CHAPTER 16

# Supporting Authorized Network Access for Guests

This chapter provides information on managing network user access, sponsor accounts, and how to create the necessary policies for these network users.

This chapter contains the following sections:



## Cisco ISE Guest Services

Cisco Identity Services Engine (ISE) guest services enables you to provide secure network access to guests, visitors, contractors, consultants, and customers. You can support guest users with both base and advanced Cisco ISE licenses, and you can choose from several deployment options depending on your company's infrastructure and feature requirements.

**Related Topics**

- Guest Deployment Scenarios, page 16-26
- Chapter 7, "Cisco ISE Licenses"

## Guest Services End-User Portals

Cisco ISE provides web-based portals to manage guest access to the network.

# Sponsor Portal

The Sponsor portal is one of the primary components of Cisco ISE guest services. Using the Sponsor portal, sponsors can create and manage temporary accounts for authorized visitors to securely access the corporate network or the Internet. After creating an account, sponsors also can use the Sponsor portal to provide account details to the guest by printing, emailing, or texting.

**Related Topics**

- Chapter 15, "Setting Up and Customizing End-User Web Portals"
- Configuring the Sponsor Portal, page 16-8

# Guest Portal

When people outside your company attempt to use your company's network to access the Internet, they are routed to the Guest portal. You can use the Guest portal to identify and authorize temporary access to internal networks and services to external users. Sponsors can create temporary usernames and passwords for authorized visitors who can then access the network by entering these credentials in the Guest portal login page.

Cisco ISE enables you to create multiple Guest portals, which you can use to allow guest access based on different criteria. For example, you might have a Guest portal for monthly contractors that is separate from the portal used for daily visitors. You also have the option to route mobile users to a mobile-optimized version of the Guest portal.

**Related Topics**

- Guest Deployment Scenarios, page 16-26
- Configuring the Guest Portal, page 16-10

## Support for Multiple Guest Portals

Cisco ISE provides you with the ability to host multiple portals on the Cisco ISE server, including a predefined DefaultGuestPortal. The default portal themes have standard Cisco branding that you can customize through the Admin portal. You can also choose to customize a portal by uploading HTML pages that are specific to your organization.

**Related Topics**

- Configuring the Guest Portal, page 16-10

## Mobile Guest Portal

Cisco ISE enables you to deliver a mobile-optimized version of the Guest portal, which provides an improved user experience for guests accessing your network using their mobile devices. Because this is an optional feature, you must enable it when you create the Guest portal.

**Related Topics**

Providing a Mobile-Optimized Guest Portal, page 16-11

## Device Registration Web Authentication Portal

The Device Registration Web Authentication (DRW) portal is an alternative Guest portal that does not require guests to enter usernames and passwords. Instead, Cisco ISE works together with the wireless LAN controller (WLC) to grant network access directly to the guest's device.

If you support the DRW portal, Cisco ISE provides you with a default guest identity group, GuestEndpoints, which enables you to cohesively track guest devices.

**Related Topics**

- Device Registration WebAuth, page 16-31

## Client Provisioning Portal

The Client Provisioning portal provides posture assessments and remediations for guest users. When guests request network access, you can route them to the Client Provisioning portal and require them to first download the client provisioning agent.

The Client Provisioning portal is available only with a Central WebAuth (CWA) guest deployment. If you select this option, the guest login flow performs a CWA and the Guest portal will be redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) to the network access device to reauthenticate the client connection once the posture has been assessed.

**Related Topics**

- NAD with Central WebAuth Process Flow, page 16-26
- Configuring Client Provisioning, page 22-1

# Managing Sponsor and Guest Accounts

Guest services require two special types of users—guests and sponsors. From the Admin portal, you must define the access privileges and feature support for sponsors. Sponsors then access the Sponsor portal to create and manage guest accounts.

## Guest Accounts

Guests typically represent authorized visitors, contractors, customers, or other temporary users who require access to your network. However, you can also use guest accounts for employees if you prefer to use one of the guest deployment scenarios to allow employees to access the network. Only sponsors can create guest users, and you must access the Sponsor portal to view a list of guest users.

## Guest Role and Identity Groups

The guest identity group is defined by the guest role. When sponsors create a guest account, they must associate the account with a guest role. Guest roles allow a sponsor to assign different levels of access to a guest account. These guest roles are associated with particular network access policies. For example, Cisco ISE includes these default guest roles:

- Guest: Users must first sign into through the Guest captive portal before they will be able to access other parts of the network (such as with Central Web Authentication (CWA)).
- ActivatedGuest: Users can bypass the Guest portal and access the network by providing credentials to the native supplicant on their device (such as with IEEE 802.1X (dot1x) authentication.)

You can also create additional user identity groups specific to your organization to use with sponsor accounts (**Administration > Identity Management > Groups > User Identity Groups**.)

**Related Topics**

Creating a User Identity Group, page 14-5

# Configuring Guest Roles

When you create new identity groups to use as guest roles, you must indicate which of the default behaviors to apply to them: Guest or Activated Guest.

**Before You Begin**

Create a new user identity group to use for guests.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest >Guest Roles Configuration**.

**Step 2** Select the identity group you created.

**Step 3** Click > or < to assign the identity group to one of the following groups:

- **Guest**: Users must first sign into through the Guest captive portal before they will be able to access other parts of the network (such as with Central Web Authentication (CWA)).
- **ActivatedGuest**: Users can bypass the Guest portal and access the network by providing credentials to the native supplicant on their device (such as with IEEE 802.1X (dot1x) authentication.)

**Step 4** Click **Save**.

**What to Do Next**

Create or modify sponsor groups to use this guest role.

**Related Topics**

- Creating a User Identity Group, page 14-5
- Creating Sponsor Groups, page 16-5

# Sponsor Accounts and Identity Groups

Sponsors are a special type of internal user who can create guest accounts using the Sponsor portal. Like other internal users, Cisco ISE authenticates sponsors through a local database, or through external Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory identity stores. If you are not using an external source, you must create user accounts in Cisco ISE (**Administration > Identity Management > Identities > Users**).

You must then assign users to the appropriate sponsor identity group. The sponsor identity groups specify the users who can use the Sponsor portal, and they are mapped in the default to the default sponsor groups in the sponsor group policies.

Cisco ISE includes these default sponsor user identity groups:

- SponsorAllAccount
- SponsorGroupAccounts
- SponsorOwnAccounts

You can also create additional user identity groups specific to your organization to use with sponsor accounts (**Administration > Identity Management > Groups > User Identity Groups**).

**Related Topics**

Adding Users, page 14-3

Creating a User Identity Group, page 14-5

# Sponsor Groups

The sponsor group configuration defines the permissions and settings for sponsor users. The policies map user identity groups to sponsor groups.

Cisco ISE includes these default sponsor groups:

- SponsorAllAccounts—Sponsors who can manage all guest accounts in your Cisco ISE network.
- SponsorGroupGrpAccounts—Sponsors who can manage only guest accounts created by sponsor users from the same sponsor group.
- SponsorGroupOwnAccounts—Sponsors who can manage only the guest accounts that they have created.

