Wired Dot1x Version 1.05 Configuration Guide

Document ID: 64068

Contents

Introduction

This document provides a sample configuration for wired dot1x version 1.05.

This guide covers certificates created with a Microsoft CA and self−signing certificates, which are supported as of Access Control Server (ACS) 3.3. Using a self−signing certificate streamlines initial PEAP installation considerably since no external CA is required. At this time, the default expiration period of the self−signing certificate is only one year and cannot be changed. This is fairly standard when it comes to server certificates, but since the self−signed certificate also acts as the root CA certificate, this can mean installing the new certificate on every client, every year when using the Microsoft supplicant (unless you do not select the Validate Server Certificate option). It is recommend that you use a self−signing certificates only as a temporary measure until a traditional CA can be used. If you wish to use a self−signing certificate, see the section.

802.1x was designed to authenticate hosts on a wired network instead of actual users. Attempting to authenticate users via 802.1x on a wired network may result in undesired behavior such as an 802.1x authenticated user not being logged off the network until the NIC card releases the port.

Prerequisites

Requirements

Before attempting this configuration, ensure that you meet these requirements:

- switches running Cisco IOS® Software Release 12.1(12c)EA1 and later (EI only) or CatOS 6.2 and later
- ACS 3.2
- Windows 2000 SP3 (with hotfix), SP4, or XP SP1

Components Used

This document is not restricted to specific software and hardware versions.

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

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Microsoft Certificate Services Installation

In this section, you are presented with the information to configure the features described in this document.

Note: Internet Information Server (IIS) must be installed before you install the CA. Avoid giving the CA the same name as an ACS server; doing so may cause PEAP clients to fail authentication because they get confused when a root CA certificate is found with the same name as the server certificate. This problem is not unique to Cisco clients.

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, choose **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. Of course, if you do not plan on using 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.

ACS for Windows Certificate Setup

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 are using 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 may work for HTTPS but will 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 will just hang while attempting authentication.
    - **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.

Set Up 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**.

ACS Appliance Certificate Setup

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 attempting authentication.
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**.

Create a Server Certificate Using CSR

Complete these steps:

1. From your FTP server, browse to the CA (http://IP_of_CA_server/certsrv/).
2. Choose **Request a certificate**.
3. Click **Next**.
4. Choose **Advanced request**.
5. Click **Next**.
6. Choose **Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**.
7. Paste the output from Step 6 into the **Base64 Encoded Certificate Request** field.
8. Click **Submit**.
9. Click **Download CA certificate**.
10. Click **Save**.
11. Name the certificate.
12. Save the certificate to your FTP directory

Download CA Certificate to the FTP Server

Complete these steps:

1. From your FTP 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 **Save**.
7. Name the certificate.
8. Save the certificate to your FTP directory

Install the CA Certificate on the Appliance

Complete these steps:

1. Choose **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.
2. Click **Download CA certificate file**.
3. In the FTP Server field, enter the IP address or hostname of the FTP server
4. In the Login field, enter a valid username that Cisco Secure ACS can use to access the FTP server.
5. Iin the Password field, enter user's password.
6. In the Remote FTP Directory field, enter the relative path from the FTP server root directory to the directory containing the CA certificate file.

7. In the Remote FTP File Name field, enter the name of the CA certificate file.
8. Click **Submit**.
9. Verify the filename in the field.
10. Click **Submit**.
11. Choose **System Configuration > Service Control** to restart the ACS services.

Configure Global Authentication Settings

Complete these steps:

1. On the ACS server, click **System Configuration**.
2. Click **Global Authentication Setup**.

Complete these steps for ACS v3.2 and later:

1. Check the **Allow EAP−MSCHAPv2 if using Microsoft PEAP** box.
2. Check the **Allow EAP−GTC if using Cisco PEAP** box.
3. Check the **Allow MS−CHAP Version 1 Authentication** box.
4. Check the **Allow MS−CHAP Version 2 Authentication** box.
5. Click **Submit**.

