CHAPTER 21

User Access Management

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:

Overview

Cisco Identity Services Engine (ISE) Guest service allows users, such as guests, visitors, contractors, consultants, and customers to access a network (using HTTPS), whether the network is a corporate intranet or the public Internet. The network is defined through a VLAN and downloadable access control list (DACL) configuration in the network access device (NAD).

Cisco ISE Guest service allows users with the appropriate privileges to easily create sponsor accounts and temporary guest accounts. The Cisco ISE Guest Service performs full authentication of sponsors.

Note Cisco ISE currently supports up to 37K active Guest accounts.

Sponsors and Guests

Sponsors are users who can create guest accounts. Cisco ISE allows sponsors to provide account details to the guest by printout, e-mail, or short message service (SMS). The entire experience, from user account creation to guest network access, is stored for audit and reporting purposes.

When a guest user first attaches to the local network, either through a wireless or hard-wire connection, the user is placed in a segregated network with limited access. You can define this segregated network through the VLAN and DACL configuration on the wireless LAN controller (WLC) or NAD. In order for a guest user to function properly, the WLC or NAD must support captive HTTPS portal login scenarios where login URLs can be mapped to RADIUS servers.

Default Portals

The Cisco ISE Guest Service provides the following configurable default portals:

- Guest portal
- Sponsor portal
- Device registration web authentication portal

The Cisco ISE Guest Service supports customizable default portals to handle Guest User login, as well as the ability to create and manage Guest User accounts. Guest accounts are defined for specified time periods that are established at the time of creation.

Guest Services Functionality

To gain full access to the network, a guest opens a browser window and makes an HTTPS request by entering the URL for a web site, such as www.xyz.com or abcde.com. The guest has not been authorized and so has limited initial access.

The Guest User Portal is configured as the captive portal for WLC Local WebAuth. In the case of wired NAD, a URL-redirect value is returned to the NAD from Cisco ISE during an initial MAB lookup failure. The guest is ultimately presented with a login page where they can enter a username and password.

Cisco ISE Guest Services support the following functions:

- NAD with Central WebAuth, page 21-3
- Wireless LAN Controller with Local WebAuth, page 21-4
- Wired NAD with Local WebAuth, page 21-5
- Device Registration WebAuth, page 21-8

NAD with Central WebAuth

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 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 your client's machine is hard wired to a NAD, the guest service interaction takes the form of a failed 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 machine connects and the NAD initiates a MAB request.
5. The Cisco ISE server processes the MAB request and does not find an end point 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 or 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 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

This section covers the following scenario for wireless LAN controllers with Local WebAuth:

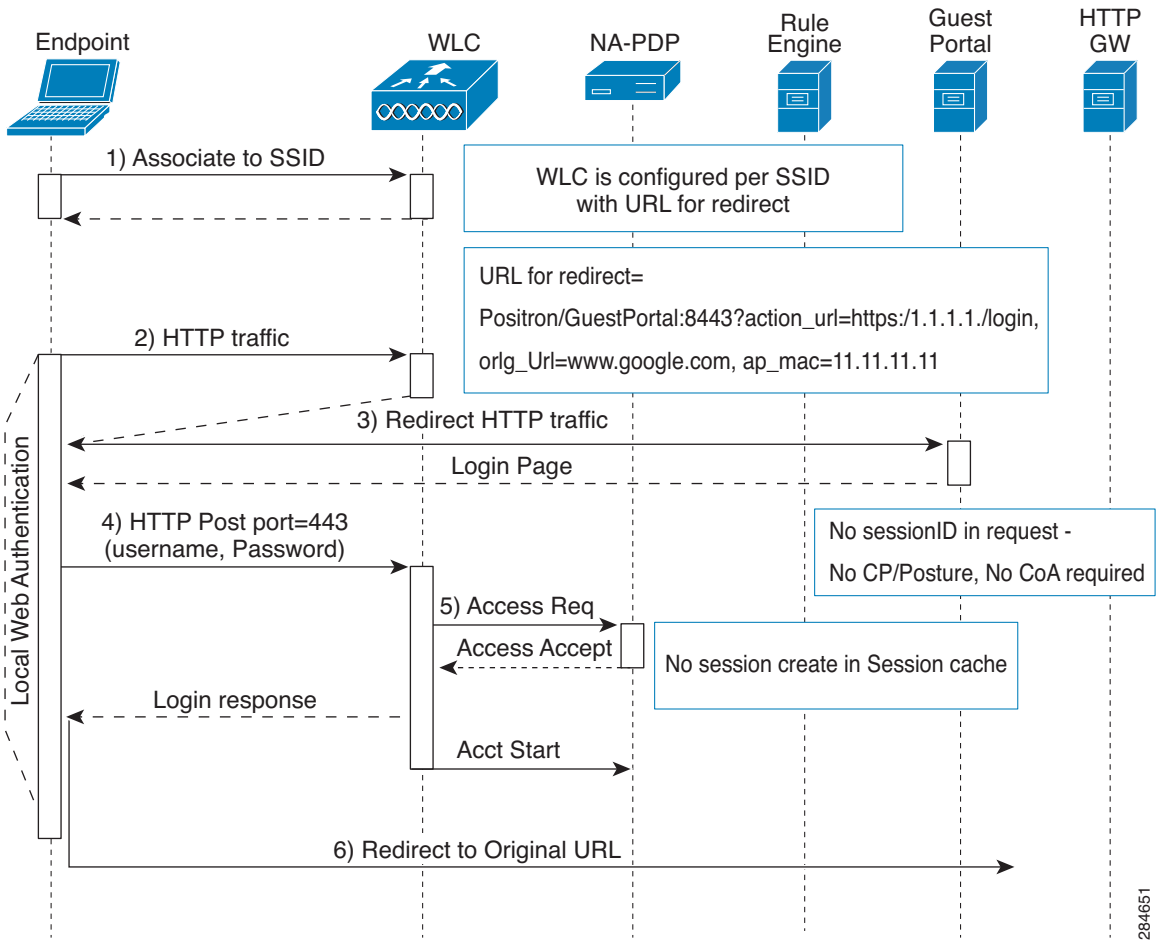
- Non-Posture Flow, page 21-4

Non-Posture Flow

A non-posture flow is a process of authentication without further validation. 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 21-1.

Figure 21-1 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.

Configuring the Switch

This section describes the process of configuring the switch for Wired NAD with Local WebAuth.

To configure the switch for Wired NAD with Local WebAuth, complete the following steps:

Step 1 Configure the HTML Login Page, page 21-6.

Step 2 Enable the HTTPS Server on the Switch, page 21-6.

Step 3 Upload Success, Expiry, and Failure Pages, page 21-7.

Step 4 Configure Web Authentication, page 21-7.

Configure the HTML Login 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.

```
<!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.

Enable the HTTPS Server on the Switch

To use web-based authentication, you must enable the HTTPS server within the switch. To do so, use the following commands:

Command	Purpose
ip http secure-server	Enables HTTPS server.

Upload Success, Expiry, and Failure Pages

Additional pages for success, expiry, and failure can also be uploaded to the NAD. You can use customized HTML pages; there is no Cisco ISE specific information required.

Configure Web Authentication

To configure web authentication, complete the following steps:

Step 1 Configure web authentication to display four substitute HTML pages to the user in place of the switch default HTML pages during web-based authentication.

Step 2 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 3 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 4 Using the following guidelines, configure your customized authentication proxy web pages:

- To enable the custom web pages feature, specify all four custom HTML files. If you specify fewer than four files, the internal default HTML pages are used.
- The four custom HTML files must be present on the flash memory of the switch. The maximum size of each HTML file is 8 KB.
- Any images on the custom pages must be on an accessible HTTPS server. Configure an intercept ACL within the admission rule.
- Any external link from a custom page requires configuration of an intercept ACL within the admission rule.
- To access a valid DNS server, any name resolution required for external links or images requires configuration of an intercept ACL within the admission rule.
- If the custom web pages feature is enabled, a configured auth-proxy-banner is not used.
- If the custom web pages feature is enabled, the redirection URL for successful login feature is not available.
- To remove the specification of a custom file, use the **no** form of the command.

The following example shows how to configure custom authentication proxy web pages:

```
Switch(config)# ip admission proxy http login page file flash:login.htm
Switch(config)# ip admission proxy http success page file flash:success.htm
```

