

NAC (limpie el acceso): Configure el acceso de invitado

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Tipos de acceso de invitado](#)

[Solo botón Guest Button de la configuración](#)

[Cuenta de invitado del usuario local de la configuración](#)

[Portal externo del invitado con el API](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo configurar los diversos tipos de acceso de invitado en el acceso limpio de Cisco o de dispositivo NAC con el Access Manager limpio (CAM).

[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.

Tipos de acceso de invitado

Hay tres tipos principales de acceso de invitado:

- **Solo botón Guest Button** Permite el acceso de invitado a través de un solo botón Guest Button. Proporciona la página del usuario compatible para validar/niega. Proporciona la directiva, el ancho de banda y la sesión/los controles de la inactividad. No registra los nombres de usuario individuales del invitado. No previene el relogin/la reutilización del invitado.
- **Cuenta de invitado del usuario local** Permite que el pasillo admin edite el campo del usuario local solamente. Permite crear/las cuentas de invitado del múltiplo de la cancelación de los usuarios/del cambio. Registra los nombres de usuario individuales del invitado en el usuario en línea. Proporciona el AUP, los controles policy/bw/session/inactivity. No borra automáticamente las cuentas de invitado.
- **Portal externo del invitado con el acceso limpio API** Soporta el portal remoto del invitado con API (https). Permite crear/las cuentas de invitado del múltiplo de la cancelación de los usuarios/del cambio. Soporta el externo DB/AD para toda la creación de la cuenta de invitado del empleado. **Note:** El Usuario invitado puede ser autenticado usando el HTTPS solamente, pero no con el HTTP. Los hotspots se soportan vía el HTTPS solamente.

Solo botón Guest Button de la configuración

Usted puede utilizar el solo botón Guest Button en dos modos:

- **Acceso de invitado atado con alambre (MEJOR)** Para el uso en las salas de conferencia, cuartos de entrenamiento, quioscos del visitante Los usuarios pueden acceder solamente la red del invitado cuando son permitidos o acompañados por los empleados Restringe el acceso de invitado a Internet solamente Puede tener diversas páginas de registro basadas en el VLA N atado con alambre (el márketing)
- **Acceso de invitado inalámbrico (DEPENDENDE)** Bueno si los AP alcanzan dentro del campus solamente Los usuarios en el estacionamiento pueden obtener el acceso de invitado

Complete estos pasos:

1. **Cree el rol del usuario:** En el CAM, elija **User Management (Administración de usuario) > rol del usuario** para crear el papel de **Usuario invitado**, como se muestra. Opcional: Especifique una reorientación URL sobre el login del invitado.

List of Roles | **Edit 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: (0 - 4095)

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

2. Elija **User Management (Administración de usuario) > control de tráfico > IP** para crear una política de tráfico para el invitado, tal como “al router de Internet a través del puerto 80/443 solamente.”

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

IP - Host

[Add Policy to All Roles](#)

Guest				Add Policy
Action	Protocol	Untrusted	Trusted	Enable Edit Del Move
Allow	TCP	*:*	172.19.0.0/255.255.0.0 :80,443	<input checked="" type="checkbox"/>
Allow	UDP	*:*	*:53	trusted dns server
Block	ALL			

(↑ DNS in Real-IP and NAT Gateway; DNS/DHCP in Virtual Gateway.)

3. Eligen **User Management (Administración de usuario) > los usuarios locales > nuevo** para crear al nuevo **Usuario**

List of Local Users | **Edit Local User**

Disable this account

User Name:

Password:

Confirm Password:

