvd.   : 0
Author. Sess. timeouts : 0
Acct. start reqs. sent : 0
Acct. WD reqs. sent    : 0
Acct. Stop reqs. sent  : 0
Acct. Success rcvd.    : 0
Acct. Errors rcvd.     : 0
Acct. Follows rcvd.    : 0
Acct. Sess. timeouts   : 0
Malformed Pkts. rcvd.  : 0
Socket failures        : 0
```

Connection failures : 0

4.2 TACACS Re-tries

Supermicro switches retry transmission of messages to the TACACS server, if there is no response from the server. This retry count can be configured by user.
Follow the steps below to configure TACACS server re-tries.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	tacacs-server retransmit <1-100>	Configure TACACS server re-tries in the range 1-100.
Step 3	End	Exits the configuration mode.
Step 4	show tacacs	Displays the TACACS configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The “no tacacs-server retransmit” command resets the TACACS server re-tries to its default value.

The example below shows the commands used to configure TACACS server re-tries.
SMIS# configure terminal
SMIS(config)# tacacs-server retransmit 5
SMIS(config)# end

4.3 TACACS use-server

Supermicro switches provide option to configure multiple TACACS servers. User can specify one of these available servers to be used at a time.
Follow the steps below to configure TACACS server to be used.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	tacacs use-server address<ip-address>	Configure TACACS server to be used.
Step 3	End	Exits the configuration mode.
Step 4	show tacacs	Displays the TACACS configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The “no tacacs use-server address<ip-address>” command deletes the TACACS client.

The example below shows the commands used to configure TACACS server to be used.

```
SMIS# configure terminal
SMIS(config)# tacacs use-server address 10.10.10.1
SMIS(config)# end
SMIS# show tacacs
Server : 1
    Address         : 10.10.10.1
    Single Connection : no
    TCP port        : 49
    Timeout         : 200
    Secret Key      : key123
Server : 2
    Address         : 50.50.50.1
    Single Connection : no
    TCP port        : 49
    Timeout         : 5
    Secret Key      : key789
Client uses server: 10.10.10.1
Authen. Starts sent    : 0
Authen. Continues sent : 0
Authen. Enables sent   : 0
Authen. Aborts sent    : 0
Authen. Pass rvcd.     : 0
Authen. Fails rcvd.    : 0
Authen. Get User rcvd. : 0
Authen. Get Pass rcvd. : 0
Authen. Get Data rcvd. : 0
Authen. Errors rcvd.   : 0
Authen. Follows rcvd.  : 0
Authen. Restart rcvd.  : 0
Authen. Sess. timeouts : 0
Author. Requests sent  : 0
Author. Pass Add rcvd. : 0
Author. Pass Repl rcvd : 0
Author. Fails rcvd.    : 0
Author. Errors rcvd.   : 0
Author Follows rcvd.   : 0
Author. Sess. timeouts : 0
Acct. start reqs. sent : 0
Acct. WD reqs. sent    : 0
Acct. Stop reqs. sent  : 0
Acct. Success rcvd.    : 0
Acct. Errors rcvd.     : 0
Acct. Follows rcvd.    : 0
Acct. Sess. timeouts   : 0
Malformed Pkts. rcvd.  : 0
Socket failures        : 0
```

Connection failures : 0

4.4 TACACS Login Authentication Mode

Supermicro switches provide an option to configure TACACS login authentication mode. Users can specify one of the mode PAP or CHAP .

In TACACS+ mode, authentication request is sent to the configured TACACS+ server. The user name and passwords are authenticated using TACACS+ server.

Follow the steps below to configure the TACACS login authentication mode to be used.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	aaa authentication tacacs { chap | pap }	Configures TACACS authentication mode to be used.
Step 3	End	Exits the configuration mode.
Step 4	show Tacacs	Displays the TACACS configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of the startup configuration.

The “no aaa authentication tacacs” command deletes the TACACS login mode.

The example below shows the commands used to configure the TACACS login mode to be used.