```
Switch(config)# ip admission proxy http fail page file flash:fail.htm
Switch(config)# ip admission proxy http login expired page flash flash:expired.htm
```

Step 5 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

This section outlines the authentication process a guest user goes through using device registration web authentication (DRW), as well as how to set up Device Registration WebAuth on a Cisco ISE network. This section contains the following topics:

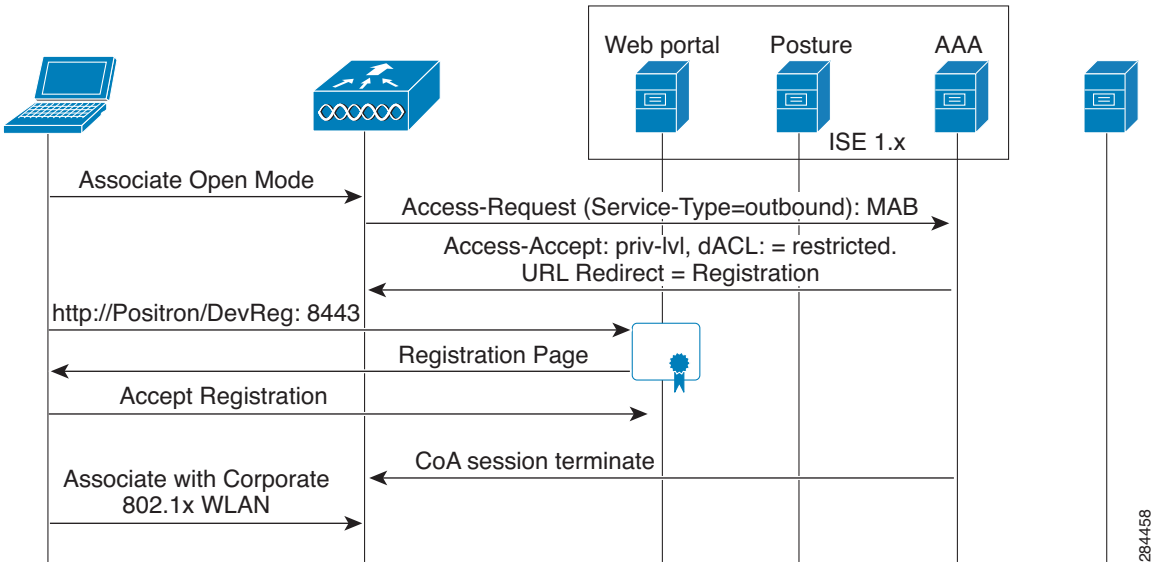
- Device Registration Web Authentication Process, page 21-8
- Configuring Device Registration WebAuth, page 21-10

Note The WLC must be configured so that it sends the client MAC address in the calling station ID value when making RADIUS access requests to Cisco ISE.

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.

Figure 21-2 Device Registration WebAuth Flow



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 (DWR) to perform VLAN IP Release and Renew, thereby changing the CoA type for both wired and wireless to Change of Auth.

Configuring Device Registration WebAuth

This section explains the process for configuring Device Registration WebAuth, and the following general steps:

1. Configure the Device Registration WebAuth, page 21-10.
2. Create a DRW Authorization Profile, page 21-10.
3. Create a DRW Authorization Policy Rule, page 21-10.

Note You must have Cisco ISE administrator privileges, to configure Device Registration WebAuth (DRW).

Configure the Device Registration WebAuth

You can configure Device Registration WebAuth (DRW) using the process outlined in the following steps:

1. Go to **Administration > Web Portal Management > Settings > Multi-Portal Configurations** in the Cisco ISE Admin user interface.
2. Choose to set the Device Registration WebAuth portal as the default Guest Portal, then choose the standard HTML pages provided in Cisco ISE, or you can upload customized HTML pages and images.
3. You can create multiple versions of each portal type, assigning each version a unique name. 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.
4. Select an endpoint identity group to which newly created endpoints are then assigned. The identity group is then used in the authorization policies to control endpoint access.
5. Next, Create a DRW Authorization Profile, page 21-10.

Create a DRW Authorization Profile

Device Registration WebAuth requires that you set up a special authorization profile. To create an authorization profile for DRW, use the steps outlined in the following process:

1. Go to the **Policy > Policy Elements > Results > Authorization > Authorization Profiles** page in the Cisco ISE Admin user interface.
2. Create an authorization profile using the name of the Device Registration WebAuth portal that you specified in Configure the Device Registration WebAuth, page 21-10.
3. Next, Create a DRW Authorization Policy Rule, page 21-10.

For more information, see Cisco ISE Authorization Policies and Profiles, page 17-5.

Create a DRW Authorization Policy Rule

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

To create a DRW authorization policy rule, use the steps outlined in the following process:

1. Create a new authorization policy or modify an existing policy, as described in Creating a New Authorization Policy, page 17-15 or Duplicating and Modifying an Existing Authorization Policy, page 17-17.
2. Add the DRW authorization profile as the permissions in an authorization policy rule.

   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

3. You can also use the endpoint identify group to affect the rule evaluation and final client access.

   The endpoint identity group is set to the selection that you make on the Multi-Portal Configurations page (Administration > Web Portal Management > Settings > Multi-Portal Configurations) in the Cisco ISE Admin user interface.

For more information on authorization policies and policy rules, see Chapter 17, "Managing Authorization Policies and Profiles."

Cisco ISE Guest Service Components

The Cisco ISE Guest service is composed of three main components:

- Guest—The guest user is the person who needs a guest user account to access the network.
- Sponsor—The sponsor user is the person who creates the guest user account. This person is often an employee of the organization. For example, a lobby ambassador who creates and manages guest user accounts through a sponsor-oriented web portal. Cisco ISE authenticates sponsors through a local database, or through external Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory identity stores.
- Admin—The admin user is the administrator who configures and maintains the Cisco ISE appliance.

Cisco ISE Guest Service Default Portals

The Cisco ISE Guest Services consists of the following portals:

- Cisco ISE Admin Portal, page 21-12
- Sponsor Portal, page 21-12
- Guest User Portal, page 21-12
- Device Registration WebAuth Portal, page 21-12

Cisco ISE Admin Portal

The admin portal facilitates in configuring global policies for the sponsor and guest users. You can configure user groups and policies from the admin portal. From the Cisco ISE Admin portal you can configure the following:

- Sponsor Groups.
- Sponsor group policies.
- General settings like purge and port.
- Sponsor portal settings like the language templates, sponsor portal customization, sponsor authentication source.
- Guest settings like username policy, password policy, guest portal policy, guest details policy, multi-portal settings, time profiles.
- Client uploadable multi portals.

Sponsor Portal

The sponsor portal facilitates the creation and management of guest user accounts. The sponsor portal allows you to perform the following functions:

- Creating, editing, deleting, suspending, reinstating guest user accounts.
- Viewing guest details.

Guest User Portal

The Guest User Portal facilitates the guest user login and consists of the following elements:

- Guest User Login screen with username and password fields.
- Accept Use Policy screen. This is an optional Terms of Use agreement.
- Required Password Change screen, which is optional at first login and later with configurable password expiration.
- Allow Password Change screen where the user can optionally change their password.
- Self Registration screen, which is an optional screen allows guests to set up their own user account.
- Device Registration.

Device Registration WebAuth Portal

The Device Registration WebAuth (DRW) portal facilitates guest user login through a wireless connection, providing the same elements as the Guest User Portal.

Note The wireless LAN controller (WLC) must be configured to send the client MAC address in the calling station ID value when making RADIUS access requests to the Cisco ISE server.

Guest Licensing

Guest services are available in Cisco ISE with both base and advanced licensing. When you first install Cisco ISE, Guest services are available with the 90-day evaluation license that comes as part of Cisco ISE. After that, you must enter a base or advanced license through the Administrator user interface to keep both the Guest and Sponsor portals from returning an HTTP 503 error response, reporting to users that the service is not available.

For more information on Cisco ISE licensing, see Chapter 12, "Managing Licenses."

Guest High Availability and Replication

Cisco ISE guest services make use of the Distributed Management System of the Cisco ISE to allow for multiple Cisco ISE nodes to communicate with one another in a deployment. In a multi-node distributed deployment, you specify a single node to be the master or the designated primary node. You make configurations for all the nodes in the deployment on the primary node, and then the configurations are replicated to the secondary nodes.

You must register a secondary node with the designated primary node in the deployment. Once a node is registered, the primary database is replicated to the secondary node it restarts as a node in the deployment.

Cisco ISE guest services function on either a primary or secondary nodes. When running on a secondary node, changes to the guest user accounts made through the Guest or Sponsor portals are propagated to the primary, and then replicated throughout the deployment.

Guest portals must be located on the same secondary nodes where the Cisco ISE Network Access is configured to handle RADIUS requests in the NAD.

For example, if node A is used to handle RADIUS requests for a NAD, the Guest portal must also be enabled on the same node A for the guest services to work correctly.

See "Guest Service Control" section on page 21-14 for details on enabling guest services on a node.

The Sponsor portal should be allowed to work on any node in a deployment, as long as that node also has Policy Services functionality enabled. For Sponsor portal updates to occur, the primary node with Administration persona must be online. If the node with Administration persona is offline, you can only view the account details. You cannot make any changes to the account.

The Guest portal can run on a node that assumes the Policy Services persona when the primary node with Administration persona is offline. However, it has the following restrictions:

- Self registration is not allowed
- Device Registration is not allowed
- The AUP is shown at every login even if first login is selected
- Change Password is not allowed and accounts are given access with the old password.
- Maximum Failed Login is not be enforced

You can make Guest administration user interface action only from the primary Admin user interface. All configuration made for guest service is the same for all nodes in the deployment.

Multiportal uploads to the primary is replicated to the secondary nodes and installed as part of the standard data replication system.

Guest and Sponsor portal port number configuration is replicated to secondary nodes and the secondary node is restarted once the replication is complete.

Note The whole deployment uses the same configuration for the portal ports.

Guest Service Control

The Guest and Sponsor portal can be disabled on a Cisco ISE node through the Cisco ISE Admin user interface.

To enable or disable Guest and Sponsor portals on any node, complete the following steps:

Step 1 Choose **Administration > System > Deployment**

The Deployment Nodes page appears, displaying all of the Cisco ISE nodes in the deployment.

Step 2 Click the node you wish to modify, and click **Edit**.

Step 3 On the General Settings tab, check or uncheck the **Enable Session Service** check box. This enables or disables the Guest and Sponsor services portal.

Operating System and Browser Support

Refer to the *Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x* document for information on operating systems and browsers supported by the Cisco ISE Guest services.

Configuring Guest Policy Conditions

Cisco ISE provides a way to create conditions that are individual, reusable policy elements that can be referred from other rule-based policies. You can create conditions from within the policy pages and as separate policy elements to be reused by other types of Cisco ISE policies such as Sponsor group or Client Provisioning policies. Whenever a policy is being evaluated, the conditions that comprise it are evaluated first.

The guest simple and compound conditions are used while you create sponsor group policies.

Simple Conditions

Simple conditions consist of an attribute, an operator, and a value. You can create simple conditions from within the policy pages and also as separate policy elements that can be reused in policies. Cisco ISE allows you to create, edit, and delete simple authentication conditions. This page lists all the simple authentication policy conditions that you have defined in Cisco ISE.

See "Configuring Policy Elements Conditions" section on page 17-17, for more detailed information.

See "Creating Simple Conditions" section on page 21-15, for information on how to define simple conditions.

Related Topics

- Creating Simple Conditions, page 21-15
- Creating a New Sponsor Group Policy, page 21-17

Creating Simple Conditions

To create simple conditions as separate policy elements, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Guest > Simple Conditions**.

The Guest Simple Condition page appears.

Step 2 Click **Add**.

Step 3 Enter the following information:

- Name—Name of the reusable condition.
- Description—An optional description for the condition.
- Attribute—Choose the attribute on which you want to build the condition. Click the drop-down arrow to select the attribute from the dictionary.
- Operator—Choose the operator from the drop-down list. This list is populated only after you select the attribute.
- Value—Choose a value from the drop-down list. This list is populated only after you select the attribute.

Note For some attributes, you can enter the value.

Step 4 Click **Submit**.

You can now use this condition to create sponsor group policies.

Next Step

See the "Creating a New Sponsor Group Policy" section on page 21-17 for information on how to define a sponsor group policy using the simple conditions that you have created.

Compound Conditions

Compound conditions are made up of two or more simple conditions. You can create compound conditions as reusable objects from within the policy creation page or from the Conditions page. This page lists all the compound conditions that you have defined in Cisco ISE.

See "Configuring Policy Elements Conditions" section on page 17-17, for more detailed information.

See "Creating Compound Conditions" section on page 21-16 for information on how to create compound conditions.

Related Topics

- Creating Compound Conditions, page 21-16
- Creating a New Sponsor Group Policy, page 21-17

Creating Compound Conditions

To create a compound condition from the Conditions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Guest > Compound Conditions**.

The Guest Compound Conditions page appears. This page lists any compound conditions that have been defined.

Step 2 Click **Add**.

Step 3 Enter a name for the compound condition. You can enter an optional description.

Step 4 Click **Select Existing Condition from Library** to select an existing simple condition or click **Create New Condition** to select an attribute, operator, and value from the expression builder.

a. If you have chosen to create a new condition, from the Expression drop-down list, choose an attribute from the dictionary based on which you want to create a condition.

b. After you have selected an attribute:

- Choose an operator (Equals, Not Equals, Matches, and so on) from the drop-down list.
- Choose the value from the drop-down list, if available or enter a value in the text box.
- To save this condition to be reused in other policies, click **Add Condition to Library** from the Action icon that appears in the same row.
- Enter a name for this condition in the Condition Name text box and click the () icon.

  The condition is saved as a simple condition and will be available for use in other policies.

Step 5 To add more conditions, click the Action icon.

Step 6 Click **Add Attribute/Value** to create a new condition or click **Add Condition from Library** to add an existing simple condition.

Step 7 Select the operand from the drop-down list box. You can select either AND or OR and the same operand will be used between all the conditions in this compound condition.

Step 8 Repeat the process from Step 5 to add more conditions.

Step 9 After you have added all the conditions, click **Submit** to create this compound condition.

Next Step

See the "Creating a New Sponsor Group Policy" section on page 21-17 for information on how to define a sponsor group policy using the compound conditions that you have created.

Sponsor Group Policy

The sponsor portal processes the sponsor group policy that allows you to log into the sponsor portal. The sponsor portal obtains the guest sponsor group from the matching sponsor group policy that allows you to access the sponsor portal. The guest sponsor groups contain a set of permissions and user settings that enable you to access the sponsor portal when you log into the sponsor portal. The sponsor portal uses the access permissions in the selected guest sponsor group to limit access within the portal. If your credentials fail, or if the sponsor group policy does not match the user settings that are defined for you when you log into the sponsor portal, then the portal returns you to the Sponsor Portal Login page.

A sponsor group policy contains one or more user roles and identity groups. It also contains one or more attribute conditions that allow you to assign the guest sponsor group. The conditions that are used in the sponsor group policy are the attributes that are selected from the dictionary attribute. One or more sponsor group policies assign you to the guest sponsor group.