Complete these steps for ACS v3.1 and later:

1. Check the **Allow PEAP** box.
2. Check the **Allow MS−CHAP Version 1 Authentication** box.
3. Check the **Allow MS−CHAP Version 2 Authentication** box.
4. Click **Submit**.

Set Up the ACS to Allow Machine Authentication

Complete these steps:

1. Choose **External User Databases > Database Configuration**.
2. Click **Windows Database**.
3. Click **Configure**.
4. Check the **Permit PEAP machine authentication** box.
5. Click **Submit**.

Set Up the AP on the ACS

Complete these steps to set up the AP on the ACS:

1. On the ACS server, click **Network Configuration** on the left.
2. To add a AAA client, click **Add Entry**.
3. Enter these values in the boxes:

    - AAA Client IP Address IP_of_your_AP
    - Key Make up a key (make sure the key matches the AP shared secret key)
    - Authenticate Using RADIUS (Cisco Aironet)
4. Click **Submit**.
5. Restart.

Configure the Switch for Dot1x

Refer to these documents for dot1x configuration:

- Catalyst 2950
- Catalyst 3550
- Catalyst 4500
- Catalyst 6500

Dot1x Timers Configuration

Complete these steps to configure the dot1x timers as RADIUS A/V pairs:

- Configure the Session−Timeout RADIUS attribute (Attribute [27]) which specifies the time after which reauthentication occurs.
- Configure the Termination−Action RADIUS attribute (Attribute [29]) which specifies the action to be taken during reauthentication. When the attribute value is set to Default, the IEEE 802.1X session ends, and connectivity is lost during reauthentication. When the attribute value is set to RADIUS−Request, the session is not affected during reauthentication.

Note: The values for attributes 27 and 29 can be assigned on a per−group basis, under the RADIUS (IETF) section. Set attribute 27 to the reauthentication period, and 29 to RADIUS−request.

On the switch, perform this configuration for the switch to accept the values of RADIUS attributes from the RADIUS server:

```
(config−if)#dot1x reauthentication
(config−if)#dot1x timeout reauth−period server
```

Set Up the Client for PEAP with Machine Authentication

Join the Domain

Complete these steps:

Note: In order to complete this step, the computer must have one of these connections to the CA:

- wired connection
- wireless connection with 802.1x security disabled

1. Log in to Windows XP with an account that has administrator privileges.
2. Right−click on **My Computer**.
3. Choose **Properties**.
4. Click the **Computer Name** tab.
5. Click **Change**.
6. In the Computer name field, enter the hostname.
7. Choose **Domain**.
8. Enter the name of the domain.
9. Click **OK**.
10. A login dialog is displayed. Log in with an account that has permission to join the domain.
11. Once the computer has successfully joined the domain, restart the computer. The machine becomes member of the domain, has a certificate for the CA installed, and a password for machine authentication is automatically generated.

If the client joined the domain prior to the installation of the CA, or the CA certificate was not installed on the client, complete these steps:

Note: The need for this is indicated by authentication failures often (but not always) with errors such as `Authentication failed during SSL handshake`.

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 the certificate.
13. Choose **Local Computer**.
14. Click **OK**.
15. Click **Next**.
16. Click **Finish**.
17. Click **OK** on the import was successful box.

Set Up XP SP1 for PEAP with Machine Authentication

Complete these steps:

1. Choose **Start > Control Panel > Network Connections**.
2. Choose **Properties**.
3. Click the **Authentication** tab.
4. Check the **enable IEEE 802.1x...** box.
5. For EAP type, choose **Protected EAP**.
6. Click **Properties**.
7. Check the **Authenticate as computer....** box.
8. Choose **Properties**.
9. Check the box for the CA
10. Click **OK**.
11. Click **OK**.

