Sponsor Portal User Guide for Cisco Identity Services Engine, Release 3.3

First Published: 2023-04-12

CONTENTS

CHAPTER 1

Sponsor Portal Users Guide

✎

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Additional References

See Cisco ISE End-User Resources for additional resources that you can use when working with Cisco ISE.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.

- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Network Access for Guests

With the increased use of and dependency on mobile devices, such as laptops, tablets, and mobile phones, people have become accustomed to being able to access the Internet from anywhere. However, access to corporate networks requires more security than free Wi-Fi at a local coffee shop. Network security is critical to maintaining your company's confidentiality and data integrity. Network security prevents unauthorized users from hacking your company's network.

To protect your company's network and to ensure that only authorized guests can access it, your company uses Cisco Identity Service Engine (ISE) guest services. Cisco ISE ensures that only authorized guests, such as visitors, contractors, consultants, and customers can access your network.

Note   If you an ISE administrator, accessing the Sponsor portal from the ISE administrators console, please see this link Manage Accounts link.

Your Role as a Sponsor

As a sponsor, you are responsible for using the Sponsor portal to create and manage guest accounts for authorized visitors to your organization. These accounts enable visitors to access your company's network or provide access to the Internet. When creating these accounts, follow your company guidelines for providing network access to visitors. Cisco ISE saves the entire guest process for auditing and reporting purposes, which your company can use to verify that only authorized visitors have been granted network access.

Sponsor Portal

Use the Sponsor portal to create temporary accounts for authorized visitors to securely access your corporate network or the Internet. After creating the account, you can use the Sponsor portal to provide account details to the guest by printing, e-mailing, or texting. You can also use the Sponsor portal to suspend, extend, and delete accounts as well as approve or deny guests access to your network using the tabs at the top of the page.

- Create Accounts - Create guest accounts individually, by generating a group of accounts, or by importing accounts from a spreadsheet (CSV) using a Cisco-supplied template.

- Manage Accounts - Edit, delete, suspend, reinstate and extend guest accounts. Resend account details to guests.

- Pending Accounts - Approve or deny selected guest accounts.

- Notices - Check the status of background operations when creating or managing a large number of guest accounts.

Your system administrator configures the features of your sponsor account, so you might not have access to all the features available on the Sponsor portal.

Related Topics

Unable to Sign On Because Account is Locked , on page 3

Sign on to the Sponsor Portal

The Sponsor portal is a web-based portal that you use to create guest accounts for authorized visitors. Once you are signed into the Sponsor portal, you will be automatically logged out after a period of inactivity, which is configured by your system administrator.

Before you begin

Obtain the Sponsor portal URL and your username and password from your system administrator.

Step 1 Open a web browser and enter the Sponsor portal URL provided to you by your system administrator.

Your administrator customizes this URL, but it typically has a format such as: https://*ipaddress:portnumber*/sponsorportal/PortalSetup.action?portal=portalID or https://sponsorportal.yourcompany.com

Step 2 Enter your username and password and click **Sign On**.

Step 3 Click **Accept** if you are asked to agree to your company's network usage terms and conditions before logging into the Sponsor portal.

If you log in successfully on your desktop, the **Create Accounts** page, which is the home page for the Sponsor portal displays. If signing on from your mobile device, a welcome page displays. If not, contact your system administrator for assistance.

Unable to Sign On Because Account is Locked

By default, if you incorrectly enter your password for your sponsor account five times in a row, the Sponsor portal temporarily locks you out of the system for two minutes. You can make additional attempts after that, but only one attempt at a time is possible before you are locked out again for the configured amount of time. Your system administrator can change this default setting to require fewer or more failed attempts before temporarily locking your account; as well as the amount of time you are locked out.

CHAPTER **2**

Create Guest Accounts

Sponsor Portal Create Accounts Page

You can use the **Create Accounts** page to create accounts for the following authorized visitors:

• Guests whose personal information, such as last name, email address, or phone number, is available to you.

• Guests whose personal information is not available or when you need to create multiple accounts quickly.

• Guests whose information is available in an external database in the form of a file that you can import.

Create a Known Guest Account

You can create individual accounts for guests whose personal information is available, one account at a time.

