Software Authentication Manager Commands

This module describes the Cisco IOS XR software commands used to configure Software Authentication Manager (SAM).

For detailed information about SAM concepts, configuration tasks, and examples, see the *Configuring Software Authentication Manager on* the Cisco ASR 9000 Series Router module in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers* .

sam add certificate

To add a new certificate to the certificate table, use the **sam add certificate** command.

sam add certificate *filepath location* {**trust** | **untrust**}

Syntax Description

filepath	Absolute path to the source location of the certificate.
location	Storage site of the certificate. Use one of the following: **root**, **mem**, **disk0**, **disk1**, or **other flash device name on router**.
trust	Adds the certificate to the certificate table without validation by the Software Authentication Manager (SAM). To add a root certificate, you must use the **trust** keyword. Adding a root certificate with the **untrust** keyword is not allowed.
untrust	Adds the certificate to the certificate table after the SAM has validated it. Adding a root certificate with the **untrust** keyword is not allowed. To add a root certificate, you must use the **trust** keyword.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

For security reasons, the **sam add certificate** command can be issued only from the console or auxiliary port of the networking device; the command cannot be issued from a Telnet connection to any other interface on the networking device.

The certificate must be copied to the network device before it can be added to the certificate table. If the certificate is already present in the certificate table, the SAM rejects the attempt to add it.

When adding root certificates, follow these guidelines:

- Only the certificate authority (CA) root certificate can be added to the root location.
- To add a root certificate, you must use the **trust** keyword. Adding the root certificate with the **untrust** keyword is not allowed.

Use of the **trust** keyword assumes that you received the new certificate from a source that you trust, and therefore have enough confidence in its authenticity to bypass validation by the SAM. One example of acquiring a certificate from a trusted source is downloading it from a CA server (such as Cisco.com) that requires user authentication. Another example is acquiring the certificate from a person or entity that you can verify, such as by checking the identification badge for a person. If you bypass the validation protection offered by the SAM, you must verify the identity and integrity of the certificate by some other valid process.

Certificates added to the memory (**mem**) location validate software installed in memory. Certificates added to the **disk0** or **disk1** location validate software installed on those devices, respectively.

Note If the **sam add certificate** command fails with a message indicating that the certificate has expired, the networking device clock may have been set incorrectly. Use the **show clock** command to determine if the clock is set correctly.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to add the certificate found at **/bootflash/ca.bin** to the certificate table in the root location without first validating the certificate:

```
RP/0/RSP0/CPU0:router# sam add certificate /bootflash/ca.bin root trust

SAM: Successful adding certificate /bootflash/ca.bin
```

The following example shows how to add the certificate found at **/bootflash/css.bin** to the certificate table in the memory (**mem**) location after validating the certificate:

```
RP/0/RSP0/CPU0:router# sam add certificate /bootflash/css.bin mem untrust

SAM: Successful adding certificate /bootflash/css.bin
```

Related Commands

Command	Description
sam delete certificate, on page 4	Deletes a certificate from the certificate table.
show sam certificate, on page 10	Displays records in the certificate table, including the location of the certificates.
show clock	Displays networking device clock information. For more information, see *System Management Command Reference for Cisco ASR 9000 Series Routers*.

sam delete certificate

To delete a certificate from the certificate table, use the **sam delete certificate** command.

sam delete certificate *location certificate-index*

Syntax Description

location	Storage site of the certificate. Use one of the following: **root**, **mem**, **disk0**, **disk1**, or **other flash device name on the router**.
certificate-index	Number in the range from 1 to 65000.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

For security reasons, the **sam delete certificate** command can be issued only from the console port of the networking device; the command cannot be issued from a Telnet connection to any other interface on the networking device.

Use the **show sam certificate summary** command to display certificates by their index numbers.

Because the certificate authority (CA) certificate must not be unknowingly deleted, the Software Authentication Manager (SAM) prompts the user for confirmation when an attempt is made to delete the CA certificate.