These sponsor groups have names similar to the default user identity groups to assist you in associating the correct identity group and sponsor group when creating the sponsor policies.

You can customize the features available to particular sponsor groups thereby limiting or expanding functionality of the Sponsor portal. For example:

- You can restrict sponsors from viewing guest accounts created by other sponsors.
- You can restrict access to different functions, such as creating accounts, modifying accounts, and sending account details to guests by e-mail or SMS text messages.
- You can set the sponsor group permission to prevent a group of sponsors from logging in for a short period of time while some configuration is being changed.

**Related Topics**

- Creating Sponsor Groups, page 16-5
- Creating a Sponsor Group Policy, page 16-6
- Sponsor Group Settings, page A-47

# Creating Sponsor Groups

You can create additional sponsor groups in addition to the default sponsor groups provided by Cisco ISE.

**Step 1** Choose **Administration > Web Portal Management > Sponsor Groups**.

**Step 2** Click **Add**.

**Step 3** Update the fields on each of these tabs:

- **General**—provide the name and description for the new sponsor group
- **Authorization Levels**—identify the features available to sponsors in this group, such as: creating accounts, sending notifications, and suspending accounts.
- **Guest Roles**—choose the guest roles to which the sponsor can assign the guest user.
- **Time Profiles**—choose the time profiles for which the sponsor can set on the guest accounts.

**Step 4** Click **Submit**.

**Related Topics**

- Sponsor Groups, page 16-5
- Sponsor Group Settings, page A-47

# Sponsor Group Policies

Sponsor group policies associate user identity groups with sponsor groups. Each sponsor group policy contains at least one identity group, and it can also contain other attribute conditions with which you define the sponsor group. You can map internal users or users from an external identity store (such as LDAP or Active Directory) to sponsor groups.

Internal users are mapped to sponsor groups by assigning an identity group role that is used in a sponsor group policy. If both the identity group role and the conditions of the sponsor group policy match the internal user, that user will be mapped to the sponsor group associated with that sponsor group policy.

For the external user to be identified as a sponsor user, the attributes from the external identity store need to match the conditions in the sponsor group policy that map the external user to a local sponsor group. If the external user possesses the attribute conditions that are defined in a sponsor group policy, then the user is assigned to the guest sponsor group that is selected in the sponsor group policy.

# Creating a Sponsor Group Policy

The sponsor group policy specifies the conditions that determine access and functionality available to a sponsor when logging into the Sponsor portal.

The sponsor group policy comprises:

- one or more identity groups
- one or more attributes or conditions

**Before You Begin**

You can apply existing conditions to your Sponsor Group Policies. If needed, define additional conditions, before creating your policies.

**Step 1** Choose **Administration > Web Portal Management > Sponsor Group Policy**.

**Step 2** Click the Action icon and choose an option.

**Step 3** Enter a name for the new policy.

**Step 4** Choose the identity group to be associated with the policy.

**Step 5** (Optional) Choose additional conditions by choosing one of these options:

- **Select Existing Condition from Library** to choose an existing simple, compound, or time and date condition
- **Create New Condition** to choose an attribute, operator, and value from the expression builder.

**Step 6** Choose the sponsor group to associate with this sponsor group policy.

**Step 7** Click **Save**.

**Related Topics**

- Creating Simple Conditions, page 18-2
- Creating Compound Conditions, page 18-3
- Adding Users, page 14-3
- Creating Sponsor Groups, page 16-5

# Mapping Active Directory Groups to Sponsor Groups

You can map external identity groups to sponsor groups.

**Before You Begin**

Before beginning this task, you must configure the Active Directory identity groups.

**Step 1** Choose **Administration > Web Portal Management > Sponsor Group Policy**.

**Step 2** Click the Action icon and choose an option.

**Step 3** Enter a name for the new policy.

**Step 4** Choose **Any** as the Identity Group because there is no group mapping with the internal groups.

**Step 5** Choose the condition you created for the Active Directory identity store

**Step 6** Choose the sponsor group to associate with this AD condition.

**Step 7** Click **Save**.

**Related Topics**

- Active Directory as an External Identity Source, page 14-9
- Configuring Active Directory User Groups, page 14-14

# Configuring the Sponsor Portal

You must configure some settings for the Sponsor portal before sponsors can access it to create accounts for guest users. You cannot configure some settings such as the Sponsor portal timeout value. The default timeout value is 20 minutes of inactivity.

## Sponsor Identity Source Sequence

Sponsor identity source sequences are used with the login credentials of the sponsor to authenticate and authorize sponsors for access to the Sponsor portal. The identity source sequence defines which stores should be accessed and in what order they should be accessed to resolve the authentication of a sponsor user, and it can include the local Cisco ISE identity stores and external stores.

Cisco ISE includes a default sponsor identity source sequence (Sponsor_Portal_Sequence), which includes the default identity store, Internal Users.

**Related Topics**

- Specifying the Identity Source Sequence for Sponsors, page 16-8
- Creating Identity Source Sequences, page 14-38

## Specifying the Identity Source Sequence for Sponsors

To allow a sponsor user to log into the Sponsor portal, you must choose an identity source sequence to be used for all sponsor accounts. This sequence is used with the login credentials of the sponsor to authenticate and authorize the sponsor for access to the Sponsor portal.

**Before You Begin**

Create the identity source sequence. Or, you can use the Sponsor_Portal_Sequence, which is the default sequence included with Cisco ISE.

**Step 1** Choose **Administration > Web Portal Management > Settings > Sponsor > Authentication Source**.

**Step 2** Choose the identity source sequence from the **Identity Store Sequence** drop-down list.

**Step 3** Click **Save**.

**Related Topics**

- Sponsor Identity Source Sequence, page 16-8
- Identity Source Sequences, page 14-38
- Creating Identity Source Sequences, page 14-38

# Customizing Guest Notifications

When sponsors create guest accounts, they can provide the account credentials to guest users by printing, emailing, or texting the details. When you create sponsor groups, you determine whether to authorize sponsors to use these notifications.

## Customizing E-mail Notifications

You can specify the subject and the body of the e-mail that will be sent to guests with their account details.

**Before You Begin**

Configure the SMTP server to enable notifications and configure the sponsor groups to support the email notification.

**Step 1** Choose **Administration > Web Portal Management > Settings** > **Sponsor > Language Template**.

**Step 2** Click the language for which you want to apply the policy, for example, English.

**Step 3** Click **Configure Email Notification**.

**Step 4** Enter the subject of the e-mail in the **Subject** field.

**Step 5** Enter the e-mail body in the **Layout** field.

**Step 6** Click **Save**.

**Related Topics**

- Configuring the SMTP Server to Support Notifications, page 5-5
- Creating Sponsor Groups, page 16-5
- E-Mail Notification Template, page D-1

## Customizing SMS Text Message Notifications

You can specify the short message service (SMS) gateway, the subject and the message of the SMS text message that will be sent to guests with their account details.