A internal user that you create and store in the Cisco ISE database, and that is locally assigned to a user role or an identity group, can be a sponsor user. For the internal user to be identified as a sponsor user, the user needs to be assigned to a guest sponsor group. If you assign the internal user to a user role or identity group, and the internal user possesses the attribute conditions that are defined in the sponsor group policy, then the internal user is assigned to the guest sponsor group that is selected in the sponsor group policy.

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 more information on how to map identity groups to sponsor groups, see "Mapping Active Directory Groups to Sponsor Groups" section on page 21-23.

The sponsor user can also originate from an external identity store like LDAP or Active Directory. 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 guest 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.

The Cisco ISE deployment contains the following guest sponsor groups by default:

- SponsorAllAccount—Contains a set of permissions by default that allow you to perform the tasks on all the guest accounts.
- SponsorGroupOwnAccounts—Contain a set of permissions that allow you to perform the tasks on the guest accounts that you own.
- SponsorGroupGrpAccounts—Contain a set of permissions that allow you to perform the tasks on the guest accounts that you own, as well as all guest accounts that belong to the sponsors associated to the same sponsor group.

You can also create your own sponsor group and associate it to any identity group in the sponsor group policy.

Related Topics

Creating a New Sponsor Group Policy, page 21-17

Creating a New Sponsor Group Policy

Prerequisites:

Before you begin this procedure you should have created the following condition types:

- Simple Conditions, page 21-14
- Compound Conditions, page 21-15

To create a new sponsor group policy, complete the following steps:

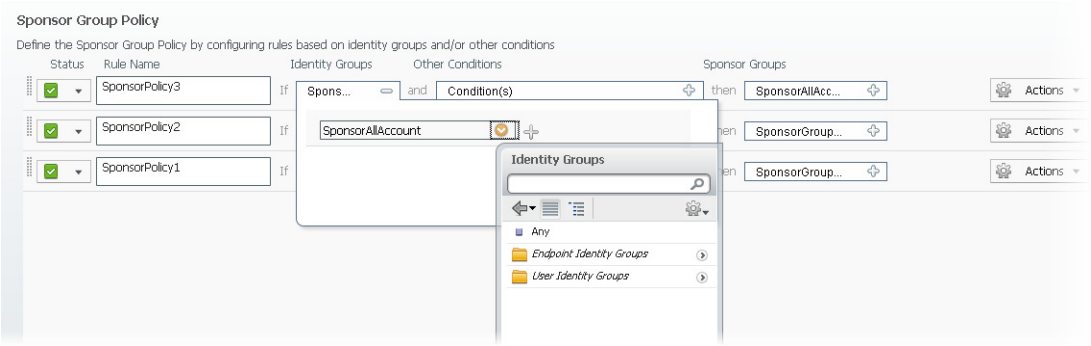
Step 1 Choose **Administration > Web Portal Management > Sponsor Group Policy**.

Step 2 Click the Action icon and choose either **Insert New Rule Above** or **Insert New Rule Below**.

A new policy entry appears in the position you designated in the Sponsor Group Policy page.

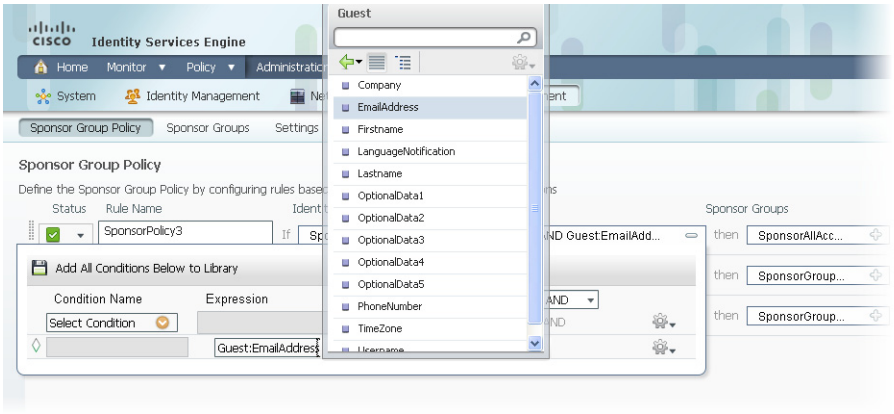
Step 3 Enter values for the following sponsor policy fields:

- Policy Name—Enter a name for the new policy.
- Identity Groups—Choose a name for the identity group associated with the policy.
  - Click **+** (“plus” sign) to display a drop-down list of group choices, or choose **Any** for the policy for this identity group to include all users.

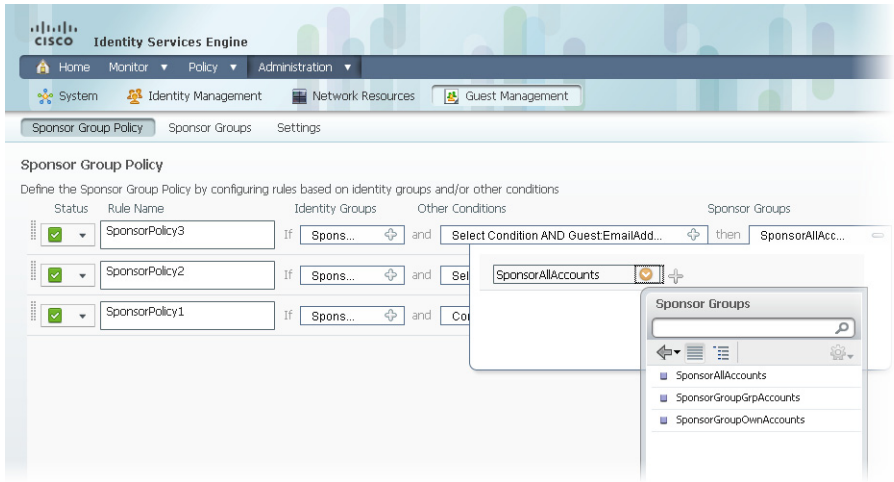


- Other Conditions—Choose the types of conditions or attributes for the identity group associated with the policy. Click **+** next to Condition(s) to display the following list of condition and attribute choices to configure:
  - Select Existing Condition from the Library—This lets you choose a Condition Name option from the drop-down list (Simple Conditions, Compound Conditions, or Time and Date Conditions) as needed.

  - Create new condition (Advanced option)—This displays a list of dictionaries that contain specific attributes related to the dictionary type.



- Sponsor Groups—Choose the sponsor group to associate with this sponsor group policy. Click **+** next to Sponsor Group to choose a group option from the drop-down list.



Step 4 Click **Save** to save your changes to the Cisco ISE system database and create this new sponsor group policy.

Modifying an Existing Sponsor Group Policy

To modify an existing sponsor group policy, complete the following steps:

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

Step 2 To choose the sponsor group policy you want to modify, click **Actions** for that policy row and select **Duplicate above** or **Duplicate below**.

A duplicate policy entry appears in the Standard panel of the Sponsor Group Policy page (either above or below the existing policy that you selected).

Step 3 Enter a new name for this policy in the **Policy Name** text box.

Step 4 Modify the desired values to create the new sponsor group policy in the corresponding fields by selecting different option choices.

Step 5 Click **Save** to save your changes to the Cisco ISE database, which creates this new sponsor group policy.

Deleting an Existing Sponsor Group Policy

To delete an existing authorization policy, complete the following steps:

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

Step 2 To select the sponsor group policy you want to delete, click **Actions** for that policy row and click **Delete**.

A confirmation dialog appears in the Standard pane of the Sponsor Group Policy page.

Step 3 Click **Delete** to confirm that you want to delete the sponsor group policy.

Step 4 Click **Save** to save your changes to the Cisco ISE system database and delete this sponsor group policy.

Note If you do not click **Save**, you will only delete the sponsor group policy locally.

Related Topics

Sponsor Group Policy, page 21-16

Sponsor Groups

Guest sponsor groups contain the permissions and settings for the sponsor user. Sponsor users belonging to a particular sponsor group have a certain set of permissions and settings when logged into the sponsor portal. You can set role-based permissions for sponsors to allow or restrict access to different functions, such as creating accounts, modifying accounts, and sending account details to guests by e-mail or short message service (SMS).

For example, if you want a set of sponsors to be unable to log in for a short period of time while some configuration is being changed, you can set the sponsor group permission to prevent login. This way you can restrict a set of sponsor users from logging in without having to remove the sponsor group.

This section covers the following procedures:

- Creating and Editing Sponsor Groups, page 21-21
- Deleting the Sponsor Group, page 21-22

Creating and Editing Sponsor Groups

To create a sponsor group, complete the following steps:

Step 1 Choose **Administration > Web Portal Management > Sponsor Groups**, which displays the Guest Sponsor Groups page.

Step 2 Click one of the following:

- **Add**—To create a new sponsor group
- **Edit**—To edit an existing sponsor group

Step 3 Give the name and description for the new sponsor group on the General tab.

Step 4 Complete the following settings on the Authorization Levels tab:

a. Set **Yes** or **No** permission for the following:

- Allow Login
- Create Accounts
- Create Random Accounts
- Import CSV
- Send Email
- Send SMS
- View Guest Password
- Allow Printing Guest Details

b. Choose one of the following options for View/Edit Accounts:

- **No**—Sponsors are not allowed to edit any guest accounts.
- **All Accounts**—Sponsors are allowed to edit/view all guest accounts.
- **Group Accounts**—Sponsors are allowed to edit guest accounts created by anyone in the same sponsor user group.
- **Own Account**—Sponsors are allowed to edit only the guest accounts they created.

c. Choose one of the following options for Suspend/Reinstate Accounts:

- **No**—Sponsors are not allowed to suspend any guest accounts.
- **All Accounts**—Sponsors are allowed to suspend or reinstate all guest accounts.
- **Group Accounts**—Sponsors are allowed to suspend guest accounts created by anyone in the same sponsor user group.
- **Own Account**—Sponsors are allowed to suspend only the guest accounts they created.

d. Account Start Time—This setting restricts the number of days the sponsor can specify for starting the guest account. This is applicable only for the Start End type of time profile.

e. Maximum Duration of Account—This setting specifies the maximum duration for which a guest account can be active. The expiration date is based on the maximum duration of the account or the time profile duration, whichever is minimum. This value overrides the maximum duration value set by the sponsor during the creation of the guest account when this value is less than the one specified in the time profile.

Step 5 Choose the guest roles that the sponsor group user would be allowed to assign to the guest user, on the Guest Roles tab.

Guest roles allow a sponsor to assign different levels of access to a guest account. These roles are used in the authorization policies to relate guest user accounts to identity groups.

Step 6 Choose the following time profiles that the sponsor group user would be allowed to assign to the guest accounts, on the Time Profiles tab:

- DefaultOneHour—The guest user can login within one hour of the account creation, after which the account expires. This means that the account start time is equal to the user creation time and end time is one hour from the start time.
- DefaultFirstLogin—The account start time starts when the guest user first logs in to the guest portal. The end time depends on the configuration which is set in that time profile.
- DefaultStartEnd—The sponsor can select both the account start and end time.

Time profiles provide a way to give different levels of time access to different guest accounts. Sponsors under any sponsor group do not have permission to make any changes to the time profiles.

Step 7 Click **Submit**.

For More Information

See "Configuring Network Access and Sponsor Users" section on page 4-9 for more information on guest roles.

See "Time Profiles" section on page 21-69 for more information on time profiles.

Related Topics

- Sponsor Groups, page 21-20
- Deleting the Sponsor Group, page 21-22

Deleting the Sponsor Group

This section shows you how to delete an existing sponsor group.

Note You are not allowed to delete sponsor groups that are in use in a sponsor group policy.

To delete sponsor groups, complete the following steps

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

Step 2 Check the check box to select the sponsor group(s) to be deleted.

Step 3 Click **Delete**.

For More Information

See "Sponsor Group Policy" section on page 21-16 for more information on sponsor group policy.

Related Topics

- Sponsor Groups, page 21-20
- Creating and Editing Sponsor Groups, page 21-21

Mapping Active Directory Groups to Sponsor Groups

Prerequisite

Before beginning this task, you should have understood and successfully performed Configuring Active Directory Groups, page 5-11.

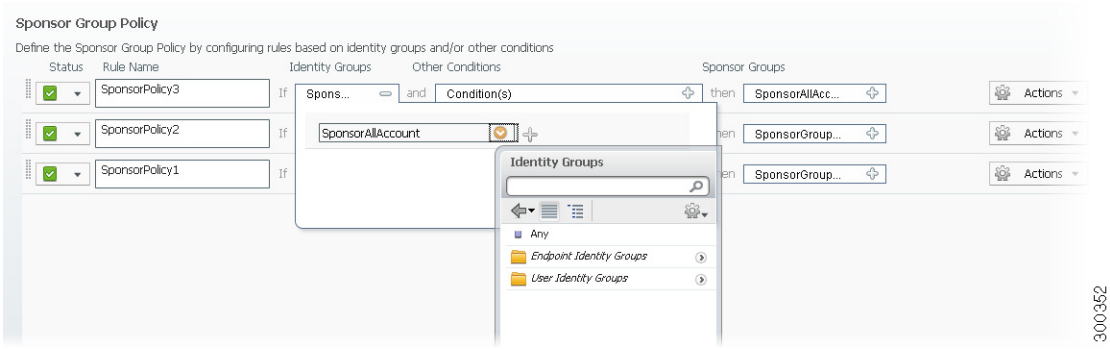
To map the Active Directory (AD) groups to the sponsor groups:

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

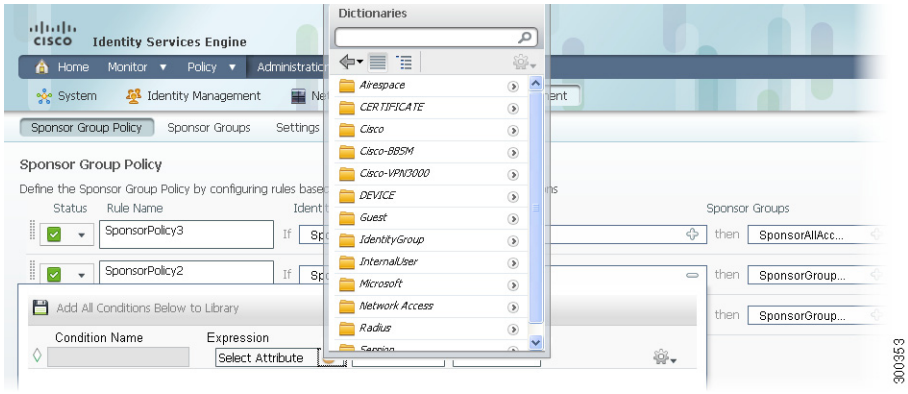
The Sponsor Group Policies page appears.

Step 2 Enter values for the following sponsor policy fields:

- Policy Name—Enter a name for the new policy.
- Identity Groups—Choose **Any** as the Identity Group because there is no group mapping with the internal groups.



- Other Conditions—Create a condition that maps the external groups to one of the populated groups. When you create the condition you will find a dictionary entry for the AD identity store that you would have created while configuring AD.
- Sponsor Group—Choose the Sponsor Group to which you want this AD condition to map.



Step 3 Click **Save**.

Related Topics

- Sponsor Group Policy, page 21-16
- Creating a New Sponsor Group Policy, page 21-17
- Sponsor Groups, page 21-20

Creating and Testing Sponsor User to Access the Sponsor Portal

Before you can log into the Sponsor portal, you must first create a sponsor user. There are no predefined sponsor users in Cisco ISE. This section shows you how to create a sponsor user, and then test the sponsor user by logging into the sponsor portal.

Creating a Sponsor User

Prerequisite

You should have created a sponsor group, as described in Creating and Editing Sponsor Groups, page 21-21.

To create a sponsor user and assign the user to a sponsor group, complete the following steps:

Step 1 Go to **Administration > Identity Management > Identities > Users**.

Step 2 Click the plus sign (**+**) to create a new network access user.

Step 3 Enter values for the Network Access User fields.

For more information, see Configuring Network Access and Sponsor Users, page 4-9.

Step 4 Choose one of the following sponsor user groups from the drop-down list:

- SponsorAllAccounts
- SponsorGroupAccounts
- SponsorOwnAccounts

Note These selections are identity groups and not sponsor groups. Sponsor groups are determined from the identity group based on the sponsor policies.

Step 5 Click **Submit**. The sponsor user is created.

Step 6 To test the sponsor user, proceed with Logging into the Sponsor Portal to Test a Sponsor User, page 21-24.

Logging into the Sponsor Portal to Test a Sponsor User

This task shows you how to log into the Sponsor portal and test the sponsor user account you created in the previous section.

Prerequisite

You must have successfully completed the task of Creating a Sponsor User, page 21-24.

To log into the Sponsor portal and test a user account, complete the following steps:

Step 1 To log into the sponsor portal, open a browser window and enter the following URL in the address field, substituting the *ipaddress* variable for the IP address of the Cisco ISE server:
https://*ipaddress*:8443/sponsorportal

The sponsor portal login screen appears.

Step 2 Log in using the credentials you specified when you created the sponsor user.

Next Step

See the "Setting Ports for the Sponsor and Guest Portals" section on page 21-26 for information on how to assign ports for the Sponsor and Guest portals.

Creating Guest Users

Guests represent authorized visitors, contractors, customers, or other temporary users who require access to your network. If you enable self-registration, guest users can create their own accounts, or sponsors can create and view guest users using the Sponsor portal. You do not create or manage guest users using the Admin portal.

Using the Admin portal, you can create internal users and assign them to the Guest identity group. However, this simply places the internal user in this identity group to be used for performing policy evaluations. For example, you could use it to define the authorization policy to allow employees to use their personal devices on the network.

SMTP Server Settings for E-mail Notifications

You must set up a Simple Mail Transfer Protocol (SMTP) server to send e-mail notification to the guest user. This server is also used to send e-mail to the short message service (SMS) gateway to deliver the SMS text message.

To set the SMTP server, complete the following steps:

Step 1 Choose **Administration > System > Settings > SMTP Server.** The SMTP Server Settings page appears.

Step 2 In the SMTP Server field, type the host name of the outbound SMTP server to which you need to deliver e-mail. For the e-mail notification to function appropriately, the SMTP host server must be accessible from the Cisco ISE server. The maximum length for this field is 60 characters.

Step 3 Choose the **Enable Notifications** option to enable mail functionality globally.

Step 4 Choose **Use email address from Sponsor**, to send guest notification e-mail from the e-mail address of the sponsor.

Step 5 If you want to specify a different e-mail address, choose **Use Default email address** and type the e-mail address from which you want guest notification e-mails to be sent (for example, username@xyz.com).

Step 6 Click **Save**.

For More Information

See *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x* for more information on the sponsor portal and how to create guest users.

Related Topic

- Setting Ports for the Sponsor and Guest Portals, page 21-26
- Purging Guest User Records, page 21-27

General Settings

You can configure general settings like the port and SMTP server settings.

- Setting Ports for the Sponsor and Guest Portals, page 21-26
- Purging Guest User Records, page 21-27

Setting Ports for the Sponsor and Guest Portals

The sponsors and guests access the portal using HTTPS. The default settings for the sponsor and guest portals is HTTPS on port 8443.

To configure the protocols and port numbers for the sponsor and guest portals, complete the following steps:

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

Step 2 Assign a port number for Guest Portal Settings. Port 8443 is the default.

Step 3 Assign a port number for Sponsor Portal Settings. Port 8443 is the default.

Step 4 To specify a Default Sponsor URL, check the check box and enter a fully qualified domain name (FQDN) in the text field, such as: guest.yourcompany.com

Step 5 Click **Save**.

Accessing the Sponsor Portal

To access the sponsor portal enter the following URL, substituting the ip_address variable with the IP address of the Cisco ISE server:

```
https://ip_address:8443/sponsorportal
```

Accessing the Guest Portal

To access the guest portal enter the following URL, substituting the ip_address variable with the IP address of the Cisco ISE server:

```
https://ip_address:8443/guestportal/Login.action
```

For More Information

See *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x* for more information on the sponsor portal.

Related Topics

Purging Guest User Records, page 21-27

Purging Guest User Records

You can purge the expired guest user records from the system. You can configure the purge settings for an automatic purge at a regular interval of time or you can perform a manual purge by clicking **Purge Now**.

To schedule the purge of expired guest user records, complete the following steps:

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

The Purge Settings page appears.

Step 2 To schedule a purge operation, check the **Enable purge settings for expired guest accounts** check box.

Step 3 Configure the following available options:

a. Enter the purge interval, in number of days. The valid range is 1-365.

b. Specify the hour of the day when the purge should occur.

Date of last purge displays the date and time when the last purge operation occurred.

Date of next purge displays the date and time when the next purge operation is scheduled to occur.

Step 4 To immediately execute a purge of expired guest user records, click **Purge Now**.

This executes a purge manually even if the Enable purge settings for expired guest accounts check box is not checked. This option provides you the freedom to purge records whenever you desire.

Step 5 Click **Save**.

There might be a 15 minute sleep cycle after the scheduled purge time. After this sleep cycle, the system checks for the correct hour and date to start the purge.

If the Cisco ISE server is down and the purge operation did not execute, the purge will not run again until the next time the server is running at the time of the scheduled purge.

By default, the purge operation is enabled and executes every 15 days, at 23:00 hrs.

Note Purge only runs on primary or standalone nodes.

Related Topics

Setting Ports for the Sponsor and Guest Portals, page 21-26

Sponsor Settings

You can configure the following sponsor settings under this sub menu:

Specifying an Authentication Source

To allow a sponsor user to log into the sponsor portal, you have to choose an identity store sequence. This sequence is used with the login credentials of the sponsor to authenticate and authorize the sponsor for access to the sponsor portal. The sequence can include external stores as well as the local Cisco ISE identity store. The identity store sequence defines which stores should be accessed and in what order they should be accessed to resolve the authentication of a sponsor user.

There is one sequence value used for all the sponsor logins. It is up to the administrator to set up one of these sequences at install time.

By default, internal users are allowed to access the sponsor portal. You can set an identity store sequence to over ride this default setting. Also, internal NSF users must be assigned to an identity group that is related to a sponsor group through a sponsor group policy, to gain access to the sponsor portal.

Note External sponsors will not have access to the sponsor portal until the identity store sequence value is selected.

When the primary node with Administration persona is down, Sponsor administrators cannot create new guest user accounts. During this time, the guest and sponsor portals will provide read-only access to already created guest and sponsor users respectively. Also, a sponsor admin who has never logged into the sponsor portal before the primary Administration node went offline, will not be able to login to the sponsor portal until a secondary Administration node is promoted or the primary Administration node becomes available.

Prerequisite

Before beginning this task, you should have successfully completed Creating Identity Source Sequences, page 5-52.

To set the identity store sequence for sponsor authentication, complete the following steps:

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

Step 2 From the Identity Store Sequence drop-down list, choose the sequence to be used for the sponsor authentication.

Step 3 Click **Save**.

For More Information

See *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x* for more information on the sponsor portal.

Related Topics

- Creating a Custom Portal Theme, page 21-29
- Applying Language Templates, page 21-32

Specifying a Simple URL for Sponsor Portal Access

As a Cisco ISE admin, you can specify a fully qualified domain name (FQDN) URL so that it automatically resolves to the sponsor portal on a given node in a deployment. For example, you could set https://guest.company.com so that it resolves to the sponsor portal.

Warning **Making a change to the ports or FQDN value restarts all the nodes in the deployment, placing the new settings in the server.xml file of each node.**

To specify a FQDN URL for sponsor portal, complete the following steps:

Step 1 In the Cisco ISE Admin user interface, choose **Administration > Web Portal Management > Settings**.

Step 2 In the Settings panel on the left, select **General > Ports**. The Guest / Sponsor Portal Settings page appears on the left.

Note If the sponsor portal is configured on any port other than 80, the sponsor is automatically redirected to the actual port that is configured. This redirection replaces the address in the sponsor's browser window.

Step 3 Under Sponsor Portal Settings, select the **Default Sponsor URL** check box and enter a fully qualified domain name URL in the text field. For example, you might enter guest.yourcompanyname.com.

Step 4 Click **Save**.

All nodes in the deployment restart, placing the new settings in the server.xml file of each node.

Step 5 Configure the network DNS server so that it resolves the FQDN to the Cisco ISE sponsor portal node.

Creating a Custom Portal Theme

You can customize a portal theme, changing text, banners, background color, and images. This functionality allows you to change the appearance of a portal without having to upload customized HTML files to the Cisco ISE server.

This section shows you how to create a custom portal theme, by setting and applying customized options. You can follow the same steps to modify an existing customized portal theme.

Note Supported image formats include jpg, jpeg, gif, and png.

To customize a portal theme, complete the following steps:

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

The Portal Theme page appears on the right.

Step 2 Customize the portal theme in the following ways:

- Change the Login Page Logo, page 21-30
- Change the Login Page Background Image, page 21-30
- Customize the Banner Logo, page 21-31
- Customize the Banner Background Image, page 21-31
- Change the Login Background Color, page 21-31
- Customize the Banner Background Color, page 21-31
- Customize the Content Background Color, page 21-32

Step 3 Click **Save**.

Change the Login Page Logo

This setting allows you to change the logo on the portal Login page. You can choose the default Cisco logo or upload a custom image.

When you upload the image, it is automatically resized to fit an image size of 46 pixels (height) by 86 pixels (width). To avoid distortion, resize your image to fit these dimensions.

To upload a custom login page logo, complete the following steps:

Step 1 Choose **Upload New File** from the drop-down list.

Step 2 Click **Browse**, navigate to and select the desired image file.

Step 3 Click **Open**.

Change the Login Page Background Image

This setting allows you to change the background image on the portal login page. You can choose the default Cisco background or upload a custom background image.

To upload a custom background image, complete the following steps:

Step 1 Select **Upload New File** from the drop-down menu.

Step 2 Click **Browse**, navigate to and select the desired image file.

Step 3 Click **Open**.

Customize the Banner Logo

This setting allows you to change the portal banner logo. You can choose the default Cisco banner or upload a custom banner logo.

When you upload the image, it is automatically resized to fit an image size of 46 pixels (height) by 86 pixels (width). To avoid distortion, resize your image to fit these dimensions.

To upload a custom banner logo, complete the following steps:

Step 1 Choose **Upload New File** from the drop-down list.

Step 2 Click **Browse**, navigate to and select the desired image file.

Step 3 Click **Open**.

Customize the Banner Background Image

This setting allows you to change the portal banner background image. You can choose the default Cisco background or upload a custom background image.

To upload a custom banner background, complete the following steps:

Step 1 Choose **Upload New File** from the drop-down list.

Step 2 Click **Browse**, navigate to and select the desired image file.

Step 3 Click **Open**.

Change the Login Background Color

This setting allows you to change the background color of the portal login page.

To change the login page background color, complete the following steps:

Step 1 Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format, such as the following: FFFFFF.

Each pair of hexadecimal digits expresses an RGB value from 0-255.

Step 2 Click **Show Color** to display the specified color.

Customize the Banner Background Color

This setting allows you to change the banner background color of the portal.

To set the login background color, complete the following steps:

Step 1 Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format, such as the following: FFFFFF.

Each pair of hexadecimal digits expresses an RGB value from 0-255.

Step 2 Click **Show Color** to display the representative color.

Customize the Content Background Color

This setting allows you to change the content background color for the portal pages.

To change the content background color for the portal, complete the following steps:

Step 1 Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format such as FFFFFF.

Each pair of hexadecimal digits expresses an RGB value from 0-255.

Step 2 Click **Show Color** to display the representative color.

Note The login page background image or the banner image always override the content background color, unless the images are transparent.

For More Information

See *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x* for more information on the sponsor portal.

Related Topics

- Specifying an Authentication Source, page 21-28
- Applying Language Templates, page 21-32

Applying Language Templates

All the Cisco ISE supported language templates are active by default for a given browser locale. A Cisco ISE administrator has the option of modifying a standard language template, or creating a custom template for the sponsor portal user interface and the guest account notification text. This allows the administrator to control the language displayed for guests in print, e-mail, or text-messages.

For information on UTF-8 support in language templates, see UTF-8 Character Support in the User Interface, page 21-34.

Note You are not allowed to create a new language template that uses the same browser locale mapping as an existing language template. Each language template must use a unique browser locale mapping.

This section describes the following topics and procedures:

Internationalization and Localization

Cisco ISE internationalization adapts the user interface for supported languages. Localization of the user interface incorporates locale-specific components and translated text. In Cisco ISE, Release 1.1.x internalization and localization support includes text in the user interface, such as labels, messages, as well as user input in text fields.

Supported Languages

Cisco ISE provides localization and internalization support for the following languages for the sponsor and guest portals:

Table 21-1 Supported Languages and Browser Locales

Language	Browser Locale
Chinese traditional	zh-tw
Chinese simplified	zh-cn
English	en
French	fr-fr
German	de-de
Italian	it-it
Japanese	ja-jp
Korean	ko-kr
Portuguese	pt-br (Brazilian)
Russian	ru-ru
Spanish	es-es

Internationalization and localization applies to all supported internet browsers.

Note Different browsers may use different locale IDs. The administrator can duplicate language templates on the Administrator portal to resolve any browser locale differences.

Guest Portal

The Guest portal can be localized to present user interface elements in all supported language locales. This includes text, field names, button labels, and messages. You can configure supported language templates on the administrator portal.

Default templates for supported languages are included in a standard Cisco ISE installation. If an un-supported locale is requested by client browser, the English locale default portal is displayed.

The following Guest portal input fields support UTF-8:

- Login user name
- Login password
- All fields on the self-registration page

UTF-8 Character Support in the User Interface

The following table lists the fields in the Cisco ISE Admin user interface, and applicable Guest Portal fields, that support UTF-8 characters for data entry and viewing.

Note

- Cisco ISE does not support administrator passwords with UTF-8 characters.
- Cisco ISE does not support UTF-8 characters in certificates.

Table 21-2 Admin User Interface UTF-8 Character Fields

Admin User Interface Element	UTF-8 Fields
Network access user configuration	• User name • First name • Last name • e-mail
User list	• All filter fields • Values shown on the User List page • Values shown on the left navigation quick view
User password policy	• Advanced > Password may not contain characters
Administrator list	• All filter fields • Values shown on the Administrator List page • Values shown on the left navigation quick view
Admin login page	• User name
RSA	• Messages • Prompts
RADIUS token	• Authentication tab > Prompt
Posture Requirement	• Name • Remediation action > Message shown to Agent User • Requirement list display
Posture conditions	• File condition > File path • Application condition > Process name • Service condition > Service name • Conditions list display

Table 21-2 Admin User Interface UTF-8 Character Fields (continued)

Admin User Interface Element	UTF-8 Fields
Guest settings	• Sponsor > Language Template: all supported languages, all fields • Guest > Language Template: all supported languages, all fields • Guest > Password Policy
System settings	• SMTP Server > Default e-mail address
Operations > Alarms > Rule	• Criteria > User • Notification > e-mail Notification user list
Operations > Reports	• Operations > Live Authentications > Filter fields • Operations > Reports > Catalog > Report filter fields
Operations > Troubleshoot	• General Tools > RADIUS Authentication Troubleshooting > Username
Policies	• Authentication > value for the av expression within policy conditions • Authorization / posture / client provisioning > other conditions > value for the av expression within policy conditions
Attribute value in policy library conditions	• Authentication > simple condition / compound condition > value for the av expression • Authentication > simple condition list display • Authentication > simple condition list > left navigation quick view display • Authorization > simple condition / compound condition > value for the av expression • Authorization > simple condition list > left navigation quick view display • Posture > Dictionary simple condition / Dictionary compound condition > value for the av expression • Guest > simple condition / compound condition > value for the av expression

Configuring Sponsor Language Templates

As a Cisco ISE administrator, you can add, modify, and delete custom language templates for both the sponsor and guest portals. You can also duplicate standard language templates, which you then modify to create a custom template. This section shows you how to configure language templates for the sponsor portal.

Note If you create a custom language template with a name that conflicts with a default template name, your template is automatically renamed after an upgrade and restore. After an upgrade and restore, default templates revert back to their default settings, and any templates with names that conflict with defaults are renamed as follows: user_{LANG_TEMP_NAME}.

For information on how to specify language templates for the guest portal, see Configuring Guest Language Templates, page 21-45.

This section covers the following topics:

Selecting a Standard Language Template

This procedure shows you how to specify any of the standard language templates for the sponsor portal, and configure the options.

To specify a standard language template, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Web Portal Management > Settings**.

Step 2 In the Settings panel on the left, select **Sponsor > Language Template** to set the language for the sponsor portal.

Step 3 Select one of the language templates from the list.

Step 4 Specify configuration options for the template, as described in Step 4 of Adding a Custom Sponsor Language Template, page 21-36.

Adding a Custom Sponsor Language Template

This section shows you how to create a custom language template that you can apply to the sponsor portal.

Note You are not allowed to create a new language template using the same browser locale mapping as an existing language template. Each language template must use a unique browser locale mapping.

To add a custom sponsor language template, complete the following steps:

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

Step 2 Click **Add** to create a new language template.

Step 3 Enter a unique **Name** and **Description** for the language template, followed by a valid **Browser Locale Mapping**.

Step 4 Set the options on the following popup dialogs:

- Configure View All Guest Accounts
- Configure Create Single Guest Account
- Configure Create Random Guest Accounts
- Configure Import Guest Accounts
- Configure Bulk Create Status Display
- Configure Bulk Print Tabular Display
- Configure Sponsor Settings Customizations
- Configure e-mail Notification
- Configure SMS Text Notification
- Configure Print Notification
- Configure Date/Time Formats
- Configure Info/Error Messages
- Configure Popup Dialog Messages
- Configure Miscellaneous Items (Login/Banner/Drawer)

Step 5 Click **Submit**.

Some example configurations are presented in the following sections:

- Configuring a Template to Create a Single Guest Account, page 21-38
- Configuring a Template for Guest Notification, page 21-39

Related Topics

- Internationalization and Localization, page 21-33
- Selecting a Standard Language Template, page 21-36
- Editing and Duplicating a Sponsor Language Template, page 21-37
- Deleting a Custom Sponsor Language Template, page 21-38

Editing and Duplicating a Sponsor Language Template

This section shows you how to edit an existing language template, or duplicate and then modify a language template.

Note It is recommended that you copy and rename a default template to a unique name before making modifications. This ensures that you have the original template to go back to in case of an error.

To edit and duplicate a language template, complete the following steps:

Step 1 Choose **Administration > Web Portal Management > Settings > Sponsor > Language Template** to configure a template for the sponsor portal.

Step 2 Select a language template from the list and do one of the following:

- Click **Edit** and modify the **Description** and valid **Browser Locale Mapping**, as necessary.

- Click **Duplicate** and enter a unique **Name** and **Description** for the language template, followed by a valid **Browser Locale Mapping**.

Step 3 Modify the template configuration options as described in Step 4 of Adding a Custom Sponsor Language Template, page 21-36.

Step 4 Click **Submit**.

Related Topics

- Internationalization and Localization, page 21-33
- Selecting a Standard Language Template, page 21-36
- Adding a Custom Sponsor Language Template, page 21-36
- Deleting a Custom Sponsor Language Template, page 21-38

Deleting a Custom Sponsor Language Template

This section shows you how to delete a custom language template that is no longer needed.

Note You can only delete custom language templates. You are not allowed to delete any of the standard default language templates.

To delete a custom language template, complete the following steps:

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

Step 2 Select the custom language template from the list, and click **Delete**.

Related Topics

- Internationalization and Localization, page 21-33
- Selecting a Standard Language Template, page 21-36
- Adding a Custom Sponsor Language Template, page 21-36
- Editing and Duplicating a Sponsor Language Template, page 21-37

Configuring a Template to Create a Single Guest Account

The Create Single Guest Account template includes the fields that appear in the Create Single Guest Account page in the sponsor portal. You can customize each field name and button in the manner and language in which you want them to appear in the sponsor portal.

Note The default configuration is English on all fields, unless changed.

To configure the Create Single Guest Account template, complete the following steps:

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

The Sponsor Portal Language Templates page appears.

Step 2 Check the check box to select a template and Click **Edit**.

The Edit Language Template page appears.

Step 3 Click **Configuring Template for Create Single Guest Account**.

Step 4 Edit the desired fields.

Step 5 Click **Save**.

Related Topics

- Configuring a Template for Guest Notification, page 21-39
- Applying Language Templates, page 21-32
- Selecting a Standard Language Template, page 21-36
- Deleting a Custom Sponsor Language Template, page 21-38

Configuring a Template for Guest Notification

When a guest account is created, the details of the account need to be passed from the sponsor to the guest. The Cisco ISE guest services provides the following ways to do this:

- Manually read the details to the guest from the screen.
- Print out the details out on paper.
- Send the details in an e-mail.
- Send the details as an SMS text message.

E-mail and SMS text message notification require e-mail servers to be configured.

The following sections describe how to configure different notification templates:

- Configuring a Template for E-mail Notification, page 21-39
- Configuring a Template for SMS Text Message Notification, page 21-41
- Configuring a Template for Print Notification, page 21-42

Configuring a Template for E-mail Notification

In the Email Notification template you can specify the subject and the body of the e-mail that will be sent to guests for their account notification.

To configure the e-mail Notification template, complete the following steps:

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

The Sponsor Portal Language Templates page appears.

Step 2 Check the check box to select a language template from the list and click **Edit**.

Step 3 Click **Configuring Template for Email Notification**.

Step 4 Type the subject of the e-mail in the Subject text box. This value appears as the subject of the e-mail notification when it is sent to the guest.

Step 5 Type the e-mail body in the Layout text box. This contains the account login information for the guest user.

You can use HTML tags and special variables for formatting the language template for e-mail notification. The following is an example of the login information for the body of an e-mail in an English language template:

Welcome to the Guest Portal, your username is %username% and password is %password%

The *%username%* and *%password%* strings will be replaced with the username and password values from the Guest User account.

In the e-mail body, you can use the following special variables to provide the details for the created guest account:

- %USERNAME% = The username created for the guest.
- %PASSWORD% = The password created for the guest.
- %STARTTIME% = The time from which the guest account will be valid.
- %ENDTIME% = The time at which the guest account will expire.
- %FIRSTNAME% = The first name of the guest.
- %LASTNAME% = The last name of the guest.
- %EMAIL% = The e-mail address of the guest.
- %TIMEZONE% = The time zone of the user.
- %MOBILENUMBER% = The mobile number of the guest.
- %OPTION1% = Optional field for editing.
- %OPTION2% = Optional field for editing.
- %OPTION3% = Optional field for editing.
- %OPTION4% = Optional field for editing.
- %OPTION5% = Optional field for editing.
- %DURATION% = Duration of time for which the account will be valid.
- %RESTRICTEDWINDOW% = The time window during which the guest is not allowed to log in.
- %TIMEPROFILE% = The name of the time profile assigned.

Note The special variables must be provided with either uppercase or lowercase letters. For example, the string for username should be %USERNAME% or %username%. Do not provide the string as %UserName%, which will not work.

Step 6 Click **Save**.

Related Topics

- Configuring a Template for Print Notification, page 21-42
- Configuring a Template to Create a Single Guest Account, page 21-38

Configuring a Template for SMS Text Message Notification

In the SMS Text Message Notification template you can set the SMS gateway, the subject and the message of the SMS.

The SMS Notification uses a third-party SMS gateway that allows e-mail messages sent to the gateway containing formatted text messages to be forwarded through SMS to the specified end user account. An example of an SMS gateway is clickatell.com. You should have a valid account with the third party. Cisco does not provide a default account. SMS messages are sent by e-mail to this gateway with a specific format defined by the third-party gateway.

To configure the SMS Text Message Notification template, complete the following steps:

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

The Sponsor Portal Language Templates page appears.

Step 2 Choose a language template from the list and click **Edit**.

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

Step 4 Type the subject of the text SMS. This value appears as the subject of the SMS notification when it is sent to the guest.

Step 5 Type the SMS gateway in the Destination text box.

Step 6 Type the SMS body in the Layout text box. This contains the account login information for the guest user.

You can use HTML tags and special variables for formatting the language template for SMS notification. You can use the following special variables, which will be replaced with the details from the created guest account:

- %USERNAME% = The username created for the guest.
- %PASSWORD% = The password created for the guest.
- %STARTTIME% = The time from which the guest account will be valid.
- %ENDTIME% = The time at which the guest account will expire.
- %FIRSTNAME% = The first name of the guest.
- %LASTNAME% = The last name of the guest.
- %EMAIL% = The e-mail address of the guest.
- %TIMEZONE% = The time zone of the user.
- %MOBILENUMBER% = The mobile number of the guest.
- %OPTION1% = Optional field for editing.
- %OPTION2% = Optional field for editing.
- %OPTION3% = Optional field for editing.
- %OPTION4% = Optional field for editing.
- %OPTION5% = Optional field for editing.
- %DURATION% = Duration of time for which the account will be valid.
- %RESTRICTEDWINDOW% = The time window during which the guest is not allowed to log in.
- %TIMEPROFILE% = The name of the time profile assigned.

Note The special variables must be provided with either uppercase or lowercase letters. For example, the string for username should be %USERNAME% or %username%. Do not provide the string as %UserName%, which will not work.

To send the text message to the mobile phone number of the guest, use the variable %MOBILENUMBER%. The %MOBILENUMBER% variable is replaced by the mobile phone number as entered by the sponsor.

Step 7 Click **Save**.

Related Topics

- Configuring a Template for E-mail Notification, page 21-39
- Configuring a Template for Print Notification, page 21-42
- Configuring a Template to Create a Single Guest Account, page 21-38

Configuring a Template for Print Notification

In the Print Notification template, you can set the guest account details, which the sponsor can bring up in a browser, print, and hand to the guest after the account is created.

To configure the SMS Text Message Notification template, complete the following steps:

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

The Sponsor Portal Language Templates page appears.

Step 2 Select a language template from the list and click **Edit**.

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

Step 4 In the Page Header text box, enter the header of the page that will be printed.

Step 5 In the Layout text box, enter the text to be printed. This contains the account login information for the guest user.

