

# NAC (Clean Access): Configure Guest Access

Document ID: 107496

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions

#### Types of Guest Access

- Configure Single Guest Button
- Configure Local User Guest Account
- External Guest Portal through API

#### Related Information

## Introduction

This document describes how to configure the various types of guest access on the Cisco Clean Access or NAC appliance with the Clean Access Manager (CAM).

## 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.

## Types of Guest Access

There are three main types of guest access:

- **Single Guest Button**

- ◆ Allows guest access through a single Guest button.
- ◆ Provides Acceptable User Page to Accept/Deny.
- ◆ Provides policy, bandwidth and session/inactivity controls.
- ◆ Does not log individual guest usernames.
- ◆ Does not prevent guest relogin/reuse.

- **Local User Guest Account**

- ◆ Allows lobby admin to edit the Local User field only.
- ◆ Allows users to create/delete/change multiple guest accounts.
- ◆ Logs individual guest usernames in Online User.
- ◆ Provides AUP, policy/bw/session/inactivity controls.
- ◆ Does not automatically delete guest accounts.

- **External Guest Portal through Clean Access API**

- ◆ Supports remote guest portal through APIs (https).
- ◆ Allows users to create/delete/change multiple guest accounts.
- ◆ Supports external DB/AD for all employee guest account creation.

**Note:** The guest user can be authenticated by using HTTPS only, but not through HTTP. The hotspots are supported via HTTPS only.

## Configure Single Guest Button

You can use the single guest button in two modes:

- **Wired Guest Access (BEST)**

- ◆ For use in conference rooms, training rooms, visitor Kiosks
- ◆ Users can only access the Guest network when allowed or accompanied by employees
- ◆ Restricts Guest access to the Internet only
- ◆ Can have different login pages based on Wired VLAN (marketing)

- **Wireless Guest Access (DEPENDS)**

- ◆ Good if the APs reach within campus only
- ◆ Users in the parking lot can obtain Guest access

Complete these steps:

1. **Create User Role:**

- a. In CAM, choose **User Management > User Role** in order to create the **Guest** user role, as shown.
- b. Optional: Specify a Redirect URL upon Guest Login.

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):

Out-of-Band User Role VLAN:

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

2. Choose **User Management > Traffic Control > IP** in order to create a Traffic Policy for **Guest**, such as "to Internet router through port 80/443 only."

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

**IP** · Host

Guest | Untrusted-> Trusted | Select

[Add Policy to All Roles](#)

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

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

3. Choose **User Management > Local Users > New** in order to create the new **guest** user.

List of Local Users | Edit Local User

Disable this account

User Name:

Password:

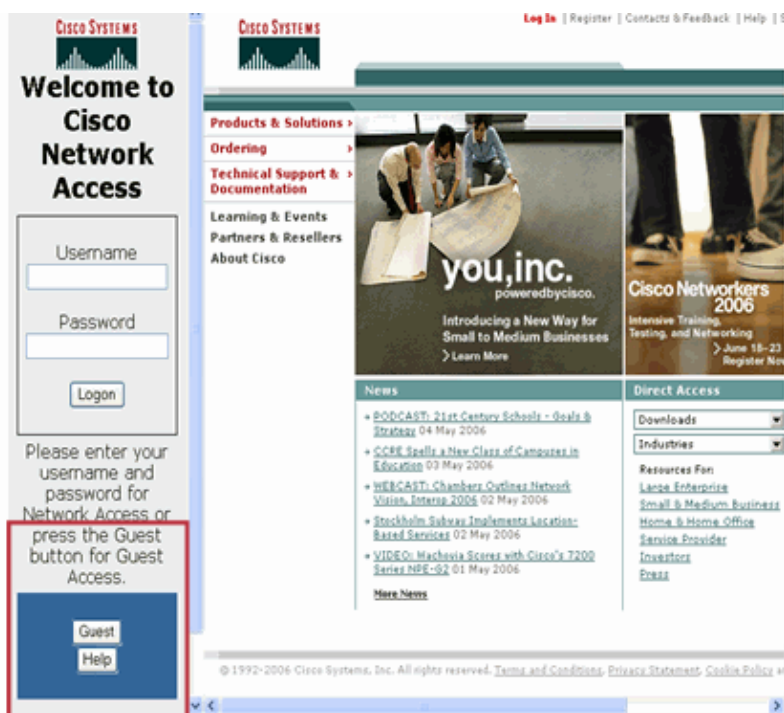
Confirm Password:

Description:

Role:

4. Choose **Administration > User Pages > Login Page > Add** in order to specify information for the User Page, such as Image, Title, Guest Label, and Instructions.