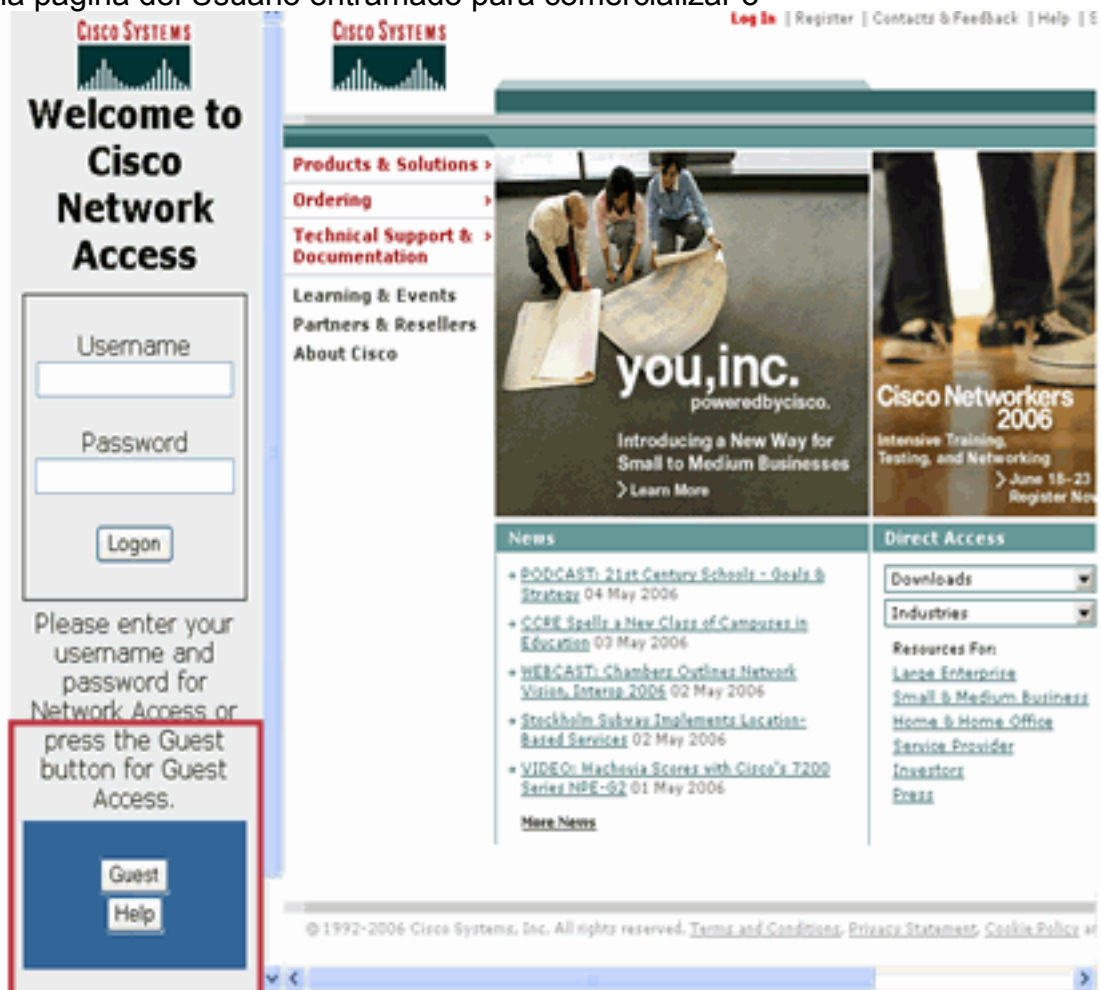
Description:

Role:

invitado.

4. Eligen la **administración > las páginas del usuario > la página de registro > Add** para especificar la información para la página del usuario, tal como imagen, título, escritura de la etiqueta del invitado, e instrucciones.

5. Crean una página del Usuario entramado para comercializar o



calificar.

El acceso correcto de la trama (e.g a cisco.com solamente) se permite en la función no autenticada. Una vez que el usuario hace clic en al invitado, el usuario puede acceder el Internet también.

[Cuenta de invitado del usuario local de la configuración](#)

Cuenta de invitado del usuario local

- El pasillo Admin debe abrir una sesión para limpiar el Access Manager con el acceso de usuario local restringido solamente.
- El pasillo Admin debe crear/cancelación/modifica las cuentas de invitado manualmente.
- Los registros de acontecimientos muestran la creación específica de la cuenta de invitado por el grupo fecha/hora y el login de la cuenta de invitado.
- El permite varias reorienta las páginas basadas en los tipos de roles de invitado. Por ejemplo, el guest_to_training reorienta a www.cisco.com/go/training.
- No previene el relogin de la cuenta de invitado hasta borrado del usuario local.
- Mejor para el media a la creación baja de la cuenta de invitado, tal como 20 visitantes por la semana.

