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)**

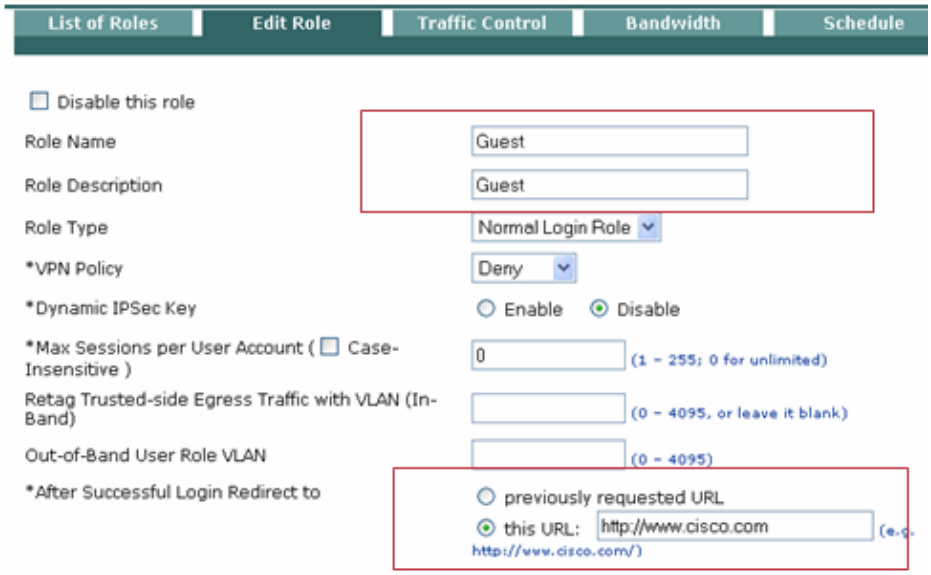
    - ♦ For use in conference rooms, training rooms, visitor Kiosks
    - ♦ Users can only access the Guest network when allowed or accompanied by employees
    - ♦ Restricts Guest access to the Internet only
    - ♦ Can have different login pages based on Wired VLAN (marketing)
- **Wireless Guest Access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

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

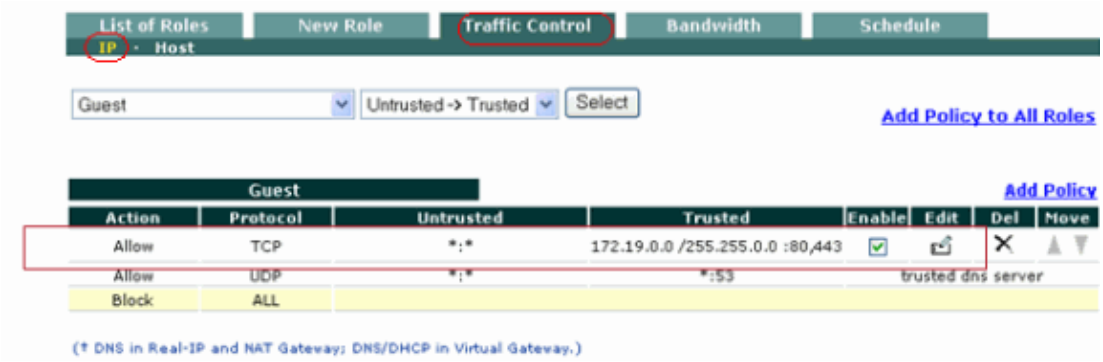
Complete these steps:

1. **Create User Role:**

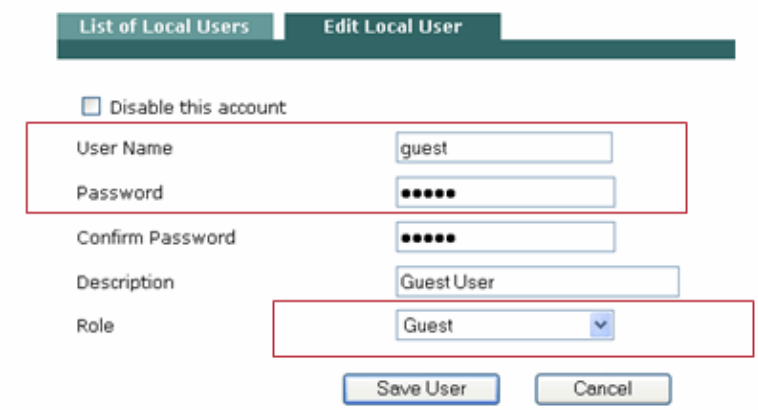
    a. In CAM, choose **User Management > User Role** in order to create the **Guest** user role, as shown.
    b. Optional: Specify a Redirect URL upon Guest Login.



