

NAC (CCA): Autenticación de la configuración en el Access Manager limpio (CAM) con el ACS

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Pasos para configurar la autenticación encendido CCA con el ACS](#)

[Configuración de ACS](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo configurar la autenticación en el Access Manager limpio (CAM) con el Cisco Secure Access Control Server (ACS). Para una configuración similar usando ACS 5.x y posterior, refiera al [NAC \(CCA\): Configure la autenticación en el Access Manager limpio con ACS 5.x y posterior](#).

[prerrequisitos](#)

[Requisitos](#)

Esta configuración es aplicable a la versión 3.5 y posterior CAM.

[Componentes Utilizados](#)

La información en este documento se basa en la versión 4.1 CAM.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

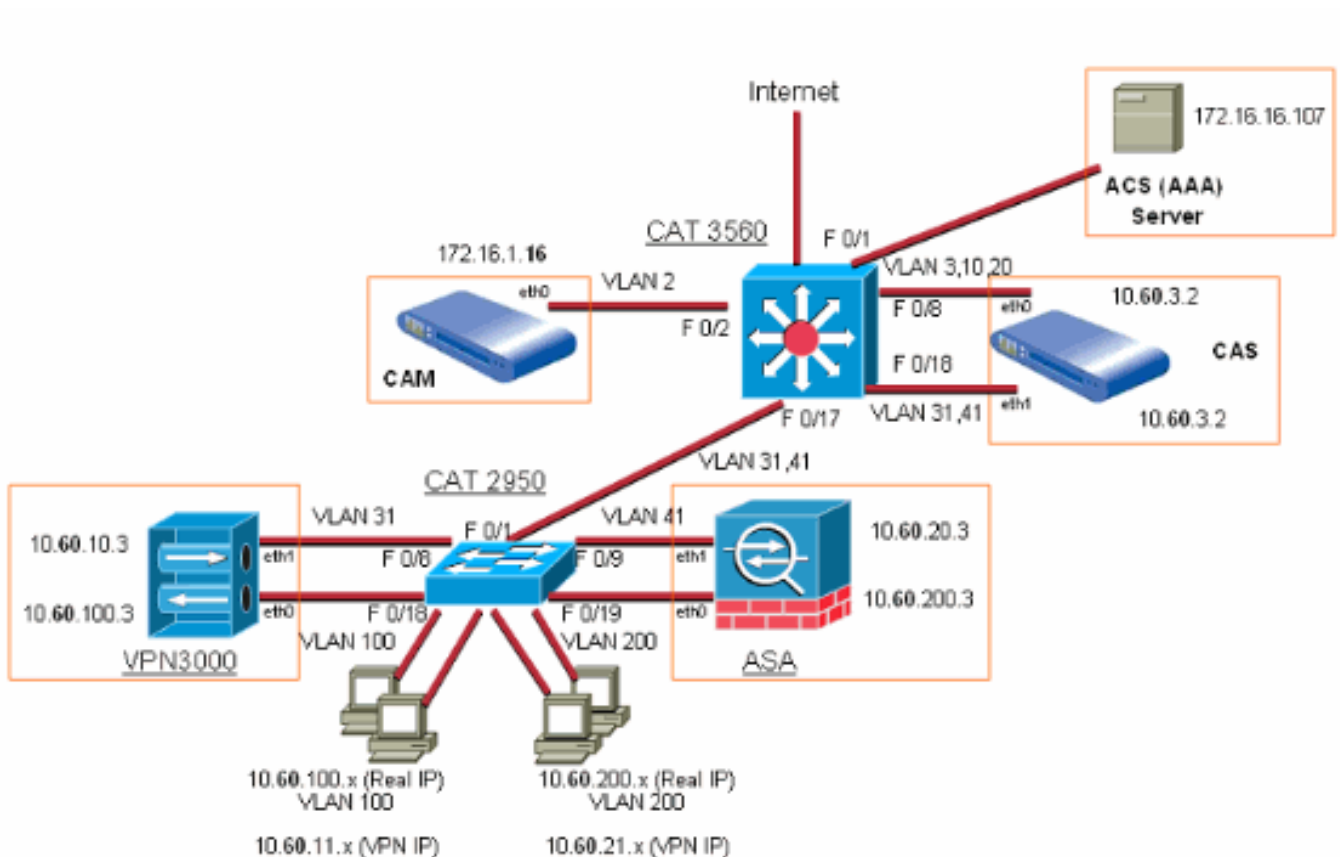
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Pasos para configurar la autenticación encendido CCA con el ACS

Complete estos pasos:

1. Agregue los nuevos papeles Cree un papel AdminEn el CAM, elija User Management (Administración de usuario) > los rol del usuario > nuevo papel.