**Before You Begin**

- Configure the SMTP server, which is used to send e-mail to the SMS gateway to deliver the SMS text message.
- Configure the sponsor groups to support the SMS text notification.
- You must have an account with a third-party SMS gateway. Cisco ISE sends the text messages as e-mail messages to the gateway, which are then forwarded through SMS to the specified user.

**Step 1** Choose **Administration > Web Portal Management > Settings** > **Sponsor > Language Template**.

**Step 2** Click the language for which you want to apply the policy.

**Step 3** Click **Configure SMS Text Message Notification**.

**Step 4** Enter the subject of the text message in the **Subject** field.

**Step 5** Enter the address of a third-party SMS gateway in the **Destination** field.

**Step 6** Enter the text body in the **Layout** field.

**Step 7** Click **Save**.

**Related Topics**

- Configuring the SMTP Server to Support Notifications, page 5-5
- Creating Sponsor Groups, page 16-5
- SMS Text Message Notification Template, page D-2

## Customizing Print Notifications

You can specify the page header and the body of the page that will be printed for guests with their account details.

**Before You Begin**

Configure the sponsor groups to support the print notification.

**Step 1** Choose **Administration > Web Portal Management > Settings** > **Sponsor > Language Template**.

**Step 2** Click the language for which you want to apply the policy, for example, English.

**Step 3** Click **Configure Print Notification**.

**Step 4** Enter a title in the **Page Header** field.

**Step 5** Enter the body of the printout in the **Layout** field.

**Step 6** Click **Save**.

**Related Topics**

- Creating Sponsor Groups, page 16-5
- Print Notification Template, page D-3

# Configuring the Guest Portal

You must configure settings for the Guest portal before allowing guests to use it to access the network. Some settings apply globally to all Guest portals and other require you to set them for each portal individually.

## Adding a New Guest Portal

You can add a new Guest portal or edit an existing one.

**Step 1** Choose **Administration > Web Portal Management > Settings** > **Guest > Multi-Portal Configurations**.

**Step 2** Click **Add**.

**Step 3** Update the fields on each of these tabs:

- **General**—enter a portal name and description and choose a portal type.
- **Operations**—enable the customizations for the specific portal
- **Customization**—choose a language template for displaying the Guest portal with localized content
- **File Uploads**—displays only if you have chosen a portal type requiring you to upload custom HTML files.
- **File Mapping**— identify and choose the HTML files uploaded for the particular guest pages. Displays only if you have chosen a portal type requiring you to upload custom HTML files.
- **Authentication**—indicate how users should be authenticated during guest login.

**Step 4** Click **Submit**.

**Related Topics**

- Multi-Portal Configuration Settings, page A-56
- Cisco ISE Authentication Policies, page 19-1
- Configuring a Simple Authentication Policy, page 19-21
- Configuring a Rule-Based Authentication Policy, page 19-22

# Providing a Mobile-Optimized Guest Portal

You can allow mobile users to access a mobile-optimized version of the Guest portal.

**Before You Begin**

Create a Guest portal or modify the DefaultGuestPortal. This setting is specific to each Guest portal.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration.**

**Step 2** Check the Guest portal to update and click **Edit**.

**Step 3** Click the **Operations** tab.

**Step 4** Check **Enable Mobile Portal**.

**Step 5** Click **Save**.

**Related Topics**

- Adding a New Guest Portal, page 16-10
- Multi-Portal Configuration Settings, page A-56
- Customizing the Web Portal Images and Color Scheme, page 15-5

# Customized Guest Portal

You have two options available for customizing the Guest portal:

- Apply the same custom color schemes, banners, and logos to all Guest, Sponsor, and My Devices portals by choosing **Administration > Web Portal Management > Settings** > **General > Portal Theme**. (See "Customizing the Web Portal Images and Color Scheme" section on page 15-5 for details.)
- Create custom HTML pages for complete control over the Guest portal look and feel.

  When you create custom HTML files, these changes apply only to the Guest portal. The other portals use the settings defined in the portal theme. To better synchronize the look and feel amongst the portals, upload your custom logos and banners to the portal theme too.

**Related Topics**

- Sample HTML for Custom Pages for the Guest Portal, page D-3
- Creating Custom HTML Files for Guest Portal, page 16-13
- Uploading HTML Files for Guest Portal, page 16-14
- Mapping HTML Files to Guest Portal Pages, page 16-15

## HTML Pages Required for Custom Guest Portals

To support a fully-customized guest portal, you must provide a minimum set of HTML pages based on the features you want to support:

- Login Page—Required
- Successful Guest Login Page—Required
- Error Page—Required
- Acceptable Use Policy Page—Required only if you require guests to acknowledge an acceptable use policy.
- Change Password Page—Required only if you require guests to change their passwords when signing in for the first time.
- Self-Registration Page—Required only if you allow guests to create their own accounts (self service).
- Self-Registration Result Page—Required only if you allow guests to create their own accounts (self service).
- Device Registration Page—Required if you are supporting device registration for guest users.

**Related Topics**

- Requiring Guests to Change Password, page 16-17
- Requiring an Acceptable Use Policy for Guests, page 16-19
- Allowing Guests to Add Devices, page 16-22
- Allowing Guests to Create Accounts, page 16-22

## Sequence of Customized HTML Pages Used by Guest Portal

The sequence and display of the customized HTML pages depends on the features you have enabled in the Cisco ISE Admin. Some example sequences include:

- Basic sequences
  - Login Page (required) > Successful Guest Login Page (required)
  - Login Page (required) > Change Password Page > Successful Guest Login Page (required)
- Device registration sequences
  - Login Page (required) > Device Registration Page > Successful Guest Login Page (required)
  - Login Page (required) > Change Password Page > Device Registration Page > Successful Guest Login Page (required)
- Acceptable use policy sequences
  - Login Page (required) > Acceptable Use Policy Page > Successful Guest Login Page (required)
  - Login Page (required) > Acceptable Use Policy Page > Change Password Page > Successful Guest Login Page (required)
  - Login Page (required) > Acceptable Use Policy Page > Change Password Page > Device Registration Page > Successful Guest Login Page (required)
- Self-registration sequences
  - Login Page (required) > Self-Registration Page > Self-Registration Result Page > Successful Guest Login Page (required)

**Related Topics**

- Requiring Guests to Change Password, page 16-17
- Requiring an Acceptable Use Policy for Guests, page 16-19
- Allowing Guests to Add Devices, page 16-22
- Allowing Guests to Create Accounts, page 16-22

## Creating Custom HTML Files for Guest Portal

You must manually code the custom HTML pages to use for the Guest portal. When you use your own HTML pages, the details policy, language templates, and portal themes do not apply. So, if these features are important to you, you need to write the HTML code to deliver similar functionality, or use the standard portal theme pages instead.

**Before You Begin**

Familiarize yourself with the Cisco-provided HTML pages (see the "Sample HTML for Custom Pages for the Guest Portal" section on page D-3.) At a minimum, you must create the Login, Guest Success, and Error Page files.

