

Enable HTTPS with SSL Certificate services Configuration for Cisco Secure ACS Admin Sessions

Document ID: 64049

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Procedures

- Install the Microsoft Certificate (CA) Server
- Create a Server Certificate
- Create a New Certificate Template
- Approve the Certificate from the CA
- Download the Server Certificate to the ACS Server
- Install the CA Certificate on the ACS Server
- Setup ACS to Use the Server Certificate
- Create and Install a Self-Signed Certificate
- Turn on HTTPS for Admin Sessions

Verify

- Failed to create 'CertificateAuthority.Request' object Error Message
- Loading...

Troubleshoot

Related Information

Introduction

By default, Cisco Secure Access Control Server (ACS) uses HTTP for its administrative sessions. This sample configuration discusses:

- use of HTTPS for accessing the Cisco Secure ACS HTML interface
- certificate configuration (which is required before you can enable HTTPS)

This document was originally written to accommodate certificates created with a Microsoft Certificate Authority (CA), but has been updated to add steps for using a self-signing certificate, which is supported as of ACS 3.3. The use of a self-signing certificate streamlines setup considerably because the external CA is not required.

Note: If you wish to use a self-signing certificate, go to the Create and Install Self-Signed Certificate (only if not using an external CA) section of this document.

Note: If you use outside vendor certificate services, be sure that you obtain the proper certificate for your web server from vendors like Verisign. Different certificates might be offered for Microsoft IIS and Apache.

Prerequisites

Requirements

You should open a local admin session before enabling HTTPS. Keep this session open after you enable it. Test the connection with a remote session so that if it does not work (for whatever reason), you are able to deselect the Use HTTPS Transport for Administration Access option. Once you have verified this, you can close the local session.

Components Used

The information in this document is based on these software and hardware versions:

- ACS 3.1.1 or later required
- Microsoft CA Server
- Internet Information Server (IIS) (must be installed before you install the CA)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Procedures

In this section, you are presented with the information to install the Microsoft CA Server.

Install the Microsoft Certificate (CA) Server

Complete these steps:

1. Choose **Start > Settings > Control Panel**.
2. Inside the Control Panel, open **Add/Remove Programs**.
3. In Add/Remove Programs, select **Add/Remove Windows Components**.
4. Choose **Certificate Services**.
5. Click **Next**.
6. Click **Yes** to the IIS message.
7. Choose a stand-alone (or Enterprise) root CA.
8. Click **Next**.
9. Name the CA.

Note: All the other boxes are optional.

Note: Avoid giving the CA the same name as the ACS server. This can cause the PEAP clients to fail authentication because they become confused when a root CA certificate is found with the same name as the server certificate. This problem is not unique to Cisco clients. If you do not plan to use PEAP, this does not apply.

10. Click **Next**.
11. The database default is correct.
12. Click **Next**.

IIS must be installed before you install the CA.

Create a Server Certificate

Complete these steps:

1. From your ACS server, browse to the CA (http://IP_of_CA_server/certsrv/).
2. Check the **Request a certificate** box.
3. Click **Next**.
4. Choose **Advanced request**.
5. Click **Next**.
6. Choose **Submit a certificate request to this CA using a form**.
7. Click **Next**.
8. Type a name in the name (CN) box.
9. For Intended Purpose, choose **Server Authentication Certificate**.

Note: If you use the Enterprise CA, choose **Web Server** from the first drop-down list.

10. Choose these under Key Option to create a new template:

- ◆ **CSP Microsoft Base Cryptographic Provider v1.0**
- ◆ **Key Size;024**

Note: Certificates created with a key size greater than 1024 might work for HTTPS but do not work for PEAP.

Note: The Windows 2003 Enterprise CA allows key sizes greater than 1024, but using a key larger than 1024 does not work with PEAP. Authentication might appear to pass in ACS, but the client just hangs while the authentication is attempted.

- ◆ **Keys as Exportable**

Note: Microsoft has changed the Web Server template with the release of the Windows 2003 Enterprise CA. With this template change, keys are no longer exportable, and the option is greyed out. There are no other certificate templates supplied with certificate services that are for server authentication, or that give the ability to mark keys as exportable in the drop-down menu. In order to create a new template that does so, see the Create a New Certificate Template section.

- ◆ **Use Local Machine Store**

Note: All other choices should be left as default.

11. Click **Submit**.
12. You should get this message: **Your certificate request has been received**.

Create a New Certificate Template

Complete these steps:

1. Choose **Start > Run > certmpl.msc**.
2. Right-click **Web Server template**.
3. Choose **Duplicate Template**.
4. Give the template a name, such as ACS.
5. Click the **Request Handling** tab.
6. Choose **Allow private key to be exported**.
7. Click the **CSPs** button.
8. Choose **Microsoft Base Cryptographic Provider v1.0**.
9. Click **OK**.

Note: All other options should be left as default.

10. Click **Apply**.
11. Click **OK**.
12. Open the CA MMC snap-in.
13. Right-click **Certificate Templates**.
14. Choose **New > Certificate Template to Issue**.
15. Choose the new template you created.
16. Click **OK**.
17. Restart the CA.

The new template is included in the Certificate Template drop-down list.