Step 1   Click **Known** on the **Create Accounts** page.

Your system administrator configures which fields display on this page and are required for creating guest accounts. Some fields are mandatory (marked with *) and display with default information that you can change.

Step 2   Retain or update the **Guest Type** you want to assign to the guest.

The various types of guests and their access privileges are defined by your system administrator.

The maximum number of devices that guests can simultaneously connect to the network and the maximum duration time for network access are displayed for the guest type you select.

Step 3   If displayed and required, enter the guest's personal information, such as **First name** and **Last name** or **Email address** to create the username.

The personal information you enter will be used to generate a username. If not entered, a username is generated randomly, depending on the username policies set by your system administrator.

Step 4 Retain or update the defaults for the mandatory settings and enter information in the other fields, as desired.

The system administrator can configure multiple selections for **Language**, **SMS Provider**, **Location**, and **SSID**. However, if only one selection is specified, it will not display, but is automatically assigned when you create the guest account. You can view this selection in the guest account details after the account is created.

Note When setting time durations for accounts, the start and end times you define are applicable in the time zone for the location you pick.

Step 5 Click **Create** to create the guest account.
An **Account Information** dialog box displays with the account details, including the guest username and password.

What to do next

You can email or print the account details for guests, if these facilities are available to you. You can also text the account details to guests, if your system administrator has enabled this functionality.

Related Topics

Create Random Guest Accounts

You can create a set of multiple random guest accounts in advance, record the details separately, and store them in the system for future use. For example, if you are a lobby ambassador who needs to distribute guest accounts on a regular basis, you can save time by using these generic, randomly created accounts.

Step 1 Click **Random** on the **Create Accounts** page.

Your system administrator configures which fields display on this page and are required for creating guest accounts. Some fields are mandatory (marked with *****) and display with default information that you can change.

Step 2 Retain or update the **Guest Type** you want to assign to the guest.

The various types of guests and their access privileges are defined by your system administrator.

The maximum number of devices that guests can simultaneously connect to the network and the maximum duration time for network access are displayed for the guest type you select.

Step 3 Enter the **Number of Accounts** to create.

The maximum number of random guest accounts displayed that you can create at a time is configured by your system administrator.

Step 4 Based on how your system administrator configured this setting, you can either enter, edit or use the predefined **Username Prefix** to add to each account name.

The remainder of the username is generated randomly adhering to the username policies set by your system administrator.

Step 5   Retain or update the defaults for the mandatory settings and enter information in the other fields, as desired.

The system administrator can configure multiple selections for **Language**, **Location**, and **SSID**. However, if only one selection is specified, it will not display, but is automatically assigned when you create the guest accounts. You can view this selection in the guest account details after the accounts are created.

Note   When setting time durations for accounts, the start and end times you define are applicable in the time zone for the location you pick.

Step 6   Click **Create** to create the specified number of random guest accounts.
If you created:

- 50 or less random accounts—An **Account Information** dialog box displays with the randomly generated usernames and passwords for the multiple accounts you created.

- More than 50 random accounts—A message informs you that the accounts are being created in the background and to check the **Notices** page for a status on the operation.

What to do next

When you generate random guest accounts, you probably do not have guest information such as email addresses or phone numbers. You can print the account details and manually distribute the login credentials to the guests. If you created more than 50 accounts, open the specific notice on the **Notices** page to view account details for up to 50 accounts. To view all the accounts created, go to the **Manage Accounts** page.

Related Topics

Import Guest Accounts

If your company maintains account information for authorized visitors in an external database or file, you can create guest accounts for these users by importing their information into the Sponsor portal. The file containing the account information must be a .csv file, which the Sponsor portal then parses and creates new guest user accounts for each entry in the file.

Before you begin

- Make sure that you have the necessary permissions to import guest account information.

- You cannot import guest account information from a mobile device (running Apple iOS, Android, and so on), so ensure that you are importing account information using a desktop device (running Apple OSX, Windows, and so on).

You can import username and password, but those rows are not added to the CSV template when you download it. You can add those headings. The columns must be named properly in order for the ISE to recognize the content:

- **Username**—Can be either `User Name` or `UserName`

- **Password**—Must be `password`

Step 1   Click **Import** on the **Create Accounts** page.