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)

Retag 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

ingrese un nombre único, **admin**, para el papel en el campo de nombre del papel. Ingrese el **papel de Usuario administrador** como descripción opcional del papel. Elija el **papel normal del login** como el tipo del papel. Configure **(OOB) el rol del usuario fuera de banda del VLA N** con el VLA N apropiado. Por ejemplo, elija el VLAN ID y especifique el ID como 10. Cuando está acabado, el tecleo **crea el papel**. Para restablecer las propiedades predeterminadas en la forma, **restauración del tecleo**. El papel ahora aparece en la lista de lengüeta de los papeles tal y como se muestra en de los [VLA N de la etiqueta para la sección OOB Papel-basada de las asignaciones](#). Cree un rol del usuario En el CAM, elija **User Management (Administración de usuario) > los rol del usuario > nuevo papel**.

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)

Retag 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

ingrese un nombre único, los **usuarios**, para el papel en el campo de nombre del papel. Ingrese el **papel de usuario normal** como descripción opcional del papel. Configure **(OOB) el rol del usuario fuera de banda del VLAN** con el VLAN apropiado. Por ejemplo, elija el VLAN ID y especifique el ID como 20. Cuando está acabado, el tecleo **crea el papel**. Para restablecer las propiedades predeterminadas en la forma, **restauración del tecleo**. El papel ahora aparece en la lista de lengüeta de los papeles tal y como se muestra en de los [VLAN de la etiqueta para la sección OOB Papel-basada de las asignaciones](#).

2. **VLAN de la etiqueta para las asignaciones OOB Papel-basadas** En el CAM, elija **User Management (Administración de usuario) > los rol del usuario > lista de papeles** para ver la lista de papeles hasta ahora.

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

3. Agregue al servidor de autenticación RADIUS (el ACS) Elija User Management (Administración de usuario) > los servidores de autenticación > nuevo.

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	***** NOT SET	
NAS-Identifier		NAS-IP-Address	172.16.1.61	
<small>(Either a NAS-Identifier or NAS-IP-Address must be specified)</small>				
NAS-Port		NAS-Port-Type		
<input type="checkbox"/> Enable Failover		Failover Peer IP		
<input type="checkbox"/> Accept RADIUS packets with empty attributes from some old RADIUS servers				
<small>(* Asterisks indicate required fields.)</small>				
Description				
<input type="button" value="Add Server"/>		<input type="button" value="Cancel"/>		

Del menú desplegable del tipo de autenticación, elija el **radio**. Ingrese el nombre del proveedor como **ACS**. Ingrese Nombre del servidor como **auth.cisco.com**. **Puerto de servidor** — El número del puerto **1812** en el cual el servidor de RADIUS está escuchando. **Tipo del radio** — El método de autenticación de RADIUS. Los métodos aceptados incluyen EAPMD5, el PAP, la GRIETA, el MSCHAP y el MSCHAP2. Se utiliza el **papel predeterminado** si asocia al ACS no se define ni se fija correctamente, o si el atributo de RADIUS no se define ni se fija correctamente en el ACS. **Secreto compartido** — El límite del secreto compartido RADIUS a la dirección IP del cliente especificado. **Nas-ip-address** — Este valor que se enviará con todos los paquetes de la autenticación de RADIUS. El tecleo **agrega el servidor**.

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

4. Usuarios de ACS del mapa CCA a los rol del usuarioElija User Management (Administración de usuario) > los servidores de autenticación > las reglas de la asignación > Add que asocian el link para asociar al Usuario administrador en el ACS CCA al papel de Usuario administrador.

User Management -> Auth Servers

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

Provider Name: ACS | Priority: 1

Role Name: **admin** | Description:

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

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		

- Elija User Management (Administración de usuario) > los servidores de autenticación > las reglas de la asignación > Add que asocian el link para asociar al usuario normal en el ACS CCA al rol del usuario.

User Management -> Auth Servers

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

Provider Name: ACS | Priority: 2

Role Name: **users** | Description:

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

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		

Aquí está el rol del usuario del resumen de la asignación:

ACS	Role	Expression	edit	delete	Priority
	admin	(0,25,2 equals Admin)			▲ ▼
	users	(0,25,2 equals Users)			▲ ▼

[Add Mapping Rule](#)

5. Proveedores alternos del permiso en la página del usuario Elija la administración > las páginas del usuario > la página de registro > Add > contenido para habilitar los proveedores alternos en la página del ingreso del usuario al sistema.