```
SMIS# configure terminal

SMIS(config)# aaa authentication tacacs chap

SMIS(config)# end

SMIS# show tacacs
Server : 1
    Address          : 192.168.2.11
    Single Connection : no
    TCP port         : 49
    Timeout          : 5
```

```
    Key Type          : 0
    Secret Key        : testing123
    Mode              : Chap
Client uses server: 192.168.2.11

Authen. Starts sent       : 14
Authen. Continues sent : 0
Authen. Enables sent      : 0
Authen. Aborts sent       : 0
Authen. Pass rvcd.        : 11
Authen. Fails rcvd.       : 3
Authen. Get User rcvd. : 0
Authen. Get Pass rcvd. : 0
Authen. Sess. timeouts    : 0
Author. Requests sent     : 0
Author. Pass Add rcvd.  : 0
Author. Pass Repl rcvd :    0
Author. Fails rcvd.       :  0
Author. Errors rcvd.      : 0
Author Follows rcvd.      : 0
Author. Sess. timeouts    : 0
Acct. start reqs. sent    : 0
Acct. WD reqs. sent       : 0
Acct. Stop reqs. sent     : 0
Acct. Success rcvd.  : 0
Acct. Errors rcvd.       : 0
Acct. Follows rcvd.      : 0
Acct. Sess. timeouts     : 0
Malformed Pkts. rcvd. : 0
Socket failures           : 0
Connection failures       : 0
```

4.5 TACACS Authorization Status

Supermicro switches provide an option to configure TACACS authorization status. Users can specify one of the option Enable or Disable.

If authorization status is enabled, during TACACS+ authentication switch will also send out the authorization request to TACACS+ server. The authorization requests are used to get privilege levels for TACACS+ users. When authorization status is disabled, all TACACS+ authenticated users will be logged in with default privilege level 1. When authorization status is enabled, the TACACS+ authentication users will be logged in with privilege levels configured in TACACS+ server.

Follow the steps below to configure the TACACS authorization to be used.

Step	Command	Description

Step 1	configure terminal	Enters the configuration mode.
Step 2	aaa authorization group Tacacs	Configures TACACS authorization to be used.
Step 3	End	Exits the configuration mode.
Step 4	show tacacs	Displays the TACACS configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of the startup configuration.

The “no aaa authorization group tacacs” command disables the TACACS authorization status.

The example below shows the commands used to configure the TACACS authorization status to be used.