**Step 1** Open an HTML or text editing application.

**Step 2** Enter your custom HTML code using the Cisco-provided sample HTML pages as a reference.

**Step 3** Create and save a separate HTML file for each page:

- Login Page (required)

- Successful Guest Login Page (required)
- Error Page (required)
- Acceptable Use Policy Page
- Change Password Page
- Self-Registration Page
- Self-Registration Result Page
- Device Registration Page

**What to Do Next**

After creating the HTML pages, you must upload them to Cisco ISE and map them to the appropriate Guest portal pages.

**Related Topics**

- Sample HTML for Custom Pages for the Guest Portal, page D-3
- Uploading HTML Files for Guest Portal, page 16-14
- Mapping HTML Files to Guest Portal Pages, page 16-15

## Uploading HTML Files for Guest Portal

Upload the HTML files to fully customize the Guest portal.

**Before You Begin**

You must create the custom HTML files.

**Step 1** Choose **Administration > Web Portal Management > Settings** > **Guest > Multi-Portal Configurations**.

**Step 2** Choose one of these portal types:

- **Custom Default Portal**
- **Custom Device Web Authorization Portal**

**Step 3** Click the **File Uploads** tab.

**Step 4** Click **Update File** to select and upload each HTML file.

**Step 5** Click **Submit**.

**Related Topics**

- Sample HTML for Custom Pages for the Guest Portal, page D-3
- Creating Custom HTML Files for Guest Portal, page 16-13
- Mapping HTML Files to Guest Portal Pages, page 16-15

## Mapping HTML Files to Guest Portal Pages

After uploading the custom HTML files, you must map them to the appropriate page in the Guest portal.

**Before You Begin**

You must create and upload the custom HTML files.

**Step 1** Choose **Administration > Web Portal Management > Settings** > **Guest > Multi-Portal Configurations**.

**Step 2** Choose one of these portal types:

- **Custom Default Portal**
- **Custom Device Web Authorization Portal**

**Step 3** Click the **File Mapping** tab.

**Step 4** Click the drop-down menus to assign the uploaded HTML page to the appropriate file.

**Step 5** Click **Submit**.

- Sample HTML for Custom Pages for the Guest Portal, page D-3
- Creating Custom HTML Files for Guest Portal, page 16-13
- Uploading HTML Files for Guest Portal, page 16-14

# Configuring the Guest Username and Password Policies

You must set username and password policies for guest accounts.

## Configuring the Guest Username Policy Based on Names or E-mail Accounts

You can create a guest username based on the e-mail address or the first and last name of the guest. This is a global setting affecting all Guest portals, but changes do not affect the existing accounts.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Username Policy.**

**Step 2** Choose one of these options:

- **Create username from email address**
- **Create username from the first name and last name**

**Step 3** Enter the Minimum Username length for the guest usernames. The valid range is 1-20.

**Step 4** Click **Save**.

**Related Topics**

- Guest Username Policy Settings, page A-61

## Configuring the Username Policy for Random Guest Accounts

You can create a guest username based upon a random mixture of alphabetic, numeric or special characters. The random guest username policy is used when the sponsor creates random accounts. This is a global setting affecting all Guest portals, but changes do not affect the existing accounts.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Username Policy.**

**Step 2** Enter the characters that will be used to generate the random usernames.

**Step 3** Enter the minimum number to use from each set of characters.

**Step 4** Click **Save**.

**Related Topics**

- Guest Username Policy Settings, page A-61

## Configuring the Guest Password Policy

The guest password policy determines how the password should be generated for all guest accounts. You can create a password policy based upon a mixture of alphabetic, numeric, or special characters.

This is a global setting affecting all Guest portals. However, changes to the guest password policy do not affect the existing accounts until the guest user passwords have expired and need to be changed.

**Step 1** Choose **Administration > Web Portal Management > Settings** > **Guest > Password Policy.**

**Step 2** Enter the allowable alphabetic, numeric, and special characters.

**Step 3** Enter the minimum number to use from each set of characters.

**Step 4** Click **Save**.

## Setting the Guest Password Expiration Time

You can set the number of days after which the guest password will expire, requiring the guest to reset their password. This is a global setting affecting all Guest portals.

**Before You Begin**

To use this option, you must also set the option requiring guests to change their passwords at expiration.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Portal Policy.**

**Step 2** Enter the number of days in the **Guest Password Expiration** field.

**Step 3** Click **Save**.

**Related Topics**

- Requiring Guests to Change Password, page 16-17

- Guest Portal Policy Settings, page A-59

## Requiring Guests to Change Password

You can allow or require guest users to change their password after their initial account credentials are created by the sponsor. If guest users change their passwords, sponsors cannot provide guests with their login credentials if they are lost. The sponsor must create a new guest account.

You can either allow guests to change their passwords, or you can require that they do it at expiration and at first login.

**Before You Begin**

Create a Guest portal or modify the DefaultGuestPortal. This setting is specific to each Guest portal.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration.**

**Step 2** Check the Guest portal to update and click **Edit**.

**Step 3** Click the **Operations** tab.

**Step 4** Check either or both options:

- **Allow guest users to change password**
- **Require guest users to change password at expiration and first login**

**Step 5** Click **Save**.

**Related Topics**

- Adding a New Guest Portal, page 16-10
- Multi-Portal Configuration Settings, page A-56

## Specifying the Maximum Failed Login Attempts

You can set the maximum number of failed login that can occur before a guest account is suspended, requiring the sponsor to reinstate the account. This is a global setting affecting all Guest portals.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Portal Policy.**

**Step 2** Enter the value in the **Maximum Login Failures** field.

**Step 3** Click **Save**.

**Related Topics**

Guest Portal Policy Settings, page A-59

# Defining Guest Features

You can specify required information and allowable parameters for the Guest portals.

## Specifying the Required Data for Guest Accounts

The details policy specifies the data required to create a guest account. You must define the fields that appear when sponsors create a new guest account or when guests register themselves, such as: name, company, email, and phone. This is a global setting affecting all Guest portals.

**Before You Begin**

If you create custom portals by uploading your own HTML pages, the details policy does not apply to your custom HTML code. So, if this functionality is important to you, you will need to write the HTML code to deliver similar functionality, or use the standard portal pages instead.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Details Policy.**

**Step 2** Specify whether each field is mandatory, optional or unused.

**Step 3** Click **Save**.

**What to Do Next**

You can fully customize these field names. For example, if you want to change the name of the Optional Data fields to a field commonly used by your company, you can change the text that displays on the Guest portal. See Customizing Portal UI Fields and Error Messages, page 15-5 for details.

## Limiting the Number of Supported Devices per Guest

You can limit the number of devices that can be registered to each guest.

This is a global setting affecting all Guest portals. You can set this value below the maximum number of devices currently registered to a guest account, but this change will not affect the existing registered devices.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Portal Policy.**

**Step 2** Enter the value in the **Device Registration Portal Limit** field.

**Step 3** Click **Save**.

**Related Topics**

Guest Portal Policy Settings, page A-59

## Restricting Guests to One Active Network Session

You can restrict guests to having only one device connected to the network at a time. When guests attempt to connect with a second device, the currently-connected device is automatically disconnected from the network.