Set Up Windows 2000 for PEAP Machine Authentication

Complete these steps:

1. If you are running SP3, download and install the 802.1x hotfix: http://support.microsoft.com/default.aspx?kbid=313664 . This is not required for SP4.
2. Choose **Start > Settings > Control Panel > Network and Dial−up Connections**.
3. Right−click the network connection.
4. Choose **Properties**.
5. Click the **Authentication** tab.
6. Choose **Enable network access control using IEEE 802.1x**.
7. Choose **Protected EAP (PEAP)** from the EAP type drop−down list.
8. Check the **Authenticate as computer...** box.
9. Choose **Properties**.

10. Check the box for the CA
11. Click **OK**.
12. Click **OK**.

Note: If there is no **Authentication** tab, the 802.1X service is installed in a disabled state. In order to solve this, you must enable the **Wireless Configuration** service in the list of services.

Note: If the **Authentication** tab is present, but is unavailable, this indicates that the network adapter driver does not support 802.1x correctly. Check the 802.1x hotfix page or the vendor's website for supported drivers.

Complete these steps to enable the wireless configuration:

1. Right−click **My Computer**.
2. Click **Manage**.
3. Click **Services and Applications**.
4. Click **Services**.
5. Set the startup value for the service to Automatic.
6. Start the service.

Dynamic VLAN Assignment for 802.1x and ACS

This option is supported in IOS 12.1(12c)EA1 (EI only) or 12.1(14)EA1 or CatOS 7.2 and later

Note: 802.1x was designed to authenticate hosts on a wired network instead of actual users. Attempting to authenticate users via 802.1x on a wired network may result in undesired behavior such as the dynamic VLAN assignment assigned to a user not being changed until the NIC card releases the port (computer is restarted or powercycled).

Complete these steps:

1. Choose **Interface Configuration > RADIUS (IETF)**.
2. Check the **[064] Tunnel−Type for user/group** box.
3. Check the **[065] Tunnel−Medium−Type for user/group** box.
4. Check the **[081] Tunnel−Private−Group−ID for user/group** box.
5. Click **Submit**.
6. Choose **user/group setup**.
7. Check the **[064] Tunnel−Type** box.
8. Choose **1** from the Tag drop−down list.
9. Choose **VLAN** for the Value drop−down list.
10. Choose **0** for all subsequent Tag drop−down lists.
11. Check the **[065] Tunnel−Medium−Type** box.
12. Choose **1** from the Tag drop−down list.
13. Choose **802** from the Value drop−down list.
14. Choose **0** for all subsequent Tag drop−down lists.
15. Check the **[081] Tunnel−Private−Group−ID** box.
16. Choose **1** from the Tag drop−down list.
17. Use the name of the VLAN that needs to be pushed. It can be the default name and is found by issuing the **show vlan** command.
18. Choose **0** for all subsequent Tag drop−down lists.
19. Click **Submit**.

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 website: Internet Explorer Stops Responding at "Downloading ActiveX Control" Message When You Try to Use a Certificate Server .

Troubleshoot

Problem

The switch fails to contact the secondary ACS server when the primary ACS server goes down at Dot1x authentication; this error occurs:`"Authen session timed out: Challenge not provided by client."`

Solution

This error occurs when the dead−timer is not configured on the switch, which causes the switch to continue to try the primary server that is down. This causes the authentication to fail. In order to resolve this problem, configure the dead−timer on the switch so that the switch contacts the secondary ACS server after it waits for the configured time (in seconds) or the number of retries to reach the primary server before considers the primary server to be declared dead or unavailable. Now authentication succeeds with the secondary server, which is active. The dead−time can be configured with this command: **radius−server dead−criteria [time seconds [tries number] | tries number** in global configuration mode.

Related Information

- **Cisco Secure Access Control Server for Unix**
- **Cisco Secure Access Control Server for Windows**
- **Identify−Based Networking Systems Configuration Guide**
- **Technical Support & Documentation − Cisco Systems**

Updated: May 14, 2009 Document ID: 64068