```
SMIS# configure terminal

SMIS(config)# aaa authorization group tacacs

SMIS(config)# end

SMIS(config)# show tacacs
Server : 1
      Address          : 192.168.2.11
      Single Connection : no
      TCP port         : 49
      Timeout          : 5
      Key Type         : 0
      Secret Key       : test123
      Mode             : Pap
Client uses server: 192.168.2.11
Authorization Enable
 Authen. Starts sent         : 8
 Authen. Continues sent : 0
 Authen. Enables sent      : 0
 Authen. Aborts sent        : 0
 Authen. Pass rvcd.         : 5
 Authen. Fails rcvd.         : 3
 Authen. Get User rcvd. : 0
 Authen. Get Pass rcvd. : 0
 Authen. Sess. timeouts   : 0
 Author. Requests sent     : 4
 Author. Pass Add rcvd.  : 0
```

Author. Pass Repl rcvd : 0
Author. Fails rcvd. : 0
Author. Errors rcvd. : 0
Author Follows rcvd. : 0
Author. Sess. timeouts : 0
Acct. start reqs. sent : 0
Acct. WD reqs. sent : 0
Acct. Stop reqs. sent : 0
Acct. Success rcvd. : 0
Acct. Errors rcvd. : 0
Acct. Follows rcvd. : 0
Acct. Sess. timeouts : 0
Malformed Pkts. rcvd. : 0
Socket failures : 0
Connection failures : 0

4.6 TACACS Privilege

Req. #	Description	Comments

1.0	The privilege configured in TACACS+ server should be used while logging in to Supermicro switch using TACACS+ authentication.
	
	There are many types of service used by different vendors on the market. For Supermicro switches the supported service type is 'config'.
	
	E.g. user configuration in TACACS+ server:
	user = test15 {
	name = "Test15 User"
	pap = cleartext "test15"
	service=**config** {
	priv-lvl = 15
	}
	}
		This is an umbrella requirement to cover the functionality.

1.1	TACACS+ users without privilege configured also should be able to login to switch with the default privilege level 1.
	
	E.g. user configuration in TACACS+ server:
	user = test1 {
	name = "Test1 User"
	pap = cleartext "test1"
	}	

1.2	This privilege function should be enabled only when user enables it in CLI, Web, and SNMP. Proposed new CLI command to enable: aaa authorization group tacacs In Web, it should be enabled in "Management Security" page. In SNMP, the following OID can be used: 1.3.6.1.4.1.2076.77.1.6.0	For e.g. the new command "aaa authorization
1.3	If this function is not enabled (using the command in Req. 2), switch should behave as before. It means the irrespective of the privilege configured on the TACACS+ server, it will login the users with the default privilege 1.	
1.4	The TACACS+ privilege function should work in telnet, ssh and Web login.	
1.5	The new authorization status configuration (Req. 2) should be saved and restored.	

5 SSH

Supermicro switches act as a SSH client and support both SSH version 1 and SSH version 2.

Parameter	Default Value
SSH status	Enabled
SSH version compatibility	Off
SSH port	22
SSH Key	RSA
Cipher Algorithm	3DES-CBC
SSH Version	2
Authentication	HMAC-SHA1

Follow the steps below to configure SSH.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth ([hmac-md5] [hmac-sha1]) | port <(1024-65535)>}	*versioncompatibility*- Specify whether switch should process both version 1 and version 2 SSL messages. *cipher* – Specify the encryption algorithm.

		auth –Specify the authentication algorithm. *port* - Specify SSH port in range 1024-65535
Step 3	End	Exits the configuration mode.
Step 4	show ip ssh	Displays the SSH configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The "no ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth ([hmac-md5] [hmac-sha1]) | port <(1024-65535)>}" command disables SSH.

The example below shows the commands used to configure SSH.

```
SMIS# configure terminal
SMIS(config)# ip ssh version compatibility
SMIS(config)# end
SMIS# show ip ssh
Version         : Both
Cipher Algorithm : 3DES-CBC
Authentication   : HMAC-SHA1
Trace Level      : None
SMIS# configure terminal
SMIS(config)# ip ssh cipher des-cbc
SMIS(config)# end
SMIS# show ip ssh
Version         : 2
Cipher Algorithm : DES-CBC
Authentication   : HMAC-SHA1
Trace Level      : None

SMIS# configure terminal
SMIS(config)# ip ssh auth hmac-md5
SMIS(config)# end
SMIS# show ip ssh
Version         : 2
Cipher Algorithm : 3DES-CBC
Authentication   : HMAC-MD5
Trace Level      : None
```

6 SSL

SSL provides server authentication, encryption, and message integrity, as well asHTTP client authentication, to allow secure HTTP communications.To use this feature, thecryptographic (encrypted) software image must be installed on the switch.

Parameter	Default Value
HTTP Secure server status	Enabled
HTTP Secure server encryption	rsa-null-md5
HTTP Secure server keys	None
SSL Server certificate	None
SSL Server certificate request	None

6.1 Secure HTTP (https)

On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over theInternet. *HTTP with SSL encryption (HTTPS)*provides a secure connection to allow such functions as configuringa switch from a Web browser.

Follow the steps below to configure Secure HTTP.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha][dh-rsa-3des-sha][rsa-exp1024-des-sha] | crypto key rsa [usage-keys (512|1024)] }	Configure Secure HTTP. *server* – Enables HTTPS server *ciphersuite* – Specify one or many of the supported encryption algorithm to be used. *crypto key rsa*–Encryption Key, either 512 or 1024.
Step 3	End	Exits the configuration mode.
Step 4	show ip http secure server status	Displays the SSL configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The “no ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha][dh-rsa-3des-sha][rsa-exp1024-des-sha] |
crypto key rsa [usage-keys (512|1024)] }” command enables the agent.

The example below shows the commands used to configure Secure HTTP.