This is a global setting affecting all Guest portals.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Portal Policy.**

**Step 2** Check the **Allow only one guest session per user** option.

**Step 3** Click **Save**.

**Related Topics**

Guest Portal Policy Settings, page A-59

Guest Devices Keep Losing Network Access, page G-34

## Requiring an Acceptable Use Policy for Guests

You can display an acceptable use policy which guests must accept to fully enable their account. If guests do not accept the policy, they will not obtain network access.

**Before You Begin**

Create a Guest portal, or use an existing one. The acceptable use policy is specific to each Guest portal.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration.**

**Step 2** Check the Guest portal to update and click **Edit**.

**Step 3** Click the **Operations** tab.

**Step 4** Choose one of these options to determine whether guest users must agree to an acceptable use policy:

- Not Used
- First Login
- Every Login

**Step 5** Click **Save**.

**Related Topics**

Multi-Portal Configuration Settings, page A-56

## Customizing the Acceptable Use Policy for Guests

If you require guests to acknowledge an acceptable use policy, you must update the templates to reflect your company's policy. This is a global change that impacts all Guest portals.

**Step 1** Choose **Administration > Web Portal Management > Settings** > **Guest** > **Language Template**.

**Step 2** Click the language for which you want to apply the policy.

**Step 3** Click **Configure Acceptable Use Policy Page** and update the title and text to follow your company's policy.

**Step 4** Click **Save**.

**Related Topics**

Multi-Portal Configuration Settings, page A-56

## Creating New Guest Time Profiles.

You can create custom guest time profiles that sponsors can use when creating guest accounts.

**Step 1** Choose **Administration > Web Portal Management > Settings** > **Guest > Time Profiles.**

**Step 2** Click **Add**.

**Step 3** Assign a name and description to the time profile. This name will display to sponsors when creating guest accounts.

**Step 4** Choose a time zone to be used for the time restrictions.

**Step 5** Choose an account type and duration.

**Step 6** Enter the day of the week and "from" and "to" times for the restriction times to prevent guest users from accessing the network or to log them off during these times.

**Step 7** Click the settings icon to add additional restrictions.

**Step 8** Click **Submit**.

**Related Topics**

- Guest Time Profile Settings, page A-60
- Default Guest Time Profiles, page 16-20

## Default Guest Time Profiles

Time profiles provide a way to give different levels of time access to different guest accounts. Sponsors must assign a time profile to a guest when creating an account, but they cannot make changes to the time profiles. However, you can customize them and specify which time profiles can be used by particular sponsor groups. Beginning with Cisco ISE 1.2 time profiles are referred to as the *account duration* in the Sponsor portal.

Cisco ISE 1.2 includes these default time profiles, which replace the profiles available previously:

- DefaultFirstLoginEight—the account is available for 8 hours starting when the guest user first successfully connects to the Guest portal. This replaces the DefaultFirstLogin time profile.
- DefaultEightHours—the account is available for 8 hours starting when sponsors first create the account. This replaces the DefaultOneHour time profile.
- DefaultStartEnd—sponsors can specify dates and times on which to start and stop network access.

If you upgrade to Cisco ISE 1.2, the older time profiles are still available, but you can delete them if you are not using them. If the older time profiles are assigned to a sponsor group, a message alerts you before deleting. If you perform a new installation of Cisco ISE 1.2, only the new time profiles display.

**Related Topics**

- Guest Time Profile Settings, page A-60
- Creating New Guest Time Profiles., page 16-20

## Enabling Posture for Guest Users

If you are implementing the Guest portal using the Central WebAuth (CWA) guest deployment, you can enable posture policies for guest users, such as checking for virus protection software.

**Step 1** Choose **Administration > Web Portal Management > Settings** > **Guest > Multi-Portal Configurations**.

**Step 2** Click **Add**.

**Step 3** Click the **Operations** tab.

**Step 4** Check the **Guest users should download the posture client** option.

**Step 5** Click **Submit**.

**Related Topics**

- Self-Provisioning Portal, page 17-2
- Specifying Ports and Ethernet Interfaces for End-User Portals, page 15-2
- Multi-Portal Configuration Settings, page A-56

## Specifying the Identity Source Sequence for Guests

To allow a guest user to log into the Guest portal, you must choose an identity source sequence to be used for each Guest portal. This sequence is used with the login credentials of the guest to authenticate and authorize the guest for network access.

You can set up multiple authentication sources that are checked in sequence, which can be useful when you have users in multiple stores or want to use a blend of employees and traditional guests in the same flow.

**Before You Begin**

- Create the identity source sequence, or you can use the Guest_Portal_Sequence, which is the default included with Cisco ISE.
- Create a Guest portal, or use an existing one. This setting is specific to each Guest portal.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration.**

**Step 2** Check the Guest portal to update and click **Edit**.

**Step 3** Click the **Authentications** tab.

**Step 4** Choose the appropriate identity source sequence.

**Step 5** Click **Save**.

**Related Topics**

Multi-Portal Configuration Settings, page A-56

# Allowing Guest Users to Create Own Accounts and Add Devices

Sponsors typically create login credentials for guest users, but you can bypass this role and allow guests to create their own accounts using self service and self registration.

## Allowing Guests to Create Accounts

You can allow users to create their own accounts when they are redirected to the Guest portal.

**Before You Begin**

Create a Guest portal and set the guest role and time profile.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration.**

**Step 2** Check the Guest portal to update and click **Edit**.

**Step 3** Click the **Operations** tab.

**Step 4** Check the **Guest users should be allowed to do self service** option.

**Step 5** Click **Save**.

**Related Topics**

- Multi-Portal Configuration Settings, page A-56
- Setting the Guest Role for Self Registration, page 16-23
- Setting the Time Profile for Self Registration, page 16-23

## Allowing Guests to Add Devices

You can allow guests to add devices regardless whether they are signing in using credentials created by the sponsor or by registering on their own.

**Before You Begin**

Create a Guest portal, or use an existing one. This setting is specific to each Guest portal.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration.**

**Step 2** Check the Guest portal to update and click **Edit**.

**Step 3** Click the **Operations** tab.

**Step 4** Check the **Guest users should be allowed to do device registration** option.

**Step 5** Click **Save**.

**Related Topics**

Multi-Portal Configuration Settings, page A-56

## Setting the Guest Role for Self Registration

You must choose the default guest role to assign to the guest user after self registration. The guest role is used by authorization policies to change the type of access guests have to the network and also:

- Ties the guest user to the associated identity group based on the policies defined in the system
- Controls whether or not the user is treated as an activated guest or not

This is a global setting affecting all Guest portals.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Portal Policy.**

**Step 2** Choose the default guest role from the **Self Registration Guest Role** field.

**Step 3** Click **Save**.

**Related Topics**

- Guest Portal Policy Settings, page A-59
- Allowing Guests to Create Accounts, page 16-22

## Setting the Time Profile for Self Registration

Choose the default time profile to assign to the guest user after self-registration. The time profiles determine the time periods in which guests can register access the network. Only CreateTime and FirstLogin type time profiles are available, and both are treated as FromCreation accounts when creating a self-registered guest user account.