Your system administrator configures which fields display on this page and are required for creating guest accounts. Some fields are mandatory (marked with *) and display with default information that you can change.

Step 2   Retain or update the **Guest Type** you want to assign to the guest.

Your system administrator defines the various types of guests and their access privileges.

The maximum number of devices that guests can simultaneously connect to the network and the maximum duration time for network access are displayed for the guest type you select.

Step 3   Click **Download Template** to get a template to use for the import file. Ensure that the file you are importing conforms to the required structure before importing it.

In the template file, update the Mobile number column format to ensure that the plus sign (+) is retained. Ensure that the required format is applied even if you edit the template at a later time. Carry out the following steps:

    a. In the downloaded template file, select the **Mobile number** column.

    b. Right-click anywhere in the selected column.

    c. Choose **Format Cells**.

    d. From the **Number** tab, choose **Custom**.

    e. In the **Type** text box, delete **General** and enter **+0**.

    f. Click **OK**.

Step 4   Click **Browse** to locate and select the .csv file that contains the guest information is required to create the guest accounts.

> **Note**   If the .csv file includes non-English characters, then enable UTF-8 character encoding, before importing the file. If UTF-8 character encoding is not enabled, the non-English characters are not parsed properly.

Step 5   Retain or update the defaults for the mandatory settings and enter information in the other fields, as desired.

The system administrator can configure multiple selections for **Language**, **Location**, and **SSID**. However, if only one selection is specified, it does not display, but is automatically assigned when you create the guest accounts. You can view this selection in the guest account details after the accounts are created.

> **Note**   When setting time durations for accounts, the start and end times you define are applicable in the time zone for the location you pick.

Step 6   Click **Import** to import the account information from the external database or file.
A message informs you that the accounts are being created in the background and to check the **Notices** page for a status on the operation.

What to do next

You can email or print the account details for guests, if these facilities are available to you. You can also text the account details to guests, if your system administrator has enabled this functionality.

On the **Notices** page, open the specific notice to view account details for up to 50 accounts. If you imported more than 50 accounts, go to the **Manage Accounts** page, to view all the accounts created.

Related Topics

Privacy of Guest Passwords

You can create guest accounts for authorized visitors requiring access to your company's network and internal resources. When you create accounts, whether it is for a known guest, or randomly for a multiple set of guests, or when importing a batch of guest accounts from an external database, Cisco ISE generates passwords for these accounts.

If your system administrator set you up with the required privileges, you can view these system generated passwords:

- When managing guest accounts in the account details for each account.
- If you choose to be notified of the account details at the same time you notify your guests.

However, if your guests are permitted to change their passwords and do so after they log into the Guest portals, you can no longer view these passwords, as they are considered private.

If guests lose or forget their passwords after they change them, you cannot simply resend their passwords to them. You have to reset their passwords to random passwords and notify them of the new passwords.

Create Account Settings

You can retain the defaults or change these settings when creating guest accounts. Your system administrator may enable additional settings for which you may need to enter information.

Table 1: Create Account Settings

Field	Usage Guidelines
Guest Type	Select the type of guests whose accounts you are creating. If only one guest type is configured by your system administrator, you can only use this type to create guest accounts.
	Cisco ISE includes these default guest types to map guests to their appropriate network access privileges:
	• **Daily**—Default settings allow guests network access for just 1-5 days.
	• **Weekly**—Default settings allow guests network access for a couple of weeks.
	• **Contractor**—Default settings allow guests network access for up to a year.
	Your system administrator might restrict this list or create additional guest types.
	The system administrator can set up guest types to **Allow guest to bypass the Guest portal**. In this case, the guest accounts created using this guest type are enabled automatically, and their states display as **Active**, even if the guests have not yet logged into a Cisco ISE web portal. If this option is not configured, the accounts are not enabled until the guests actually log into a web portal and their initial states display as **Created**.