If a certificate stored on the system is no longer valid (for example, if the certificate has expired), you can use the **sam delete certificate** command to remove the certificate from the list.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to delete the certificate identified by the index number 2 from the memory location:

```
RP/0/RSP0/CPU0:router# sam delete certificate mem 2

SAM: Successful deleting certificate index 2
```

The following example shows how to cancel the deletion of the certificate identified by the index number 1 from the root location:

```
RP/0/RSP0/CPU0:router# sam delete certificate root 1

Do you really want to delete the root CA certificate (Y/N): N
SAM: Delete certificate (index 1) canceled
```

The following example shows how to delete the certificate identified by the index number 1 from the root location:

```
RP/0/RSP0/CPU0:router# sam delete certificate root 1

Do you really want to delete the root CA certificate (Y/N): Y
SAM: Successful deleting certificate index 1
```

Related Commands

Command	Description
sam add certificate, on page 2	Adds a new certificate to the certificate table.
show sam certificate, on page 10	Displays records in the certificate table, including the location of the certificates stored.

sam prompt-interval

To set the interval that the Software Authentication Manager (SAM) waits after prompting the user for input when it detects an abnormal condition at boot time and to determine how the SAM responds when it does not receive user input within the specified interval, use the **sam prompt-interval** command. To reset the prompt interval and response to their default values, use the **no** form of this command.

sam prompt-interval *time-interval* {**proceed** | **terminate**}
no sam prompt-interval *time-interval* {**proceed** | **terminate**}

Syntax Description

time-interval	Prompt time, in the range from 0 to 300 seconds.
proceed	Causes the SAM to respond as if it had received a “yes” when the prompt interval expires.
terminate	Causes the SAM to respond as if it had received a “no” when the prompt interval expires.

Command Default

The default response is for the SAM to wait 10 seconds and then terminate the authentication task.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **sam prompt-interval** command to control the action taken when the system detects an exception condition, such as an expired certificate during initialization of the SAM at boot time. The following message appears when the software detects the abnormal condition of a certificate authority (CA) certificate expired:

```
SAM detects expired CA certificate. Continue at risk (Y/N):
```

The SAM waits at the prompt until you respond or the time interval controlled by the **sam prompt-interval** command expires, whichever is the earlier event. If you respond “N” to the prompt, the boot process is allowed to complete, but no packages can be installed.

The following message appears when the software detects the abnormal condition of a Code Signing Server (CSS) certificate expired:

```
SAM detects CA certificate (Code Signing Server Certificate Authority) has expired. The
validity period is Oct 17, 2000 01:46:24 UTC - Oct 17, 2015 01:51:47 UTC. Continue at risk?
 (Y/N) [Default:N w/in 10]:
```

If you do not respond to the prompt, the SAM waits for the specified interval to expire, and then it takes the action specified in the **sam prompt-interval** command (either the **proceed** or **terminate** keyword).

If you enter the command with the **proceed** keyword, the SAM waits for the specified interval to expire, and then it proceeds as if you had given a “yes” response to the prompt.

If you enter the command with the **terminate** keyword, the SAM waits for the specified interval to expire, and then it proceeds as if you had given a "no" response to the prompt. This use of the command keeps the system from waiting indefinitely when the system console is unattended.

Note After the software has booted up, the *time-interval* argument set using this command has no effect. This value applies at boot time only.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to tell the SAM to wait 30 seconds for a user response to a prompt and then terminate the requested SAM processing task:

```
RP/0/RSP0/CPU0:router/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# sam prompt-interval 30 terminate
```

Related Commands

Command	Description
show sam sysinfo, on page 20	Displays the current status information for the SAM.

sam verify

To use the Message Digest 5 (MD5) hash algorithm to verify the integrity of the software component on a flash memory card and ensure that it has not been tampered with during transit, use the **sam verify** command.

sam verify {*locationfile-system*} {**MD5** | **SHA** [*digest*]}

Syntax Description

location	Name of the flash memory card slot, either disk0 or disk1.
file-system	Absolute path to the file to be verified.
MD5	Specifies a one-way hashing algorithm to generate a 128-bit hash (or message digest) of the specified software component.
SHA	Specifies the Secure Hash Algorithm, a hashing algorithm that takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest provides security against brute-force collision and inversion attacks.
digest	(Optional) Message digest generated by the hashing algorithm, to be compared in determining the integrity of the software component.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **sam verify** command to generate a message digest for a given device. The message digest is useful for determining whether software on a flash memory card has been tampered with during transit. The command generates a hash code that can be used to compare the integrity of the software between the time it was shipped and the time you received it.

