Guest Access User Interface Reference

Guest Portal Settings

Portal Identification Settings

The navigation path for these settings is **Guest Access** > **Configure** > **Guest Portals or Sponsor Portals** > **Create, Edit or Duplicate** > **Guest Portals or Sponsor Portals Settings and Customization**.
Use these settings to identify the portal and select the language files to be used for all the portal pages.

Field	Usage Guidelines
Portal Name	Enter a unique portal name to access this portal. Do not use this portal name for any other Sponsor and Guest portals and non-guest portals, such as Blacklist, Bring Your Own Device (BYOD), Client Provisioning, Mobile Device Management (MDM), or My Devices portals. This name appears in the authorization profile portal selection for redirection choices, and is used in the list of portals for easy identification among other portals.
Description	Optional.

Field	Usage Guidelines
Portal test URL	A system-generated URL displays as a link after you click **Save**. Use it to test the portal. Click the link to open a new browser tab that displays the URL for this portal that is being served by a Policy Services Node (PSN) with Policy Services turned on. If Policy Services are not turned on, the PSN will not serve web pages for any portals other than the Admin portal. **Note** The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work.
Language File	Each portal type supports 15 languages by default, which are available as individual properties files bundled together in a single zipped language file. Export or import the zipped language file to use with the portal. The zipped language file contains all the individual language files that you can use to display text for the portal. The language file contains the mapping to the particular browser locale setting (for example, for French: fr, fr-fr, fr-ca) along with all of the string settings for the entire portal in that language. A single language file contains all the supported languages, so that it can easily be used for translation and localization purposes. If you change the browser locale setting for one language, the change is applied to all the other end-user web portals. For example, if you change the French.properties browser locale from fr,fr-fr,fr-ca to fr,fr-fr in the Hotspot Guest portal, the change is applied to the My Devices portal also.

Portal Settings for Hotspot Guest Portals

The navigation path for these settings is **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Portal Settings**.

- **HTTPS Port—**Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you change this page. If you do change this page, update the port setting to comply with this restriction.

If you assign ports used by a non-guest (such as My Devices) portal to a guest portal, an error message will display.

- **Allowed interfaces—**Select the PSN interfaces which can run a portal. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.
  - You must configure the Ethernet interfaces using IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.
  - Configure **ip host x.x.x.x yyy.domain.com** in ISE CLI to map secondary interface IP to FQDN, which is used to match Certificate Subject Name / Alternate Subject Name.
- **Certificate group tag—**Select the group tag of the certificate group to use for the portal's HTTPS traffic.
- **Endpoint identity group—**choose an endpoint identity group to track guest devices. Cisco ISE provides the **GuestEndpoints** endpoint identity group to use as a default. You can also create additional endpoint identity groups if you choose to not use the default.

  Choose an endpoint identity group to track employee devices. Cisco ISE provides the **RegisteredDevices** endpoint identity group to use as a default. You can also create additional endpoint identity groups if you choose to not use the default.
- **Purge endpoints in this identity group when they reach __ days—**Change the number of days since the registration of a user's device before it is purged from the Cisco ISE database. Purging is done on a daily basis and the purge activity is synchronized with the overall purge timing. The change is applied globally for this endpoint identity group. If changes are made to the Endpoint Purge Policy based on other policy conditions, this setting is no longer available for use.
- **CoA Types**
  - CoA Reauthenticate: Causes the NAD to reauthenticate the guest.
  - CoA Terminate: Issues a Change of Authorization (CoA) Terminate to remove the suspended guests from the network.

Note If you chose CoA-Terminate(Admin-Reset), it could take 10-20 seconds before the user is redirected to the portal. This could cause timeout issues, resulting in incorrect Hotspot flow.

Note The VLAN DHCP Release Page Settings section is editable only when the CoA reauthenticate type is selected.

- **Display Language—**Specify which language is used in the portal: the user's browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.

Acceptable Use Policy (AUP) Page Settings for Hotspot Guest Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Acceptable Use Policy (AUP) Page Settings**.
Use these settings to define the AUP experience for the users (guests, sponsors or employees as applicable).

Field	Usage Guidelines
Include an AUP page	Display your company's network-usage terms and conditions on a separate page to the user.
Require an access code	Assign an access code as the login credential that multiple guests should use to gain access to the network. An access code is primarily a locally known code that is given to physically present guests (either visually via a whiteboard or verbally by a lobby ambassador). It would not be known and used by someone outside the premises to access the network. You can use this option in addition to the usernames and passwords that are provided as the login credentials to individual guests.
Require scrolling to end of AUP	Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.

Post-Access Banner Page Settings for Hotspot Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Post-Access Banner Page Settings**.
Use this setting to inform guests of their access status and any other additional actions, if required.

Field	Usage Guidelines
Include a Post-Access Banner page	Display additional information after the guests are successfully authenticated and before they are granted network access.

Portal Settings for Credentialed Guest Portals

The navigation path for these settings is: **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Portal Settings**.

- **HTTPS Port—**Enter a Port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded ISE and were using Port values outside this range, they are honored until you make any change to this page. If you do change this page, you must update the Port setting to comply with this restriction.

  If you assign Ports used by a non-guest (such as My Devices) portal to a guest portal, an error message displays.

- **Allowed interfaces—**Select the PSN interfaces where this portal can run. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical and bonded interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.

  - The Ethernet interfaces must use IP addresses on different subnets.
  - The interfaces you enable here must be available on all the PSNs that are running portals, including VM-based ones (when Policy Services turned on). This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP. If the interface IP is not the same as the domain, then configure **ip host x.x.x.x yyy.domain.com** in the ISE CLI to map your interface IP to FQDN in the certificate.

