

# NAC (CCA): Configure Authentication on the Clean Access Manager (CAM) with ACS

Document ID: 107396

---

## Introduction

### Prerequisites

- Requirements
- Components Used
- Conventions

### Configure

- Network Diagram
- Steps to Configure Authentication on CCA with ACS
- ACS Configuration

### Verify

### Troubleshoot

### NetPro Discussion Forums – Featured Conversations

### Related Information

---

## Introduction

This document describes how to configure the authentication on the Clean Access Manager (CAM) with Cisco Secure Access Control Server (ACS).

## Prerequisites

### Requirements

This configuration is applicable to CAM version 3.5 and later.

### Components Used

The information in this document is based on CAM version 4.1.

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.

## Configure

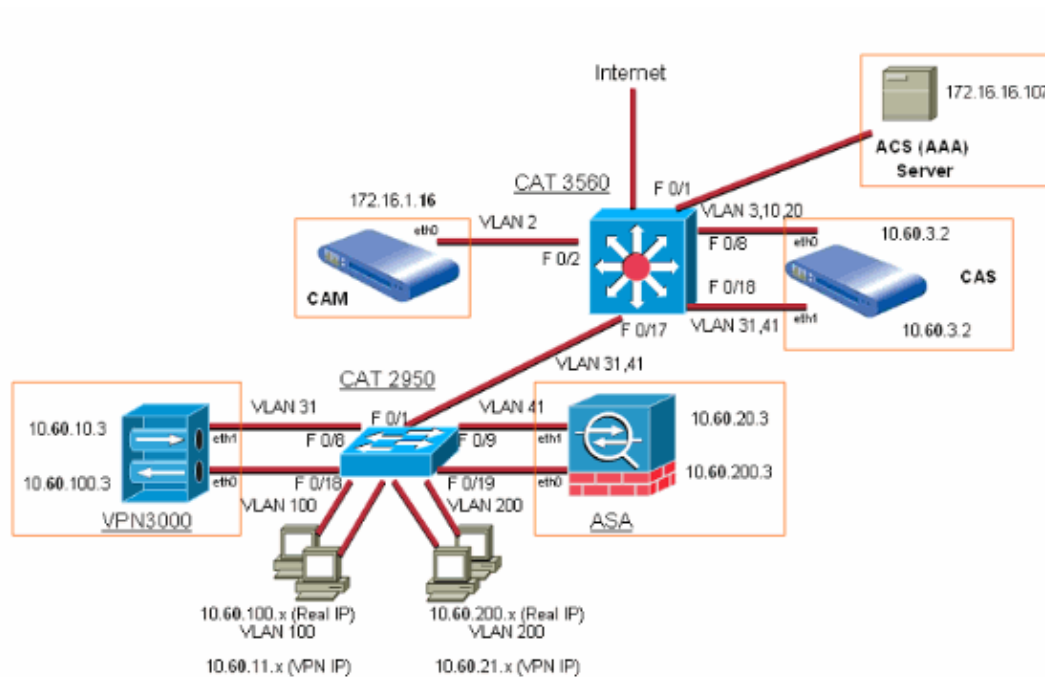
In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool (registered customers only) to obtain more information on the commands

used in this section.

## Network Diagram

This document uses this network setup:



## Steps to Configure Authentication on CCA with ACS

Complete these steps:

### 1. Add New Roles

#### a. Create an Admin Role

◇ In the CAM, choose **User Management > User Roles > New Role**.

**User Management > User Roles**

List of Roles | **New Role** | Traffic Control | Bandwidth | Schedule

Disable this role

Role Name:

Role Description:

Role Type:

\*VPN Policy:

\*Dynamic IPsec Key:  Enable  Disable

\*Max Sessions per User Account (Case-Insensitive):  (1 - 255; 0 for unlimited)

KeTag Trusted-side Egress Traffic with VLAN (In-Band):  (0 - 4095, or leave it blank)

**\*Out-of-Band User Role VLAN:**

\*After Successful Login Redirect to:  previously requested URL  
 this URL:  (e.g. <http://www.cisco.com/>)

Redirect Blocked Requests to:  default access blocked page  
 this URL or HTML message:

\*Roam Policy:  Deny  Allow

\*Show Logged-on Users:  IPsec info  PPP info  
 User info  Logout button

- ◇ Enter a unique name, **admin**, for the role in the Role Name field.
- ◇ Enter **Admin User Role** as an optional Role Description.
- ◇ Choose **Normal Login Role** as the Role Type.
- ◇ Configure the **Out-of-Band (OOB)** user role VLAN with the appropriate VLAN. For example, choose the VLAN ID and specify the ID as 10.
- ◇ When finished, click **Create Role**. In order to restore default properties on the form, click **Reset**.
- ◇ The role now appears in the List of Roles tab as shown in the Tag VLANs for OOB Role-based mappings section.