For example, if you are given a flash memory card with preinstalled software and a previously generated MD5 message digest, you can verify the integrity of the software using the **sam verify** command:

```
sam verify device MD5 digest
```

The *device* argument specifies the flash device. The *digest* argument specifies the message digest supplied by the originator of the software.

If the message digest matches the message digest generated by the **sam verify** command, the software component is valid.

Note You should calculate the hash code on the contents of the flash memory code at the destination networking device using a different set of files from the one loaded on the flash memory card. It is possible for an unauthorized person to use the same software version to produce the desired (matching) hash code and thereby disguise that someone has tampered with the new software.

Task ID

Task ID	Operations
crypto	execute

Examples

The example shows a third **sam verify** command, issued with a mismatched message digest, to show the Software Authentication Manager (SAM) response to a mismatch. The following example shows how to use MD5 to generate a message digest on the entire file system on the flash memory card in slot 0 and then use that message digest as input to perform the digest comparison:

```
RP/0/RSP0/CPU0:router# sam verify disk0: MD5

Total file count in disk0: = 813
082183cb6e65a44fd7ca95fe8e93def6

RP/0/RSP0/CPU0:router# sam verify disk0: MD5 082183cb6e65a44fd7ca95fe8e93def6

Total file count in disk0: = 813
Same digest values

RP/0/RSP0/CPU0:router# sam verify disk0: MD5 3216c9282d97ee7a40b78a4e401158bd

Total file count in disk0: = 813
Different digest values
```

The following example shows how to use MD5 to generate a message digest and then uses that message digest as input to perform the digest comparison:

```
RP/0/RSP0/CPU0:router# sam verify disk0: /crl_revoked.bin MD5

38243ffbbe6cdb7a12fa9fa6452956ac

RP/0/RSP0/CPU0:router# sam verify disk0: /crl_revoked.bin MD5 38243ffbbe6cdb7a12fa9fa6452956ac

Same digest values
```

show sam certificate

To display records in the certificate table, use the **show sam certificate** command.

Syntax Description

detail	Displays all the attributes for the selected table entry (specified by the *location* and *certificate-index* arguments).
location	Specifies where the entry to display is stored. Use one of the following values: • **root—**Certificate is stored on the root device. • **mem—**Certificate is stored in memory. • *device-name*—Certificate is stored on the named device. Use the values disk0, disk1, or the name of any other flash-device on the router. You can research flash-device names using the **show filesystem** command.
certificate-index	Index number for the entry in the Certificate Table that you want to display, in the range from 1 to 65000.
brief	Displays a subset of attributes for entries in a Certificate Table.
location	Specifies where the entries to display are stored. Use one of the following values: • **all**—Displays a subset of attributes for all certificates. • **root—**Displays a subset of attributes for all certificates stored on the root device. • **mem—**Displays a subset of attributes for all certificates stored in memory. • *device-name*—Displays a subset of attributes for all certificates stored on the named device. Use the values disk0, disk1, or the name of any other flash-device on the router. You can research flash-device names using the **show filesystem** command.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show sam certificate** command when you want to display all the certificates stored in the system. Attributes are certificate number, certificate flag, serial number, subject name, issued by, version, issuing algorithm, not-before and not-after dates, public key, and signature.

To get the certificate number, use the *certificate-index* argument. When used with the **brief** keyword, the **all** keyword displays selected attributes for all the entries in the table.

Task ID

Task ID	Operations
none	—

Examples

In the example, the root location has one certificate, and disk0 has one certificate. The following sample output is from the **show sam certificate** command:

```
RP/0/RSP0/CPU0:router# show sam certificate
            brief

            all

-------------------- SUMMARY OF CERTIFICATES -------------------

Certificate Location    :root
Certificate Index       :1
Certificate Flag        :VALIDATED
  Serial Number  :32:E0:A3:C6:CA:00:39:8C:4E:AC:22:59:1B:61:03:9F
  Subject Name   :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Issued By      :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Validity Start :[UTC] Tue Oct 17 01:46:24 2000
  Validity End   :[UTC] Sat Oct 17 01:51:47 2015
  CRL Distribution Point

file://\\CodeSignServer\CertEnroll\Code%20Signing%20Server%20Certificate
%20Authority.crl

Certificate Location    :mem
Certificate Index       :1
Certificate Flag        :VALIDATED
  Serial Number  :01:27:FE:79:00:00:00:00:00:05
  Subject Name   :
        cn=Engineer code sign certificate
  Issued By      :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Validity Start :[UTC] Tue Oct  9 23:14:28 2001
  Validity End   :[UTC] Wed Apr  9 23:24:28 2003
  CRL Distribution Point

file://\\CodeSignServer\CertEnroll\Code%20Signing%20Server%20Certificate %20Authority.crl
```

