



Complete First-Time Setup

- [First-Time Setup Workflow, on page 1](#)
- [Compatible Browsers, on page 1](#)
- [Log In for the First Time, on page 1](#)
- [Integrate Cisco ISE with Cisco DNA Center, on page 4](#)
- [Configure Authentication and Policy Servers, on page 9](#)
- [Configure SNMP Properties, on page 11](#)

First-Time Setup Workflow

After you finish configuring all of the Cisco DNA Center appliances you have installed, perform the tasks described in this chapter to prepare Cisco DNA Center for production use. Note the following points:

- For the parameter information you need to complete this work, see [Required First-Time Setup Information](#).
- If you plan to deploy high availability (HA) in your production environment, you will need to redistribute services among your cluster nodes to optimize HA operation (see [Activate High Availability](#)). Complete this step after you have configured the SNMP settings for your appliances.

Compatible Browsers

The Cisco DNA Center GUI is compatible with the following HTTPS-enabled browsers:

- Google Chrome: Version 62.0 or later.
- Mozilla Firefox: Version 54.0 or later.

We recommend that the client systems you use to log in to Cisco DNA Center be equipped with 64-bit operating systems and browsers.

Log In for the First Time

After you have installed and configured the Cisco DNA Center appliance, you can log in to its GUI. Use a compatible, HTTPS-enabled browser when accessing Cisco DNA Center.

When you log in for the first time as the admin superuser (with the username `admin` and the `SUPER-ADMIN-ROLE` assigned), you are asked to complete a first-time setup wizard that helps you enhance system security and complete the essential setup tasks. Although you can skip each of the steps in the wizard, we recommend that you complete all of them as indicated, so that your system is ready for use as soon as possible.

You should also create new Cisco DNA Center users. We recommend that you create at least one additional user account to be used for daily operations, and that this user account have the `NETWORK-ADMIN-ROLE`.

Before you begin

To log in to Cisco DNA Center and complete the first-time setup wizard, you will need:

- The `admin` superuser username and password you specified when following the steps in [Configure the Primary Node](#).
- The requisite information, as described in [Required First-Time Setup Information](#).

Step 1 After the Cisco DNA Center appliance reboot is completed, launch your browser.

Step 2 Enter the host IP address to access the Cisco DNA Center GUI, using **HTTPS://** and the IP address of the Cisco DNA Center GUI that was displayed at the end of the configuration process.

After entering the IP address, one of the following messages appears (depending on the browser you are using):

- Google Chrome: `Your connection is not private`
- Mozilla Firefox: `Warning: Potential Security Risk Ahead`

Step 3 Ignore the message and click **Advanced**.

One of the following messages appears:

- Google Chrome:


```
This server could not prove that it is GUI-IP-address; its security certificate is not trusted
by your computer's
operating system. This may be caused by a misconfiguration or an attacker intercepting your
connection.
```
- Mozilla Firefox:


```
Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust GUI-IP-address because
its certificate issuer is unknown,
the certificate is self-signed, or the server is not sending the correct intermediate
certificates.
```

These messages appear because the controller uses a self-signed certificate. For information on how Cisco DNA Center uses certificates, see the "Certificate and Private Key Support" section in the [Cisco Digital Network Architecture Center Administrator Guide](#).

Step 4 Ignore the message and do one of the following:

- Google Chrome: Click the **Proceed to GUI-IP-address (unsafe)** link.
- Mozilla Firefox: Click **Accept the Risk and Continue**.

The Cisco DNA Center **Login** window appears.

Step 5 In the **Login** window, enter the admin's username (admin) and password that you set when you configured Cisco DNA Center, then click **Log In**.

The **Reset Login** window appears.

Step 6 Enter the old password, enter and confirm a new password for the admin superuser, and then click **Save**.

The **Enter Cisco.com ID** window appears.

Step 7 Enter the username and password for the cisco.com user, then click **Next**.

If the cisco.com user login does not match any known Cisco Smart Account user login, the **Smart Account** window appears.

Step 8 If the **Smart Account** window appears, enter the username and password for your organization's Smart Account, or click the corresponding link to open a new Smart Account. After you are finished, click **Next**.

The **IP Address Manager** window appears.