**b. Create a User Role**

- ◇ In the CAM, choose **User Management > User Roles > New Role**.

User Management > User Roles

List of Roles | **New Role** | Traffic Control | Bandwidth | Schedule

Disable this role

Role Name:

Role Description:

Role Type:

\*VPN Policy:

\*Dynamic IPsec Key:  Enable  Disable

\*Max Sessions per User Account (Case-Insensitive):  (1 - 255; 0 for unlimited)

KeTag Trusted-side Egress Traffic with VLAN (In-Band):  (0 - 4095, or leave it blank)

\*Out-of-Band User Role VLAN:

\*After Successful Login Redirect to:  previously requested URL  
 this URL:  (e.g. <http://www.cisco.com/>)

Redirect Blocked Requests to:  default access blocked page  
 this URL or HTML message:

\*Roam Policy:  Deny  Allow

\*Show Logged-on Users:  IPsec info  PPP info  
 User info  Logout button

- ◇ Enter a unique name, **users**, for the role in the Role Name field.
- ◇ Enter **Normal User Role** as an optional Role Description.
- ◇ Configure the **Out-of-Band (OOB)** user role VLAN with the appropriate VLAN. For example, choose the VLAN ID and specify the ID as 20.
- ◇ When finished, click **Create Role**. In order to restore default properties on the form, click **Reset**.
- ◇ The role now appears in the List of Roles tab as shown in the Tag VLANs for OOB Role-based mappings section.

## 2. Tag VLANs for OOB Role-based mappings

In the CAM, choose **User Management > User Roles > List of Roles** in order to see the list of roles so far.

User Management > User Roles

List of Roles | New Role | Traffic Control | Bandwidth | Schedule

Role Name	IPsec	Roam	VLAN	Description	Policies	SW	edit	Del
Unauthenticated Role	deny	deny		Role for unauthenticated users				X
Temporary Role	deny	deny		Role for users to download requirements				X
Quarantine Role	deny	deny		Role for quarantined users				X
Allow_All	deny	deny						X
admin	deny	deny	10	Admin User Role				X
users	deny	deny	20	Normal User Role				X

## 3. Add RADIUS Auth Server (ACS)

- a. Choose **User Management > Auth Servers > New**.

**User Management > Auth Servers**

**Auth Servers** | Lookup Servers | Mapping Rules | Auth Test | Accounting

List · **New**

Authentication Type: **Radius** | Provider Name: **ACS**

Server Name: **auth.cisco.com** | Server Port: **1812**

Radius Type: **PAP** | Timeout (sec): **5**

Default Role: **Allow\_All** | Shared Secret: **\*\*\*\*\***

NAS-Identifier: | NAS-IP-Address: **172.16.1.61**

(Either a NAS-Identifier or NAS-IP-Address must be specified)

NAS-Port: | NAS-Port-Type: | Failover Peer IP: | Enable Failover:  | Accept RADIUS packets with empty attributes from some old RADIUS servers:

(\* Asterisks indicate required fields.)

Description: | **Add Server** | Cancel

- b. From the Authentication Type drop-down menu, choose **Radius**.
- c. Enter the Provider Name as **ACS**.
- d. Enter the Server Name as **auth.cisco.com**.
- e. **Server Port** The port number **1812** on which the RADIUS server is listening.
- f. **Radius Type** The RADIUS authentication method. Supported methods include EAPMD5, PAP, CHAP, MSCHAP and MSCHAP2.
- g. **Default Role** is used if mapping to ACS is not defined or set correctly, or if the RADIUS attribute is not defined or set correctly on the ACS.
- h. **Shared Secret** The RADIUS shared secret bound to the specified client's IP address.
- i. **NAS-IP-Address** This value to be sent with all RADIUS authentication packets.
- j. Click **Add Server**.