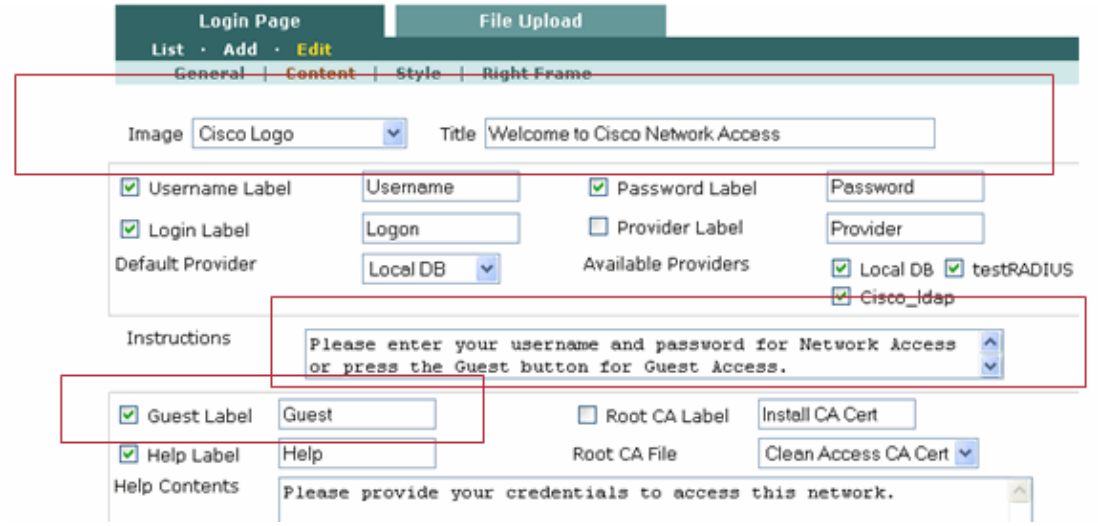
2. Choose **User Management > Traffic Control > IP** in order to create a Traffic Policy for **Guest**, such as "to Internet router through port 80/443 only."



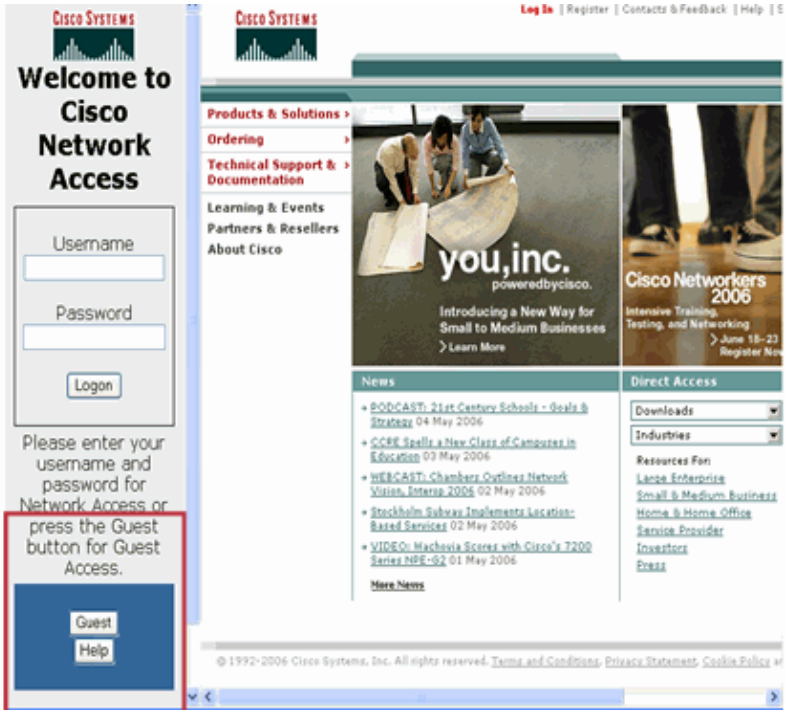
3. Choose **User Management > Local Users > New** in order to create the new **guest** user.



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.

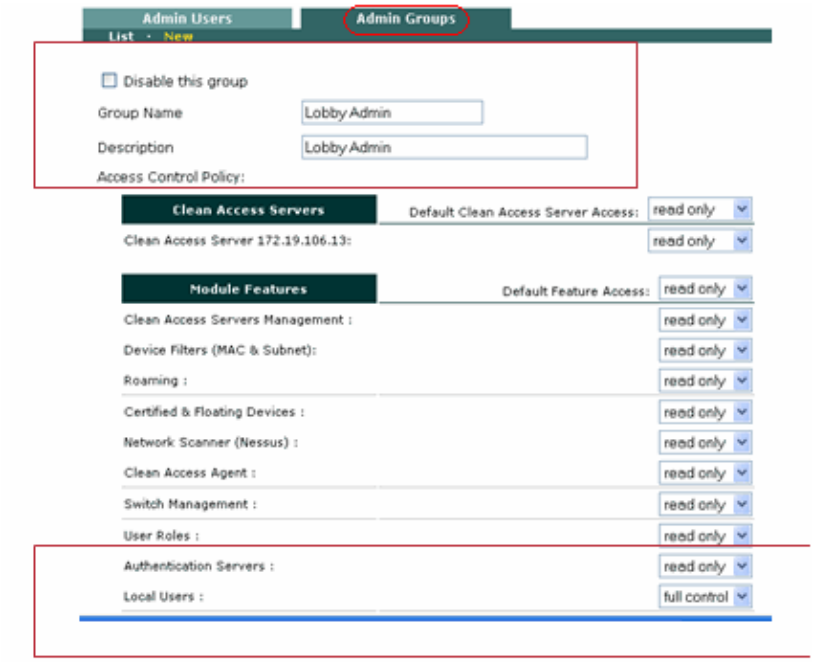
Configure Local User Guest Account

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.
- 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.