Field	Usage Guidelines
SMS Provider	This field displays only if more than one SMS provider has been configured for selection by your system administrator. If only one provider is configured, it will not display as it is the only option available for this Sponsor portal. If you know your guest's cellular provider and it is listed under **SMS Provider**, select it to send a SMS notification with the login credentials to the guest. If the cellular provider is not listed, then select the default global provider listed. Include the country code of the guest's phone number if using the default global provider. The supported phone number formats include: +1 ### ### ####, ###-###-####, (###) ### ####, ##########, 1########## and so on.
Group Tag	Groups certain guests accounts for tracking and searching purposes. For instance, you can assign a tag to all the guests attending training at a certain location. You can then search for these guests to either extend their account duration if the training is not completed in time or delete their accounts after the training is finished.
Location	This field displays only if more than one location has been configured for selection by your system administrator. If only one location is configured, it will not display as it is the only option available for this Sponsor portal. Select the location to be used for the guest accounts. This determines the time zones that applies to the guests and helps define valid time ranges and other time parameters that apply to their accounts. The time left for a guest account is related to the specific location assigned to it, and not the sponsor's local time.
SSID	This field displays only if more than one SSID has been configured for selection by your system administrator. If only one SSID is configured, it will not display as it is the only option available for this Sponsor portal. Select the SSID of the network that guests will log into. This SSID is included in the account notifications sent to the guests.

Field	Usage Guidelines
Language	This field displays only if more than one language has been configured for selection by your system administrator. If only one language is configured, it will not display as it is the only option available for this Sponsor portal. Choose the language used when sending account notifications (email, text, and print) to the guests.
Access Information—From	Displays First Login to indicate that the start and end time stamp is not set until the guest logs in and after the first login the guest account is activated. The From field is applicable to all guest types and Guest Information (Known, Random, and Import).
Access Information—Duration	Displays the maximum duration that is allowed for a guest account.

Manage Guest Accounts

Sponsor Portal Manage Accounts Page

On the **Manage Accounts** page you can manage the guest accounts you created and any other accounts that you have the authority to manage.

• Edit and delete guest accounts

• Extend guest account duration

• Suspend guest accounts

• Reinstate expired guest accounts

• Resend and reset passwords for guests

Edit Guest Accounts

You can edit any guest account, regardless of the state it is in.

Step 1   On the **Manage Accounts** page, select the guest account that you want to edit.

Step 2   Click **Edit**.

Step 3 Edit any of the fields that display.

For instance, you may want to change the defaults for **Language** and **Location** that you retained when you first created the guest accounts. You may want to add information such as names, email addresses, and phone numbers that was not available when you first created random guest accounts. If you change (reduce or extend) the time duration for an account, the time left is changed based on the specific location assigned to it, and not the sponsor's local time.

Step 4 Click **Save**.

Step 5 View the changes you made to their account information.

Related Topics

Resend Guest Passwords

Guests may sometimes be unable to log into the network because they have lost or forgotten their passwords. You can help these guests regain access to the network by resending their original passwords.

Before you begin

- You cannot resend passwords to guests who have changed them. If these guests have lost or forgotten their new passwords, you must reset them and notify the guests.

- You can resend passwords for accounts that are either Created or Active.

- You cannot resend passwords for accounts that are either Pending Approval, Suspended, Expired, or Denied.

Step 1 On the **Manage Accounts** page, select the guest accounts whose passwords you want to resend.

Step 2 Click **Resend** to send the guests their account details again.

Step 3 In the **Resend** pop-up window, select the various notification options (for both guests and sponsors) and click **OK**.

When sending notification to guests, there are options for sending account information to yourself, as well.

- Send me a summary—Lists the guest name and password. The password will not show if it is blocked by your administrator.

- Copy me—Sends you an email that is the same as the one sent to the guest. The password will not show if it is blocked by your administrator.

Related Topics

Extend Guest Account Durations

You can extend the account durations for guests before or after their accounts expire, so that they can access the network for longer than originally permitted. You can also extend the account durations when editing guest accounts.

If guest accounts have expired, they are no longer able to connect to the network. An automated process runs periodically (based on criteria set by your system administrator) that removes (purges) all expired accounts from the system. If that happens before you can extend the account duration for an expired account, you will need to create new accounts for these guests.