Provider Name	Authentication Type	Description	Mapping	Edit	Delete
Local DB	local	Cisco local authentication			
ACS	radius	RADIUS Authentication			
Cisco VPN	vpn	Remote VPN Support			

#### 4. Map ACS Users to CCA User Roles

- a. Choose **User Management > Auth Servers > Mapping Rules > Add Mapping Link** in order to map admin user in ACS to the CCA admin user role.

User Management -> Auth Servers

List of Servers | New Server | **Mapping Rules** | Auth Test | Accounting

Provider Name: ACS

Role Name: **admin**

Rule Expression: ( 0,25,2 equals Admin )

Priority: 1

Description: [ ]

Save Mapping

Condition Type: Attribute | Operator: equals

Vendor: Standard

Attribute Name: Class | Attribute Value: Admin

Data Type: String

Save Condition | Cancel

#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	Attribute	0,25,2	equals	Admin	[ ]	[X]

b. Choose **User Management > Auth Servers > Mapping Rules > Add Mapping Link** in order to map normal user in ACS to the CCA user role.

User Management -> Auth Servers

List of Servers | New Server | **Mapping Rules** | Auth Test | Accounting

Provider Name: ACS

Role Name: **users**

Rule Expression: ( 0,25,2 equals Users )

Priority: 2

Description: [ ]

Save Mapping

Condition Type: Attribute | Operator: equals

Vendor: Standard

Attribute Name: Class | Attribute Value: Users

Data Type: String

Save Condition | Cancel

#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	Attribute	0,25,2	equals	Users	[ ]	[X]

c. Here is the user role mapping summary:

User Management > Auth Servers

List of Servers | New Server | **Mapping Rules** | Auth Test | Accounting

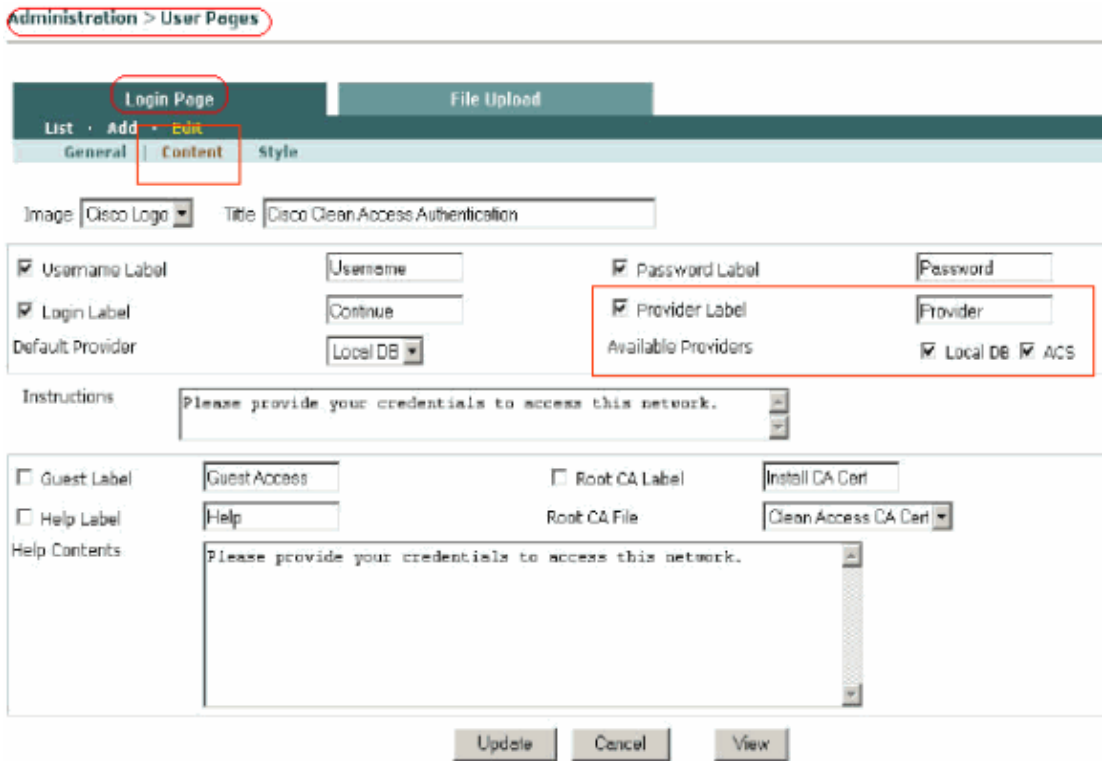
All Servers | View

ACS	Role	Expression	Edit	Delete	Priority
	admin	( 0,25,2 equals Admin )	[ ]	[X]	▲ ▼
	users	( 0,25,2 equals Users )	[ ]	[X]	▲ ▼