Step 9 If your organization uses an external IP address manager (IPAM), do the following and then click **Next**:

- Enter your IPAM server's name and URL.
- Enter the username and password required for server access.
- Choose your IPAM provider (such as Infoblox).
- Choose the specific view of IP addresses available in the IPAM server database that you want Cisco DNA Center to use.

The **Enter Proxy Server** window appears.

Step 10 Enter the proxy server information your organization will use, then click **Next**:

- Include the server username and password if your proxy server requires a login.
- To validate this information before proceeding (recommended), ensure that the **Validate Settings** check box is checked.

The software **EULA** window appears.

Step 11 Click **Next** to accept the software End User License Agreement and continue.

The **Ready to go!** window appears.

Step 12 Click any of the links in this window, or click **Go to System 360** to display the System 360 dashboard and start using Cisco DNA Center.

We recommend that you click the **User Management** link to display the **User Management** window. Then click **Add** to begin adding new Cisco DNA Center users. After you have entered the new user's name and password, and selected the user's role, click **Save** to create the new user. Repeat this as needed until you have added all the new users for your initial deployment. Be sure to create at least one user with the NETWORK-ADMIN-ROLE.

What to do next

Complete other administrative setup tasks, in any order:

- [Integrate Cisco ISE with Cisco DNA Center](#)
- [Configure Authentication and Policy Servers, on page 9](#)
- [Configure SNMP Properties](#)

Integrate Cisco ISE with Cisco DNA Center

This release of Cisco DNA Center provides a mechanism to create a trusted communications link with Cisco ISE and permits Cisco DNA Center to share data with Cisco ISE in a secure manner. After Cisco ISE is registered with Cisco DNA Center, any device that Cisco DNA Center discovers, along with relevant configuration and other data, is pushed to Cisco ISE. Users can use Cisco DNA Center to discover devices and then apply both Cisco DNA Center and Cisco ISE functions to them because these devices will be exposed in both applications. Cisco DNA Center and Cisco ISE devices are all uniquely identified by their device names.

As soon as they are provisioned and belong to a particular site in the Cisco DNA Center site hierarchy, Cisco DNA Center devices are pushed to Cisco ISE. Any updates to a Cisco DNA Center device (such as changes to IP address, SNMP or CLI credentials, Cisco ISE shared secret, and so on) will flow to the corresponding device instance on ISE automatically. Note that Cisco DNA Center devices are pushed to Cisco ISE only when these devices are associated with a particular site where Cisco ISE is configured as its AAA server.

Before you begin

Before attempting to integrate Cisco ISE with Cisco DNA Center, ensure that you have met the following prerequisites:

- You have deployed one or more Cisco ISE version 2.3 (and later) hosts on your network. For information on installing Cisco ISE, see the [Cisco Identity Services Engine Install and Upgrade guides](#) for version 2.3 and later.
- If you have a standalone ISE deployment, you must integrate with the Cisco ISE node and enable the pxGrid service and External RESTful Services (ERS) on that node.



Note Cisco ISE 2.4 and later supports pxGrid 2.0 as well as pxGrid 1.0. Although pxGrid 2.0 allows up to 4 pxGrid nodes in the Cisco ISE deployment, Cisco DNA Center does not currently support more than 2 pxGrid nodes.

- If you have a distributed Cisco ISE deployment:
 - You must integrate Cisco DNA Center with the Cisco ISE admin node, the primary policy administration node (PAN), and enable ERS on the PAN.



Note Is a best practice to use ERS through the PAN. But for backup, enable ERS on the PSNs.

- As with single-node deployments, you must enable the pxGrid service on one of the Cisco ISE nodes within the distributed deployment. Although you can choose to do so, you do not have to enable pxGrid on the PAN. You can enable pxGrid on any of the other Cisco ISE nodes in your distributed deployment.
- The PSNs you configure in Cisco ISE to handle Trustsec/SD Access content and PACs must also be defined in **Work Centers > Trustsec > Trustsec Servers > Trustsec AAA Servers**. For more information, see the Segmentation document in the Administrator Workflow for your release of Cisco ISE.
- You have enabled communication between Cisco DNA Center and Cisco ISE on the following ports: 22, 443, 5222, 8910, and 9060.
- The Cisco ISE host on which pxGrid is enabled must be reachable from Cisco DNA Center on the IP address of the Cisco ISE eth0 interface.
- The Cisco ISE node can reach the fabric underlay network via the appliance's NIC.
- The Cisco ISE node has SSH enabled.
- The Cisco ISE admin node certificate must contain the Cisco ISE IP address or FQDN in either the certificate subject name or the SAN.
- The Cisco DNA Center system certificate must list both the Cisco DNA Center appliance IP address and FQDN in the Subject Alternative Name (SAN) field.