This is a global setting affecting all Guest portals.

**Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Portal Policy.**

**Step 2** Choose the selected time profile from the **Self Registration Time Profile** field.

**Step 3** Click **Save**.

**Related Topics**

- Guest Portal Policy Settings, page A-59
- Allowing Guests to Create Accounts, page 16-22

# Monitoring Sponsor and Guest Activity

Cisco ISE provides the following ways to view and monitor sponsor and guest activities:

- Suspended and Expired Guest Accounts, page 16-24
- Purging Expired Guest Accounts, page 16-24
- Metric Meter, page 16-25
- Guest Activity Report, page 16-25
- Guest Accounting Report, page 16-25

- Guest Sponsor Summary, page 16-25
- Audit Logging for Guest and Sponsor Portals, page 16-26

# Suspended and Expired Guest Accounts

When guest accounts are suspended or expired, the affected guest users cannot access the network.

Guest accounts can be suspended in two ways:

- Guest reached the maximum number of login attempts (as defined in **Administration > Web Portal Management > Settings > Guest > Portal Policy**).
- Sponsor manually suspended the account from the Sponsor portal.

When any guest account reaches the end of its account duration (as defined by the sponsor when creating the account), the account expires.

Sponsor users can reactivate or reinstate suspended and expired accounts. However, expired accounts are automatically purged based on the criteria you set (in **Administration > Web Portal Management > Settings > General > Purge**.) After an account is purged, sponsors must create new accounts.

When expired guest accounts are purged, the associated endpoints and reporting and logging information is still retained.

# Purging Expired Guest Accounts

Cisco ISE automatically purges expired guest accounts every 15 days, but you can modify the settings with these conditions:

- If the Cisco ISE server is down when the purge is schedule to run, it will not run again until the next time the server is running at the time of the scheduled purge.
- The system checks every 15 minutes to see if it is time to run the purge. Thus, depending on the timing of this automated process and scheduled purge, there might be up to a 15 minute delay in starting the purge.

You can force expired guest user accounts to purge immediately without waiting for a scheduled purge. If a guest account created using FromFirstLogin is not used (user never logs in), it does not expire and is not purged. You must manually delete it in the Sponsor portal.

**Step 1** Choose **Administration > Web Portal Management > Settings > General > Purge**.

**Step 2** Choose one of these options:

- Check the **Enable purge settings for expired guest accounts** check box to schedule a purge and specify the frequency and time of day when a purge should occur.
- Click **Purge Now** to immediately purge the expired guest-user records.

**Step 3** Click **Save**.

**Related Topics**

- Guest Purge Settings, page A-52

# Metric Meter

Cisco ISE provides an at-a-glance view of active guests in the network in a metric meter that appears on the Cisco ISE dashboard.

# Guest Activity Report

The Guest Activity report provides details about the websites that guest users are visiting. You can use this report for security auditing purposes to demonstrate when guest users accessed the network and what they did on it. This report is available at: **Operations > Reports > Endpoints and Users > Guest Activity**.

To use this report you must first:

- Enable the passed authentications logging category. Choose **Administration > Logging > Logging Categories** and select Passed authentications.
- Enable these options on the firewall used for guest traffic:
  - Inspect HTTP traffic and send data to Cisco ISE Monitoring node. Cisco ISE only requires the the IP address and accessed URL for the Guest Activity report so, if possible, limit the data to include just this information.
  - Send syslogs to Cisco ISE Monitoring node

**Related Topics**

- Reporting, page 26-1
- Configuring Integrated URL Logging and Reporting of Guest Traffic in a Cisco Network

# Guest Accounting Report

The Guest Accounting report displays the guest login history for an indicated time period. All users assigned to the ActivatedGuest or Guest identity groups appear in this report. This report is available at: **Operations > Reports > Endpoints and Users > Guest Accounting**.

**Related Topics**

Reporting, page 26-1

# Guest Sponsor Summary

The Guest Sponsor Summary report displays all guest users created by each sponsor, and it also indicates the number of self-registered guest users. You can click on a sponsor name to display details about the guest users.This report is available at: **Operations > Reports > Endpoints and Users > Guest Sponsor Summary**.

**Related Topics**

Reporting, page 26-1

## Audit Logging for Guest and Sponsor Portals

During specific actions within the Guest and Sponsor portals, audit log messages are sent to the underlying audit system. By default, these messages appear in the /opt/CSCOcpm/logs/localStore/iseLocalStore.log file.

You can configure these messages to be sent by syslog to the Monitoring and Troubleshooting system and log collector. The monitoring subsystem presents the Sponsor and Guest activity logs.

Guest login flow gets logged in the audit logs regardless whether the guest login has passed or failed.

**Related Topics**

Chapter 25, "Monitoring and Troubleshooting,"

# Guest Deployment Scenarios

Cisco ISE supports several deployment options enable secure guest access. You can provide wired or wireless guest connectivity and local or central web authorization.

## NAD with Central WebAuth Process Flow

This scenario applies to wireless and wired network access devices. In this scenario, the guest user's credentials are added to the Cisco ISE session cache and a Change of Authorization (CoA) is requested with the network access device (NAD). The NAD makes a new authorization request to the Cisco ISE server. The session cache attributes are used to fully authenticate and authorize the guest user.

**Note** WLC added support (7.2 or later) for CoA for Central WebAuth, so that a NAD can connect to the Cisco ISE network via wired or wireless means using the same configuration method.

If the client's device is connected to a NAD, the guest service interaction takes the form of a failed MAC Authentication Bypass (MAB) request that leads to a Guest portal Central WebAuth login.

The following steps outline the process for Central WebAuth triggered by a MAB failure:

1. The client connects to the NAD through a hard-wired connection. There is no 802.1X supplicant on the client.
2. An authentication policy with a service type for MAB allows a MAB failure to continue and return a restricted network profile containing a URL-redirect for Central WebAuth user interface.
3. The NAD is configured to post MAB requests to the Cisco ISE RADIUS server.
4. The client device re-connects and the NAD initiates a MAB request.
5. The Cisco ISE server processes the MAB request and does not find an endpoint for the client machine. This MAB failure resolves to the restricted network profile and returns the URL-redirect value in the profile to the NAD in an access-accept.

   To support this function, ensure that an Authorization Policy exists featuring the appropriate "NetworkAccess:UseCase=Hostlookup" and "Session:Posture Status=Unknown" conditions. The NAD uses this value to redirect all client HTTPS traffic on port 8443 to the URL-redirect value. The standard URL value in this case is: https://ip:port/guestportal/gateway?sessionId=NetworkSessionId&action=cwa.

6. The client initiates an HTTP or HTTPS request to any URL using the client browser.
7. The NAD redirects the request to the URL-redirect value returned from the initial access-accept.
8. The gateway URL value with action CWA redirects to the Guest portal login page.
9. The client enters the username and password and submits the login form.
10. The guest action server authenticates the user credentials provided.
11. If the credentials are valid, the username and password are stored in the local session cache by the guest action server.
12. For a non-posture flow (authentication without further validation), the following applies:

    If the Guest portal is not configured to perform Client Provisioning, the guest action server sends a CoA to the NAD through an API call. This CoA will cause the NAD to reauthenticate the client using the RADIUS server. This reauthentication makes use of the user credentials stored in the session cache. A new access-accept is returned to the NAD with the configured network access. If Client Provisioning is not configured and the VLAN is in use, the Guest portal performs VLAN IP renew.

