

# Catalyst 3550系列交換機和ACS 4.2版上的802.1x有線身份驗證配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[交換機配置示例](#)

[ACS配置](#)

[驗證](#)

[疑難排解](#)

## 簡介

本檔案將提供思科存取控制伺服器(ACS)版本4.2和用於有線驗證的遠端存取撥入使用者服務(RADIUS)通訊協定的基本IEEE 802.1x組態範例。

## 必要條件

### 需求

思科建議您：

- 確認ACS和交換機之間的IP可達性。
- 確保ACS和交換機之間的使用者資料包協定(UDP)埠1645和1646處於開啟狀態。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Catalyst 3550 系列交換器
- Cisco安全ACS版本4.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

# 設定

## 交換機配置示例

1. 若要定義RADIUS伺服器 and 預先共用金鑰，請輸入以下命令：

```
Switch(config)# radius-server host 192.168.1.3 key cisco123
```

2. 若要啟用802.1x功能，請輸入以下命令：

```
Switch(config)# dot1x system-auth-control
```

3. 若要全域性啟用身份驗證、授權和記帳(AAA)以及RADIUS身份驗證和授權，請輸入以下命令：

註：如果需要從RADIUS伺服器傳遞屬性，則必須執行此操作；否則，您可以跳過它。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(Config)# aaa authorization network default group radius
Switch(Config)# aaa accounting dot1x default start-stop group radius
```

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan
Switch(config-if)# authentication port-control auto (12.2.50 SE and later)
Switch(config-if)# dot1x port-control auto (12.2.50 SE and below)
Switch(config-if)# dot1x pae authenticator (version 12.2(25)SEE and below)
Switch(config-if)# dot1x timeout quiet-period
Switch(config-if)# dot1x timeout tx-period
```

## ACS配置

1. 要在ACS中將交換機新增為AAA客戶端，請導航到Network Configuration > Add entry AAA client，然後輸入以下資訊：  
IP地址:<IP>共用金鑰:<key>驗證使用：Radius(Cisco IOS<sup>®</sup>/PIX 6.0)

**Network Configuration**

AAA Client Hostname: switch  
 AAA Client IP Address: 192.168.1.2  
 Shared Secret: cisco123

**RADIUS Key Wrap**  
 Key Encryption Key:   
 Message Authenticator Code Key:   
 Key Input Format:  ASCII  Hexadecimal

Authenticate Using: RADIUS (Cisco IOS/PIX 6.0)

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client
- Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Right sidebar text:  
 You can use the wildcard asterisk (\*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.\* in the AAA Client IP Address box.  
 You can define ranges within an octet of an IP address. For example, if you want every AAA client with an IP address between 192.168.13.12 and 192.168.13.221 to be represented by a single AAA client entry, enter 192.168.13.12-221 in the AAA Client IP Address box.  
[\[Back to Top\]](#)  
**Shared Secret**  
 The Shared Secret is used to encrypt TACACS+ or the RADIUS AAA client and ACS. The shared secret must be configured in the AAA client and ACS identically, including case sensitivity.  
[\[Back to Top\]](#)  
**Network Device Group**  
 From the list, click the name of the Network Device Group (NDG) to which this AAA client belongs.  
 Note: To enable NDGs, click **Interface Configuration > Advanced Options > Network Device Groups**.  
[\[Back to Top\]](#)  
**RADIUS Key Wrap**

2. 要配置身份驗證設定，請導航到 **System Configuration > Global Authentication Setup**，然後驗證 **Allow MS-CHAP Version 2 Authentication** 竅取方塊是否已選中：

**System Configuration**

EAP-TLS session timeout (minutes): 120

Select one of the following options for setting username during authentication:  
 Use Outer Identity  
 Use CN as Identity  
 Use SAN as Identity

**LEAP**  
 Allow LEAP (For Aironet only)

**EAP-MD5**  
 Allow EAP-MD5

AP EAP request timeout (seconds): 20

**MS-CHAP Configuration**

- Allow MS-CHAP Version 1 Authentication
- Allow MS-CHAP Version 2 Authentication

[Back to Help](#)

Right sidebar text:  
 Use this page to specify settings for various authentication protocols.  