[Administration > User Pages](#)

ACS	Role	Expression	edit	delete	Priority
	admin	(0,25,2 equals Admin)			▲ ▼
	users	(0,25,2 equals Users)			▲ ▼

[Add Mapping Rule](#)

Login Page | File Upload

List · Add · **Edit**

General | **Content** | Style

Image: Title:

Username Label:
 Password Label:

Login Label:
 Provider Label:

Default Provider:
 Available Providers: Local DB ACS

Instructions:

Guest Label:
 Root CA Label:

Help Label:
 Root CA File:

Help Contents:

Configuración de ACS

1. Elija la configuración de la interfaz para asegurarse que el atributo de clase [025] RADIUS (IETF) está

Interface Configuration

RADIUS (IETF)

User	Group
<input type="checkbox"/>	<input checked="" type="checkbox"/> [006] Service-Type
<input type="checkbox"/>	<input checked="" type="checkbox"/> [007] Framed-Protocol
<input type="checkbox"/>	<input checked="" type="checkbox"/> [009] Framed-IP-Netmask
<input type="checkbox"/>	<input checked="" type="checkbox"/> [010] Framed-Routing
	⋮
<input type="checkbox"/>	<input checked="" type="checkbox"/> [024] State
<input type="checkbox"/>	<input checked="" type="checkbox"/> [025] Class
<input type="checkbox"/>	<input checked="" type="checkbox"/> [027] Session-Timeout
<input type="checkbox"/>	<input checked="" type="checkbox"/> [028] Idle-Timeout

habilitado.

2. Agregue al cliente RADIUS al servidor ACSElija la configuración de red para agregar al cliente AAA CAM como se

Network Configuration

Edit

AAA Client Setup For CAM

AAA Client IP Address	<input type="text" value="172.16.1.16"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (IETF)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	
<input type="button" value="Submit"/> <input type="button" value="Submit + Restart"/> <input type="button" value="Delete"/> <input type="button" value="Delete + Restart"/> <input type="button" value="Cancel"/>	

muestra:

elijo **Submit + Restart**. **Nota:** Asegurese que la clave RADIUS hace juego con el cliente AAA y utiliza RADIUS (IETF). Elija la **configuración de red** para agregar al cliente AAA CAS como se

Network Configuration

Edit

AAA Client Setup For CAS

AAA Client IP Address	<input type="text" value="10.60.3.2"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (IETF)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

muestra:

ecleo **Submit + Restart**. **Nota:** Para las estadísticas del gateway de VPN RADIUS, CCA la directiva debe permitir que los paquetes de las estadísticas RADIUS (UDP 1646/1813) de la dirección IP de CAS pasen el unauthenticated a la dirección IP del servidor ACS. Elija la **configuración de red** para agregar al cliente AAA ASA como se

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

muestra:

Direc

cionamiento izquierdo de la interfaz del PIX/ASA del usuario (típicamente interfaz interior) Fije el tipo a RADIUS (Cisco IOS/PIX).

3. Agregue a los grupos de /Configure en el servidor ACS Cree el admin

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

group

Fije el atributo de clase [025] del IETF RADIUS para apropiarse del valor de grupo. El valor debe hacer juego eso configurada en asociar de CAS. **Cree al grupo de**

Group Settings : Users



IETF RADIUS Attributes 	
<input type="checkbox"/> [006] Service-Type	Login
<input type="checkbox"/> [007] Framed-Protocol	PPP
<input type="checkbox"/> [009] Framed-IP-Netmask	0.0.0.0
<input type="checkbox"/> [010] Framed-Routing	None
⋮	
<input checked="" type="checkbox"/> [025] Class	Users

usuarios

Agregue/grupo de la configuración para que cada rol del usuario limpio del acceso sea asociado. Agregue/los usuarios de la configuración en el servidor

User Setup

Edit

User: chyps

Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

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:

ACS

Agre

que/usuario de ACS de la configuración para que cada usuario limpio del acceso sea autenticado por el ACS. Fije la membresía del grupo ACS. El ACS también soporta la autenticación de representación a otros servidores externos.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

En la sección de la supervisión ACS, usted puede ver la información sobre las autenticaciones pasajeras como se muestra:

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

CAM (AAA client) IP address

Remote Authenticated User IP address

(address as seen by CAS—assigned by VPN gateway)

Semejantemente, usted puede ver el tiro de pantalla para las estadísticas RADIUS:

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

Real IP address of Remote Authenticated User

CAM (AAA client) IP address

Remote Authenticated User IP address

(address as seen by CAS—assigned by VPN gateway)

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Página de soporte del dispositivo NAC de Cisco](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)