- **Certificate group tag—**Select the group tag of the certificate group to use for the portal's HTTPS traffic.
- **Authentication Method —** Choose which identity source sequence (ISS) or Identity Provider (IdP) to use for user authentication. The ISS is a list of Identity Stores that are searched in sequence to verify user credentials. Some examples include: Internal Guest Users, Internal Users, Active Directory, LDAP Directory.

  Cisco ISE includes a default sponsor Identity Source Sequence for sponsor portals, Sponsor_Portal_Sequence.

- Endpoint identity group**—**Choose an endpoint identity group to track guest devices. Cisco ISE provides the **GuestEndpoints** endpoint identity group to use as a default. You can also create additional endpoint identity groups if you choose to not use the default.

  Choose an endpoint identity group to track employee devices. Cisco ISE provides the **RegisteredDevices** endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

- **Display Language—**Specify which language is used in the portal: the user's browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.

Portal Configuration Rules

Portals assigned to the same HTTPS Port can use the same Gigabit Ethernet interface or another interface. If they use the same Port and interface combination, they must use the same certificate group tag. For example:

- Valid combinations include:
  - Sponsor portal: Port **8443**, Interface **0**, Certificate tag **A**, and My Devices portal: Port **8443**, Interface **0**, Certificate group **A**.
  - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: Port **8445**, Interface **0**, Certificate group **B**.
  - Sponsor portal: Port **8444**, Interface **1**, Certificate group **A** and Blacklist portal: Port **8444**, Interface **0**, Certificate group **B**.
- Invalid combinations include:
  - Sponsor portal: Port **8443**, Interface **0**, Certificate group **A** and My Devices portal: **8443**, Interface **0**, Certificate group **B**.
  - Sponsor portal: Port **8444**, Interface **0**, Certificate tag **A** and Blacklist portal: Port **8444**, Interface **0**, Certificate group **A**.

Login Page Settings for Credentialed Guest Portals

The navigation path for this page is: **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Login Page Settings**.

Use these settings to define the login experience for users (guests, sponsors or employees as applicable), the parameters for failed login attempts, and AUP information for this page.

Field	Usage Guidelines
Require an access code	Assign an access code as the login credential that multiple guests should use to gain access to the network. An access code is primarily a locally known code that is given to physically present guests (either visually via a whiteboard or verbally by a lobby ambassador). It would not be known and used by someone outside the premises to access the network. You can use this option in addition to the usernames and passwords that are provided as the login credentials to individual guests.
Maximum failed login attempts before rate limiting	Specify the number of failed login attempts from a single browser session before Cisco ISE starts to throttle that account. This does not cause an account lockout. You can specify the time between attempts after this number of failed logins is reached in **Time between login attempts when rate limiting**.
Time between login attempts when rate limiting	Set the length of time in minutes that a user must wait before attempting to log in again, after failing to log in the number of times defined in **Maximum failed login attempts before rate limiting**.

Field	Usage Guidelines
Include an AUP (on page/as link)	Display your company's network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.
Require acceptance	Require users to accept an AUP before their account is fully enabled. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.
Require scrolling to end of AUP	This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.
Allow guests to create their own accounts	Provide an option on this portal's Login page for guests to register themselves. If this option is not selected, sponsors create guest accounts. Enabling this also enables tabs on this page for you to configure **Self-Registration Page Settings** and **Self-Registration Success Page Settings**. If guests choose this option, they are presented with the Self-Registration form where they can enter the requested information to create their own guest accounts.
Allow guests to change password after login	Allow guests to change their password after successfully authenticating and accepting the AUP, if it is required. If guests change their passwords, sponsors cannot provide guests with their login credentials if lost. The sponsor can only reset the guest's password back to a random password.

Self-Registration Page Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Self Registration Page Settings**. Use these settings to enable guests to register themselves and specify the information they need to provide on the Self-Registration form.

Field	Usage Guidelines
Assign self-registered guests to guest type	Choose the guest type to which all the self-registered guests using this portal should be assigned.

Field	Usage Guidelines
Account valid for	Specify the duration for the account in days, hours, or minutes after which the account will expire unless you or the sponsor extend the account duration in the Sponsor portal.
Require a registration code for self registration	Assign a code that the self-registering guests must enter to successfully submit their Self-Registration form. Similar to the access code, the registration code is provided to the guest offline to prevent someone who is outside the premises from accessing the system.
Fields to include / Required	Check the fields that you want to display on the Self-Registration form. Then check which fields are mandatory for the guests to complete in order to submit the form and receive a guest account. You may want to require fields such as **SMS Service Provider** and **Person being Visited** to gather important information from self-registering guests.
Guests can choose from these locations to set their time zone	Enter locations that the self-registering guests can select at registration time using the list of locations that you have defined. This automatically assigns the related time zones as the valid access times for these guests. The location names should be clear to avoid ambiguity during selection (for example, Boston Office, 500 Park Ave New York, Singapore, etc.) If you only provided one location, it is automatically assigned as the default location and does not display in the portal for guests to view. Additionally, **Location** is disabled in the list of **Fields to include**.
SMS Service Provider	Display SMS providers on the Self-Registration form to enable self-registering guests to choose their own SMS provider. You can then use the guest's SMS service to send them SMS notifications to minimize expenses for your company.
Guests can choose from these SMS providers	Select the SMS providers that should display on the Self-Registration form. If you only selected one as the default SMS provider for the guest to use, it will not display on the Self-Registration form.