This table describes the significant fields shown in the display.

Table 1: show sam certificate summary all Field Descriptions

Field	Description
Certificate Location	Location of the certificate; one of the following: **root**, **mem**, **disk0**, or **disk1** , or other flash device name.
Certificate Index	Index number that the Software Authentication Manager automatically assigns to the certificate.
Certificate Flag	One of the following: TRUSTED, VALIDATED, EXPIRED, or REVOKED.

Field	Description
Serial Number	Unique serial number of the certificate, assigned by its issuer.
Subject Name	Name of the entity for which the certificate is issued.
Issued By	Name of the entity that issued the certificate.

The following sample output from the **show sam certificate** command shows how to display particular SAM details:

```
RP/0/RSP0/CPU0:router# show sam certificate detail mem 1
------------------------------------------------------------

Certificate Location    :mem
Certificate Index       :1
Certificate Flag        :VALIDATED

----------------------- CERTIFICATE ------------------------
  Serial Number  :01:27:FE:79:00:00:00:00:00:05
  Subject Name   :
        cn=Engineer code sign certificate
  Issued By      :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Validity Start :[UTC] Tue Oct  9 23:14:28 2001
  Validity End   :[UTC] Wed Apr  9 23:24:28 2003
  CRL Distribution Point

file://\\CodeSignServer\CertEnroll\Code%20Signing%20Server%20Certificate
%20Authority.crl
  Version 3 certificate
  Issuing Algorithm:MD5withRSA
  Public Key BER (294 bytes):
 30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01      [0.."0...*.H.....]
 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01      [........0.......]
 00 be 75 eb 9b b3 d9 cb 2e d8 c6 db 68 f3 5a ab      [..u.........h.Z.]
 0c 17 d3 84 16 22 d8 18 dc 3b 13 99 23 d8 c6 94      [....."...;..#...]
 91 15 15 ec 57 ea 68 dc a5 38 68 6a cb 0f 4b c2      [....W.h..8hj..K.]
 43 4b 2d f9 92 94 93 04 df ff ca 0b 35 1d 85 12      [CK-.........5...]
 99 e9 bd bc e2 98 99 58 fe 6b 45 38 f0 52 b4 cb      [.......X.kE8.R..]
 a9 47 cd 22 aa ce 70 0e 4c 9b 48 a1 cf 0f 4a db      [.G."..p.L.H...J.]
 35 f5 1f 20 b7 68 cb 71 2c 27 01 84 d6 bf 4e d1      [5.. .h.q,'....N.]
 ba e1 b2 50 e7 f1 29 3a b4 85 3e ac d7 cb 3f 36      [...P..):..>...?6]
 96 65 30 13 27 48 84 f5 fe 88 03 4a d7 05 ed 72      [.e0.'H.....J...r]
 4b aa a5 62 e6 05 ac 3d 20 4b d6 c9 db 92 89 38      [K..b...= K.....8]
 b5 14 df 46 a3 8f 6b 05 c3 54 4d a2 83 d4 b7 02      [...F..k..TM.....]
 88 2d 58 e7 a4 86 1c 48 77 68 49 66 a1 35 3e c4      [.-X....HwhIf.5>.]
 71 20 aa 18 9d 9f 1a 38 52 3c e3 35 b2 19 12 ad      [q .....8R<.5....]
 99 ad ce 68 8b b0 d0 29 ba 25 fd 1e e0 5d aa 12      [...h...).%...]..]
 9c 44 89 63 89 62 e3 cb f3 5d 5f a3 7c b7 b9 ef      [.D.c.b...]_.|...]
 01 89 5b 33 35 a8 81 60 38 61 4e d8 4f 6a 53 70      [..[35..`8aN.OjSp]
 35 02 03 01 00 01                                    [5.....]
  Certificate signature (256 bytes):
 67 f6 12 25 3f d4 d2 dd 6a f7 3e 55 b8 9f 33 53      [g..%?...j.>U..3S]
 20 4d d1 17 54 08 8a 70 22 35 92 59 9c 03 9c 0f      [ M..T..p"5.Y....]
 ce 46 3c 06 74 d0 a9 8e b1 88 a2 35 b3 eb 1b 00      [.F<.t......5....]
 5c 6d bb 1d b5 ad 17 19 f2 c6 96 87 9b e7 15 01      [\m.............]
 b2 04 af 7d 92 60 d9 ee ef bc 60 4e 2e af 84 e2      [...}.`....`N....]
 42 fe 07 71 7e fc ee ee f5 d1 6d 71 e7 46 f0 97      [B..q~.....mq.F..]
 e0 e8 b3 0e f9 07 e0 de 6e 36 5a 56 1e 80 10 05      [........n6ZV....]
 59 d9 88 ba f7 a3 d1 f6 cd 00 12 9f 90 f0 65 83      [Y.............e.]
```

```
e9 0f 76 a4 da eb 1b 1b 2d ea bd be a0 8a fb a7      [..v.....-.......]
a5 18 ff 9f 5c e9 99 66 f0 d3 90 ae 49 3f c8 cc      [....\..f....I?..]
32 6b db 64 da fd f5 42 ea bc f3 b0 8a 2f 17 d8      [2k.d...B...../..]
cf c0 d8 d4 3a 41 ae 1d cf 7a c6 a6 a1 65 c2 94      [....:A...z...e..]
8a ba ea d3 da 3e 8a 44 9b 47 35 10 ab 61 1b 4f      [.....>.D.G5..a.O]
82 dd 59 16 d5 f2 1d f3 c2 08 cc 1c 7f ab be 9c      [..Y.............]
be 52 73 ea e0 89 d7 6f 4d d0 d8 aa 3d 50 d6 b0      [.Rs....oM...=P..]
e1 ea 3b 27 50 42 08 d6 71 eb 66 37 b1 f5 f6 5d      [..;'PB..q.f7...]]
```