Approve the Certificate from the CA

Complete these steps:

1. Choose **Start > Programs > Administrative Tools > Certificate Authority**.
2. On the left windowpane, expand the certificate.
3. Choose **Pending Requests**.
4. Right-click on the certificate.
5. Choose **all tasks**.
6. Choose **Issue**.

Download the Server Certificate to the ACS Server

Complete these steps:

1. From your ACS server, browse to the CA (http://IP_of_CA_server/certsrv/).
2. Choose **Check on a Pending Certificate**.
3. Click **Next**.
4. Select the certificate.
5. Click **Next**.
6. Click **Install**.

Install the CA Certificate on the ACS Server

Note: These steps are not required if ACS and the CA are installed on the same server.

Complete these steps:

1. From your ACS server, browse to the CA (http://IP_of_CA_server/certsrv/).
2. Choose **Retrieve the CA certificate or certificate revocation list**.
3. Click **Next**.
4. Choose **Base 64 encoded**.
5. Click **Download CA certificate**.
6. Click **Open**.
7. Click **Install certificate**.
8. Click **Next**.
9. Choose **Place all certificates in the following store**.
10. Click **Browse**.
11. Check the **Show physical stores** box.
12. On the left windowpane, expand **Trusted root certification authorities**.
13. Choose **Local Computer**.

14. Click **OK**.
15. Click **Next**.
16. Click **Finish**.
17. Click **OK** on the import was successful box.

Setup ACS to Use the Server Certificate

Complete these steps:

1. On the ACS server, choose **System Configuration**.
2. Choose **ACS Certificate Setup**.
3. Choose **Install ACS certificate**.
4. Choose **Use certificate from storage**.
5. Type in the CN name (the same name that was used in Step 8 of the Create a Server Certificate section).
6. Click **Submit**.
7. On the ACS server, click **system configuration**.
8. Choose **ACS Certificate Setup**.
9. Choose **Edit Certificate Trust List**.
10. Check the box for the CA.
11. Click **Submit**.

Create and Install a Self-Signed Certificate

Note: This section only applies if you are not using an external CA.

Complete these steps:

1. On the ACS server, click **System Configuration**.
2. Click **ACS Certificate Setup**.
3. Click **Generate Self-signed Certificate**.
4. Type the certificate subject in the form cn=XXXX. In this example, cn=ACS33 is used. For more self-signed certificate configuration options, refer to System Configuration: Authentication and Certificates.
5. Type the full path and name of the certificate to be created in the Certificate file box. For example, c:\acscerts\acs33.cer.
6. Type the full path and name of the private key file to be created in the Private key file box. For example, c:\acscerts\acs33.pvk.
7. Enter and confirm the private key password.
8. Choose **1024** from the key length drop-down list.

Note: While the ACS can generate key sizes greater than 1024, using a key larger than 1024 does not work with PEAP. Authentication might appear to pass in ACS, but the client hangs while authentication is attempted.

9. From the Digest to sign with list, choose the hash digest to be used to encrypt the key. In this example, the digest to sign with at SHA1 is used.
10. Check **Install generated certificate**.
11. Click **Submit**.

Turn on HTTPS for Admin Sessions

Complete these steps:

1. Choose **Administration Control > Access Policy**.
2. Check the **Use HTTPS Transport for Administration Access** box.
3. Click **Submit**.

You should now be able to open a session to `https://IP_of_ACS:2002`. You are prompted for a login.

Note: You should open a local admin session before you enable HTTPS. Keep this session open after you enable it. Test the connection with a remote session so that if it does not work (for whatever reason), you are able to deselect the **Use HTTPS Transport for Administration Access** option. Once you verify this, you can close the local session.

Note: If you do happen to lock yourself out, you can hack the registry to turn off HTTPS for admin sessions. In order to do this, you need to change the registry key from a value of two to a value of one. For example, `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv3.2\CSAdmin\Config\HT`
`TPSSupport`.

Verify

Failed to create 'CertificateAuthority.Request' object Error Message

This section provides information you can use to confirm your configuration is working properly.

Complete these steps:

1. Choose **Start > Administrative Tools > IIS**.
2. Choose **Web Sites > Default Web Site**.
3. Right-click **CertSrv**.
4. Choose **Properties**.
5. Click the **Configuration** button in the Application settings section of the **Virtual Directory** tab.
6. Click the **Options** tab.
7. Choose **Enable session state**.

Note: All other options should be left as default.

8. Click **OK**.
9. Click **OK**.
10. Restart IIS.

If your browser locks with a Downloading ActiveX Control message, refer to this article on the Microsoft Web site: Internet Explorer Stops Responding at "Downloading ActiveX Control" Message When You Try to Use a Certificate Server .

Loading...

If the CSP field state is "Loading....," make sure you are not running a software firewall on the machine submitting the request. ZoneLabs' ZoneAlarm can cause this issue. Other software can also cause this issue.

Troubleshoot

There is no troubleshooting information available at this time.

Related Information

- [ACS Solution Engine \(Appliance\) for HTTPS Management Configuration Example](#)
 - [Cisco Secure ACS for Windows Support Page](#)
 - [Technical Support – Cisco Systems](#)
-

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Mar 29, 2007

Document ID: 64049