Field	Usage Guidelines
Custom Fields	Select additional information that you would like collect from the self-registering guests. Then check which fields are mandatory for the guests to complete in order to submit the Self-Registration form and receive a guest account. These fields are listed in alphabetical order by name.
Include an AUP (on page/as link)	Display your company's network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.
Require acceptance	Require users to accept an AUP before their account is fully enabled. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.
Require scrolling to end of AUP	This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.
Only allow guests with an email address from	Specify the whitelisted email address domains from which the self-registering guests can enter in **Email Address** and successfully receive their account credentials; for example, cisco.com, example.com. In this example, if the guests entered *myname@cisco.com* as their email address, after successful account creation, they receive their login credentials. However, if they entered *myname@hotmail.com* (or any other address not from cisco.com or example.com), no account is created and they do not get credentials. Leaving this field blank allows registration from any domain, unless there are blacklist domains listed in **Do not allow guests with email address from**.
Do not allow guests with an email address from	Specify the blacklisted email address domains from which the self-registering guests cannot enter in **Email Address** and successfully receive their account credentials; for example, cisco.com, example.com. In this example, if the guests entered *myname@cisco.com* as their email address, no account is created and they do not get credentials.

Field	Usage Guidelines
Require self-registered guests to be approved	Specify that the self-registering guests using this portal require approval from a sponsor before receiving their guest credentials. Then specify one of the options under **After registration submission, direct guest to** in this page: • Self-Registration Success page • Login page with instructions about how to obtain login credentials • URL If enabled, you should also enable one or both: **Email** or **SMS** under **Send credential notification upon approval using** in this page. Enabling Require self-registered guests to be approved enables the following extra configuaration fields, which have the following attributes: Approve/Deny Link Settings—Additional settings allow you to configure: • **Links are valid for**, number of days. • Require approver to enter a username and password for authentication—Authenticate sponsors based on the following ordered list of sponsor portals • Authenticate sponsors based on the following ordered list of sponsor portals—If there are multiple sponsors that can approve this account, then chose the portal that the sponsor must log on to in order to approve the account.

Field	Usage Guidelines
Email approval request to	If you select: • **sponsor email addresses listed below**, enter the email addresses of sponsors designated as approvers, or an email address or a mailer to which ALL guest approval requests should be sent. • **person being visited**, the **Person being visited** and **Required** options in Fields to include will also be enabled (if they were previously disabled). These fields will be displayed on the Self-Registration form requesting this information from the self-registering guests. These persons will receive an email notification stating that self-registering guests require approval.
Self-Registration Success page	Direct successfully self-registered guests to the Self-Registration Success page, which displays the fields and messages you have specified in **Self Registration Success Page Settings**. It may not be desirable to display all the information, because the system may be awaiting account approval (if enabled on this page) or delivering the login credentials to an email address or phone number based on the whitelisted and blacklisted domains specified in this page. If you enabled **Allow guests to log in directly from the Self-Registration Success page** in **Self-Registration Success Page Settings**, successfully self-registered guests can log in directly from this page. If it is not enabled, they are directed to the portal's Login page after the Self-Registration Success page is displayed.

Field	Usage Guidelines
Login page with instructions about how to obtain login credentials	Direct successfully self-registered guests back to the portal's Login page and display a message, such as "Please wait for your guest credentials to be delivered either via email, SMS, or print format and proceed with logging in." To customize the default message, click on the **Portal Page Customization** tab and select **Self-Registration Page Settings**. The system may be awaiting account approval (if enabled on this page) or delivering the login credentials to an email address or phone number based on the whitelisted and blacklisted domains specified in this page.
URL	Direct successfully self-registered guests to the specified URL while waiting for their account credentials to be delivered. The system may be awaiting account approval (if enabled on this page) or delivering the login credentials to an email address or phone number based on the whitelisted and blacklisted domains specified in this page.
Email	Choose email as the option by which successfully self-registered guests receive their login credential information. If you choose this option, **Email address** becomes a required field in the list of **Fields to include** and you can no longer disable this option.
SMS	Choose SMS as the option by which successfully self-registered guests receive their login credential information. If you choose this option, **SMS Service Provider** becomes a required field in the list of **Fields to include** and you can no longer disable this option.

Self Registration Success Page Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Self Registration Success Page Settings**. Use these settings to notify successfully self-registered guests of the credentials they need to gain access to the network.

Field	Usage Guidelines
Include this information on the Self-Registration Success page	Check the fields that you want to display for the successfully self-registered guests on the Self-Registration Success page. If sponsor approval of the guest is not required, check **Username** and **Password** to display these credentials for the guest. If sponsor approval is required, these fields are disabled, because the credentials can only be delivered to the guest after they have been approved.
Allow guest to send information to self using	Check the options by which the successfully self-registered guest can send credential information to themselves: **Print**, **Email**, or **SMS**.
Include an AUP (on page/as link)	Display your company's network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.
Require acceptance	Require users to accept an AUP before their account is fully enabled. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.
Require scrolling to end of AUP	This field displays if you chose the **AUP on page** option. Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.
Allow guests to log in directly from the Self-Registration Success page	Display a **Login** button at the bottom of the Self-Registration Success page. This enables the guest to bypass the Login page and automatically deliver the login credentials to the portal and display the next page in the portal flow (for instance, the AUP page).

Acceptable Use Policy (AUP) Page Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Acceptable Use Policy (AUP) Page Settings**.
Use these settings to define the AUP experience for the users (guests, sponsors or employees as applicable).

Field	Usage Guidelines
Include an AUP page	Display your company's network-usage terms and conditions on a separate page to the user.

Field	Usage Guidelines
Use different AUP for employees	Display a different AUP and network-usage terms and conditions for employees only. If you choose this option, you cannot also choose **Skip AUP for employees**.
Skip AUP for employees	Employees are not required to accept an AUP before accessing the network. If you choose this option, you cannot also choose **Use different AUP for employees**.
Require scrolling to end of AUP	Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.
On first login only	Display an AUP when the user logs into the network or portal for the first time only.
On every login	Display an AUP each time the user logs into the network or portal.
Every __ days (starting at first login)	Display an AUP periodically after the user first logs into the network or portal.

Guest Change Password Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Guest Change Password Settings**.
Use this setting to require all guests to change their passwords after they first log in.

