



Intel® Active Management Technology

Cisco* ACS Configuration Guide for Intel® AMT Posture Data

April 2008

Legal Notice

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. Intel products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

The Intel products discussed in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting www.intel.com.

Intel® is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

The following are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries:

Intel® Active Management Technology
Intel® AMT

*Other names and brands may be claimed as the property of others.
Copyright © 2006–2008 Intel Corporation. All rights reserved.

Cisco* ACS Configuration Guide for Intel® AMT Posture Data

Reference Guide for Network/IT Administrators

This document only describes the Intel® AMT Posture Plug-in specific attributes required for configuring the server side (for example, in a Cisco* ACS 4.0 product). It does not describe the configuration for Cisco ACS 4.0 posture validation, including Intel AMT posture validation. For this information, please refer to the *Cisco ACS Configuration Guide*.

Step 1: Install and configure Cisco ACS 4.0 server.

Step 2: Add Intel AMT posture specific AVPs to Cisco ACS 4.0. To accomplish this, the following items must be performed by the administrator:

- a. Go to the directory where the Cstutil tool for Cisco ACS 4.0 is installed. The typical directory command for this is:

```
cd %program files%\ciscosecure acs v4.0\bin\
```

- b. Use Cstutil to add Intel AMT posture AVPs by using the following command:

```
cstutil -addAVP attr.txt [attr.txt file is shown below.]
```

- c. Restart ACS using following commands:

```
net stop CSAdmin
net stop CSAuth
net stop CSLog
net start CSLog
net start CSAuth
net start CSAdmin
```

Step 3: After the Intel AMT posture AVPs have been added to Cisco ACS 4.0, the administrator should be able to use them to configure posture validation rules inside the ACS 4.0 web interface. Refer to the Cisco ACS 4.0 configuration guide for instructions on configuration of posture validation rules.

Intel AMT Attributes

The Cisco NAC Posture Plug-in for Intel® AMT shall provide the following data about Intel® Active Management Technology (the parameters are always in network order):

Attribute Number	Length (bytes)	Name	Details
32800	4	AMTPostureVersion	Posture version (always 01 00 00 00 in Intel AMT Release 2.5) (always 2 in Intel AMT Release 4.0 and 5.0)
32801	4	AMTTimeStamp	Time of posture creation (seconds since 1 January 1970)
32802	4	AMTPostureId	Value incremented on each posture request. Reset when firmware is reset.

Attribute Number	Length (bytes)	Name	Details
32803	4	AMTPostureSender	0=Host 1= Intel AMT
5	8	AMTVersion	Firmware code version
32804	4	AMTSecParams	Security parameters: BIT0: Operational Mode (0=SMB, 1=Enterprise) BIT1: TLS enabled (1=Enabled) BIT2: TLS remote mutual authentication enabled (1=Enabled) BIT3: TLS local mutual authentication enabled (1=Enabled) BIT4: TLS PSK enabled (1=Enabled) BIT5-BIT6: Provisioning State (0=Pre, 1=In, 2=Post) BIT7: Network Interface (1=Enabled) BIT8: Web UI (1=Enabled) BIT9: IDER State (1=Enabled) BIT10: SOL State (1=Enabled) BIT11: FW Update (1=Enabled)
32805	4	AMTHwInfo	BIT0: (1=Crypto enabled; 0=Crypto disabled)
32806	4	AMTCurrentBootDevice	Current boot device (0x00=authorized hard disk, 0x01=network, 0x02=New HDD, 3=Removable device, 0xFF=Boot device not supplied by BIOS)
32807	4	AMTAuthorizedBoots	Number of times the device has been booted from the primary ATA hard disk when the disk manufacturer's ID and serial number are the same as the previous saved boot data
32808	4	AMTNetworkBootCounter	Number of times the device has been booted from the network
32809	4	AMTHddBootCounter	Number of times the device has been booted from a new hard disk drive
32810	4	AMTRemovableBootCounter	Number of times the device has been booted from a removable disk
32811	4	AMTIdersessionState	IDER session state (1=session open; 0=closed)
32812	4	AMTIdersessionIPV4	Console IP address (relevant only when an IDER session is open; default is 0.0.0.0)
32813	2	AMTIdersessionPort	Console port (relevant only when an IDER session is open; default is 00 00.)
32814	64	AMTFqdn	Device FQDN
32815	16	AMTUuid	Device UUID
32816	4	AMTDigestMethodCode	Method for hashing the posture before signing it (0 = HMAC_SHA1)
32817	256	AMTSignature	An RSA-encrypted hash of selected AVPs in the posture, including the UUID and FQDN, but not including the time stamp. If there is no signature, the default value is 0.
32818	up to 256	AMTCertIssuerCode	Issuer of the certificate that the Intel AMT device used to sign the posture
32819	up to 20	AMTCertSerialNumCode	Serial number of the certificate that the Intel AMT device used to sign the posture. Default is 0.
32820	352	AMTAgentPresence	Counters and state of software agents configured for EAC. See below (Posture version 2 only)

Note: The information in this table corresponds to the attr.txt file below.