This table describes the significant fields shown in the display.

Table 2: show sam certificate detail mem 1 Field Descriptions

Field	Descriptions
Certificate Location	Location of the certificate; one of the following: **root**, **mem**, **disk0**, or **disk1**.
Certificate Index	Index number that the SAM automatically assigns to the certificate.
Certificate Flag	One of the following: TRUSTED, VALIDATED, EXPIRED, or REVOKED.
Serial Number	Unique serial number of the certificate, assigned by its issuer.
Subject Name	Name of the entity for which the certificate is issued.
Issued By	Name of the entity that issued the certificate.
Version	The ITU-T X.509 version of the certificate. The version can be 1 (X.509v1), 2 (X.509v2), or 3 (X.509v3).
Issuing Algorithm	Hash and public key algorithm that the issuer uses to sign the certificate.
Public Key	Subject public key for the certificate.
Certificate signature	Encrypted hash value (or signature) of the certificate. The hash value of the certificate is encrypted using the private key of the issuer.

show sam crl

To display the records in the certificate revocation list (CRL) table, use the **show sam crl** command.

show sam crl {**summary** | **detail** *crl-index*}

Syntax Description

summary	Displays selected attributes for all entries in the table.
detail	Displays all the attributes for the selected table entry (specified by the *crl-index* argument).
crl-index	Index number for the entry, in the range from 1 to 65000.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show sam crl** command when you want to display all the revoked certificates currently stored on the system. Attributes are CRL index number, issuer, and update information.

To get the CRL index number, use the **summary** keyword.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show sam crl** command for the **summary** keyword:

```
RP/0/RSP0/CPU0:router# show sam crl summary

---------------------- SUMMARY OF CRLs -------------------------

CRL Index       :1
Issuer:CN = Code Sign Server Certificate Manager, OU = Cisco HFR mc , O =
Cisco,
  L = San Jose, ST = CA, C = US, EA =<16> iosmx-css-cert@cisco.com
Including updates of:
                      Sep 09, 2002 03:50:41 GMT
```

This table describes the significant fields shown in the display.