```
SMIS# configure terminal
SMIS(config)# no ip http secure server
SMIS(config)# end
SMIS# show ip http secure server status
HTTP secure server status      : Disabled
HTTP secure server ciphersuite  : RSA-DES-SHA:RSA-3DES-SHA:RSA-EXP1024-DES-SHA:
HTTP crypto key rsa 1024
```

6.2 Certificate Signing Request (CSR)

An SSL certificate provides security for online communications. Before requesting an SSL certificate, a Certificate Signing Request (CSR) must be generated and submitted to the Certification Authority (CA).Certificate authorities (CAs) manage certificate requests and issue certificates to participating network devices. These services provide centralized security key and certificate management for the participating devices. CA servers are called as trustpoints, e.g. thawte.com.
Supermicro switches create a Certificate Signing Request (CSR) using RSA key pair and Switch Identification.

Follow the steps below to configure Certificate Signing Request (CSR).

Step	Command	Description
Step 1	ssl gen cert-req algo rsa sn <SubjectName>	Configure Certificate Signing Request (CSR). *SubjectName* – Switch ID or IP-address.
Step 2	show ssl server-cert	Displays the SSL configuration.
Step 3	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The example below shows the commands used to configure Certificate Signing Request (CSR).

```
SMIS# ssl gen cert-req algo rsa sn SMIS
-----BEGIN CERTIFICATE REQUEST-----
MIIBTjCBuAIBADAPMQ0wCwYDVQQDEwRTTUlTMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQChj0JzVX1/gZ4SMGekRdrsAnftWnKHG3VypWTtySqkvTwhnZ206Q2o
cBYJNKY4ZCykOXG81mfUhqPfVLyO8sbK+RYzEeTMX9lw9iq9yOySOlvxY6IoYNsg
O++JS02khz0SAbpRkhtGuwmBiZQtSj+8Ea3dG8ReoixpcYDVVdIrDQIDAQABoAAw
DQYJKoZIhvcNAQEEBQADgYEAXR8Nz40QeC8wqwzqy+iozT5iUMKOkelXTE8mDydt
AvRyc7a3EPraGjyOL5W1H94z+wW2wkxXTRzKuLzAEYRH9f84XB2uCAdL+jkuSBJc
5qd3j4yBtOIu/pxOsdKKwuq6LWbi44DCXg97SkE+pOYa7nWojVkjc2SbjvK5CTgG
89s=
-----END CERTIFICATE REQUEST-----