Field	Usage Guidelines
Require guest to change password at first login	Require guests to change the password after they first log in. If a guest loses their login credentials after they log in and change their password, sponsors can only reset the guest's password back to a random password. To require internal users using a guest portal to change their password upon their next login, choose **Administration** > **Identity Management** > **Identities** > **Users**. Select the specific internal user from the Network Access Users list and enable the change password check box.

Guest Device Registration Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Guest Device Registration Settings**.
Use these settings to either ensure that Cisco ISE automatically registers guest devices when they log in to or to allow guests to manually register their devices after they log in.

The maximum number of devices is specified for each guest type in **Guest Access** > **Configure** > **Guest Types**.

Field	Usage Guidelines
Automatically register guest devices	Automatically create an endpoint for the device from which the guest is accessing this portal. The endpoint will be added to the endpoint identity group specified for this portal and is subject to the identity group's purge policy. An authorization rule can now be created to allow access to endpoints in that identity group, so that web authentication is no longer required. If the maximum number of registered devices is reached, the system automatically deletes the first registered device, registers the device the guest is trying to log in with, and notifies them. Choose **Guest Access** > **Configure** > **Guest Types** to change the maximum number of devices with which a guest can register.
Allow guests to register devices	Guests can register their devices manually by providing a name, description and MAC address. The MAC address is associated with an endpoint identity group. If the maximum number of registered devices is reached, the guest is required to delete at least one device before being allowed to register another device.

BYOD Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **BYOD Settings**.
Use these settings to enable Bring Your Own Device (BYOD) functionality for non-guests, such as employees, using the Credentialed Guest portals to access your corporate network.

Field	Usage Guidelines
Allow employees to use personal devices on the network	Add the Employee Bring Your Own Device (BYOD) Registration page to this portal allowing employees to go through the employee device registration process, and possibly native supplicant and certificate provisioning, depending on the settings for Client Provisioning for the employee's personal device type (for example, iOS, Android, Windows (excluding RT or mobile), OSX).
Endpoint identity group	Choose an endpoint identity group to track guest devices. Cisco ISE provides the **GuestEndpoints** endpoint identity group to use as a default. You can also create additional endpoint identity groups if you choose to not use the default.
Purge endpoints in this identity group when they reach __ days	Change the number of days since the registration of a user's device before it is purged from the Cisco ISE database. Purging is done on a daily basis and the purge activity is synchronized with the overall purge timing. The change is applied globally for this endpoint identity group. If changes are made to the Endpoint Purge Policy based on other policy conditions, this setting is no longer available for use.
Allow employees to choose to get guest access only	Let employees access your guest network and avoid additional provisioning and registration that may be required to access your corporate network.
Display Device ID field during registration	Display the device ID to the user during the registration process, even though the device ID is pre-configured and cannot be changed while using the BYOD portal .

Field	Usage Guidelines
Originating URL	After successfully authenticating to the network, redirect the user's browser to the original website that the user is trying to access, if available. If not available, the Authentication Success page displays. Make sure that the redirect URL is allowed to work on port 8443 of the PSN by the access-control list on the NAD and by authorization profiles configured in ISE for that NAD. For Windows, MAC and Android devices, control is given to the Self-Provisioning Wizard app, which performs the provisioning. Therefore, these devices are not redirected to the originating URL. However, iOS (dot1X) and unsupported devices (that are allowed network access) will be redirected to this URL.
Success page	Display a page indicating that the device registration was successful.
URL	After successfully authenticating to the network, redirect the user's browser to the specified URL, such as your company's website.

Post-Login Banner Page Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals or Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Post-Login Banner Page Settings**.
Use this setting to notify users (guests, sponsors or employees as applicable) of additional information after they log in successfully.

Field	Usage Guidelines
Include a Post-Login Banner page	Display additional information after the users successfully log in and before they are granted network access.

Guest Device Compliance Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Guest Device Compliance Settings**. Use these settings to require guests, and employees using the guest portal, to undergo client provisioning of their devices in order to gain access to the network.

Field	Usage Guidelines
Require guest device compliance	Route guests to the Client Provisioning page and require them to first download the posture agent. This enables posture policies for guests, such as checking for virus protection software and so on. If the guest is an employee using the Credentialed Guest portals to access the network and: • If you enabled **Allow employees to use personal devices on the network** in the **BYOD Settings**, the employee is redirected to the BYOD flow and will not undergo client provisioning. • If you enabled both **Allow employees to use personal devices on the network** and **Allow employees to choose to get guest access only** in the **BYOD Settings**, and the employee chooses guest access, they are routed to the Client Provisioning page.

VLAN DHCP Release Page Settings for Guest Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **VLAN DHCP Release Page Settings**.
Use these settings to enable the release and renewal of the guest device IP address.

Field	Usage Guidelines
Enable VLAN DHCP release	Use to refresh the IP address for Windows or Mac OS devices after a VLAN change in both wired and wireless environments for a guest. This affects the Central WebAuth (CWA) flow during final authorization when the network access changes the guest VLAN to a new VLAN. The guest's old IP address must be released before the VLAN change and a new guest IP address must be requested through DHCP once the new VLAN access is in place. The IP address release renew operation varies by the browser and operating system used; Internet Explorer uses ActiveX controls, and Firefox and Google Chrome use Java applets. For non-Internet Explorer browsers, Java must be installed and enabled on the browser. The VLAN DHCP Release option does not work on mobile devices. Instead, guests are requested to manually reset the IP address. This method varies by devices. For example, on Apple iOS devices, guests can select the Wi-Fi network and click the **Renew Lease** button.
Delay to release __ seconds	Enter the delay to release time. It should be brief because the release must occur immediately after the applet is downloaded and before the Cisco ISE server directs the NAD to re-authenticate with a CoA request.
Delay to CoA __ seconds	Enter the time to delay Cisco ISE from executing the CoA. Provide enough time (use the default value as a guideline) to allow the applet to download and perform the IP release on the client.
Delay to renew __ seconds	Enter the delay to renew value. This time is added to the IP release value and does not begin timing until the control is downloaded. Provide enough time (use the default value as a guideline) so that the CoA is allowed to process and the new VLAN access granted.