Complete estos pasos:

1. Elija la **administración > los Usuarios administradores > a los grupos Admin** para crear el **admin group del pasillo**. Seleccione el **control total** en el menú desplegable para el campo de los usuarios

The screenshot shows the Cisco Admin Groups configuration interface. The 'Admin Groups' tab is active. A red box highlights the 'Group Name' and 'Description' fields, both containing 'Lobby Admin'. Below this, there are sections for 'Clean Access Servers', 'Module Features', and 'User Roles'. A red box highlights the 'Local Users' dropdown menu, which is set to 'full control'.

Section	Default Access
Clean Access Servers	read only
Clean Access Server 172.19.106.13:	read only
Module Features	read only
Clean Access Servers Management :	read only
Device Filters (MAC & Subnet):	read only
Roaming :	read only
Certified & Floating Devices :	read only
Network Scanner (Nessus) :	read only
Clean Access Agent :	read only
Switch Management :	read only
User Roles :	read only
Authentication Servers :	read only
Local Users :	full control

locales.

2. Elija la **administración > los Usuarios administradores > a los Usuarios administradores** para crear el nombre de usuario del **pasillo** con una contraseña, **xxxxx**. El tecleo **crea el Admin**, y el tecleo **crea el**

Admin Users | Admin Groups

Active Sessions · List · **New**

Disable this account

Admin User Name: Lobby

Password: ●●●●●●

Confirm Password: ●●●●●●

Group Name: Lobby Admin

Description: Lobby Admin

Create Admin Reset

Admin.

3. Cree los papeles de usuario múltiple basados en el uso del tiempo, tal como Guest_4hours, Guest_8hours, e invitado (1 hora).

Guest_4hours	deny	deny	Guest for 4 hours		
Guest_8hours	deny	deny	Guest for 8 hours		

4. Edite los rol del usuario basados en el horario.

Guest_4hours	240	Guest access for 4 hours	
Guest_8hours	480	Guest access for 8 hours	