[Add Mapping Rule](#)

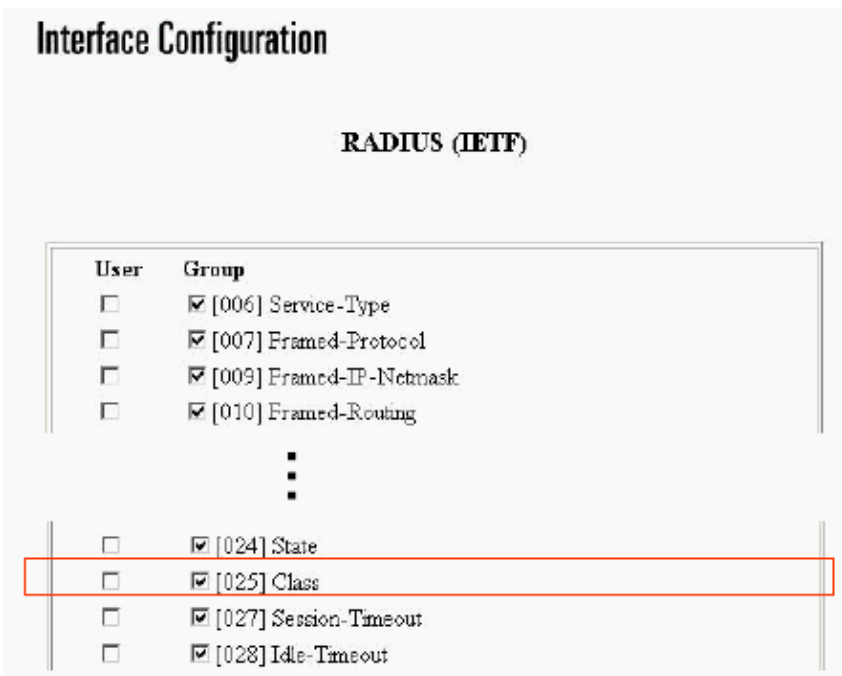
## 5. Enable Alternate Providers on User Page

Choose **Administration > User Pages > Login Page > Add > Content** in order to enable alternate providers on the user login page.



## ACS Configuration

1. Choose **Interface Configuration** in order to make sure that the RADIUS (IETF) Class attribute [025] is enabled.



2. Add RADIUS Client to ACS Server

- a. Choose **Network Configuration** in order to add the AAA client CAM as shown:

## Network Configuration

Edit

### AAA Client Setup For CAM

AAA Client IP Address	172.16.1.16
Key	cisco123
Authenticate Using	RADIUS (IETF)

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

Submit   Submit + Restart   Delete   Delete + Restart   Cancel

Click **Submit + Restart**.

**Note:** Make sure that the RADIUS key matches with the AAA client and uses RADIUS (IETF).

b. Choose **Network Configuration** in order to add the AAA client CAS as shown:

## Network Configuration

Edit

### AAA Client Setup For CAS

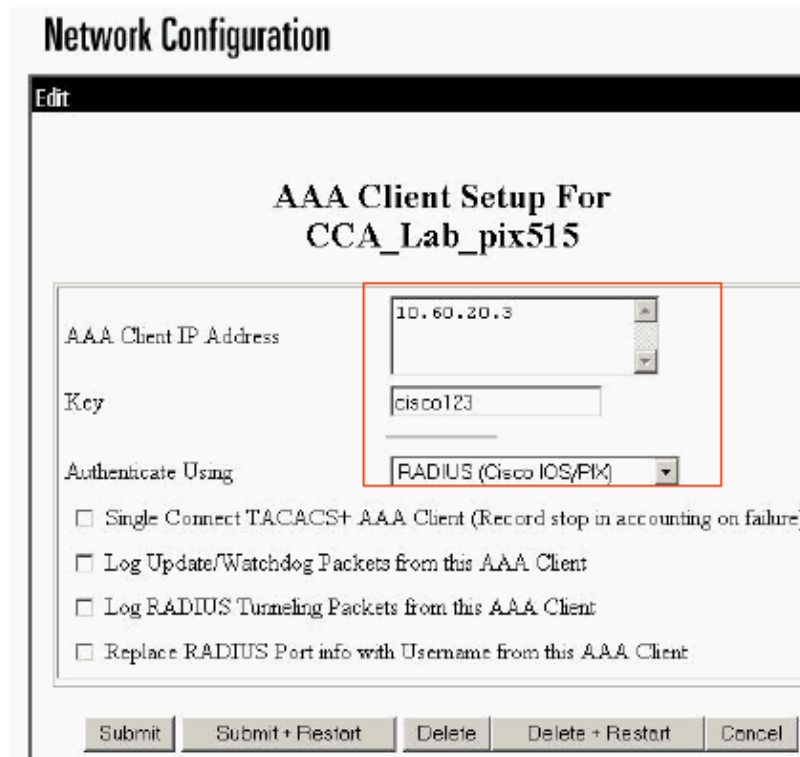
AAA Client IP Address	10.60.3.2
Key	cisco123
Authenticate Using	RADIUS (IETF)

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

Click **Submit + Restart**.

**Note:** For VPN gateway RADIUS accounting, CCA policy must allow RADIUS accounting packets (UDP 1646/1813) from the CAS IP address to pass unauthenticated to the ACS server IP address.

c. Choose **Network Configuration** in order to add the AAA client ASA as shown:



**Network Configuration**

Edit

### AAA Client Setup For CCA\_Lab\_pix515

AAA Client IP Address: 10.60.20.3

Key: cisco123

Authenticate Using: RADIUS (Cisco IOS/PIX)

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

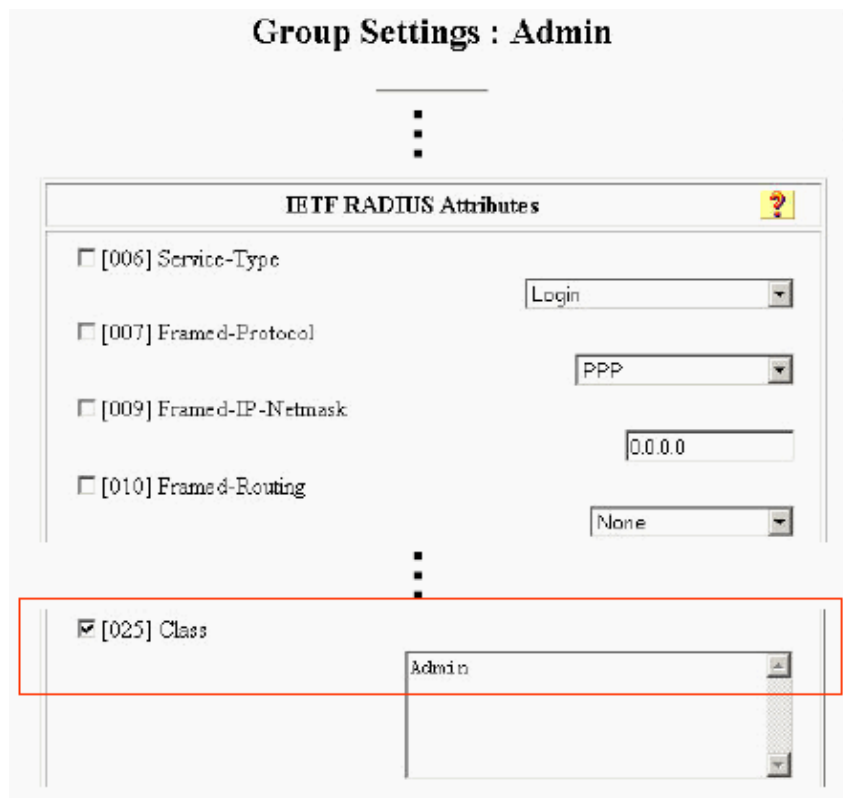
Replace RADIUS Port info with Username from this AAA Client

Submit Submit + Restart Delete Delete + Restart Cancel

- ◇ User near-side PIX/ASA interface address (typically inside interface)
- ◇ Set type to RADIUS (Cisco IOS/PIX).

