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

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.