Authentication Success Settings for Guest Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Authentication Success Settings**.
Use these settings to notify the users (guests, sponsors, or employees as applicable) of authentication success or display a URL. Under **Once authenticated, take guest to:**, configure the following fields:

- **Originating URL—**After successfully authenticating to the network, redirect the user's browser to the original website that the user is trying to access, if available. If not available, the Authentication Success page displays.

  For Windows, MAC and Android devices, control is given to the Self-Provisioning Wizard app, which performs the provisioning. Therefore, these devices are not redirected to the originating URL. However, iOS (dot1X) and unsupported devices (that are allowed network access) will be redirected to this URL.

- **Authentication Success page—**Notification of successful authentication of the user.
- **URL—**After successfully authenticating to the network, redirect the user's browser to the specified URL, such as your company's website.

Note If you redirect a Guest to an external URL after authentication, there may be a delay while the URL address is resolved and the session is redirected. Make sure that the redirect URL is allowed to work on port 8443 of the PSN by the access-control list on the NAD and by authorization profiles configured in ISE for that NAD.

Support Information Page Settings for Guest Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Support Information Page Settings**.
Use these settings to display the information that your Help Desk can use to troubleshoot access issues experienced by users (guests, sponsors or employees as applicable).

Field	Usage Guidelines
Include a Support Information Page	Display a link to an information page, such as **Contact Us**, on all enabled pages for the portal.
MAC address	Include the MAC address of the device on the Support Information page.
IP address	Include the IP address of the device on the Support Information page.
Browser user agent	Include the browser details such as the product name and version, layout engine and version of the user agent originating the request on the Support Information page.
Policy server	Include the IP address of the ISE Policy Service Node (PSN) that is serving this portal on the Support Information page.
Failure code	If available, include the corresponding number from the log message catalog. You can access and view the message catalog by navigating to **Administration** > **System** > **Logging** > **Message Catalog**.

Field	Usage Guidelines
Hide field	Do not display any field labels on the Support Information page if the information that they would contain is non-existent. For example, if the failure code is unknown, and therefore blank, do not display **Failure code**, even if it is selected.
Display label with no value	Display all selected field labels on the Support Information page, even if the information that they would contain is non-existent. For example, if the failure code is unknown, display **Failure code**, even if it is blank.
Display label with default value	Display this text in any selected field on the Support Information page, if the information that they would contain is non-existent. For example, if you enter Not Available in this field, and the failure code is unknown, the **Failure code** will display as **Not Available**.

Sponsor Portal Application Settings

Portal Identification Settings

The navigation path for these settings is **Guest Access** > **Configure** > **Guest Portals or Sponsor Portals** > **Create, Edit or Duplicate** > **Guest Portals or Sponsor Portals Settings and Customization**.
Use these settings to identify the portal and select the language files to be used for all the portal pages.

Field	Usage Guidelines
Portal Name	Enter a unique portal name to access this portal. Do not use this portal name for any other Sponsor and Guest portals and non-guest portals, such as Blacklist, Bring Your Own Device (BYOD), Client Provisioning, Mobile Device Management (MDM), or My Devices portals. This name appears in the authorization profile portal selection for redirection choices, and is used in the list of portals for easy identification among other portals.
Description	Optional.

Field	Usage Guidelines
Portal test URL	A system-generated URL displays as a link after you click **Save**. Use it to test the portal. Click the link to open a new browser tab that displays the URL for this portal that is being served by a Policy Services Node (PSN) with Policy Services turned on. If Policy Services are not turned on, the PSN will not serve web pages for any portals other than the Admin portal. **Note** The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work.
Language File	Each portal type supports 15 languages by default, which are available as individual properties files bundled together in a single zipped language file. Export or import the zipped language file to use with the portal. The zipped language file contains all the individual language files that you can use to display text for the portal. The language file contains the mapping to the particular browser locale setting (for example, for French: fr, fr-fr, fr-ca) along with all of the string settings for the entire portal in that language. A single language file contains all the supported languages, so that it can easily be used for translation and localization purposes. If you change the browser locale setting for one language, the change is applied to all the other end-user web portals. For example, if you change the French.properties browser locale from fr,fr-fr,fr-ca to fr,fr-fr in the Hotspot Guest portal, the change is applied to the My Devices portal also.

Portal Settings for Sponsor Portals

Configure these settings to identify the portal and select the language files to be used for all the portal pages.

-
- **HTTPS Port—**Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you change this page. If you do change this page, update the port setting to comply with this restriction.

If you assign ports used by a non-guest (such as My Devices) portal to a guest portal, an error message will display.

- **Allowed interfaces—**Select the PSN interfaces which can run a portal. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.
    - You must configure the Ethernet interfaces using IP addresses on different subnets.
    - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
    - The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.
    - Configure **ip host x.x.x.x yyy.domain.com** in ISE CLI to map secondary interface IP to FQDN, which is used to match Certificate Subject Name / Alternate Subject Name.
- **Certificate group tag—**Select the group tag of the certificate group to use for the portal's HTTPS traffic.
- **Authentication Method —**Choose which identity source sequence (ISS) or Identity Provider (IdP) to use for user authentication. The ISS is a list of Identity Stores that are searched in sequence to verify user credentials. Some examples include: Internal Guest Users, Internal Users, Active Directory, LDAP Directory.

  Cisco ISE includes a default sponsor Identity Source Sequence for sponsor portals, Sponsor_Portal_Sequence.
- **Employees using this portal as guests inherit login options from—**Choose the Guest Type that employees are assigned when they log on to this portal. The employee's endpoint data is stored in the endpoint identity group configured in that guest type for the attribute **Store device information in endpoint identity group**. No other attributes from the associated guest type are inherited.
- **Display Language—**Specify which language is used in the portal: the user's browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.