Table 3: show sam crl summary Field Descriptions

Field	Description
CRL Index	Index number for the entry, in the range from 1 to 65000. The index is kept in the certificate revocation list table.
Issuer	Certificate authority (CA) that issued this CRL.
Including updates of	Versions of CRLs from this CA that are included in the CRL table.

The following sample output is from the **show sam crl** command for the **detail** keyword:

```
RP/0/RSP0/CPU0:router# show sam crl detail 1

------------------------------------------------------------------

CRL Index      :1

-------------- CERTIFICATE REVOCATION LIST (CRL) -----------------

Issuer:CN = Code Sign Server Certificate Manager, OU = Cisco HFR mc , O = Cisco,
 L = San Jose, ST = CA, C = US, EA =<16> iosmx-css-cert@cisco.com
Including updates of:
                    Sep 09, 2002 03:50:41 GMT
Revoked certificates include:

   Serial #:61:2C:5C:83:00:00:00:00:00:44, revoked on Nov 03, 2002 00:59:02 GMT
   Serial #:21:2C:48:83:00:00:00:00:00:59, revoked on Nov 06, 2002 19:32:51 GMT
------------------------------------------------------------------------------
```

This table describes the significant fields shown in the display.

Table 4: show sam crl detail Field Descriptions

Field	Descriptions
CRL Index	Index number for the entry, in the range from 1 to 65000. The index is kept in the certificate revocation list table.
Issuer	CA that issued this CRL.
Including updates of	Versions of CRLs from this CA that are included in the CRL table.
Revoked certificates include	List of certificates that have been revoked, including the certificate serial number and the date and time the certificate was revoked.

show sam log

To display the contents of the Software Authentication Manager (SAM) log file, use the **show sam log** command.

show sam log [*lines-number*]

Syntax Description

lines-number	(Optional) Number of lines of the SAM log file to display, in the range from 0 to 200, where 0 displays all lines in the log file and 200 displays the most recent 200 lines (or as many lines as there are in the log file if there are fewer than 200 lines).

Command Default

The **show sam log** command without a *lines-number* argument displays all the lines in the log file.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The SAM log file records changes to the SAM tables, including any expired or revoked certificates, table digest mismatches, and SAM server restarts.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show sam log** command:

```
RP/0/RSP0/CPU0:router# show sam log

06/16/02 12:03:44 UTC Added certificate in table root/1 CN = Certificate Manage, 0x01
06/16/02 12:03:45 UTC SAM server restarted through router reboot
06/16/02 12:03:47 UTC Added CRL in table CN = Certificate Manage, updated at Nov 10, 2001
   04:11:42 GMT
06/16/02 12:03:48 UTC Added certificate in table mem:/1 CN = Certificate Manage, 0x1e
06/16/02 12:16:16 UTC SAM server restarted through router reboot
06/16/02 12:25:02 UTC SAM server restarted through router reboot
06/16/02 12:25:04 UTC Added certificate in table mem:/1 CN = Certificate Manage, 0x1e
06/16/02 12:39:30 UTC SAM server restarted through router reboot
06/16/02 12:39:30 UTC SAM server restarted through router reboot
06/16/02 12:40:57 UTC Added certificate in table mem/1 CN = Certificate Manage, 0x1e

33 entries shown
```

Each line of output shows a particular logged event such as a table change, expired or revoked certificates, table digest mismatches, or SAM server restarts.

show sam package

To display information about the certificate used to authenticate the software for a particular package installed on the networking device, use the **show sam package** command.