5. El pasillo Admin crea a un usuario local y asigna a un usuario a un rol de invitado específico, los tecleos crea al

User Management > Local Users

List of Local Users | **New Local User**

Disable this account

User Name: jdoe@abc.com

Password: ●●●●●●

Confirm Password: ●●●●●●

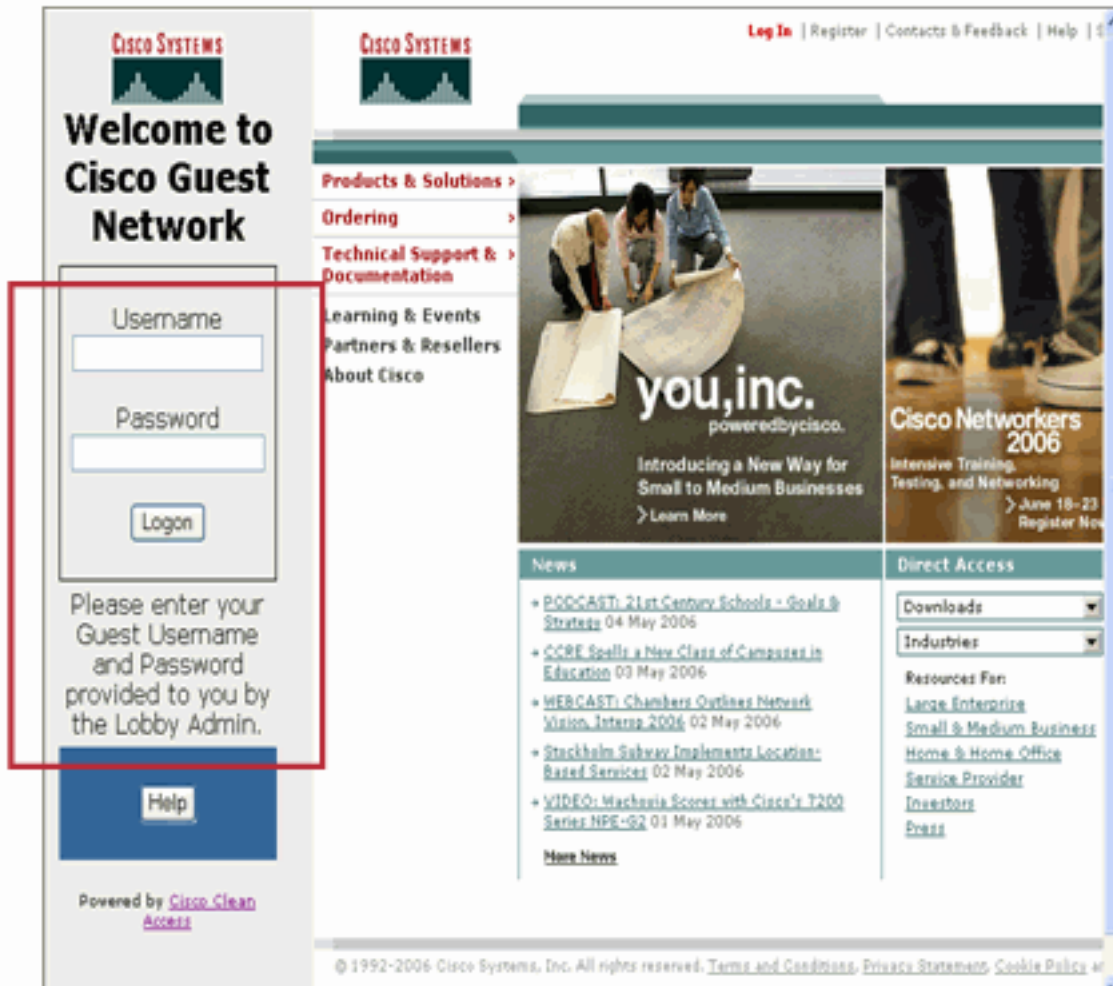
Description: Visitor from ABC Systems

Role: Guest_4hours

Create User Reset

usuario.

6. Cree una página del Usuario entrado para comercializar o



calificar

acceso correcto de la trama (e.g a cisco.com solamente) se permite en la función no autenticada. Una vez que el usuario ingresa un nombre de usuario/una contraseña, el usuario puede acceder el Internet también. Puede reorientar un tipo específico del invitado a un URL para comercializar.

[Portal externo del invitado con el API](#)

- Mejor para la alta creación de la cuenta de invitado, tal como 20 visitantes por el día.
- El mejor si hay problemas de seguridad sobre el acceso CAM al lado del pasillo Admin.
- El portal externo se puede construir por los clientes o el Advanced Services de Cisco.
- El portal puede tener hacer calendarios, el envío por correo electrónico, la impresión y señalar de las funciones.
- El portal puede realizar la factura o la información de la cuenta a cargar en cuenta.
- El script utilitario limpio del acceso API de Cisco, `cisco_api.jsp`, proporciona tres funciones que permitan que los administradores creen, que borren, y que vean las cuentas de usuario local en el CAM: `getlocaluserlist` — Devuelve una lista de usuarios locales con el Nombre de usuario y el nombre de la función. `addlocaluser` — Toma el Nombre de usuario, la contraseña, y el nombre de la función. Éxito o error de las devoluciones. `deletelocaluser` — Nombre de usuario o "TODO" de las tomas (borrar la lista entera). Éxito o error de las devoluciones.
- El temporizador de inactividad limpio del acceso de Cisco termina sesión al usuario cuando está inactivo (modo de la en-banda).

Guest Hotspot Access Codes Generator



Welcome

Generate Single
Access Code

Generate Batch
Access Codes

View/Edit

Support

NOTICES

The San Jose, CA - Bldg 15 hotspot is currently offline.

Welcome to Hotspot.cisco.com - Create and manage Access Codes for your Cisco guests

Cisco's Hotspot service provides guests with complimentary Internet access while they visit a hotspot enabled Cisco site. [Learn how Cisco's Hotspot service works](#) at the Guest Hotspot Website. Currently, Hotspots are available at select Cisco sites, but IT plans to deploy the service to all Cisco sites that have a bandwidth connection speed greater than 512kb. For a complete site-by-site listing of available guest hotspots, please visit the [Guest Hotspots Availability](#) page on the IT Services Website.

We recommend Internet Explorer for this application.

You must agree to the [Hotspot Usage Policy](#) and the [Hotspot Support Policy](#) prior to using the Hotspot Access Code Generator application.

["I have read and agree to the usage and support policies outlined in the above links."](#)

Información Relacionada

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