Login Settings for Sponsor Portals

The navigation path for this page is **Guest Access** > **Configure** > **Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Login Page Settings**.
Use these settings to define the login experience for users (guests, sponsors or employees as applicable), the parameters for failed login attempts, and AUP information for this page.

Table 1: Login Page Settings for Sponsor Portals

Field	Usage Guidelines
Maximum failed login attempts before rate limiting	Specify the number of failed login attempts from a single browser session before Cisco ISE starts to throttle that account. This does not cause an account lockout. You can specify the time between attempts after this number of failed logins is reached in **Time between login attempts when rate limiting**.
Time between login attempts when rate limiting	Set the length of time in minutes that a user must wait before attempting to log in again, after failing to log in the number of times defined in **Maximum failed login attempts before rate limiting**.
Include an AUP (on page/as link)	Display your company's network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.
Require acceptance	Require users to accept an AUP before their account is fully enabled. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.
Require scrolling to end of AUP	This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.

Acceptable Use Policy (AUP) Settings for Sponsor Portals

The navigation path for this page is **Guest Access** > **Configure** > **Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Acceptable Use Policy (AUP) Page Settings**.
Use these settings to define the AUP experience for the users (guests, sponsors or employees as applicable).

Field	Usage Guidelines
Include an AUP page	Display your company's network-usage terms and conditions on a separate page to the user.
Require scrolling to end of AUP	Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.

Field	Usage Guidelines
On first login only	Display an AUP when the user logs into the network or portal for the first time only.
On every login	Display an AUP each time the user logs into the network or portal.
Every __ days (starting at first login)	Display an AUP periodically after the user first logs into the network or portal.

Sponsor Change Password Settings for Sponsor Portals

The navigation path for this page is **Guest Access** > **Configure** > **Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Sponsor Change Password Settings**. Use these settings to define the password requirements for sponsors using the Sponsor portal.

To set the sponsor password policy, choose **Administration** > **Identity Management** > **Settings** > **User Password Policy**.

Field	Usage Guidelines
Allow sponsors to change their own passwords	Allow sponsors to change their passwords after they log into the Sponsor portal. This option will display a Change Password page only if the sponsors are part of the Internal Users database.

Post-Login Banner Settings for Sponsor Portals

The navigation path for this page is **Guest Access** > **Configure** > **Guest Portals or Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Post-Login Banner Page Settings**.
Use this setting to notify users (guests, sponsors or employees as applicable) of additional information after they log in successfully.

Field	Usage Guidelines
Include a Post-Login Banner page	Display additional information after the users successfully log in and before they are granted network access.

Support Information Page Settings for Sponsor Portals

The navigation path for this page is **Guest Access** > **Configure** > **Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Support Information Page Settings**.

Use these settings to display the information that your Help Desk can use to troubleshoot access issues experienced by users (guests, sponsors or employees as applicable).

Field	Usage Guidelines
Include a Support Information Page	Display a link to an information page, such as **Contact Us**, on all enabled pages for the portal.
MAC address	Include the MAC address of the device on the Support Information page.
IP address	Include the IP address of the device on the Support Information page.
Browser user agent	Include the browser details such as the product name and version, layout engine and version of the user agent originating the request on the Support Information page.
Policy server	Include the IP address of the ISE Policy Service Node (PSN) that is serving this portal on the Support Information page.
Failure code	If available, include the corresponding number from the log message catalog. You can access and view the message catalog by navigating to **Administration** > **System** > **Logging** > **Message Catalog**.
Hide field	Do not display any field labels on the Support Information page if the information that they would contain is non-existent. For example, if the failure code is unknown, and therefore blank, do not display **Failure code**, even if it is selected.
Display label with no value	Display all selected field labels on the Support Information page, even if the information that they would contain is non-existent. For example, if the failure code is unknown, display **Failure code**, even if it is blank.
Display label with default value	Display this text in any selected field on the Support Information page, if the information that they would contain is non-existent. For example, if you enter Not Available in this field, and the failure code is unknown, the **Failure code** will display as **Not Available**.

Notify Guests Customization for Sponsor Portals

The navigation path for these settings is **Guest Access** > **Configure** > **Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Page Customization** > **Notify Guests**.

Under **Page Customizations**, you can customize the messages, titles, content, instructions, and field and button labels that appear on the notifications that sponsors send to guests from the Sponsor portal.

Under **Settings**, you can specify whether sponsors can send usernames and passwords separately to guests using email or SMS. You can also specify whether sponsors can display a Support Information page for guests to provide information that a help desk can use to troubleshoot access issues.

Manage and Approve Customization for Sponsor Portals

The navigation path for these settings is **Guest Access** > **Configure** > **Sponsor Portals** > **Create, Edit or Duplicate** > **Portal Page Customization** > **Manage and Approve**.

Under **Page Customizations**, you can customize the messages, titles, content, instructions, and field and button labels that appear on the Manage and Approve tabs of the Sponsor portal.

These include the accounts (registered and pending) summary and detailed views, the pop-up dialogs that display based on the operations the sponsor performs on guest accounts such as edit, extend, suspend and so on, and also general portal and account action messages.

Global Settings

Global Settings for Guest and Sponsor Portals

Choose **Guest Access** > **Settings**. You can configure the following general settings that apply to Guest and Sponsor portals, guest types, and sponsor groups in Cisco ISE:

- Policies for purging guest accounts and generating usernames and passwords.
- SMTP servers and SMS gateways to use when sending email and SMS notifications to guests and sponsors.
- Locations, time zones, SSIDs, and custom fields to select from when creating guest accounts and when registering guests using Self-Registration Guest portals.

Once you configure these global settings, you can use them as needed when configuring specific Guest and Sponsor portals, guest types, and sponsor groups.

