

Cisco ACS Certificate Configuration for Intel AMT

Affects: Cisco ACS, v 4.x

PCs with Intel AMT v 4.0 or higher

Problem(s) summary: 802.1x authentication fails

Problem 1: In secured networks such as 802.1x or Cisco NAC, when the Intel AMT-enabled PC connects to the network and tries to communicate with the RADIUS Server (Cisco ACS), it will attempt 802.1x authentication with ACS; however, if the server certificate doesn't have a server authentication object ID (OID), authentication fails.

Problem 2: Cisco requires that subordinate Certificate Authorities (CAs) in the chain of trust be trusted as root CAs.

Problem 1 Description

In PCs with Intel AMT v4.0 or higher, the Intel Management Engine requires that the server certificate includes a server authentication object ID (OID). (Previous versions of Intel AMT did not require this OID.) If the certificate being used does not have a server authentication OID, then 802.1x authentication fails.

The problem is difficult to diagnose because Intel AMT-enabled PCs v3.x or lower can perform successful 802.1x authentication with ACS even if authentication with 4.x systems in the same environment fails. (Previous versions of Intel AMT do not require a server authentication OID.)

It can also be difficult to identify the kind of certificate ACS has been configured with, and difficult to identify which certificate is being pulled, for several reasons:

- ACS pulls certificates from the machine's trusted-root storage. Even if you know to troubleshoot by looking in the server's personal storage for the certificate used for authentication, you will not find it.
- ACS does not display detailed information about the certificate it has been configured to use.
- You cannot open a crypto shell from within ACS in order to look for the required certificate.
- When multiple certificates are installed, ACS does not let you select a certificate from the list. ACS will use the first certificate that has the subject name matching the Fully Qualified Domain Name (FQDN) of the ACS machine.

Problem 1 Troubleshooting

When troubleshooting to identify this certificate configuration issue, look for the following error messages.

The ACS failed-attempts log will show an error similar to this:

EAP-TLS or PEAP authentication failed during SSL handshake.

The ACS authentication log (`c:\Program Files\Cisco ACS\CSAuth\Vogs\auth.log`) will list an error similar to this:

```
AUTH 07/18/2008 14:16:17 I 0928 2940 AuthenProcessResponse: process
response for 'ent\chaosxp$iME' AUTH 07/18/2008 14:16:17 E 0381 2940
EAP: EAP-FAST: ProcessResponse: invalid TLS data size received: 0
AUTH 07/18/2008 14:16:17 I 0381 2940 EAP: EAP-FAST: Second phase: 0
authentication FAILED
```

Problem 1 Solution

To resolve this problem, you will have to make sure the certificate being used includes a server authentication OID. You must then load that certificate into the trusted-root store, and make sure it will be the first certificate found during 802.1x authentication. Because of the way ACS loads its certificates, this is not a trivial procedure.

Note: Do **not** follow this procedure for ACS servers that are already a CA.

In the following steps, you will configure ACS to use a certificate with a server authentication OID.

1. Delete all certificates with a subject matching the ACS server's subject name from the trusted-root machine store.
2. Request a certificate from a CA that contains the server authentication OID. Place that non-root certificate in the trusted-root machine store.
3. From the ACS console, reinstall the ACS certificate by pulling a certificate from the local store. ACS will pull the desired certificate because it will be the only one matching the subject name in the trusted-root machine store. ACS uses the first matching certificate it finds, which will now be the one you just installed.
4. Re-add any of the deleted certificates to the trusted-root store.
5. Reconfigure the global authentication setup and trusted-root CAs within ACS. These will be unconfigured due to the certificate change, and must be set up again.

ACS should now be configured with a known certificate that has the required properties for 802.1x authentication for communication with Intel AMT.

Problem 2 Description

Cisco ACS requires that subordinate Certificate Authorities (CAs) in the chain of trust be trusted as root CAs. When ACS is configured with only a trusted root certificate in a PKI hierarchy, and a client attempts to authenticate with a certificate that is issued by a subordinate CA in the certificate hierarchy, 802.1x authentication can fail.

Background: Certificate hierarchies exist to avoid the need to trust multiple CAs by allowing a machine to trust only the root CA. In a typically or properly configured multi-level PKI implementation, the trusted-root CA is stored in the trusted-root store. Typical PKI implementations do not require that an application trust subordinate CAs as trusted-root CAs.

CAs and Cisco ACS: In environments using a PKI hierarchy that is internal to a customer's network, Cisco ACS requires that all subordinate, non-root CAs in a certificate chain be trusted as root CAs.

Problem 2 Troubleshooting

When troubleshooting to identify this certificate configuration issue, look for the following error messages.

Note that ACS does not log the authentication failure in the ACS failed-attempts log. This makes it appear as if the Intel ME is not trying 802.1x authentication, and that the problem is a missing CA.

Details about the failed attempt can be found in the ACS authentication log (*c:\Program Files\Cisco ACS\CSAuth\logs\auth.log*). There will be an entry for the client's Security Account Manager (SAM) account name (i.e. hostname\$iME) and an error message stating "*Unknown CA.*"

Solution 2

Configure ACS to trust all subordinate certificates in the certificate chain. Refer to your Cisco ACS documentation for information about marking the certificate chain as trusted.