    The user does not have to re-enter their credentials in this process. The name and password entered for the initial login are used automatically.
13. For a posture-flow, the following applies:

    The Guest portal is configured to perform Client Provisioning, and the guest action redirects the client browser to the Client Provisioning URL. (You can also optionally configure the Client Provisioning Resource Policy to feature a “NetworkAccess:UseCase=GuestFlow” condition.)

    Because there is no Client Provisioning or Posture Agent for Linux, the Guest portal redirects to Client Provisioning, which in turn redirects back to a guest authentication servlet to perform optional IP release/renew and then CoA.

    a. With redirection to the Client Provisioning URL, the Client Provisioning subsystem downloads a non-persistent web-agent to the client machine and performs posture check of the client machine. (You can optionally configure the Posture Policy with a “NetworkAccess:UseCase=GuestFlow” condition.)
    b. If the client machine is non-compliant, ensure that you have configured an Authorization Policy that features “NetworkAccess:UseCase=GuestFlow” and “Session:Posture Status=NonCompliant” conditions.
    c. When the client machine is compliant, ensure that you have an Authorization policy configured with the conditions “NetworkAccess:UseCase=GuestFlow” and “Session:Posture Status=Compliant.” From here, the Client Provisioning issues a CoA to the NAD. This CoA will cause the NAD to reauthenticate the client using the RADIUS server. This reauthentication makes use of the user credentials stored in the session cache. A new access-accept is returned to the NAD with the configured network access.

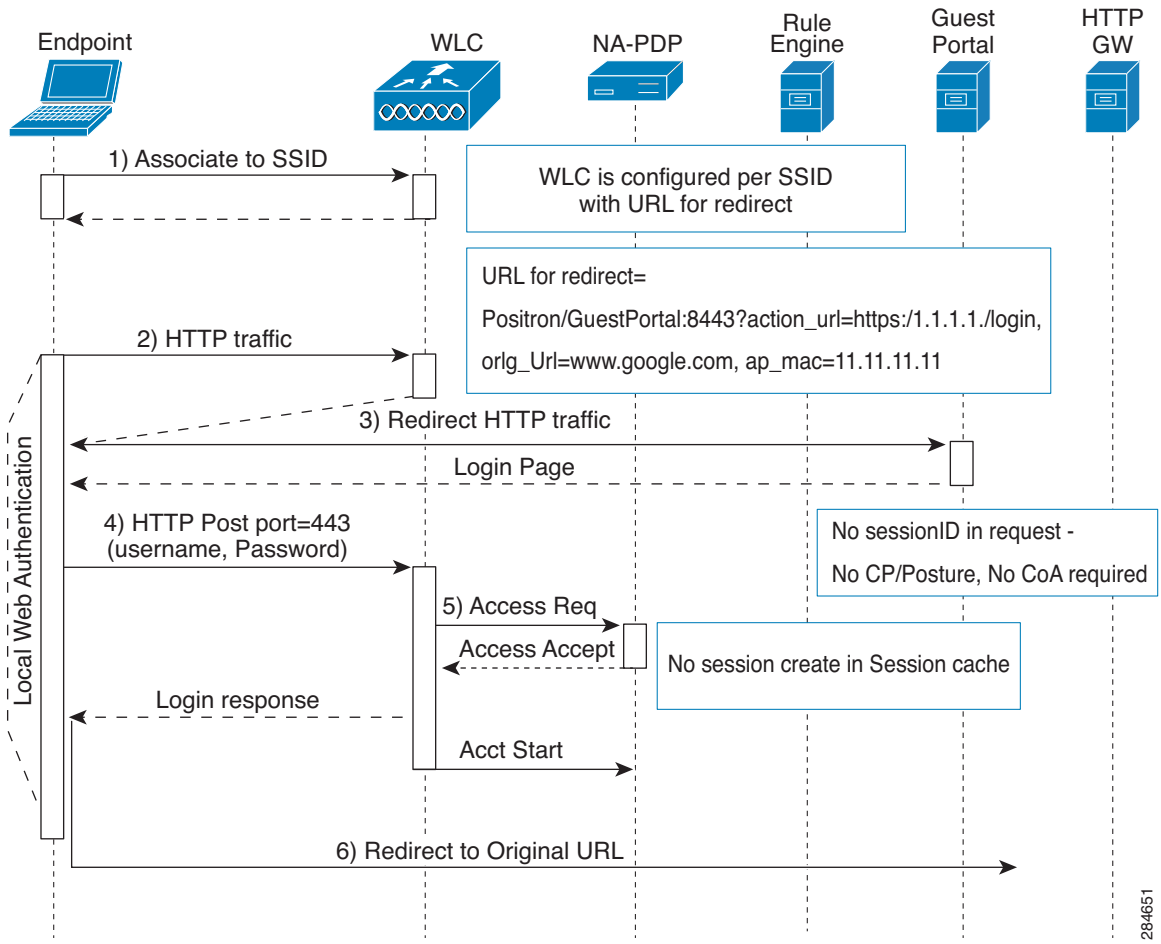
**Note** “NetworkAccess:UseCase=GuestFlow” applies for Active Directory and LDAP users logging in as guest users.

# Wireless LAN Controller with Local WebAuth

In this scenario, the user logs in and is directed to the wireless LAN controller (WLC). The WLC then redirects the user to this Guest portal where they are prompted to enter a username and password, and perform an optional accept use policy (AUP) and password change. When this is complete, the user's browser will be redirected back to the WLC to log in again.

The WLC will now be able to log the user in via RADIUS. When this is complete, the WLC will redirect the client browser to their original destination. For an illustrated example of this process flow, see Figure 16-1.

*Figure 16-1 Local WebAuth Non-Posture Flow*




# Wired NAD with Local WebAuth

In this scenario, the Guest User Login portal redirects the guest user's login request to the switch. The login request is in the form of an HTTPS URL posted to the switch, and contains the user credentials. The switch receives the user login request, and authenticates the user using a configured RADIUS server that points to the Cisco ISE RADIUS server implementation.

The following steps outline the process for Wired NAD with Local WebAuth:

1. Cisco ISE requires a login.html file with HTML redirect to be uploaded to the NAD. This login.html is returned to the client browser for any HTTPS request made.
2. The client browser in turn is redirected to the Cisco ISE Guest portal where the user's credentials are submitted.
3. After the AUP and change password is processed (if configured in the Multi-Portal configuration), the Guest portal redirects the client browser to post the user credentials on to the NAD.
4. The NAD makes a RADIUS request to the Cisco ISE to authenticate and authorize the user.