5. Create a Framed User Page for Marketing or Branding.



- ◆ Right frame access (e.g to cisco.com only) is allowed in the Unauthenticated Role.
- ◆ Once the user clicks on Guest, the user can access the Internet as well.

## Configure Local User Guest Account

### Local User Guest Account

- Lobby Admin must logon to Clean Access Manager with restricted Local User access only.
- Lobby Admin must create/delete/modify Guest accounts manually.
- Event logs show specific Guest account creation by timestamp and guest account login.
- Allows multiple redirect pages based on types of Guest roles. For example, guest\_to\_training redirects to [www.cisco.com/go/training](http://www.cisco.com/go/training).
- Does not prevent Guest account relogin until deleted from the Local User.
- Best for medium to low Guest account creation, such as 20 visitors per week.

Complete these steps:

1. Choose **Administration > Admin Users > Admin Groups** in order to create the **Lobby Admin** group. Select **full control** in the drop-down menu for the Local Users field.

Admin Users | **Admin Groups**

List · New

Disable this group

Group Name: Lobby Admin

Description: Lobby Admin

Access Control Policy:

**Clean Access Servers** Default Clean Access Server Access: read only

Clean Access Server 172.19.106.13: read only

**Module Features** Default Feature Access: 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

2. Choose **Administration > Admin Users > Admin Users** in order to create the **lobby** username with a password, **xxxxx**.

Click **Create Admin**, and click **Create Admin**.

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

3. Create multiple user roles based on time usage, such as **Guest\_4hours**, **Guest\_8hours**, and **Guest** (1 hour).

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

4. Edit the user roles based on the schedule.

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

5. The **Lobby Admin** creates a Local User and assigns a user to a specific Guest role, clicks **Create User**.

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

Disable this account

User Name:

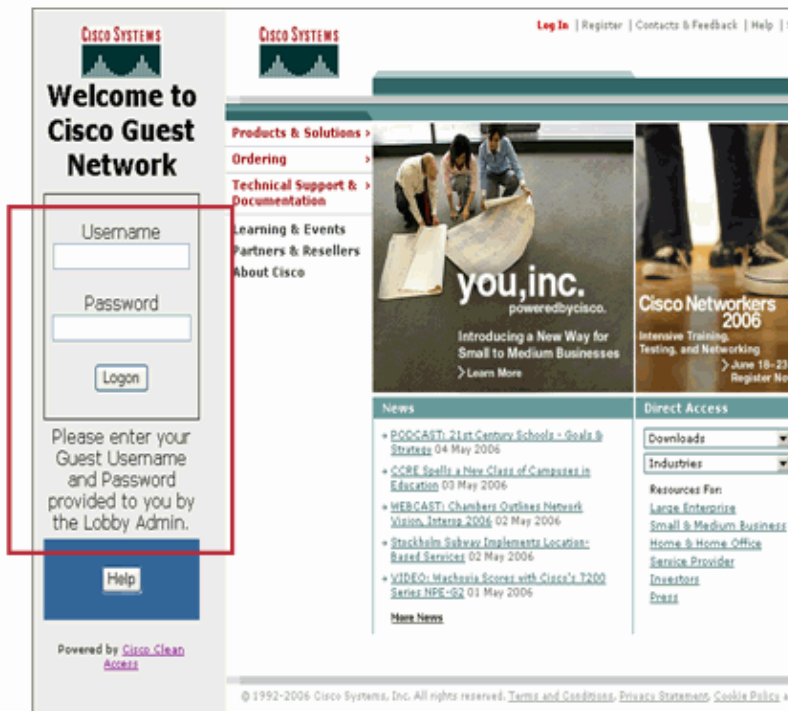
Password:

Confirm Password:

Description:

Role:

6. Create a Framed User Page for Marketing or Branding



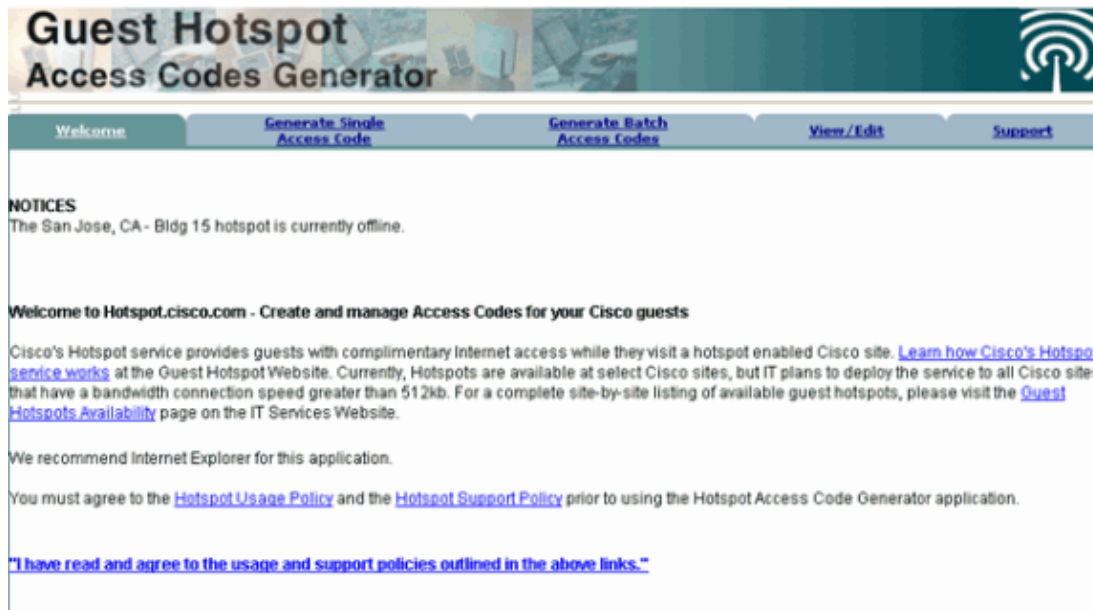
- ◆ Right frame access (e.g to cisco.com only) is allowed in the Unauthenticated Role.
- ◆ Once the user enters a username/password, the user can access the Internet as well.
- ◆ Can redirect a specific Guest type to a URL for marketing.

## External Guest Portal through API

- Best for high Guest account creation, such as 20 visitors per day.
- Best if there are security concerns over CAM access by Lobby Admin.
- External portal can be built by customers or Cisco Advanced Services.
- Portal can have calendaring, emailing, printing and reporting functions.
- Portal can perform billing or accounting information to billing.
- Cisco Clean Access API utility script, `cisco_api.jsp`, provides three functions that allow administrators to create, delete, and view local user accounts on the CAM:

- ◆ `getlocaluserlist` Returns a list of local users with user name and role name.
- ◆ `addlocaluser` Takes user name, password, and role name. Returns success or failure.
- ◆ `deletelocaluser` Takes user name or "ALL" (to delete entire list). Returns success or failure.

- Cisco Clean Access inactivity timer logouts the user when inactive (in-band mode).



The screenshot shows the 'Guest Hotspot Access Codes Generator' web application. The header features the title and a wireless signal icon. A navigation bar includes links for 'Welcome', 'Generate Single Access Code', 'Generate Batch Access Codes', 'View/Edit', and 'Support'. The main content area contains a 'NOTICES' section with a message about a San Jose hotspot being offline. Below this is a welcome message and a detailed paragraph explaining the service, including links for 'Learn how Cisco's Hotspot service works' and 'Guest Hotspots Availability'. It also includes a browser recommendation for Internet Explorer and a requirement to agree to the 'Hotspot Usage Policy' and 'Hotspot Support Policy'. At the bottom, there is a checkbox with the text: "I have read and agree to the usage and support policies outlined in the above links."

## Related Information

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

---

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

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jul 02, 2008

Document ID: 107496

---