The following tabs are on the Portal settings page:

- **Guest Account Purge Policy—**Schedule when to purge guest accounts that have expired. For more information, see Schedule When to Purge Expired Guest Accounts.
- **Custom Fields—**Add custom fields to use in Guest portals, to retrieve additional information from users. For more information, see Add Custom Fields for Guest Account Creation.
- **Guest Email Settings—**Decide whether to email notifications to guests about changes in their account. For more information, see Specify Email Addresses and SMTP Servers for Email Notifications.

- **Guest Locations and SSIDs—**Configure the Locations and the Service Set Identifiers (SSIDs) of the networks that guests can use at these Locations. For more information, see Assign Guest Locations and SSIDs.
- **Guest Username Policy—**Configure how guest user names are created. For more information, seeSet the Guest Username Policy and Rules for Guest Password Policies.
- **Guest Password Policy—**Define the guest password policies for all Guest and Sponsor portals. For more information, see Set the Guest Password Policy and Expiration.
- **SMS Gateway Settings—**Define SMS gateways that will deliver SMS notifications to guests and sponsors. For more information, see Configure SMS Gateways to Send SMS Notifications to Guests.

Guest Type Settings

The navigation path for these settings is **Guest Access** > **Configure** > **Guest Types**. Use these settings to create the types of Guests that can access your network and their access privileges. You can also specify which Sponsor Groups can create this type of Guest.

Field	Usage Guidelines
Guest type name	Provide a name (from 1-256 characters) that distinguishes this Guest Type from the default Guest Types and others that you create.
Description	Provide additional information (maximum of 2000 characters) about the recommended use of this Guest Type, for example: Use for self-registering Guests, Do NOT use for Guest account creation, etc.
Language File	Export or Import the language file to use for portals using this Guest Type.
Collect Additional Data	Select custom fields to collect additional information from Guests. Custom fields are managed on **Guest Access** > **Settings** > **Custom Fields**.

Field	Usage Guidelines
Maximum Access Time—Account Duration Starts	If you selected **From first login**, the account start time is assigned when the guest user first logs in to the guest portal. The end time is assgined the specified duration time plus the start time. If the guest user never logs in, the account remains in the Awaiting first login state until the account is removed by the **Endpoint Purge** settings. If you selected **From sponsor-specified date**, enter the maximum number of days, hours or minutes that Guests of this Guest Type can access and stay connected to the network. If you change this setting, your changes will not apply to existing Guest accounts created using this Guest Type. Value ranges from 1 to 999.
Allow access only on these days and times	Enter the time ranges and select the days of the week to specify when this Guest Type can access the network. If this guest type remains connected outside these time parameters, they will be logged off. The time ranges are related to the time zones defined by the locations assigned to the guests using this Guest Type. Click the + and - for adding and deleting restricted access times.
Configure guest account Purge Policy	You can schedule an endpoint purge job. The endpoint purge schedule is enabled by default and Cisco ISE deletes endpoints that are older than 30 days. Refer to the Endpoints Purge Settings section for more information.
Login Options—Maximum simultaneous logins	Enter the maximum number of user sessions that this Guest Type can have running concurrently.

Field	Usage Guidelines
When guest exceeds limit	When you select **Maximum simultaneous logins**, you also must also select the action to take when a user connects after that limit is reached. **When the guest exceeds limit** • **Disconnect the oldest connection** • **Disconnect the newest connection** ◦ **Redirect user to a portal page showing an error message**: An error message is displayed for a configurable amount of time, then the session is disconnected, and the user is redirected to the Guest portal. The error page's content is configured on the Portal Page Customization dialog, on the Messages > Error Messages tab.
Maximum devices guests can register	Enter the maximum number of devices that can be registered to each Guest. You can set the limit to a number lower than what is already registered for the Guests of this Guest Type. This will only affect newly created Guest accounts.
Allow guest to bypass the Guest portal	Allows users to bypass the credentialed Guest captive portal (web authentication page) and access the network by providing credentials to wired and wireless (dot1x) supplicants or VPN clients. Guest accounts go to Active state bypassing the Awaiting Initial Login state and the AUP page, even if it is required. If you do not enable this setting, users must first log in through the credentialed Guest captive portal before they will be able to access other parts of the network.
Account Expiration Notification—Send account expiration notification __ days before account expires	Send a notification to Guests before their account expires and specify how many days, hours or minutes in advance of the expiration.
View messages in	Specify the language to use when displaying email or SMS notifications as you set them up.
Email	Select email as the method used for account expiry notification.
Use customization from	Select email customization from another portal.

Field	Usage Guidelines
Messages	Enter the the text to use for account expiry notification.
Copy text from	Reuse email text that you created for another Guest Type for account expiry notification.
Send test email to me at	Ensure that the email notification displays as it should by sending it to your email address.
SMS	Select text (SMS) as the method used for account expiry notification.
Messages	Enter the the text to use for account expiry notification.
Copy text from	Reuse text messages that you created for another Guest Type.
Send test SMS to me at	Ensure that the text notification displays as it should by sending it to your cell phone.
These sponsor groups can create this guest type	Select which sponsor groups can create Guest accounts with this Guest Type. If you want to disable use of this Guest Type, do not assign it to any sponsor group. If you want to discontinue use of this Guest Type, delete the sponsor groups listed.

Sponsor Group Settings

The navigation path for these settings is **Guest Access** > **Configure** > **Sponsor Groups**. Use these settings to add members to the sponsor group, define guest types and location privileges, and set permissions related to creating and managing guest accounts.

- **Disable Sponsor Group**

  —Disable members of this sponsor group from accessing the Sponsor portal.
  For instance, you may want to temporarily prevent sponsors from logging in to the Sponsor portal while configuration changes are being made in the Admin portal. Or, you may want to disable a sponsor group that is involved in infrequent activity, such as sponsoring guests for an annual convention, until the time they need to be activated again.