## IP Address and Port Values Required for the Login.html Page

The IP address and port values must be changed in the following HTML code for the login.html page to those being used by the Cisco ISE Policy Services nodes. The default port is 8443, but you can change this value so ensure that the value you assign to the switch matches the setting in Cisco ISE.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<head>
<title>ISE Guest Portal</title>
<meta Http-Equiv="Cache-Control" Content="no-cache">
<meta Http-Equiv="Pragma" Content="no-cache">
<meta Http-Equiv="Expires" Content="0">
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1">

<meta http-equiv="REFRESH"
content="0;url=https://ip:port/guestportal/portal.jsp?switch_url=wired">

</HEAD>
<BODY>

<center>
Redirecting ... Login
<br>
<br>
<a href="https://ip:port/guestportal/portal.jsp?switch_url=wired">ISE Guest Portal</a>
</center>

</BODY>
</HTML>
```

Because the custom login page is a public web form, consider these guidelines:

- The login form must accept user entries for the username and password and must show them as **uname** and **pwd**.
- The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.

## HTTPS Server Enabled on the NAD

To use web-based authentication, you must enable the HTTPS server within the switch using the **ip http secure-server** command.

## Support for Customized Authentication Proxy Web Pages on the NAD

You can upload custom pages for success, expiry, and failure to the NAD. Cisco ISE does not require any specific customizations so you can create these pages using the standard configuration instructions included with the NAD.

## Configuring Web Authentication on the NAD

You need to complete the web authentication on the NAD by replacing the default HTML pages with your custom files.

**Before You Begin**

Create four substitute HTML pages to use instead of the switch default HTML pages during web-based authentication.

**Step 1** To specify the use of your custom authentication proxy web pages, first store your custom HTML files on the switch flash memory. To copy your HTML files to the switch flash memory, run the following command on the switch:

**copy tftp/ftp flash**

**Step 2** After copying your HTML files to the switch, perform the following commands in global configuration mode:

| | | |
|---|---|---|
| **a.** | **ip admission proxy http login page file** *device:login-filename* | Specifies the location in the switch memory file system of the custom HTML file to use in place of the default login page. The device: is flash memory. |
| **b.** | **ip admission proxy http success page file** *device:success-filename* | Specifies the location of the custom HTML file to use in place of the default login success page. |
| **c.** | **ip admission proxy http failure page file** *device:fail-filename* | Specifies the location of the custom HTML file to use in place of the default login failure page. |
| **d.** | **ip admission proxy http login expired page file** *device:expired-filename* | Specifies the location of the custom HTML file to use in place of the default login expired page. |

**Step 3** Configure the customized authentication proxy web pages following the guidelines provided by the switch.

**Step 4** Verify the configuration of a custom authentication proxy web page, as shown in the following example:

```
Switch# show ip admission configuration
Authentication proxy webpage
    Login page           : flash:login.htm
    Success page         : flash:success.htm
    Fail Page            : flash:fail.htm
    Login expired Page   : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
```

```
Max Login attempts per user is 5
```

# Device Registration WebAuth

Using device registration web authentication (DRW), you can allow guests' devices to connect to your network without requiring guest account credentials.

## Device Registration Web Authentication Process

In this scenario, the guest user connects to the network with a wireless connection that sends an initial MAB request to the Cisco ISE node. If the user's MAC address is not in the endpoint identity store or is not marked with an AUP accepted attribute set to true, Cisco ISE responds with a URL redirection authorization profile. The URL redirection presents the user with an AUP acceptance page when the user attempts to go to any URL.

The following steps outline the process for Device Registration WebAuth:

1. A guest user connects to the network using a wireless connection and has a MAC address that is not in the endpoint identity store or is not marked with an AUP accepted attribute set to true, and receives a URL redirection authorization profile. The URL redirection presents the user with an AUP acceptance page when the guest user attempts to go to any URL.
2. If the guest user accepts the AUP, their MAC address is registered as a new endpoint in the endpoint identity store (assuming the endpoint does not already exist). The new endpoint is marked with an AUP accepted attribute set to true, to track the user's acceptance of the AUP. An administrator can then assign an endpoint identity group to the endpoint, making a selection from the Web Portal Management Multi-Portal Configurations page.
3. If the guest's endpoint already exists in the endpoint identity store, the AUP accepted attribute is set to true on the existing endpoint. The endpoint's identity group is then automatically changed to the value selected in the Web Portal Management Multi-Portal Configurations page.
4. If the user does not accept the AUP or an error occurs in the creation of the endpoint, an error page appears.
5. After the endpoint is created or updated, a success page appears, followed by a CoA termination being sent to the NAD/WLC.
6. After the CoA, the NAD/WLC reauthenticates the user's connection with a new MAB request. The new authentication finds the endpoint with its associated endpoint identity group, and returns the configured access to the NAD/WLC.

**Note** The CoA type for both wired and wireless is Termination CoA. You can configure device registration authentication (DRW) to perform VLAN IP Release and Renew, thereby re-authorizing the CoA type for both wired and wireless to Change of Auth.

## Creating the Device Registration WebAuth Guest Portal

You can configure Device Registration WebAuth (DRW).

**Step 1** Choose **Administration > Web Portal Management > Settings > Multi-Portal Configurations**.

**Step 2** Enter a unique name in the **Name** field. The portal name must be used in the URL-redirect value that is returned in the authorization profile, to specify the portal as the one that is used to handle requests

**Step 3** Choose one of the following:

- **Device Web Authorization Portal**—to use standard HTML pages provided by Cisco ISE
- **Custom Device Web Authorization Portal**—to upload customized HTML pages and images.

**Step 4** Choose **GuestEndpoints** from the Endpoint Identity Group option. Cisco ISE provides this default identity group to use for the DRW portal.

**Step 5** Click **Submit**.

---

**What to Do Next**

Creating a DRW Authorization Profile, page 16-32

**Related Topics**

Cisco ISE Authorization Profiles, page 20-2

## Creating a DRW Authorization Profile

Device Registration WebAuth requires that you set up a special authorization profile.

**Before You Begin**

You must first create the DRW Guest Portal so you can use its name when configuring the authorization profile.

---

**Step 1** Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

**Step 2** Create an authorization profile using the name of the DRW Guest portal that you created previously.

---

**What to Do Next**

Creating a DRW Authorization Policy Rule, page 16-32

**Related Topics**

Cisco ISE Authorization Profiles, page 20-2.

## Creating a DRW Authorization Policy Rule

After the guest user verifies the Accept User Policy, Cisco ISE creates an endpoint, which displays in the internal endpoint identity store. The endpoint is created using the MAC address and has the AUP Accepted attribute set to true.

---

**Step 1** Choose **Policy > Authorization > Standard** to create a new authorization policy.

**Step 2** Select the **GuestEndpoints** endpoint identity group for conditions.

**Step 3** Select the DRW authorization profile for permissions.

This setting causes a URL-redirect cisco av pair to be returned to the WLC for the initial MAB request, when the request matches the authorization policy rule. The URL-redirect takes the following form, where:

*ip:port* = the IP address and port number respectively

*DRWPortal* = the unique portal name

https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*DRWPortal*&action=cwa

**Related Topics**

Configuring Authorization Policies, page 20-8.