show sam package *package-name*

Syntax Description

package-name	Location of the software package, including the memory device (**disk0:**, **disk1:**, **mem**:, and so on) and the file system path to the file. Use the **show install all** command to display the Install Manager package name and location information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show install all** command to display the installed location and name of the software package—for example, mem:ena-base-0.0.0 or disk1:crypto-exp-lib-0.4.0—and then use the **show sam package** command to display information about the certificate used to authenticate that installed package. The **show sam package** command displays the same information as the **show sam certificate** command for the **detail** keyword.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show sam package** command:

```
RP/0/RSP0/CPU0:router# show sam package mem:12k-rp-1.0.0

------------------------------------------------------------

Certificate Location    :mem
Certificate Index       :1
Certificate Flag        :VALIDATED

----------------------- CERTIFICATE ------------------------
  Serial Number  :01:27:FE:79:00:00:00:00:00:05
  Subject Name   :
        cn=Engineer code sign certificate
  Issued By      :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Validity Start :[UTC] Tue Oct  9 23:14:28 2001
```

```
  Validity End   :[UTC] Wed Apr  9 23:24:28 2002
  CRL Distribution Point

file://\\CodeSignServer\CertEnroll\Code%20Signing%20Server%20Certificate
%20Authority.crl
  Version 3 certificate
  Issuing Algorithm:MD5withRSA
  Public Key BER (294 bytes):
 30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01      [0.."0...*.H.....]
 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01      [........0.......]
 00 be 75 eb 9b b3 d9 cb 2e d8 c6 db 68 f3 5a ab      [..u.........h.Z.]
 0c 17 d3 84 16 22 d8 18 dc 3b 13 99 23 d8 c6 94      [....."...;..#...]
 91 15 15 ec 57 ea 68 dc a5 38 68 6a cb 0f 4b c2      [....W.h..8hj..K.]
 43 4b 2d f9 92 94 93 04 df ff ca 0b 35 1d 85 12      [CK-.........5...]
 99 e9 bd bc e2 98 99 58 fe 6b 45 38 f0 52 b4 cb      [.......X.kE8.R..]
 a9 47 cd 22 aa ce 70 0e 4c 9b 48 a1 cf 0f 4a db      [.G."..p.L.H...J.]
 35 f5 1f 20 b7 68 cb 71 2c 27 01 84 d6 bf 4e d1      [5.. .h.q,'....N.]
 ba e1 b2 50 e7 f1 29 3a b4 85 3e ac d7 cb 3f 36      [...P..):..>...?6]
 96 65 30 13 27 48 84 f5 fe 88 03 4a d7 05 ed 72      [.e0.'H.....J...r]
 4b aa a5 62 e6 05 ac 3d 20 4b d6 c9 db 92 89 38      [K..b...= K.....8]
 b5 14 df 46 a3 8f 6b 05 c3 54 4d a2 83 d4 b7 02      [...F..k..TM.....]
 88 2d 58 e7 a4 86 1c 48 77 68 49 66 a1 35 3e c4      [.-X....HwhIf.5>.]
 71 20 aa 18 9d 9f 1a 38 52 3c e3 35 b2 19 12 ad      [q .....8R<.5....]
 99 ad ce 68 8b b0 d0 29 ba 25 fd 1e e0 5d aa 12      [...h...).%...]..]
 9c 44 89 63 89 62 e3 cb f3 5d 5f a3 7c b7 b9 ef      [.D.c.b...]_.|...]
 01 89 5b 33 35 a8 81 60 38 61 4e d8 4f 6a 53 70      [..[35..`8aN.OjSp]
 35 02 03 01 00 01                                    [5.....]
  Certificate signature (256 bytes):
 67 f6 12 25 3f d4 d2 dd 6a f7 3e 55 b8 9f 33 53      [g..%?...j.>U..3S]
 20 4d d1 17 54 08 8a 70 22 35 92 59 9c 03 9c 0f      [ M..T..p"5.Y....]
 ce 46 3c 06 74 d0 a9 8e b1 88 a2 35 b3 eb 1b 00      [.F<.t......5....]
 5c 6d bb 1d b5 ad 17 19 f2 c6 96 87 9b e7 15 01      [\m..............]
 b2 04 af 7d 92 60 d9 ee ef bc 60 4e 2e af 84 e2      [...}.`....`N....]
 42 fe 07 71 7e fc ee ee f5 d1 6d 71 e7 46 f0 97      [B..q~.....mq.F..]
 e0 e8 b3 0e f9 07 e0 de 6e 36 5a 56 1e 80 10 05      [........n6ZV....]
 59 d9 88 ba f7 a3 d1 f6 cd 00 12 9f 90 f0 65 83      [Y.............e.]
 e9 0f 76 a4 da eb 1b 1b 2d ea bd be a0 8a fb a7      [..v.....-.......]
 a5 18 ff 9f 5c e9 99 66 f0 d3 90 ae 49 3f c8 cc      [....\..f....I?..]
 32 6b db 64 da fd f5 42 ea bc f3 b0 8a 2f 17 d8      [2k.d...B...../..]
 cf c0 d8 d4 3a 41 ae 1d cf 7a c6 a6 a1 65 c2 94      [....:A...z...e..]
 8a ba ea d3 da 3e 8a 44 9b 47 35 10 ab 61 1b 4f      [.....>.D.G5..a.O]
 82 dd 59 16 d5 f2 1d f3 c2 08 cc 1c 7f ab be 9c      [..Y.............]
 be 52 73 ea e0 89 d7 6f 4d d0 d8 aa 3d 50 d6 b0      [.Rs....oM...=P..]
```