### 3. Add /Configure Groups on ACS Server

a. Create Admin group



### Group Settings : Admin

IETF RADIUS Attributes

[006] Service-Type Login

[007] Framed-Protocol PPP

[009] Framed-IP-Netmask 0.0.0.0

[010] Framed-Routing None

[025] Class Admin

- ◇ Set the IETF RADIUS Class attribute [025] to appropriate group value.
- ◇ The value must match that configured on CAS mapping.

**b. Create User group**

**Group Settings : Users**

IETF RADIUS Attributes

[006] Service-Type Login

[007] Framed-Protocol PPP

[009] Framed-IP-Netmask 0.0.0.0

[010] Framed-Routing None

[025] Class Users

Add/configure group for each Clean Access User Role to be mapped.

**c. Add/Configure Users on ACS Server**

**User Setup**

Edit

**User: chyps**

Account Disabled

**Supplementary User Info**

Real Name: Craig Hyps

Description:

**User Setup**

Password Authentication: Windows Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked)

Password: [ ]

Confirm Password: [ ]

Separate (CHAP/MS-CHAP/ARAP)

Password: [ ]

Confirm Password: [ ]

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned: Admin

- ◇ Add/configure ACS user for each Clean Access user to be authenticated by ACS.
- ◇ Set ACS Group membership.
- ◇ ACS also supports proxy authentication to other external servers.

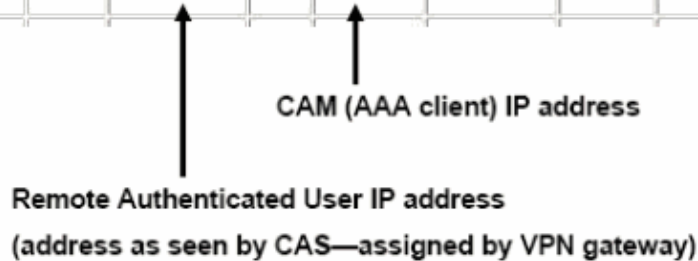
## Verify

Use this section to confirm that your configuration works properly.

In the ACS monitoring section, you can see the information on the passed authentications as shown:

**Passed Authentications active.csv**

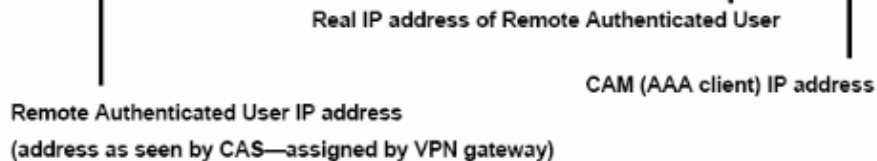
Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address	Application-Posture-Token	System-Posture-Token	Reason
08/02/2005	13:15:39	Authen OK	jsmith	Users	10.60.100.201	1039	10.60.10.3			



Similarly, you can see the screenshot for RADIUS accounting:

**RADIUS Accounting active.csv**

Date ↓	Time	User-Name	Group-Name	Calling-Station-Id	Acct-Status-Type	Acct-Session-Id	Acct-Session-Time	Service-Type	Framed-Protocol	Acct-Input-Octets	Acct-Output-Octets	Acct-Input-Packets	Acct-Output-Packets	Framed-IP-Address	NAS-Port	NAS-IP-Address
08/02/2005	15:26:49	jsmith	Users	10.60.100.201	Stop	B2C00017	7869	Framed	PPP	350872	8528952	5993	8207	10.60.11.1	1039	10.60.10.3
08/02/2005	13:15:40	jsmith	Users	10.60.100.201	Start	B2C00017		Framed	PPP					10.60.11.1	1039	10.60.10.3



## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

<a href="#">NetPro Discussion Forums – Featured Conversations for Security</a> <a href="#">Security: Intrusion Detection [Systems]</a>
---

Security: AAA
Security: General
Security: Firewalling

---

## Related Information

- [Cisco NAC Appliance Support Page](#)
  - [Technical Support & Documentation – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jun 24, 2008

Document ID: 107396

---