For more information about configuring Cisco ISE for Cisco DNA Center, see [Integration with Cisco DNA Center](#) in the *Cisco ISE Administrators Guide*.



Step 1

Enable Cisco ISE pxGrid service and ERS as follows:

- a) Log in to the Cisco ISE primary policy administration node.
- b) Choose **Administration > System > Deployment**.
The **Deployment Nodes** window opens.
- c) Click the hostname of the Cisco ISE node on which you want to enable pxGrid services.
In a distributed deployment, this can be any Cisco ISE node in the deployment.
The **Edit Node** window opens, with the **General Settings** tab selected by default.
- d) Ensure that the **pxGrid** check box is checked, then click **Save**.
- e) Choose **Administration > System > Settings**.
- f) From the left navigation pane, click **ERS Settings** to open the **ERS Settings** window.
- g) Click the **Enable ERS for Read/Write** radio button, then click **OK** in the notification prompt.
- h) Click **Save**.

Step 2

Add the Cisco ISE node to Cisco DNA Center as an AAA server, as follows:

- a) Log in to the Cisco DNA Center GUI.
- b) Click the **Menu** icon () and choose **System > System 360**.
- c) In the Identity Services Engine (ISE) pane, click the **Configure** link.
- d) From the **Authentication and Policy Servers** window, click  **Add**.
- e) Complete the following tasks in the **Add AAA/ISE server** slide-in pane:

- In the **Server IP Address** field, enter the Cisco ISE management IP address.
- Enter the **Shared Secret** used to secure communications between your network devices and Cisco ISE.
- Click the **Cisco ISE server** slider to ensure that all the Cisco ISE-related fields are shown.
- In the **Username** and **Password** fields, enter the corresponding Cisco ISE admin CLI credentials.
- Enter the **FQDN** for the Cisco ISE node.
- Enter the **Subscriber Name** (for example, cdnacenter).
- (Optional) Enter the Diffie-Hellman-Group14-SHA1 **SSH key** used to connect to Cisco ISE, The SSH key is a diffie-hellman crypto key in base64 encoded format. This key provides security for SSH connections to the Cisco ISE Administration console. You can retrieve the key with the Cisco ISE CLI command `show crypto authorized_keys` and `show crypto host_keys`.
- (Optional) Enter the **virtual IP address** of the load balancer behind which the Cisco ISE policy service nodes are located. If you have multiple policy service node farms behind different load balancers, you can enter a maximum of six virtual IP addresses.

f) Click **Save** and wait for the server status to turn to **Active**.

Step 3



Verify that Cisco ISE is connected to Cisco DNA Center and that the connection has subscribers:

- a) Log in to the Cisco ISE node with which you integrated Cisco DNA Center.
- b) Choose **Administration > pxGrid Services**.

You should see a pxGrid services subscriber with the name you entered (for example, cdnacenter) whose current status is **offline**. Note that the subscriber's status will remain **offline**, by default.

Step 4

Verify that Cisco DNA Center is connected to Cisco ISE, and that the Cisco ISE SGT groups and devices are being pushed to Cisco DNA Center, as follows:

- a) Log in to the Cisco DNA Center GUI.
- b) Click the **Menu** icon () and choose **System > System 360**.
- c) In the Identity Services Engine (ISE) pane, click the **Update** link.
- d) From the **Authentication and Policy Servers** window, verify that the status of the Cisco ISE AAA server is still **Active**.
- e) Click the **Menu** icon () and choose **Policy > Group-Based Access Control**.

The ISE SGT groups are displayed in the **Scalable Groups** table.

Group-Based Access Control: Policy Data Migration and Synchronization

When You Start Using Cisco DNA Center

In previous releases of Cisco DNA Center, the Group-Based Access Control policy function stored some policy Access Contracts and Policies locally in Cisco DNA Center. Cisco DNA Center also propagated that data to Cisco ISE. Cisco ISE provides the runtime policy services to the network, which includes group-based access control policy downloads to the network devices. Usually, the policy information in Cisco DNA Center matches the policy information in Cisco ISE. But it is possible that the data is not in sync; the data may not

be consistent. Because of this, after installing or upgrading to Cisco DNA Center, the following steps are necessary before you can use the Group-Based Access Control capabilities.