This table describes the significant fields shown in the display.

Table 5: show sam package Field Descriptions

Field	Description
Certificate Location	Location of the certificate; one of the following: **root**, **mem**, **disk0**, or **disk1**.
Certificate Index	Index number that the Software Authentication Manager (SAM) automatically assigns to the certificate.
Certificate Flag	One of the following: TRUSTED, VALIDATED, EXPIRED, or REVOKED.
Serial Number	Unique serial number of the certificate, assigned by its issuer.
Subject Name	Name of the entity for which the certificate is issued.
Issued By	Name of the entity that issued the certificate.

Field	Description
Version	ITU-T X.509 version of the certificate. The version can be 1 (X.509v1), 2 (X.509v2), or 3 (X.509v3).
Issuing Algorithm	Hash and public key algorithm that the issuer uses to sign the certificate.
Public Key	Subject public key for the certificate.
Certificate signature	Encrypted hash value (or signature) of the certificate. The hash value of the certificate is encrypted using the private key of the issuer.

Related Commands

Command	Description
show install	Displays the installed location and name of the software package. You can use the **all** keyword to display the active packages from all locations. For more information, see *System Management Command Reference for Cisco ASR 9000 Series Routers*.
show sam certificate, on page 10	Displays records in the SAM certificate table.

show sam sysinfo

To display current configuration settings for the Software Authentication Manager (SAM), use the **show sam sysinfo** command.

show sam sysinfo

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show sam sysinfo** command to determine the configuration settings of the SAM.

The display shows the status of the SAM, current prompt interval setting, and current prompt default response.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show sam sysinfo** command:

```
RP/0/RSP0/CPU0:router# show sam sysinfo

Software Authentication Manager System Information
==================================================
Status                  : running
Prompt Interval         : 10 sec
Prompt Default Response : NO
```

This table describes the significant fields shown in the display.

Table 6: show sam sysinfo Field Descriptions

Field	Description
Status	One of the following: running or not running. If the SAM is not running, the System Manager should detect that state and attempt to restart the SAM. If problems prevent the System Manager from restarting the SAM after a predefined number of repeated attempts, the SAM will not be restarted. In such a case, you should contact Cisco Technical Assistance Center (TAC) personnel.
Prompt Interval	Current setting for the prompt interval. The interval can be set in the range from 0 to 300 seconds. The value shown in the sample output (10 seconds) is the default.
Prompt Default Response	Current setting that specifies the action taken by the SAM if the prompt interval expires before the user responds to the prompt. If the user does not respond to the prompt, the SAM waits for the specified interval to expire and then takes the action specified in the **sam prompt-interval** command (either **proceed** keyword or **terminate** keyword). Entering the **sam promptinterval** command with the **proceed** keyword causes the **show sam sysinfo** command to display "Yes," meaning that the default action taken by the SAM is to wait for the prompt interval to expire and then respond as if it had received a "yes" from the user. Entering the **sam promptinterval** command with the **terminate** keyword causes the **show sam sysinfo** command to display "No," meaning that the default action taken by the SAM is to wait for the prompt interval to expire and then respond as if it had received a "no" from the user.

Related Commands

Command	Description
sam prompt-interval, on page 6	Sets the interval that the SAM waits after prompting the user for input when it detects an abnormal condition and determines how the SAM responds when it does not receive user input within the specified interval.