You can use HTML tags and special variables for formatting the language template for print notification. You can use the following special variables, which will be replaced with the details from the created guest account:

- %USERNAME% = The username created for the guest.
- %PASSWORD% = The password created for the guest.
- %STARTTIME% = The time from which the guest account will be valid.
- %ENDTIME% = The time at which the guest account will expire.
- %FIRSTNAME% = The first name of the guest.
- %LASTNAME% = The last name of the guest.
- %EMAIL% = The e-mail address of the guest.
- %TIMEZONE% = The time zone of the user.
- %MOBILENUMBER% = The mobile number of the guest.
- %OPTION1% = Optional field for editing.

- %OPTION2% = Optional field for editing.
- %OPTION3% = Optional field for editing.
- %OPTION4% = Optional field for editing.
- %OPTION5% = Optional field for editing.
- %DURATION% = Duration of time for which the account will be valid.
- %RESTRICTEDWINDOW% = The time window during which the guest is not allowed to log in.
- %TIMEPROFILE% = The name of the time profile assigned.

Note The special variables must be provided with either uppercase or lowercase letters. For example, the string for username should be %USERNAME% or %username%. Do not provide the string as %UserName%, which will not work.

Step 6 Click **Save**.

Related Topics

- Configuring a Template for E-mail Notification, page 21-39
- Configuring a Template for SMS Text Message Notification, page 21-41
- Configuring a Template to Create a Single Guest Account, page 21-38

Guest Settings

You can configure guest the following settings under this submenu:

- Configuring the Details Policy, page 21-43
- Configuring Guest Language Templates, page 21-45
- Multi-Portal Configurations, page 21-47
- Configuring Guest Portal Policy, page 21-67
- Configuring Guest Password Policy, page 21-68
- Time Profiles, page 21-69
- Configuring Guest Username Policy, page 21-71

Configuring the Details Policy

The details policy determines the data that the sponsor needs to enter to create a guest account. In the Guest details policy page, the Cisco ISE administrator must define the fields that should appear on the Sponsor Guest User Create and Edit pages and in the Guest User Self Registration page.

Note 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.

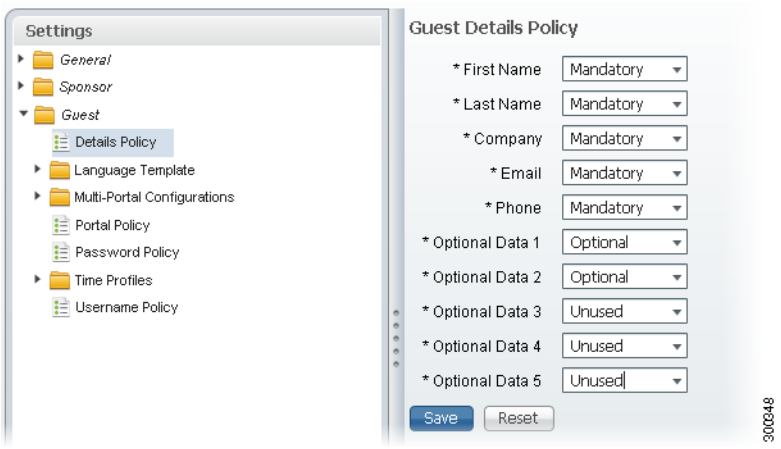
To configure a details policy, complete the following steps:

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

Step 2 Specify one of the following settings for each dialog field, as shown in Figure 21-3:

- Mandatory—If a field is set to mandatory it is displayed on the Guest User Account Create and Edit pages and it is required for the sponsor to complete.
- Optional—If a field is set to optional it is displayed on the Guest User Account Create and Edit pages. However, the sponsor can choose not to complete the field.
- Unused—If a field is set to unused it is not displayed on the Guest User Account Create and Edit page.

Figure 21-3 Details Policy Page



There are five Additional Fields that you can use to add any additional information that you require sponsors to fill out when creating guest accounts. These are described on the Details page as Additional Fields 1 through Additional Fields 5.

Note When **Create username from email address** is selected in Username Policy, you cannot disable the Email option in Guest Details Policy. See "Configuring Guest Username Policy" section on page 21-71 for more details.

See Dictionaries and Dictionary Attributes, page 7-1 for details on editing the field names.

Step 3 Click **Submit**.

Related Topics

- Configuring Guest Language Templates, page 21-45
- Multi-Portal Configurations, page 21-47
- Configuring Guest Portal Policy, page 21-67
- Configuring Guest Password Policy, page 21-68
- Time Profiles, page 21-69

- Configuring Guest Username Policy, page 21-71

Configuring Guest Language Templates

As a Cisco ISE administrator, you can add, modify, and delete custom language templates for both the sponsor and guest portals. You can also duplicate standard language templates, which you then modify to create a custom template. This section shows you how to configure language templates for the guest portal.

Note If you create a custom language template with a name that conflicts with a default template name, your template is automatically renamed after an upgrade and restore. After an upgrade and restore, default templates revert back to their default settings, and any templates with names that conflict with defaults are renamed as follows: user_{LANG_TEMP_NAME}.

For information about sponsor language templates, see Configuring Sponsor Language Templates, page 21-35.

This section covers the following topics:

- Selecting a Standard Language Template, page 21-45
- Adding a Custom Guest Language Template, page 21-45
- Editing and Duplicating a Guest Language Template, page 21-46
- Deleting a Guest Custom Language Template, page 21-47

Selecting a Standard Language Template

This procedure shows you how to specify a standard language template for the guest portal and configure its options.

To specify a standard language template, complete the following steps:

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

Step 2 Choose one of the languages from the list.

Step 3 Specify configuration options for the template, as described in Step 4 of Adding a Custom Guest Language Template, page 21-45.

Adding a Custom Guest Language Template

This section shows you how to create a custom language template that you can apply to the guest portal.

To add a custom language template, complete the following steps:

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

Step 2 Click **Add** to create a new language template.

Step 3 Enter a unique **Name** and **Description** for the language template, followed by a valid **Browser Locale Mapping**.

Step 4 Set the options on the following popup dialogs:

- Configure Template Definition
- Configure Login Page
- Configure Accept Use Policy
- Configure Change Password
- Configure Self Registration
- Configure Device Registration
- Configure VLAN/Install Release
- Configure Error Messages
- Configure Popup Dialog Messages
- Configure Miscellaneous Items

Step 5 Click **Submit**.

Some example configurations are presented in the following sections:

- Configuring a Template to Create a Single Guest Account, page 21-38
- Configuring a Template for Guest Notification, page 21-39

Related Topics

- Internationalization and Localization, page 21-33
- Selecting a Standard Language Template, page 21-36
- Editing and Duplicating a Guest Language Template, page 21-46
- Deleting a Guest Custom Language Template, page 21-47

Editing and Duplicating a Guest Language Template

This section shows you how to edit an existing guest language template, or duplicate and then modify a language template.

To edit and duplicate a language template, complete the following steps:

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

Step 2 Choose the language template from the list and do one of the following:

- Click **Edit** and modify the **Description** and valid **Browser Locale Mapping**, as necessary.
- Click **Duplicate** and enter a unique **Name** and **Description** for the language template, followed by a valid **Browser Locale Mapping**.

Step 3 Modify the template configuration options as described in Step 4 of Adding a Custom Guest Language Template, page 21-45.

Step 4 Click **Submit**.

Related Topics

- Internationalization and Localization, page 21-33
- Selecting a Standard Language Template, page 21-45
- Adding a Custom Guest Language Template, page 21-45
- Deleting a Guest Custom Language Template, page 21-47

Deleting a Guest Custom Language Template

This section shows you how to delete a custom language template that is no longer needed.

Note You can only delete custom language templates. You are not allowed to delete any of the standard default language templates.

To delete a custom language template, complete the following steps:

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

Step 2 Choose the custom language template from the list, and click **Delete**.

Related Topics

- Internationalization and Localization, page 21-33
- Selecting a Standard Language Template, page 21-45
- Adding a Custom Guest Language Template, page 21-45
- Editing and Duplicating a Guest Language Template, page 21-46

Multi-Portal Configurations

Cisco ISE provides you with the ability to host multiple portals on the Cisco ISE server. The default portal themes have standard Cisco branding that you can customize through the Cisco ISE Admin user interface. The default portal pages are dynamically generated and provide features such as change password and self registration in the Login Screen.

You can also choose to customize a portal by uploading HTML pages that are specific to your organization. These pages must use plain HTML code and must contain form actions that point to the portal backend servlets. You must define separate HTML pages for login, acceptable use policy (AUP), the change-password function, and self-registration. Additionally, when you create custom portals by uploading your own HTML pages, the details policy, language templates, and portal themes do not apply.

Note To access a custom uploaded portal, the portal URL must include the name of the portal specified during the upload.

Related Topics

- Configuring Device Registration WebAuth, page 21-10
- Hosting Multiple Portals, page 21-48
- Sample HTML Code for Creating Portal Pages, page 21-52

Hosting Multiple Portals

Prerequisite

Before beginning this task, you should have successfully understood and configured the following:

- Understanding Authentication Policies, page 16-1
- Configuring the Simple Authentication Policy, page 16-27
- Configuring the Rule-Based Authentication Policy, page 16-30

A predefined DefaultGuestPortal is available under Multi-Portal Configurations. This portal has the default Cisco look-and-feel that you can choose to customize it through the Cisco ISE Admin user interface, or you can upload HTML pages to create a customized portal. To create a personalized portal with custom HTML pages, you must first add a new portal.

Guest Portal URL

The following procedure utilizes the Guest portal URL. For reference, the Guest portal URL for the wired and wireless local web authentication is as follows:

`https://ip:8443/guestportal/portals/PortalName/portal.jsp`

Where the *PortalName* is the name of the portal as it is created during the upload.

The Guest portal redirect URL for CWA is:

`https://ip:port/guestportal/gateway?sessionId=SessionIdValue&portal=PortalName&action=cwa`

The 'ip' and 'port' values are updated by the RADIUS server as the URL-redirect is returned to the NAD. These values are the IP address and port number for the Cisco ISE guest portal server.

Note The port number 8443 is configurable through **Administration > Web Portal Management > Settings > General > Port**.

To add a new portal, complete the following steps:

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

Step 2 Click **Add**.

Step 3 On the General tab, enter a **Name** and **Description** for the new portal.

Note The name of the portal is used to access the portal and will appear in the captive portal URL specified in the network access device (NAD) for wireless LAN controller (WLC) setups. For example, a portal with the name *ClientPortal* will have the following access URL: https://*ip address:port number*/guestportal/portals/ClientPortal/portal.jsp

Step 4 Select one of the following portal types:

- Default Portal (Choose customization template and theme)
- Device Web Authentication Portal (Choose customization template and theme), and then specify an Endpoint Identity Group
- Custom Default Portal (Upload files)
- Custom Device Web Authentication Portal (Upload files), and then specify an Endpoint Identity Group

Step 5 On the **Operations** tab, do the following:

- For a Default Portal make the following selections:
  - Guest users should agree to an acceptable use policy: Not Used, First Login, Every Login. For details, see "Accept Use Policy" section on page 21-50.
  - Allow employees to directly connect their personal devices to the network. See "Self-Provisioning Flow" section on page 21-50.
  - Allow guest users to change password. See "Change Password" section on page 21-51.
  - Require guest and internal users to change password at expiration. See "Change Password" section on page 21-51.
  - Guest users should download the posture client. See "Client Provisioning Interaction with Guest Portal" section on page 21-51.

    Check the VLAN DHCP Release option to refresh Windows clients IP address after a VLAN change in both wired or wireless environments for Guest with no posture.
  - Guest users should be allowed to do self service. See "Self Registration" section on page 21-51 (If you check this option, ensure that you configure Portal policy as described in "Configuring Guest Portal Policy" section on page 21-67).
  - Guest users should be allowed to do device registration. "Device Registration" section on page 21-51.
  - Check VLAN DHCP Release option, and provide the following values in seconds: Delay to Release, Delay to CoA, and Delay to Renew. For details, see "VLAN DHCP IP Release/Renew" section on page 21-52.
- For a Device Web Authentication Portal, make the following selections:
  - Guest users should agree to an acceptable use policy: Not Used, First Login, Every Login. For details, see "Accept Use Policy" section on page 21-50.
  - Check VLAN DHCP Release option, and provide the following values in seconds: Delay to Release, Delay to CoA, and Delay to Renew. For details, see "VLAN DHCP IP Release/Renew" section on page 21-52.

Step 6 Choose the **Customization** tab, and do one of the following:

- Check the Use Browser Locale language check box.
- Uncheck the User Browser Locale language check box and select a standard Language template from the list.

Step 7 To upload custom files, select the Customize File Upload tab, upload the HTML files you have created for the Login, AUP, Change Password, and Self Registration pages. See "Sample HTML Code for Creating Portal Pages" section on page 21-52 for creating the HTML files.

These pages can include images and other links to the upload files. All uploaded files are held in a single directory with no subdirectories. Add "portals/<*portalname*>" to indicate the path to the files in the HTML code. You cannot run any backend scripts in the Cisco ISE server. Only HTML, HTM, JPEG, GIF, PNG, and CSS files are allowed.

Step 8 On the File Mapping tab, identify and choose the HTML files uploaded for the particular guest pages.

This is important for the guest flow to redirect and display the appropriate client-defined portal pages during the guest login access.

The fields under File Mapping tab are grayed out or enabled based on the selections made in the General tab.

Step 9 For a Default Portal, click the **Authentication** tab and choose the users to be authenticated during the guest login.

- Guest—Guest is the local guest user and Central WebAuth is the non-guest user. If you have a non-guest user or both a guest and non-guest user, you have to specify an identity sequence for the authentication. If Guest is chosen the default portal only authenticates guest user accounts in the local database.
- Central WebAuth—If Central WebAuth is chosen, the specified identity sequence is used to check authentication for the user. This sequence can contain both a local database and external identity stores such as Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory.

  For Central WebAuth to allow network access, appropriate authentication policies must be defined within Cisco ISE for the underlying RADIUS server to process authentication correctly.
- Both—If you chose to authenticate both, the user will be authenticated against the local database guest users first. If a user is not found, authentication will be attempted using the identity sequence.

Step 10 Click **Submit**.

Customizable Guest Portal Pages

The following are customizable Guest portal pages:

- Accept Use Policy, page 21-50
- Self-Provisioning Flow, page 21-50
- Change Password, page 21-51
- Self Registration, page 21-51
- Device Registration, page 21-51

Accept Use Policy

This page displays the network terms of use, which the user must accept to fully enable their account. If the user does not accept the policy the user will not gain expanded network access. For guest users, the AUP can be selected to appear at first login only or at every login.

Self-Provisioning Flow

To allow employees to directly connect their personal devices to the network, you should enable the self-provisioning flow. This option enables them to provision these devices using the native supplicant, which is available for Windows, Mac, iPhone, iPad, and Android devices. See "Configuring Personal Device Registration Behavior" section on page 19-30 for additional details.

If you do not want to enable self-provisioning from the devices directly, you do not need to enable this feature. Employees can still add personal devices using the My Devices Portal. See "Configuring the My Devices Portal" section on page 22-2 for additional details.

Change Password

Once the guest user or internal user has accepted the policy, Cisco ISE checks if the password has expired, if so, the Password Change screen is displayed. External users do not have their password expiration enforced.

To configure the guest password contents, see "Configuring Guest Password Policy" section on page 21-68.

To configure password policy for the internal users, see "User Password Policy" section on page 4-67.

Screens in the default portal show the password criteria for Guest or Internal Users depending on the identity of the user. You can set your own criteria in the custom portals page.

Self Registration

The Self Registration screen appears as a link on the guest user login page. This screen allows new guest users to fill in their personal information and create a new user account. Upon submission, the user account is created and the new account information is displayed on the screen. The user can print the account information.

User accounts are created with a random generated password. This password follows the password policy that is set for the guest users. The user accounts are created with the default Guest Role and Time Profile as selected in the Guest Portal Policy page.

Device Registration

The Device Registration screen appears as a link on the guest user login page. This screen allows a guest user to register their own network devices based on the MAC address of the devices.

You can configure the maximum number of devices per user from the Guest Portal Policy page and it is a global value for the entire system. The default maximum number of devices per user is five. Lowering this value will not remove existing registered devices, it will only limit the addition of new devices. The default Device Registration page has a list of existing devices for the user. Users can add new devices or remove devices from this page.

You can also add the device registration page for your custom portal. But, this page will only have the ability to add new devices. There will be no list of existing devices nor can you delete devices.

Client Provisioning Interaction with Guest Portal

The guest user portal includes interaction with the Client Provisioning application so that the client machine posture can be controlled at the time of a network access request. This interaction consists of redirecting the client browser to download a Client Provisioning agent and controlling posture before allowing full access to the network with a final user login.

You can configure the custom portal to perform client provisioning and posture. If you choose this option, the guest login flow performs a CWA, and the guest portal will be redirected to Client Provisioning after performing AUP and change password checks. In this case, the posture subsystem performs a CoA to the NAD to reauthenticate the client connection once the posture has been assessed.

Note Client Provisioning does not occur in Local Web Authentication scenarios.

If you choose **Vlan Dhcp Release**, posture will perform the client side IP release and renew operation.

Check the **Vlan Dhcp Release** option to refresh Windows clients IP address after VLAN change in both wired or wireless environments for Guest with posture.

VLAN DHCP IP Release/Renew

This affects the CWA user login flow when the network access during the final authorization switches the guest VLAN to a new VLAN. In this case, the old IP of the guest must be released before the VLAN change and a new guest IP must be requested through DHCP once the new VLAN access is in place. The Cisco ISE server redirects the guest browser to download an applet to perform the IP release renew operation.

The delay to release time should be low because it must occur immediately after the applet is downloaded and before the Cisco ISE server directs the NAD to re-authenticate with a CoA request. The default release value is 1 second.

The delay to CoA delays the Cisco ISE from executing the CoA. Enough time should be given to allow the applet to download and perform the IP release on the client. The default value is 8 seconds.

The delay to renew value is added to the IP release value and does not begin timing until the control is downloaded. The renew should be given enough time so that the CoA is allowed to process and the new VLAN access granted. The default value is 12 seconds.

For More Information

For switch configuration details and other Cisco ISE deployment information, see Chapter 9, “Setting Up Cisco ISE in a Distributed Environment.”

Related Topics

- Configuring the Details Policy, page 21-43
- Multi-Portal Configurations, page 21-47
- Configuring Guest Portal Policy, page 21-67
- Configuring Guest Password Policy, page 21-68
- Time Profiles, page 21-69
- Configuring Guest Username Policy, page 21-71

Sample HTML Code for Creating Portal Pages

You can use these examples to create HTML pages for the guest portal pages. When you create custom portals by uploading your own HTML pages, the details policy, language templates, and portal themes do not apply. So, if these features are important to you, you will need to write the HTML code to deliver similar functionality, or use the standard portal pages instead.

When you upload custom html files, these changes apply only to the guest portal. The other portals use the settings defined in the portal theme (see “Creating a Custom Portal Theme” section on page 21-29). To better synchronize the look-and-feel amongst the portals, upload your custom logos and banners to the portal theme too.

- Login Form Action and Parameters, page 21-53
- AUP Form Action and Parameters, page 21-55
- Change Password Form Action and Parameters, page 21-57
- Self-Registration Form Action and Parameters, page 21-58
- Device Registration Form Action and Parameters, page 21-61

- Self-Service Result Form Action and Parameters, page 21-62
- Error Page Form Action and Parameters, page 21-63
- Successful Guest Login Form, page 21-64

Note The following HTML examples reference a directory structure for a portal named demo2.

Login Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
<script language='javascript'>

</script>
</head>
<body class="pagebg">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="107"> </td>
  </tr>
  <tr>
    <td height="172" align="center" valign="middle"><table width="90%" border="0"
align="center" cellpadding="0" cellspacing="0">
        <tr>
          <td width="45%" height="172" align="left" valign="middle"><table width="75%"
border="0" align="left" cellpadding="0" cellspacing="0">
              <tr>
                <td width="27%"><img src="portals/demo2/logo.png" alt="" width="218"
height="63" /></td>
                <td width="73%"><table width="85%" border="0" align="right"
cellpadding="0" cellspacing="0">
                  <tr>
                    <td height="35" align="left" class="headding">ISE 1.1</td>
                  </tr>
                  <tr>
                    <td align="left" class="label">Guest Access</td>
                  </tr>
                  <tr>
                    <td align="left"> </td>
                  </tr>
                  <tr>
                    <td align="left" class="headding1">Version:1.1</td>
                  </tr>
                </table></td>
              </tr>
            </table></td>
          <td width="45%" align="right" valign="middle"><table width="50%" border="0"
cellspacing="0" cellpadding="0">
          <form id="cuesLoginForm" method="POST"
action="/guestportal/LoginCheck.action">
              <tr>
                <td width="32%" height="30" align="left" valign="middle"
class="label">Username :</td>
                <td width="68%" align="left"><input alt="Username:" name="guestUser.name"
id="username" type="text" size="20" value=""/></td>
              </tr>
              <tr>
                <td height="30" align="left" valign="middle" class="label">Password :</td>
```

```
                <td align="left"><input alt="Password:" name="guestUser.password"
id="password" type="password" size="20" value=""/></td>
              </tr>
              <tr>
                <td height="12" align="left" valign="middle"></td>
                <td height="12" align="left"></td>
              </tr>
              <tr>
                <td align="left" valign="middle"> </td>
                <td align="left"><input type="submit" name="button" id="button" value="Log
In" />
                </td>
              </tr>
              <input type="hidden" name="drpPassword" id="drpPassword"  />
               <input type="hidden" name="drpUsername" id="drpUsername"  />
             </form>
<!--          <form id="doSelfService" action="/guestportal/SelfService.action">-->
<!--            <input type="hidden" id="buttonClicked" name="buttonClicked"
value=""></input>-->
<!--           <input type="hidden" id="switch_url" name="switch_url" value=""></input>-->
<!--           <input type="hidden" id="redirect" name="redirect" value=""></input>-->
<!--           <input type="hidden" id="err_flag" name="err_flag" value=""></input>-->
<!--          </form>-->

              <!-- form for self service  -->
              <struts2:form id="selfServiceForm" action="SelfService.action">
              <input type="hidden" id="buttonClicked" name="buttonClicked"
value="${buttonClicked}"></input>
              <input type="hidden" id="switch_url" name="switch_url"
value="${switch_url}"></input>
              <input type="hidden" id="redirect" name="redirect"
value="${redirect}"></input>
              <input type="hidden" id="err_flag" name="err_flag"
value="${err_flag}"></input>
              </struts2:form>

              <struts2:form id="changePasswordForm"
action="ChangePassLoginMultiPortal.action">
                <input type="hidden" id="username" name="guestUser.name"
value="${username}"></input>
                <input type="hidden" id="password" name="guestUser.password"
value="${password}"></input>
              </struts2:form>

             <tr>
               <td align="left" valign="middle"> </td>
               <td align="left">   
               </td>
             </tr>
             <tr>
               <td align="left" valign="middle"> </td>
                <td align="left"><a href="javascript:doChangePassword();" class="link"
>Change Password</a>  
               <a href="javascript:doSelf();"  class="link">SelfService</a>  
               <a href="javascript:submitMyForm();"  class="link">Device Registration</a>
               </td>
             </tr>

           </table></td>
       </tr>
     </table></td>
  </tr>
</table>
<div id="footer">
```

```
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>

<script>
function doSelf()
{
    document.forms[0].action = "SelfService.action";
    document.getElementById("buttonClicked").value =
document.getElementById("buttonClicked").value;
    document.getElementById("redirect").value = document.getElementById("redirect").value;
    document.getElementById("switch_url").value =
document.getElementById("switch_url").value;
    document.forms[0].submit();
}

function doChangePassword()
{
    //var changePasswordForm = document.getElementById("changePasswordForm");
    //changePasswordForm.submit();
    document.forms[0].action = "ChangePassLoginMultiPortal.action";
    document.getElementById("username").value = document.getElementById("username").value;
    document.getElementById("password").value = document.getElementById("password").value;
    document.forms[0].submit();
}

function submitMyForm(){
    document.forms[0].action = "DevRegPortalLogin.action";
    document.getElementById("drpUsername").value =
document.getElementById("username").value;
    document.getElementById("drpPassword").value =
document.getElementById("password").value;
    document.forms[0].submit();
}

</script>
```