Before you begin

- You can extend accounts that are either Created, Active, or Expired.

- You cannot extend accounts that are either Suspended or Denied. You can reinstate them.

Step 1   On the **Manage Accounts** page, select the guest account that you want to extend.

Step 2   Click **Extend**.

Step 3   Enter the extension information and click **OK.**
The **Expiration Date** and **Time Left** are automatically updated with the new time duration. The time left is related to the specific location assigned to the guest account, and not the sponsor's local time.

Step 4   Verify that the Expired accounts' duration times have been extended and their states are reset as follows:

- For accounts awaiting approval, to Pending Approval.

- For accounts that are configured to bypass the credentialed Guest portal, to Active.

- For accounts that are not configured to bypass the credentialed Guest portal, to Created.

Related Topics

Suspended and Expired Guest Accounts

When guest accounts are suspended manually by you or expire, the affected guests are disconnected from the network and can no longer access it.

Regardless of their state, active, pending and so on, guest accounts expire when they reach the end of their account duration, which you defined when you created the accounts.

Suspended and expired accounts are automatically purged based on a schedule defined by your system administrator, but the default is every 15 days. After an account is purged, you must create a new account for that guest. However, you can reinstate suspended accounts and extend expired accounts before they are purged.

Suspend Guest Accounts

You can suspend the accounts of guests, which disconnects them from the network and prevents them from accessing it. However, their accounts are retained in the Cisco ISE database.

Before you begin

- You can suspend accounts that are either Created or Active.

- You cannot suspend accounts that are either Pending Approval, Expired, or Denied.

Step 1   On the **Manage Accounts** page, select the guest accounts that you want to suspend.

Step 2   Click **Suspend**. If configured by your system administrator, you may be asked to provide a reason for the suspension.

Step 3   Click **OK** to confirm.

Step 4   Verify that the accounts are now listed as Suspended.

Related Topics

Delete Guest Accounts

You can delete any guest account, regardless of the state it is in.

Step 1   On the **Manage Accounts** page, select the guest accounts that you want to delete.

Step 2   Click **Delete**.

Step 3   Click **OK** to confirm.

Step 4   Ensure that the accounts no longer appear in the account list.

Related Topics

Reset Guest Passwords

Guests may sometimes be unable to log into the network because they have lost or forgotten their passwords. You can help these guests regain access to the network by resetting their passwords.

Before you begin

- You can reset passwords regardless of whether guests have changed their passwords or not.

- You can reset passwords for accounts that are either Created or Active.

- You cannot reset passwords for accounts that are either Pending Approval, Suspended, Expired, or Denied.

Step 1 On the **Manage Accounts** page, select the guest accounts whose passwords you want to reset.

Step 2 Click **Reset Password** to generate random system passwords.
You are asked to confirm the reset and select how you want to notify the guests of their new account details, either by email, text, or print.

Step 3 In the **Reset Password** pop-up window, select the various notification options (for both guests and sponsors) and click **OK**.

When sending notification to guests, there are options for sending account information to yourself, as well.

- Send me a summary—Lists the guest name and password. The password will not show if it is blocked by your administrator.

- Copy me—Sends you an email that is the same as the one sent to the guest. The password will not show if it is blocked by your administrator.

Related Topics

Reinstate Guest Accounts

You can reinstate guest accounts that you suspended previously or denied approval.

Before you begin

- You can reinstate accounts that are either Suspended or Denied.

- You cannot reinstate accounts that are either Created, Active, Pending Approval, or Expired.

Step 1 On the **Manage Accounts** page, select the guest accounts that you want to reinstate.

Step 2 Click **Reinstate**.

Step 3 Click **OK** to confirm.

Step 4 Verify that the accounts are reinstated and their states are reset as follows:

- For Suspended accounts—To either Created or Active. Accounts change to Expired, if they expired while suspended.

- For Denied accounts—To either Created or Active. Accounts change to Expired, if they expired while denied.

Related Topics

Manage Accounts Page Details

The **Manage Accounts** page allows you to manage the guest accounts you have created and other accounts based on your privileges set by your system administrator.

Use these settings to manage guest accounts.