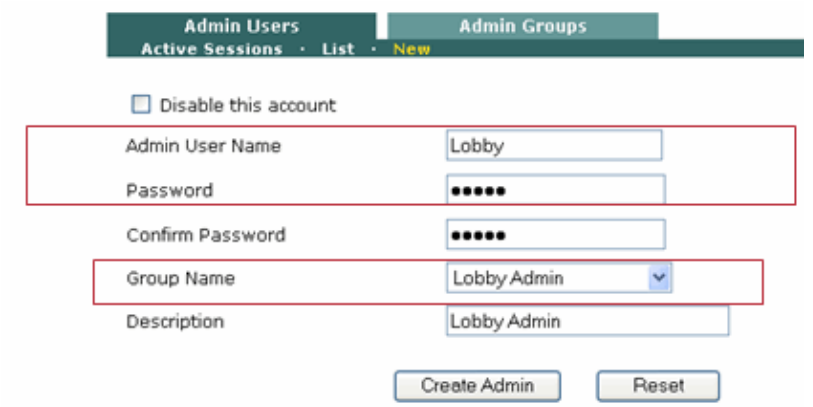
Complete these steps:

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.



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

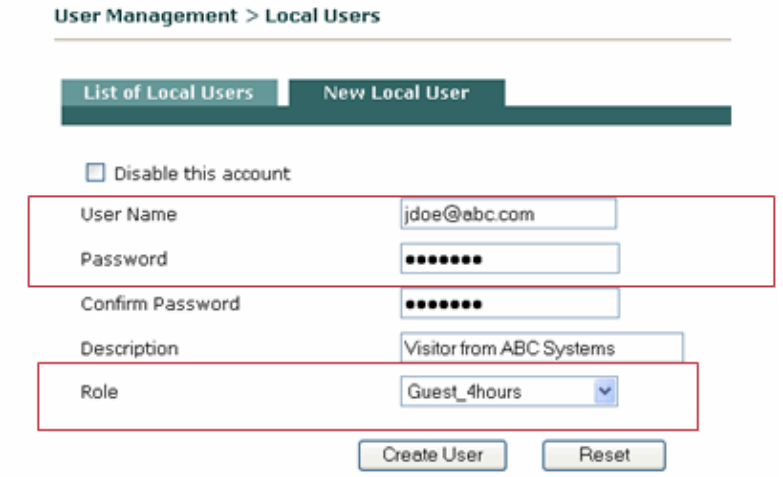
   Click **Create Admin**, and click **Create Admin**.



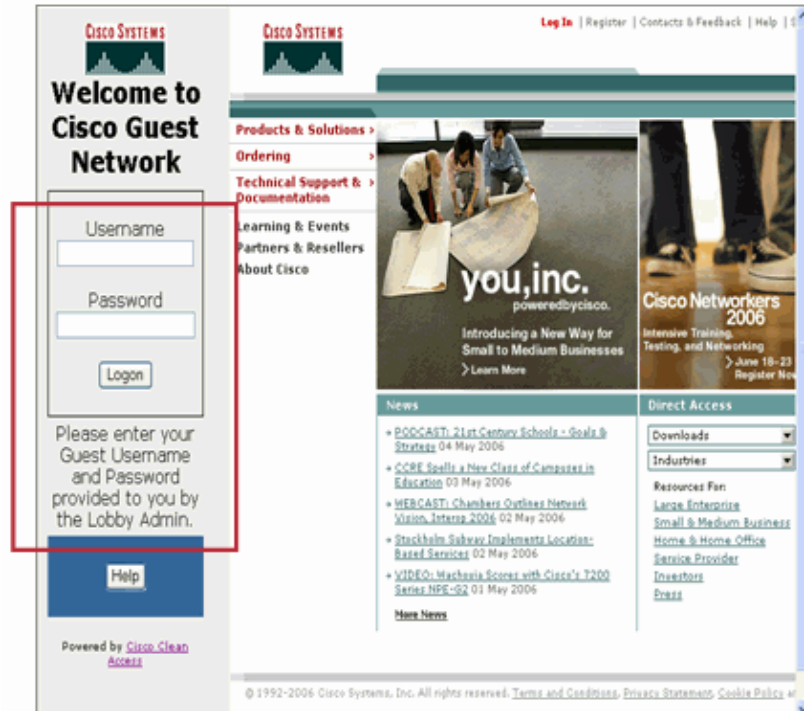
3. Create multiple user roles based on time usage, such as Guest_4hours, Guest_8hours, and Guest (1 hour).

4. Edit the user roles based on the schedule.

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



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).

Related Information

- **Cisco NAC Appliance Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jul 02, 2008 Document ID: 107496