Agent Presence Attribute

Posture version 2 supports the AMTAgentPresence attribute. This attribute reports on the status of software agents running on the host that are monitored by the Intel AMT Agent Presence feature. The attribute is a fixed length of 352 bytes. It can contain up to 16 entries, each containing 22 bytes:

Agent GUID: 16 bytes

State counters: 5 bytes- each time an agent enters one of the listed states, the corresponding one-byte counter is incremented. The states are:

- Not started – 1 byte
- Running – 1 byte
- Expired – 1 byte
- Stopped – 1 byte
- Suspended – 1 byte

Current state: 1 byte. The valid values are:

0x1	Not started
0x2	Stopped
0x4	Running
0x8	Expired
0x10	Suspended

Intel AMT adds agent presence information to the posture for a selected agent only if the agent was configured with at least one state transition configured for “EAC Action.” Once one transition is so configured, Intel AMT maintains all of the state counters for that agent.

The attribute can report on up to 16 agents. An unused entry will have its GUID field set to zero. The populated entries may not be adjacent: there may be “holes” of unused entries dispersed between populated entries.

attr.txt File

```
[attr#0]
vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32800
attribute-name=AMTPostureVersion
attribute-profile=in out
attribute-type=unsigned integer
```

```
[attr#1]
vendor-id=343
```

vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32801
attribute-name=AMTTimeStamp
attribute-profile=in out
attribute-type=date

[attr#2]
vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32802
attribute-name=AMTPostureId
attribute-profile=in out
attribute-type=unsigned integer

[attr#3]
vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32803
attribute-name=AMTPostureSender
attribute-profile=in out
attribute-type=unsigned integer

[attr#4]
vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=5
attribute-name=AMTVersion
attribute-profile=in out
attribute-type=version

[attr#5]
vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32804
attribute-name=AMTSecParams
attribute-profile=in out

attribute-type=unsigned integer

[attr#6]

vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32805
attribute-name=AMTHwInfo
attribute-profile=in out
attribute-type=unsigned integer

[attr#7]

vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32806
attribute-name=AMTCurrentBootDevice
attribute-profile=in out
attribute-type=unsigned integer

[attr#8]

vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32807
attribute-name=AMTAuthorizedBoots
attribute-profile=in out
attribute-type=unsigned integer

[attr#9]

vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32808
attribute-name=AMTNetworkBootCounter
attribute-profile=in out
attribute-type=unsigned integer

[attr#10]

vendor-id=343
vendor-name=Intel
application-id=32770

```
application-name=Intel_AMT  
attribute-id=32809  
attribute-name=AMTHddBootCounter  
attribute-profile=in out  
attribute-type=unsigned integer
```

```
[attr#11]  
vendor-id=343  
vendor-name=Intel  
application-id=32770  
application-name=Intel_AMT  
attribute-id=32810  
attribute-name=AMTRemovableBootCounter  
attribute-profile=in out  
attribute-type=unsigned integer
```

```
[attr#12]  
vendor-id=343  
vendor-name=Intel  
application-id=32770  
application-name=Intel_AMT  
attribute-id=32811  
attribute-name=AMTIdersessionState  
attribute-profile=in out  
attribute-type=unsigned integer
```

```
[attr#13]  
vendor-id=343  
vendor-name=Intel  
application-id=32770  
application-name=Intel_AMT  
attribute-id=32812  
attribute-name=AMTIdersessionState  
attribute-profile=in out  
attribute-type=ipaddr
```

```
[attr#14]  
vendor-id=343  
vendor-name=Intel  
application-id=32770  
application-name=Intel_AMT  
attribute-id=32813  
attribute-name=AMTIdersessionState  
attribute-profile=in out  
attribute-type=octet-array
```

```
[attr#15]
vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32814
attribute-name=AMTFqdn
attribute-profile=in out
attribute-type=string
```

```
[attr#16]
vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32815
attribute-name=AMTUuid
attribute-profile=in out
attribute-type=octet-array
```

```
[attr#17]
vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32816
attribute-name=AMTDigestMethodCode
attribute-profile=in out
attribute-type=unsigned integer
```

```
[attr#18]
vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32817
attribute-name=AMTSignature
attribute-profile=in out
attribute-type=octet-array
```

```
[attr#19]
vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32818
```

attribute-name=AMTCertIssuerCode
attribute-profile=in out
attribute-type=octet-array

[attr#20]
vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32819
attribute-name=AMTCertSerialNumCode
attribute-profile=in out
attribute-type=octet-array

[attr#21]
vendor-id=343
vendor-name=Intel
application-id=32770
application-name=Intel_AMT
attribute-id=32820
attribute-name=AMTAgentPresence
attribute-profile=in out
attribute-type=octet-array