Table 2: Manage Accounts Page Details

Action	Usage Guidelines	Eligible Account States
Edit	Make changes to a selected account.	All, except Suspended, Denied.
Resend	Email, text, or print account details for the selected guests.	Active, Created
Extend	Adjust the access time period or reactivate the selected expired guest accounts.	Active, Created, Expired
Suspend	Disable the selected guest accounts without deleting them from the system. You may be prompted to provide reasons for suspending an account.	Active, Created
Delete	Remove the selected guest accounts from the Cisco ISE database.	All
Reset Password	Reset the selected guest passwords to random passwords and notify the guests of the account details.	Active, Created
Reinstate	Enable the selected suspended guest accounts and approve previously denied accounts.	Suspended, Denied
Refresh	View any changes to the displayed accounts.	Not applicable

Manage Account States

The account state displays details about guest accounts.

When you delete an account, it no longer displays on this page and it is removed from the Cisco ISE database.

Table 3: Manage Account States

Current State	Description	New State
Active	Guests with these accounts have successfully signed in through a credentialed Guest portal, or bypassed the credentialed Guest captive portal. In the latter case, the accounts belong to guest types that are configured to bypass the credentialed Guest captive portal. These guests can access the network by providing their login credentials to the native supplicant on their device.	Account states change based on the action taken on them.
Created	The accounts have been created, but the guests have not yet logged in to a credentialed Guest portal. In this case, the accounts are assigned to guest types that are not configured to bypass the credentialed Guest captive portal. Guests must first sign in through the credentialed Guest captive portal before they are able to access other parts of the network.	Account states change based on the action taken on them.
Denied Accounts that expired while in a denied state remain as Denied.	The accounts are denied access to the network.	If you reinstate denied accounts, their states change to: • Active or Created based on the assigned guest type configuration. • Expired, if they expired while denied, and are purged in the next purge cycle. All denied accounts that are not reinstated are purged in the next purge cycle. Denied accounts that expired cannot be extended (reactivated); you must create new accounts.

Current State	Description	New State
Expired	The time period for the account has ended.	If you extend unexpired accounts, their states remain unchanged. If you extend (reactivate) expired accounts, their states change to: • Active, if the guests are configured to bypass the credentialed Guest captive portal. • Previous states, if the guests are not configured for bypass.
Pending Approval	The accounts are awaiting approval to access the network.	If approved, based on the guest type configuration, the account can be Active or Created. If denied, it appears on the *Manage Accounts* page as Denied.
Suspended Accounts that expired while suspended remain as Suspended.	The accounts are suspended by you, or another sponsor who has the privilege to do so.	If you reinstate suspended accounts, their states change to: • Previous states, if the accounts have not expired in the meantime. • Expired, if they expired while suspended, and are purged in the next purge cycle. However, you can extend these accounts before the next purge cycle.

Pending Guest Accounts

Sponsor Portal Pending Accounts Page

You can use the **Pending Accounts** page to process accounts for self-registering guests who are awaiting sponsor approval before they are allowed network access. You can:

- Approve one, multiple, or all pending accounts.

- Deny approval for one, multiple, or all pending accounts.

Approve Pending Accounts

You can approve accounts listed as either Pending Approval or Denied to provide guests access to the network.

Before you begin

On a desktop device, you can select multiple check boxes or use the select all checkbox to select several guest accounts simultaneously. If using a mobile device, you can only select individual accounts and approve them one at a time.

Step 1 On the **Pending Accounts** page:

- If approving multiple guest accounts on a single page, select the specific accounts and click **Approve** before moving to the next page.
- If approving all the guest accounts on a single page, check the select all checkbox above the list and click **Approve**. This will not select guest accounts on other pages.

Step 2 Click **OK** to confirm that you want to approve the selected accounts.

The approved accounts no longer display on the **Pending Accounts** page, but display on the **Manage Accounts** page.

What to do next

On the **Manage Accounts** page, verify that the approved accounts are listed as either Created or Active. If accounts expired while awaiting approval, they are now listed as Expired on this page and will no longer display on the **Pending Accounts** page.