AUP Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
</head>
<body bgcolor="#ccebfe">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="75" bgcolor="#022d4d"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0">
      <tr>
        <td width="15%" align="left" valign="middle"><img src="portals/demo2/logo.png"
alt="" width="157" height="44" /></td>
        <td width="72%" class="headding">ISE 1.1 Guest Portal</td>
        <td width="13%" align="right" valign="middle" > </td>
      </tr>
    </table></td>
  </tr>
  <tr>
    <td bgcolor="#ccebfe"><table width="98%" border="0" align="center" cellpadding="0"
cellspacing="0" class="content">
      <tr>
        <td> </td>
      </tr>
```

```
      <tr>
        <td align="left" class="headding2">Acceptable Use Policy</td>
      </tr>
      <tr>
        <td align="left" >Please accept the policy:<br /><br />

1. You are responsible for </br>(1) maintaining the confidentiality of the password and
</br>(2) all activities that occur under your username and password.
</br></br>
2. Cisco systems offers the Service for activities such as the active use of e-mail,
instant messaging, browsing the World Wide Web and accessing corporate intranets. High
volume data transfers, especially sustained high volume data transfers, are not permitted.
Hosting a web server or any other server by use of our Service is prohibited. Trying to
access someone elseâ ™s account, sending unsolicited bulk e-mail, collection of other
peopleâ ™s personal data without their knowledge and interference with other network users
are all prohibited.
</br></br>
3. Cisco systems reserves the right to suspend the Service if (1) Cisco systems reasonably
believes that your use of the Service is unreasonably excessive or (2) you are using the
Service for criminal or illegal activities.
</br></br>
4. You do not have the right to resell this Service to a third party.