SMIS# show ssl server-cert
Certificate:
```

```
    Data:
        Version: 1 (0x0)
        Serial Number: 10 (0xa)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, ST=CA, L=SanJose, O=Supermicro, OU=Switch, CN=Switch/Email
=support@supermicro.com
        Validity
            Not Before: Aug 11 22:18:10 2011 GMT
            Not After : Sep 10 22:18:10 2011 GMT
        Subject: CN=SMIS
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:a1:8f:42:73:55:7d:7f:81:9e:12:30:67:a4:45:
                    da:ec:02:77:ed:5a:72:87:1b:75:72:a5:64:ed:c9:
                    2a:a4:bd:3c:21:9d:9d:b4:e9:0d:a8:70:16:09:34:
                    a6:38:64:2c:a4:39:71:bc:d6:67:d4:86:a3:df:54:
                    bc:8e:f2:c6:ca:f9:16:33:11:e4:cc:5f:d9:70:f6:
                    2a:bd:c8:ec:92:3a:5b:f1:63:a2:28:60:db:20:3b:
                    ef:89:4b:4d:a4:87:3d:12:01:ba:51:92:1b:46:bb:
                    09:81:89:94:2d:4a:3f:bc:11:ad:dd:1b:c4:5e:a2:
                    2c:69:71:80:d5:55:d2:2b:0d
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
        21:bd:73:5e:96:82:89:13:12:a6:69:e8:9c:e6:fb:a5:0f:bc:
        0b:8d:fd:03:25:68:d9:09:73:58:7f:e1:30:64:d9:3a:99:63:
        6b:d2:ec:37:ea:33:1e:28:11:48:26:94:13:36:aa:08:14:5a:
        7a:c4:f2:14:26:54:9e:d4:b5:2d:a2:c1:ab:fe:7a:2f:b8:f6:
        23:08:93:fb:6b:7e:d9:14:da:09:90:50:b4:76:b0:17:e1:5f:
        53:75:ee:7a:5f:85:dd:90:3c:d4:28:18:ee:5c:64:f5:09:52:
        03:25:3e:f1:ed:5d:80:37:4b:ff:ad:fb:54:d0:24:11:a1:cd:
        32:6c
```

6.3 SSL Certificate

Each SSL Certificate contains

- A public/private key pair: a private key with the code and a public key used to decode it. The private key is installed on the server and is not shared with anyone. The public key is incorporated into the SSL certificate and shared with web browsers.
- Identification information. E.g. When you request an SSL certificate, a third party (such as Thawte) verifies your organization's information and issues a unique certificate to you with that information.

SSL Certificate can be configured in Supermicro switches. The certificate should be specified in PEM format.
Follow the steps below to configure SSL server certificate.

Step	Command	Description
Step 1	ip http secure	Configure Cipher Suite and Crypto Key RSA of your choice using “ip http secure” command.
Step 2	ssl gen cert-req algo rsa sn	Enter the subject name and create certificate request by using the “ssl gen cert-req algo rsa sn” command.
Step 3	show ssl server-cert	The “show ssl server-cert” command will display certificate request. Copy paste these contents to a text file, say a.csr.
Step 4	Linux commands	To generate SSL certificate openssl application can be used. The following steps can be executed in any linux machine to generate SSL certificates. For other openssl implementation refer the openssl documentation to find the equivalent steps. Execute the below commands in linux shell. 1. openssl req -x509 -newkey rsa:1024 -keyout cakey.pem -out cacert.pem 2. openssl x509 -req -in a.csr -out cert.pem -CA cacert.pem -CAkey cakey.pem –Cacreateserial This would generate certificate file cert.pem.
Step 5	ssl server-cert	Open the generate certificate file cert.pem. Delete first line (---BEGIN CERTIFICATE ---) and last line (----END CERTIFICATE--). Join all the remaining lines as single line to avoid line breaks processed. Copy paste these joined texts in “Enter Certificate” prompt– This prompt appears after entering the “ssl serv-cert” command in CLI.

		This step would configure the certificate and save it to flash.
Step 6	show ssl server-cert	Displays the SSL configuration.

Contacting Supermicro

Headquarters

Address:	Super Micro Computer, Inc. 980 Rock Ave. San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information) support@supermicro.com (Technical Support)
Web Site:	www.supermicro.com

Europe

Address:	Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML 's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information) support@supermicro.nl (Technical Support) rma@supermicro.nl (Customer Support)
Web Site:	www.supermicro.com.nl

Asia-Pacific

Address:	Super Micro Computer, Inc. 3F, No. 150, Jian 1st Rd. Zhonghe Dist., New Taipei City 235 Taiwan (R.O.C)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	support@supermicro.com.tw
Web Site:	www.supermicro.com.tw