Related Topics

Deny Pending Accounts

You can deny approval for accounts listed as either **Pending Approval** or **Approved** and prevent guest access to the network.

Before you begin

On a desktop device, you can select multiple check boxes or use the select all checkbox to select several guest accounts simultaneously. If using a mobile device, you can only select individual accounts and deny them one at a time.

Step 1   On the **Pending Accounts** page:

- If denying approval for multiple guest accounts on a single page, select the specific accounts and click **Deny** before moving to the next page.
- If denying approval for all the guest accounts on a single page, check the select all checkbox above the list and click **Deny**. This will not select guest accounts on other pages.

Step 2   Click **OK** to confirm that you want to deny approval for the selected accounts.
The denied accounts display on the **Pending Accounts** page as Denied until you leave the page. After that, they display as Denied on the **Manage Accounts** page.

What to do next

On the **Manage Accounts** page, verify that the accounts that were denied approval are listed as Denied. If the denied accounts expired while awaiting approval, they are now listed as Expired.

Related Topics

Pending Accounts Page Details

The **Pending Accounts** page allows you to approve or deny network access for guest accounts created for self-registering guests.

Use these settings to either approve or deny network access for self-registering guests. Check the select all checkbox above the list to select all the accounts on that specific page only. This will not select accounts on other pages.

Table 4: Pending Accounts Page Details

Action	Usage Guidelines	Eligible Account States
Approve	Approve one or multiple guest accounts for network access.	Pending Approval, Denied
Deny	Deny approval to one or multiple guest accounts for network access.	Pending Approval

Pending Accounts States

The account **State** displays details about guest pending accounts.

When you approve an account, it no longer displays on this page, but is listed as Active, or Created, or Expired on the **Manage Accounts** page.

Table 5: Pending Accounts States

Current State	Description	New State
Denied Accounts that expired while in a denied state remain as Denied.	The accounts are denied access to the network.	If you approve denied accounts, they no longer display on the **Pending Accounts** page. They display on the **Manage Accounts** page, where their states change: • To Active or Created based on the assigned guest type configuration. • To Expired, if they expired while awaiting approval, and are purged in the next purge cycle. All denied accounts that are not approved are also purged in the next purge cycle.

Current State	Description	New State
Pending Approval Accounts that expired while awaiting approval remain as Pending Approval.	The accounts are awaiting approval to access the network.	If you approve pending approval accounts, they no longer display on the **Pending Accounts** page. They display on the **Manage Accounts** page, where their states change: • To Active or Created based on the assigned guest type configuration. • To Expired, if they expired while awaiting approval, and are purged in the next purge cycle. If you deny approval for pending approval accounts, their states change to Denied on the**Pending Accounts** page, until you leave the page. After that, they display as Denied on the **Manage Accounts** page. All denied accounts are purged in the next purge cycle.

Notices and Notifications

Notices When Creating Random and Imported Guest Accounts

The Sponsor portal does not immediately display account details when you create:

- More than 50 random guest accounts simultaneously.

- One or more guest accounts by importing their information.

Instead, Cisco ISE allows you to continue other operations on the Sponsor portal, while it creates these guest accounts in the background. You should periodically check the **Notices** page for a notice that contains the account details.

On the **Notices** page, select the notice and view a summary of the newly-created accounts, which are also listed on the **Manage Accounts** page. You can chose various methods, such as email, SMS (text), and print, to provide the account details and login credentials to the guests and yourself.

Related Topics

Provide Account Details to Known Guests, on page 25

View and Provide Random Guest Account Details, on page 26

View and Provide Imported Guest Account Details, on page 27

Provide Account Details to Known Guests

You can email, text, or print guests their account details, depending on how your system administrator has configured the Sponsor portal. Your system administrator can also set up email and text notifications so that you send guests their usernames separately from their passwords.

Before you begin

- You should have created accounts for guests whose personal information is available.

- To provide email or printed notifications to guests, you should have these facilities available to you.

- To send text notifications to guests, your system administrator should enable the SMS feature for the sponsor group to which you belong.

- For guests to receive email or text notifications, their accounts must have email addresses or phone numbers associated with them.