</br></br>
5. Cisco systems reserves the right to revise, amend or modify these Terms & Conditions,
our other policies and agreements, and aspects of the Service itself. Notice of any
revision, amendment, or modification will be posted on Cisco systemâ ™s website and will
be effective as to existing users 30 days after posting same.
</br></br></td>
      </tr>
      <form action="/guestportal/AcceptPolicy.action" method="post">
      <tr>
        <td align="left"><input  type="checkbox" name="guestUser.acceptUsePolicy"
id="guestUser.acceptUsePolicy" value="false" onclick="javascript:enableButtons()" />Accept
terms and conditions</td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      <tr>
        <td align="left"><input  type="Submit" id="acceptButton"  value="Accept" />
               <input  type="button"  id="declineButton" value="Decline"
onclick="javascript:doDeclineTerms()"/></td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      </form>
    </table></td>
  </tr>
</table>
<form id="declineTerms" onsubmit="return true;" action="/guestportal/DeclinePolicy.action"
method="post"><table class="wwFormTable">
<input type="hidden" id="buttonClicked" name="buttonClicked" value=""></input>
<input type="hidden" id="switch_url" name="switch_url" value=""></input>
<input type="hidden" id="redirect" name="redirect" value=""></input>
<input type="hidden" id="err_flag" name="err_flag" value=""></input>
</table></form>

<div id="footer">
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>
```

```
<script>
enableButtons();
function enableButtons(){
  accepttermsCheckbox = document.getElementById('guestUser.acceptUsePolicy').checked;
  if (!accepttermsCheckbox) {
    document.getElementById('acceptButton').disabled = true;
    document.getElementById('guestUser.acceptUsePolicy').value = false;
  }
  else {
    document.getElementById('acceptButton').disabled = false;
    document.getElementById('guestUser.acceptUsePolicy').value = true;
  }
}
</script>

<script>
function doDeclineTerms()
{
    var declineTermsForm = document.getElementById("declineTerms");
    declineTermsForm.submit();
}
</script>
```

Change Password Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
</head>
<body class="pagebg">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="107"> </td>
  </tr>
  <tr>
    <td height="172" align="center" valign="middle"><table width="90%" border="0"
align="center" cellpadding="0" cellspacing="0">
        <tr>
          <td width="45%" height="172" align="left" valign="middle"><table width="75%"
border="0" align="left" cellpadding="0" cellspacing="0">
              <tr>
                <td width="27%"><img src="portals/demo2/logo.png" alt="" width="218"
height="63" /></td>
                <td width="73%"><table width="85%" border="0" align="right"
cellpadding="0" cellspacing="0">
                  <tr>
                    <td height="35" align="left" class="headding">ISE 1.1</td>
                  </tr>
                  <tr>
                    <td align="left" class="label">Guest Access</td>
                  </tr>
                  <tr>
                    <td align="left"> </td>
                  </tr>
                  <tr>
                    <td align="left" class="headding1">Version:1.1</td>
                  </tr>
                </table></td>
              </tr>
            </table></td>
          <td width="45%" align="right" valign="middle"><table width="65%" border="0"
cellspacing="0" cellpadding="0">
```

```
              <form action="/guestportal/ChangePassword.action" method="post">
              <tr>
                <td height="30" align="left" valign="middle" class="label">Enter current
password :</td>
                <td align="left"><input alt="Password:" name="currentpassword"
id="currentpassword" type="password" size="20" value=""/></td>
              </tr>
               <tr>
                <td height="30" align="left" valign="middle" class="label">Enter new
password :</td>
                <td align="left"><input alt="Password:" name="newpassword"
id="newpassword" type="password" size="20" value=""/></td>
              </tr>
               <tr>
                <td height="30" align="left" valign="middle" class="label">Re-enter new
password :</td>
                <td align="left"><input alt="Password:" name="confirmpassword"
id="confirmpassword" type="password" size="20" value=""/></td>
              </tr>
              <tr>
                <td height="12" align="left" valign="middle"></td>
                <td height="12" align="left"></td>
              </tr>
              <tr>
                <td align="left" valign="middle"> </td>
                <td align="left"><input type="submit" name="button" id="button" value="Log
In" />
                </td>
              </tr>
             </form>
            </table></td>
        </tr>
      </table></td>
  </tr>
</table>
<div id="footer">
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>
```

Self-Registration Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
</head>
<body bgcolor="#ccebfe">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="75" bgcolor="#022d4d"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0">
      <tr>
        <td width="15%" align="left" valign="middle"><img src="portals/demo2/logo.png"
alt="" width="157" height="44" /></td>
        <td width="72%" class="headding">ISE 1.1 Guest Portal</td>
        <td width="13%" align="right" valign="middle" > </td>
      </tr>
    </table></td>
  </tr>
  <tr>
    <td valign="top" bgcolor="#ccebfe"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0" class="content">
```

```
      <tr>
        <td> </td>
      </tr>
      <tr>
        <td align="left" class="headding2">Self Registration</td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      <tr>
        <td align="left"><table width="50%" border="0" align="left" cellpadding="0"
cellspacing="0" class="content">
       <form id="selfServiceForm" action="/guestportal/SelfServiceSubmit.action"
method="post">
              <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">First Name :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.firstName" id="firstName" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Last Name :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.lastName" id="lastName" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Email Address :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.emailAddress" id="emailId" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Phone Number :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.phoneNumber" id="phoneno" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Company :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.company" id="company" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Optional Data 1 :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.optionalData1" id="data1" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Optional Data 2 :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.optionalData2" id="data2" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Optional Data 3 :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.optionalData3" id="data3" type="text" size="20" /></td>
              </tr>
               <tr>
```

```
                <td width="30%" height="30" align="left" valign="middle"
class="content">Optional Data 4 :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.optionalData4" id="data4" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Optional Data 5 :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.optionalData5" id="data5" type="text" size="20" /></td>
              </tr>

        <tr>
        <td width="30%" height="30" align="left" valign="middle" class="content">TimeZone
:</td>
        <td width="70%" align="left"><select name="guestUser.timezone">
        <option value="UTC">UTC</option>
        <option value="America\New_York">America\New_York</option>
        <option value="Europe\London">Europe\London</option>
        </select></td>
        </tr>
              <tr>
                <td height="12" align="left" valign="middle"></td>
                <td height="12" align="left"></td>
              </tr>
              <tr>
                <td align="left" valign="middle"> </td>
                <td align="left"><input type="submit" name="button" id="button"
onclick="javascript:doOnSubmit()" value="Submit" />
                <input type="submit" name="button2" id="button2"
onclick="javascript:doCancel()" value="Cancel" />                </td>
              </tr>
             </form>
          </table></td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
    </table></td>
  </tr>
</table>
<div id="footer">
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>

<script>
function doOnSubmit()
{
    var selfServiceForm = document.getElementById("selfServiceForm");
    selfServiceForm.submit();
}
function doCancel()
{
    document.forms[0].action = "Login.action";
    document.forms[0].submit();
}
</script>
```

Device Registration Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
<script language='javascript'>

</script>
</head>
<body bgcolor="#ccebfe">
<form id="deviceRegistrationPortal"  action="/guestportal/RegisterDevice.action"
method="post">

    <input type="hidden" name="drpUsername" id="drpUsername" value="" />
    <input type="hidden" name="devRegLimit" id="devRegLimit" value="" />

    <input type="hidden" name="regDevices" id="regDevices" value="" />
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="75" bgcolor="#022d4d"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0">
      <tr>
        <td width="15%" align="left" valign="middle"><img src="portals/demo2/logo.png"
alt="" width="157" height="44" /></td>
        <td width="72%" class="headding">ISE 1.1 Device Registration Portal</td>
        <td width="13%" align="right" valign="middle" > </td>
      </tr>
    </table></td>
  </tr>
  <tr>
    <td align="left" valign="top" bgcolor="#ccebfe"><table width="98%" border="0"
align="center" cellpadding="0" cellspacing="0" class="content">
      <tr>
        <td> </td>
      </tr>
      <tr>
        <td align="left"><table width="100%" border="0" cellpadding="0" cellspacing="0"
bgcolor="#abcee4" style="padding:10px; border:#6b93ac solid 1px;">
          <tr>
            <td style="padding:10px 0 0 10px;">Please register your device :<br />
Please note that you can not register more than 5 devices</td>
          </tr>
          <tr>
            <td height="15"></td>
          </tr>
          <tr>
           <td style="padding:0 0 0 10px;"><table width="100%" border="0" cellspacing="0"
cellpadding="0">
  <tr>
    <td width="7%">MAC Address : </td>
    <td width="93%"><input id="registeredMac"  name="registeredMac" type="text" /></td>
  </tr>
</table></td>
          </tr>
           <tr>
            <td height="15"></td>
          </tr>
          <tr>
            <td style="padding:0 0 0 10px;"><input  type="Submit"    value="Register"
/></td>
          </tr>
          <tr>
            <td height="15"></td>
```

```
          </tr>
        </table></td>
      </tr>

      <tr>
        <td align="left"> </td>
      </tr>

      <tr>
        <td align="left">
    </td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>

    </table></td>
  </tr>
</table>
<div id="footer">
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</form>
</body>
</html>
```

Self-Service Result Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
</head>
<body bgcolor="#ccebfe">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="75" bgcolor="#022d4d"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0">
      <tr>
        <td width="15%" align="left" valign="middle"><img src="portals/demo2/logo.png"
alt="" width="157" height="44" /></td>
        <td width="72%" class="headding">ISE 1.1 Guest Portal</td>
        <td width="13%" align="right" valign="middle" > </td>
      </tr>
    </table></td>
  </tr>
  <tr>
    <td valign="top" bgcolor="#ccebfe"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0" class="content">
      <tr>
        <td> </td>
      </tr>
      <tr>
    <!--INSERT HEADER HERE --><td align="left" class="headding2"> Self Registration
created user: fsdf</td><!--END HEADER HERE -->
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      <tr>
        <td align="left"><table width="50%" border="0" align="left" cellpadding="0"
cellspacing="0" class="content">
```

```
          <!--INSERT RESULTS HERE --><tr><td width="30%" align="left" class="content">
User name: fsdf</td></tr><tr><td width="30%" align="left" class="content"> Password:
9F_</td></tr><tr><td width="30%" align="left" class="content"> First Name:
fdsf</td></tr><tr><td width="30%" align="left" class="content"> Last Name:
sdf</td></tr><tr><td width="30%" align="left" class="content"> Email Address:
</td></tr><tr><td width="30%" align="left" class="content"> Phone Number:
</td></tr><tr><td width="30%" align="left" class="content"> Company: </td></tr><tr><td
width="30%" align="left" class="content"> Optional Data 1: </td></tr><tr><td width="30%"
align="left" class="content"> Optional Data 2: </td></tr><tr><td width="30%" align="left"
class="content"> Optional Data 3: </td></tr><tr><td width="30%" align="left"
class="content"> Optional Data 4: </td></tr><tr><td width="30%" align="left"
class="content"> Optional Data 5: </td></tr><!--END RESULTS HERE -->
              <tr>
                <td height="12" align="left" valign="middle"></td>
                <td height="12" align="left"></td>
              </tr>
              <form id="loginform" action="/guestportal/Login.action" method="post">
          <tr>
                <td align="left" valign="middle"> </td>
                <td align="left"><input type="submit" name="button2" id="button2"
onclick="javascript:doOk()" value="OK" />                </td>
              </tr>
          </form>
          </table></td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
    </table></td>
  </tr>
</table>
<div id="footer">
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>

<script>

function doOk()
{
    document.forms[0].action = "Login.action";
    document.forms[0].submit();
}
</script>
```

Error Page Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Error Detected</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
<script language='javascript'>

</script>
</head>
<body class="pagebg">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="107"> </td>
  </tr>
```

```
  <tr>
    <td height="172" align="center" valign="middle"><table width="90%" border="0"
align="center" cellpadding="0" cellspacing="0">
        <tr>
          <td width="45%" height="172" align="left" valign="middle"><table width="75%"
border="0" align="left" cellpadding="0" cellspacing="0">
              <tr>
                <td width="27%"><img src="portals/demo2/logo.png" alt="" width="218"
height="63" /></td>
                <td width="73%"><table width="85%" border="0" align="right"
cellpadding="0" cellspacing="0">
                  <tr>
                    <td height="35" align="left" class="heading">Error Detected in Guest
Portal</td>

                  </tr>
                  <tr>
           <!--INSERT ERROR HERE -->
                    <td height="35" align="left" class="heading">Second</td>
           <!--END ERROR HERE -->
                  </tr>
                </table></td>
              </tr>
            </table></td>
          <td width="45%" align="right" valign="middle"><table width="50%" border="0"
cellspacing="0" cellpadding="0">

              <tr>
                <td align="left" valign="middle"> </td>
                <td align="left">   
                </td>
              </tr>

            </table></td>
        </tr>
      </table></td>
  </tr>
</table>
<div id="footer">
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>

<script>
function doSelf()
{
    document.forms[0].action = "Login.action";
    document.forms[0].submit();
}
</script>
```