- **Sponsor group name—**Enter a unique name (from 1 to 256 characters).

- **Description**

  —Include useful information (maximum of 2000 characters) such as the guest types used by this sponsor group.

- **Members—**Click to display the **Select Sponsor Group Members** box, where you can select available user identity groups (from internal and external identity stores) and add them as members of this sponsor group.
- **Sponsor Group Members—**Search and filter the list of selected sponsor groups and delete any groups you do not want to include.
- **This sponsor group can create accounts using these guest types—**Specify the guest types that the members in this sponsor group can use when creating guest accounts. For a sponsor group to be enabled, it must have at least one guest type that it can use.

  If you assign only one guest type to this sponsor group, you can choose not to display it in the Sponsor portal since it is the only valid guest type available for use. Choose **Guest Access** > **Configure** > **Sponsor Portal** > **Page Customization** > **Create Accounts** > **Guest Types** > **Settings**. Check **Hide guest type if only one is available to sponsor** to enable this option.
- **Configure Guest Types**

  —If the guest type you need is not available, click **Guest Access** > **Configure** > **Guest Types** and create a new guest type or edit an existing one.
- **Select the locations that guests will be visiting—**Select the various locations sponsors in this group can assign to guests when creating their accounts. This helps define the valid time zones for these guest accounts and specifies all the time parameters that apply to the guest, such as valid access times, and so on This does not prevent guests from connecting to the network from other locations.

  For a sponsor group to be enabled, it must have at least one location that it can use.

  If you assign only one location to this sponsor group, it will be the only valid time zone for the guest accounts created by its members. By default, it does not display in the Sponsor portal.

Sponsor Can Create

- **Multiple guest accounts assigned to specific guests (Import)—**Enable the sponsor to create multiple guest accounts by importing guest details such as first name and last name from a file.

  If this option is enabled, the **Import** button displays in the **Create Accounts** page of the Sponsor portal. The Import option is only available on desktop browsers (not mobile), such as Internet Explorer, Firefox, Safari, and so forth
- **Limit to batch of—**If this sponsor group is allowed to create multiple accounts simultaneously, specify the number of guest accounts that can be created in a single import operation.

  Although a sponsor can create a maximum of 10,000 accounts, we recommend that you limit the number of accounts you create, due to potential performance issues.
- **Multiple guest accounts to be assigned to any guests (Random)—**Enable the sponsor to create multiple random guest accounts as placeholders for guests who are not known as yet, or when they need to create many accounts quickly.

  If this option is enabled, the **Random** button displays on the **Create Accounts** page of the Sponsor portal.
- **Default username prefix—**Specify a username prefix that sponsors can use when creating multiple random guest accounts. If specified, this prefix appears in the Sponsor Portal when creating random guest accounts. In addition, if **Allow sponsor to specify a username prefix** is:
  - Enabled**—**The sponsor can edit the default prefix in the Sponsor portal.

- Not enabled—The sponsor cannot edit the default prefix in the Sponsor portal.

If you do not specify a username prefix or allow the sponsor to specify one, then the sponsor will not be able to assign username prefixes in the Sponsor portal.

- **Allow sponsor to specify a username prefix—**If this sponsor group is allowed to create multiple accounts simultaneously, specify the number of guest accounts that can be created in a single import operation.

  Although a sponsor can create a maximum of 10,000 accounts, we recommend that you limit the number of accounts you create, due to potential performance issues.

- **Start date can be no more than __ days into the future—**Enable and specify the number of days within which sponsors have to set as the start date for the multiple guest accounts they have created.

Sponsor Can Manage

- **Only accounts sponsor has created—**Sponsors in this group can view and manage only the guest accounts that they have created, which is based on the Sponsor's email account.
- **Accounts created by members of this sponsor group—**Sponsors in this group can view and manage the guest accounts created by any sponsor in this sponsor group.
- **All guest accounts—**Sponsors view and manage all pending guest accounts.

Note Regardless of the group membership, all sponsors can see all pending accounts, unless you check **Approve and view requests from self-registering guests** with the option **Only pending accounts assigned to this sponsor** under **Sponsor Can**.

Sponsor Can

- **View guests' passwords—**For guest accounts that they can manage, allow the sponsor to view the passwords.

  If the guest has changed the password, the sponsor can no longer view it; unless it was reset by the sponsor to a random password generated by Cisco ISE.

  Note If this option is disabled for a sponsor group, the members of that group cannot send email and SMS notifications regarding the login credentials (guest password) for the guest accounts that they manage.

- **Reset guest account passwords—**For guest accounts that they can manage, allow the sponsor to reset passwords for guests to a random password generated by Cisco ISE.
- **Extend guests' accounts—**For guest accounts that they can manage, allow the sponsor to extend them beyond their expiration date. The sponsor is automatically copied on email notifications sent to guests regarding their account expiration.
- **Send SMS notifications with guests' credentials—**For guest accounts that they can manage, allow the sponsor to send SMS (text) notifications to guests with their account details and login credentials.

- **Delete guests' accounts—**For guest accounts that they can manage, allow the sponsor to delete the accounts, and prevent guests from accessing your company's network.
- **Suspend guests' accounts—**For guest accounts that they can manage, allow the sponsor to suspend their accounts to prevent guests from logging in temporarily.

  This action also issues a Change of Authorization (CoA) Terminate to remove the suspended guests from the network.
- **Require sponsor to provide a reason—**Require the sponsor to provide an explanation for suspending the guest accounts.
- **Reinstate suspended guest accounts—**For guest accounts that they can manage, allow the sponsor to reinstate suspended accounts.
- **Approve requests from self-registering guests—**For guest accounts that they can manage, allow the sponsor to approve self-registering guests when they receive an email requesting their approval.
- **Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)—**For guest accounts that they can manage, allow the sponsor to access guest accounts using the Guest REST API programming interface.