Step 1   On the **Account Information** dialog box that lists the account created for the known guest, you can:

- Click **Notify** to send the account detail to the guest. The **Notify** dialog box displays with additional options.
- Click **Done** if you do not want to send notifications to the guest.

Step 2   On the **Notify** dialog box, depending on the notification options configured by your system administrator, you can:

- Check **Print** to make a printed version of the account information available to the guest. This option is not available if you access the Sponsor portal on your mobile device.
- Check **SMS** to send an SMS notification with the account information to the guest.
- Check **Email** to send an email notification with the account information to the guest.
- If you enable **Email**, check **Copy me** and enter your **Email address** to receive an email with the account details for the guest account you created.

Step 3   Click **Ok** to send the notifications or **Cancel** if you do not want to send the notifications.

View and Provide Random Guest Account Details

You cannot email or text randomly created guest accounts; you can provide these guests a printed version of their account information. However, once these accounts are created, you can edit the accounts and add email addresses and phone numbers. You can then use this information to send future email and text notifications to these guests.

Before you begin

- You should have created more than 50 random guest accounts simultaneously.

- To provide email or printed notifications to guests, you should have these facilities available to you.

- To send text notifications to guests, your system administrator should enable the SMS feature for the sponsor group to which you belong.

- For guests to receive email or text notifications, their accounts must have email addresses or phone numbers associated with them.

Step 1   On the **Notices** page, open the notice to view a summary of the account details of the newly-created random guest accounts. An **Account Information** dialog box displays up to 50 of the accounts that were created and the usernames and passwords associated with these accounts. If you created more than 50 random accounts, go to the **Manage Accounts** page to view all the accounts created.

Step 2   On the **Account Information** dialog box, you can:

• Click **Print** to make a printed version of the account details available to the guests. A message indicates that the print job will be executed in the background and you will receive another notice about the print job.

Note All of the newly created accounts are printed, regardless of which accounts are displayed in the account creation notice.

• Click **Done** if you do not want to provide the login credentials to the guests at this time. The notice is retained in the **Notices** page.
• Click **Delete Notice** if you do not require the information.

What to do next

On the **Notices** page, open the print notice to view if the selected accounts were printed successfully. Each account is printed separately, so you can provide login credentials to individual guests.

View and Provide Imported Guest Account Details

You can email, text, or print guests their account details, depending on how your system administrator has configured the Sponsor portal. Your system administrator can also set up email and text notifications so that you send guests their usernames separately from their passwords.

Before you begin

• You should have imported guest information from a .csv file to create one or more guest accounts.
• To provide email or printed notifications to guests, you should have these facilities available to you.
• To send text notifications to guests, your system administrator should enable the SMS feature for the sponsor group to which you belong.
• For guests to receive email or text notifications, their accounts must have email addresses or phone numbers associated with them.

Step 1 On the **Notices** page, open the notice to view a summary of the account details of the newly-created imported guest accounts.
An **Account Information** dialog box displays up to 50 of the accounts that were created, the usernames and passwords associated with the accounts, and other guest information that was available when importing. If you imported more than 50 accounts, go to the **Manage Accounts** page to view all the accounts created.

Step 2 On the **Account Information** dialog box, you can:

• Click **Done** if you do not want to provide the login credentials to the guests at this time. The notice is retained in the **Notices** page.
• Click **Delete Notice** if you do not require the information.
• Click **Notify** to provide account details to guests. A **Notify** dialog box displays with the notification options configured by your system administrator.

Note All of the newly created accounts are notified, regardless of which accounts are displayed in the account creation notice.

Step 3 On the **Notify** dialog box that lists the accounts created for the imported guests, you can:

- Check **Print** to make a printed version of the account information available to the guests. This option is not available if you access the Sponsor portal on your mobile device.
- Check **SMS** to send SMS notifications with the account information to the guests.
- Check **Email** to send email notifications. You must enable this option to send emails to the guests and yourself.
- Check **Accounts Created** to send email notifications with the account information directly to the guests.
- Check **Copy me** and enter your **Email address** to receive an email with the guest account information. You can select this option even if you do not choose to notify the guests directly.

Step 4   Click **Notify** to send the notifications or click **Done** if you do not want to send the notifications.