Successful Guest Login Form

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/CustomPortal/style.css" rel="stylesheet" type="text/css" />
</head>
<body bgcolor="#ccebfe">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="75" bgcolor="#022d4d"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0">
```

```
      <tr>
        <td width="15%" align="left" valign="middle"><img
src="portals/CustomPortal/logo.png" alt="" width="90" height="90" /></td>
        <td width="72%" class="headding">ISE 1.0 Guest Portal</td>
        <td width="13%" align="right" valign="middle" > </td>
      </tr>
    </table></td>
  </tr>
  <tr>
    <td valign="top" bgcolor="#ccebfe"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0" class="content">
      <tr>
        <td> </td>
      </tr>
      <tr>
    <!--INSERT HEADER HERE --><td align="left" class="headding2"> CoA Successful
</td><!--END HEADER HERE -->
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      <tr>
        <td align="left"><table width="50%" border="0" align="left" cellpadding="0"
cellspacing="0" class="content">

       <tr>
               <td height="12" align="left" valign="middle"></td>
               <td height="12" align="left"></td>
             </tr>
             <form id="loginform" action="/guestportal/Login.action" method="post">
         <tr>
               <td align="left" valign="middle"> </td>
               <td align="left"><input type="submit" name="button2" id="button2"
onclick="javascript:doOk()" value="OK" />               </td>
             </tr>
         </form>
          </table></td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
    </table></td>
  </tr>
</table>
<div id="footer">
  <div  style="padding:0 0 0 10px;">2008-2009, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>

<script>

function doOk()
{
    document.forms[0].action = "Login.action";
    document.forms[0].submit();
}
</script>
```

Sample style.css

```
@charset "utf-8";
/* CSS Document */

body {
    margin-left: 0px;
    margin-top: 0px;
    margin-right: 0px;
    margin-bottom: 0px;
}
.pagebg {
    background:url("../demo2/pageBg.jpg") repeat-x;
}
.label {
    font-family:Arial, Helvetica, sans-serif;
    color:#FFFFFF;
    font-size:12px;
}
#footer {
    height:23px;
    font-family:Arial, Helvetica, sans-serif;
    color:#022d4d;
    position:absolute;
    width:100%;
    margin:0px auto;
    text-align:left;
    bottom:-0px;
    font-size:12px;
}
.headding {
font-family:Arial, Helvetica, sans-serif;
color:#ffffff;
font-size:20px;
}
.headding1 {
font-family:Arial, Helvetica, sans-serif;
font-size:12px;
font-weight:bold;
color:#ffffff;
}
.headding2 {
font-family:Arial, Helvetica, sans-serif;
color:#022d4d;
font-size:17px;
font-weight:bold;
}
.headding3 {
font-family:Arial, Helvetica, sans-serif;
color:#022d4d;
font-size:12px;
font-weight:bold;
}
.content {
font-family:Arial, Helvetica, sans-serif;
font-size:11px;
color:#022d4d;
}
.link {font-family:Arial, Helvetica, sans-serif; font-size:11px; color:#ffffff;
text-decoration:none;}
a.link:link {font-family:Arial, Helvetica, sans-serif; font-size:11px; color:#ffffff;
text-decoration:none;}
a.link:hover {font-family:Arial, Helvetica, sans-serif; font-size:11px; color:#ffffff;
text-decoration:underline; }
```

Configuring Guest Portal Policy

The administrator can use the guest portal policy page to specify the required flow for the guest user login.

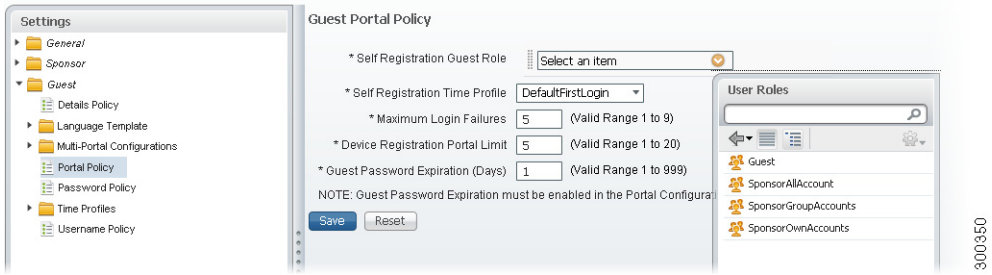
To configure a guest portal policy, complete the following steps:

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

Step 2 Configure the following options. An example is shown in Figure 21-4.

- Self Registration Guest Role—The default guest role assigned to the guest user after self-registration. This role ties the guest user to the associated Identity Group based on the policies defined in the system. For more information on configuring identity groups, see "Configuring User Identity Groups" section on page 4-41.
- Self Registration Time Profile—The default time profile assigned to the guest user after self-registration. Only CreateTime and FirstLogin type time profiles are available and both are treated as CreateTime accounts when creating a self-registered guest user account.
- Maximum Login Failures—The maximum number of failed login that can occur before a Guest User account is marked as suspended. The default value is five. A user account will be suspended after five failed login attempts. If the user account is suspended, the sponsor will have to re-enable the user account for login. This is a global setting and affects all guest portals.
- Device Registration Portal Limit—The maximum number of devices that can be registered for a guest user account. The device registration portal will not allow the guest user to add more devices if the maximum number has been reached. This value can be reduced to a value that is below the maximum number of devices currently registered to a guest account. Lowering the maximum number of registered devices will not affect the existing registered devices and these devices will remain registered.
- Guest Password Expiration—The number of days after which the guest password will expire and the guest will have to reset their password. To set this option, Guest Password Expiration must be enabled in the Portal Configuration page.

Figure 21-4 Guest Portal Policy Page



Step 3 Click **Save**.

Related Topics

- Configuring the Details Policy, page 21-43
- Multi-Portal Configurations, page 21-47

- Configuring Guest Password Policy, page 21-68
- Time Profiles, page 21-69
- Configuring Guest Username Policy, page 21-71

Configuring 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.

To configure a guest password policy, complete the following steps:

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

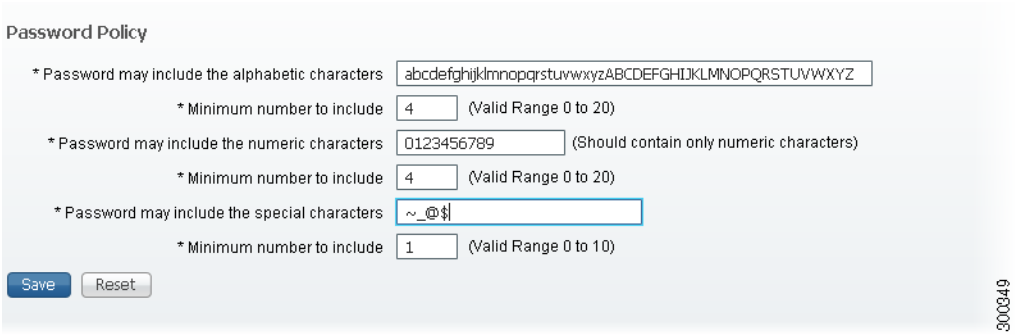
Step 2 Type the characters that will be used to generate the random characters.

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

Step 4 Click **Submit**.

Note Changes to the guest password policy only affect the existing accounts until the guest user passwords have expired and need to be changed.

Figure 21-5 Password Policy Page



Related Topics

- Configuring the Details Policy, page 21-43
- Multi-Portal Configurations, page 21-47
- Configuring Guest Portal Policy, page 21-67
- Time Profiles, page 21-69
- Configuring Guest Username Policy, page 21-71

Time Profiles

Time profiles allow a sponsor to assign different levels of access time to a guest account. For example, you can assign a time profile that allows a guest access during a workweek day but not during a weekend day.

After time profiles are created, you must change the sponsor user group to allow sponsors in that group to be able to provision accounts to the appropriate time profiles that are created. You can choose the sponsor user groups that are allowed to assign certain time profiles to guests.

By default, a sponsor user group has the ability to assign guests to the default time profile. Administrators can choose which additional time profiles the sponsor can be assigned, and they can also remove the default time profile from the user group.

Each sponsor user group must have the ability to assign guests to at least one time profile.

If a sponsor user group has only one time profile selected, sponsors will be able to select that time profile alone. If sponsors can choose more than one time profile, they can choose the time profile to be assigned to the account during the account creation from a drop-down list.

Related Topics

- Adding, Editing, or Duplicating Time Profiles, page 21-69
- Deleting Time Profiles, page 21-71
- Configuring the Details Policy, page 21-43
- Multi-Portal Configurations, page 21-47
- Configuring Guest Portal Policy, page 21-67
- Configuring Guest Password Policy, page 21-68
- Configuring Guest Username Policy, page 21-71

Adding, Editing, or Duplicating Time Profiles

To add or edit a time profile, complete the following steps:

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

Step 2 Click one of the following:

- **Add**—Creates a new time profile
- **Edit**—Edits an existing time profile
- **Duplicate**—Duplicates an existing time profile

Step 3 Enter the name and description of the new time profile.

Step 4 Choose a Time Zone for Restrictions from the drop-down list. Time Restrictions are a set of time periods during which a guest account associated with that time profile would not be granted access to the network or guest portal.

Step 5 From the Account Type drop-down list, choose one of the predefined options:

- **StartEnd**—Allows sponsors to define start and end times for account durations
- **FromFirstLogin**—Allows sponsors to define the duration of time that guests can have access after login

- **FromCreation**—Allows sponsors to define the duration of time that guest can have access after account creation

Step 6 Set the Duration for which the account will be active. The account expires after the duration set here has expired. This option is available only if you select the Account Type as FromFirstLogin or FromCreation.

Step 7 Set the Restrictions for the guest access.

These restrictions are composed of a day of the week and a start and end clock time. The Time Zone value specified in the time profile affects the clock times set in any of the Time Restrictions within the time profile. For example, a Time Restriction that specifies Monday 12:00 am to 8:00 am and Monday 6:00 pm to 11:59 pm would only grant system access between 8:00 am and 6:00 pm on Mondays within the time zone of the time profile. Any other day of the week would have no time restriction in this example and system access would be granted at any time.

Step 8 Click **Submit**.

Time profiles do not define the start and end times. This is done during the account creation. The time profile can have restrictions that fall outside the start and end time specified in a Guest account while creation. Only those restrictions that cover the start end time of the account will be applied to the account.

For a wired network the Termination-Action must be set to 0 “Default” so that the Session-Timeout is treated as a terminate session. This value must be set on the Authorization Profile as a RADIUS value.

For a WLC the Allow AAA Override must be turned on in the WLAN configuration. The RADIUS access-accept will contain a Session-Timeout value in seconds, remaining for the account. When this time has elapsed, NAD will close the connection.

At the time of Guest login the Network Access system will return the remaining time left in the guest account to the NAD that is making the access request. This is so that the NAD can enforce account expiration.

Note For the FromCreation and FromFirstLogin time profiles, the expiration date will be calculated based on the sponsor group duration or time profile duration, whichever is the minimum.

Related Topics

- Time Profiles, page 21-69
- Deleting Time Profiles, page 21-71
- Configuring the Details Policy, page 21-43
- Multi-Portal Configurations, page 21-47
- Configuring Guest Portal Policy, page 21-67
- Configuring Guest Password Policy, page 21-68
- Configuring Guest Username Policy, page 21-71

Deleting Time Profiles

To delete time profiles, complete these steps:

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

Step 2 Choose the time profiles to be deleted.

Step 3 Click **Delete**.

Related Topics

- Time Profiles, page 21-69
- Adding, Editing, or Duplicating Time Profiles, page 21-69
- Configuring the Details Policy, page 21-43
- Multi-Portal Configurations, page 21-47
- Configuring Guest Portal Policy, page 21-67
- Configuring Guest Password Policy, page 21-68
- Configuring Guest Username Policy, page 21-71

Configuring Guest Username Policy

The Guest Username Policy Configuration page allows the Cisco ISE administrator to specify how the user names will be created for the guest accounts. Username policy configuration can be done in two ways:

- General
- Random

Configuring General Guest Username Policy

You can create a guest username based on the e-mail address or the first and last name of the guest.

To configure general guest username policy, complete the following steps:

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

Step 2 Choose one of the username policy options for creating the username for the guest account:

c. **Create username from email address**—Select this option if you want the guest username to be formed from the guest's e-mail address.

d. **Create username from the first name and last name**—Select this option if you want the guest username to be formed from the first initial of the first name combined with the last name of the guest user.

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

If the guest usernames formed by the e-mail address or by the combination of first and last name are shorter than the minimum length, the username will be appended with *0* (zero) characters and a *1* at the end. If the username is not unique, numeric characters are appended to the name to make it unique.

For example, if there are two guest users named *Firstname Lastname,* the first username would be *flastname* and the second username would be *flastname1*. Similarly, if the Minimum Username length is set to eleven, then the two usernames would be generated as *flastname01* and *flastname02*.

Step 4 Click **Submit**.

Configuring Random Guest Username Policy

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.

To configure a random guest username policy, complete the following steps:

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

Step 2 Type the characters that will be used to generate the random characters.

Step 3 Enter the minimum number to use from each set of characters. The valid range is 0-20 for each character set.

Step 4 Click **Submit**.

Random username length is the combination of the three length fields that is alphabetic, numeric and special other characters. The length of the username defines the total number of unique names that can be created. For example, if 10,000 users are to be created, you will not be able to create enough unique values with a name space that is two characters in length.

Note Changes to the guest username policy do not affect the existing accounts.

Related Topics

- Configuring the Details Policy, page 21-43
- Multi-Portal Configurations, page 21-47
- Configuring Guest Portal Policy, page 21-67
- Configuring Guest Password Policy, page 21-68
- Time Profiles, page 21-69

Monitoring Sponsor and Guest Activity

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

- Metric Meter, page 21-73
- Guest Activity Report, page 21-73
- Guest Accounting, page 21-73
- Guest Sponsor Summary, page 21-73

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

This report helps you to view the Guest information for a selected time period. This report displays all the URLs that a guest user visits.

Note For the Guest Activity Report to collect and display the list of URLs visited by the guest user, you must enable guest access syslogging configuration on the NAD that inspects guest traffic in your Cisco ISE network.

To view this report, complete the following steps:

1. Choose **Operations > Reports > Catalog > User**.
2. Click on **Guest Activity**.

Guest Accounting

This report helps you to view the logged in/out information for the particular guest for a selected time period.

To view this report, complete the following steps:

1. Choose **Operations > Reports > Catalog > User**.
2. Click on **Guest Accounting**.

Guest Sponsor Summary

This report helps you to view the sponsor information along with a graphical representation for a selected time period.

To view this report, complete the following steps:

1. Choose **Operations > Reports > Catalog > User**.
2. Click on **Guest Sponsor Summary**.

For More Information

See Chapter 25, “Reporting,” for details on how to configure these reports.

See Chapter 24, “Monitoring and Troubleshooting,” for details on monitoring and troubleshooting tools.

Audit Logging

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.

See Chapter 24, “Monitoring and Troubleshooting,” for more information on logging and log collection.

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