- Integrate Cisco ISE with Cisco DNA Center, if it is not already
- Upgrade Cisco ISE, if the version is not the minimum required. See the Cisco DNA Center Release Notes for the required versions of Cisco ISE.
- Perform Policy Migration and Synchronization

What Is “Migration and Synchronization”?

Cisco DNA Center reads all the Group-Based Access Control policy data in the integrated Cisco ISE and compares that data with the policy data in Cisco DNA Center. If you upgraded from a previous version, existing policy data is retained. You must synchronize the policies before you can manage Group-Based Access Control Policy in Cisco DNA Center.

How Does Migration and Synchronization Work?

Usually, the policy data in Cisco ISE and in Cisco DNA Center is consistent, so no special handling or conversion of data is necessary. Sometimes, when there are minor discrepancies or inconsistencies, only some of the data is converted during the migration. If there is a conflict, the data in Cisco ISE is given precedence, so as not to introduce changes in policy behavior in the network. The following list describes the actions taken during migration:

- Scalable Groups: The Scalable Group Tag (SGT), which is a numeric value, uniquely identifies a Scalable Group. Cisco ISE Security Groups are compared to Scalable Groups in Cisco DNA Center.
 - When the Name and SGT value are the same, nothing is changed. The information in Cisco DNA Center is consistent with Cisco ISE and does not need to be changed.
 - When a Cisco ISE Security Group SGT value does not exist in Cisco DNA Center, a new Scalable Group is created in Cisco DNA Center. The new Scalable Group is given the default association of “Default_VN.”
 - When a Cisco ISE Security Group SGT value exists in Cisco DNA Center, but the names do not match, the name from Cisco ISE Security Group replaces the name of that Scalable Group in Cisco DNA Center.
 - When the Cisco ISE Security Group Name is the same, but the SGT value is different, the Security Group from Cisco ISE is migrated. It retains the name and tag value, and the Cisco DNA Center Scalable Group is renamed. A suffix of “_DNA” is added.

Contracts

All the SGACLs in Cisco ISE which are referenced by policies are compared to Contracts in Cisco DNA Center.

- When the SGACL and Contract have the same name and content, there is no need for further action. The information in Cisco DNA Center is consistent with Cisco ISE and does not need to be changed.
- Where the SGACL and Contract have the same name, but the content is different, the SGACL content from Cisco ISE is migrated. The previous Contract content in Cisco DNA Center is discarded.

When the SGACL name does not exist in Cisco DNA Center, a new Contract with that name is created, and the SGACL content from Cisco ISE is migrated.



Note When creating new Access Contracts based upon Cisco ISE SGACL content, Cisco DNA Center parses the text command lines, and, where possible, renders these SGACL commands as a modeled Access Contract. Each ACE line renders as an “Advanced” application line. If a Cisco ISE SGACL contains text which cannot be parsed successfully, the text content of the SGACL is not converted into modeled format. It is stored as raw command line text. These SGACL text contracts may be edited, but no parsing or syntax checking of the text content is performed during migration.

Policies

A Policy is uniquely identified by a source group - destination group pair. All Cisco ISE TrustSec Egress Policy Matrix policies are compared to the policies in Cisco DNA Center.

- When a policy for a source group - destination group references the same SGACL/Contract name in Cisco ISE, no changes are made.
- When a policy for a source group - destination group references a different SGACL/Contract name in Cisco ISE, the Cisco ISE Contract name is referenced in the policy. This overwrites the previous Contract reference in Cisco DNA Center.
- The Cisco ISE default policy is checked and migrated to Cisco DNA Center.



Note Cisco DNA Center supports a single contract in access policies. Cisco ISE has an option to use multiple SGACLs in access policies, but this option is not enabled by default in ISE, and in general is not widely used. Existing SDA customers who have been using the previous release of Cisco DNA Center to manage Group-Based Access Control policy did not use this option.