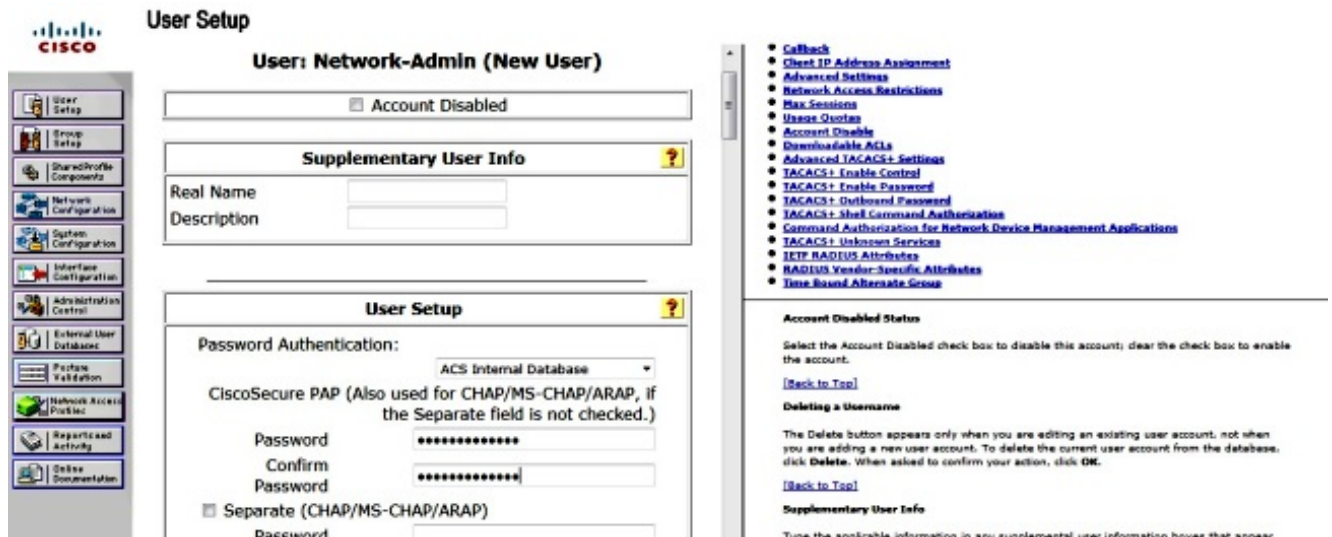
- [EAP Configuration](#)
- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP EAP Request Timeout](#)
- [MS-CHAP Configuration](#)

---

**EAP Configuration**  
 EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of another protocol such as UDP, 802.1x or RADIUS and supports multiple "authentication" types.  
[\[Back to Top\]](#)  
**PEAP**  
 PEAP is the outer layer protocol for the secure tunnel.  
 Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the **ACS Certificate Setup page**.  

- **Allow EAP-MSCHAPv2** — Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS-CHAPv2, such as Microsoft AD, and the ACS Internal Database.
- **Allow EAP-GTC** — Use to enable EAP-GTC within Cisco PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.
- **Allow System Validation** — Use to enable the SPAP (PAP-TLV) method for system validation of

3. 要配置使用者，請按一下選單上的 **User Setup**，然後完成以下步驟：  
 輸入 **User information: Network-Admin <username>**。按一下「**Add/Edit**」。輸入 **Real Name: Network-Admin <descriptive name>**。新增 **說明: <您的選擇>**。選擇 **Password Authentication: ACS Internal Database**。輸入 **密碼: ..... <password>**。確認 **Password: <password>**。按一下「**Submit**」。



## 驗證

[輸出直譯器工具](#)(僅供已註冊客戶使用)支援某些show命令。使用Output Interpreter工具檢視show指令輸出的分析。

輸入以下命令以確認您的組態是否正常運作：

- show dot1x
- show dot1x summary
- show dot1x interface
- show authentication sessions interface <interface>
- show authentication interface <interface>

```
Switch(config)# show dot1x
```

```
Sysauthcontrol Enabled
Dot1x Protocol Version 3
```

```
Switch(config)# show dot1x summary
```

```
Interface PAE Client Status
```

```
Fa0/4 AUTH
```

```
Switch(config)# show dot1x interface fa0/4 detail
```

```
Dot1x Info for FastEthernet0/4
```

```
PAE = AUTHENTICATOR
PortControl = FORCE_AUTHORIZED
ControlDirection = Both
HostMode = SINGLE_HOST
QuietPeriod = 5
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 10
```

# 疑難排解

本節提供可用於對組態進行疑難排解的偵錯命令。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

- debug dot1x all
- 調試全部身份驗證
- debug radius ( 提供偵錯層級的radius資訊 )
- debug aaa authentication ( 調試以進行身份驗證 )
- debug aaa authorization(debug for authorization)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。