If you enabled the option to allow multiple SGACLs on Cisco ISE and used this when creating policies, those policies cannot be migrated to Cisco DNA Center in this release. The specific policy features which make use of the “multiple SGACL” option that cannot be migrated are:

- Multiple SGACLs in a policy
- Policy Level catch-all rules set to “Permit” or “Deny.” Only the value of “None” is currently supported for migration to Cisco DNA Center.
- Default Policy set to use a customer-created SGACL, but only the standard values of “Permit IP”, “Permit_IP_Log”, “Deny IP”, and “Deny_IP_Log”, are currently supported for migration to Cisco DNA Center.

If any of the preceding SGACLs are detected during the policy migration and synchronization operation, a notification is generated, and you must choose between the following options to move continue:

- **Manage Group-Based Access Control policy in Cisco DNA Center:** If this option is selected, then all management of Group-Based Access Control Policy are done in Cisco DNA Center. The user interface screens in Cisco ISE for management of Cisco ISE Security Groups, SGACLs, and Egress Policies are available in Read-Only mode. If there were any issues migrating policies (due to use of multiple SGACLs in Cisco ISE), those policies have no contract selected in Cisco DNA Center. The policy uses the default

policy, and you can select a new contract for those policies after completing the migration. If there was a problem migrating the default policy, the default policy is set to “Permit”.

- **Manage Group-Based Access Control Policy in Cisco ISE:** If this option is selected, Cisco DNA Center Group-Based Access Control policy management is inactive. No changes are made to Cisco ISE and there is no effect on policy enforcement in the network. Group-Based Access Control policy is managed in Cisco ISE at the TrustSec workcenter.
- **Manage Group-Based Access Control policy in both Cisco DNA Center and Cisco ISE:** This option is NOT RECOMMENDED for general use, since policy changes made in Cisco ISE are NOT synchronized with Cisco DNA Center. The two systems cannot be kept in sync. This option is intended as a short-term or interim option, and should only be considered when you enabled the “Allow Multiple SGACLs” option in Cisco ISE. You can use this if you need more time and flexibility updating Cisco ISE.

Configure Authentication and Policy Servers

Cisco DNA Center uses AAA servers for user authentication and Cisco ISE for both user authentication and access control. Use this procedure to configure AAA servers, including Cisco ISE.

Before you begin

- If you are using Cisco ISE to perform both policy and AAA functions, make sure that Cisco DNA Center and Cisco ISE are integrated, as described .
- If you are using another product (not Cisco ISE) to perform AAA functions, make sure to do the following:
 - Register Cisco DNA Center with the AAA server, including defining the shared secret on both the AAA server and Cisco DNA Center.
 - Define an attribute name for Cisco DNA Center on the AAA server.
 - For a Cisco DNA Center multihost cluster configuration, define all individual host IP addresses and the virtual IP address for the multihost cluster on the AAA server.
- Before you configure Cisco ISE, confirm that:
 1. You deployed Cisco ISE version 2.3 or later in your network. If you have a multihost Cisco ISE deployment, integrate with the Cisco ISE admin node.
 2. SSH is enabled on the Cisco ISE node.
 3. The pxGrid service is enabled on the Cisco ISE host with which you plan to integrate Cisco DNA Center, and the ERS service is enabled for read/write operations.



Note Cisco ISE versions 2.4 and later supports pxGrid 2.0 and pxGrid 1.0. Although pxGrid 2.0 allows up to four pxGrid nodes in the Cisco ISE deployment, Cisco DNA Center does not currently support more than two pxGrid nodes.

4. The Cisco ISE GUI and Cisco ISE shell username and passwords are the same.

5. There is no proxy configured between Cisco DNA Center and Cisco ISE. If a proxy server is configured on Cisco ISE, the Cisco DNA Center IP address must bypass that proxy server.
6. There is no firewall between Cisco DNA Center and Cisco ISE. If there is a firewall, open the communication between Cisco DNA Center and Cisco ISE.
7. A ping between Cisco DNA Center and Cisco ISE succeeds with both the IP address and hostname.
8. The Cisco ISE admin node certificate contains the Cisco ISE IP address or FQDN in either the certificate subject name or the SAN.
9. If a third-party certificate is used, the certificate includes all IP addresses in the SAN field.
10. The pxGrid approval is set for automatic or manual approval in Cisco ISE to enable the pxGrid connection in Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System > Settings > External Services > Authentication and Policy Servers**.

Step 2 Click  **Add**.

Step 3 Configure the primary AAA server by providing the following information:

- **Server IP Address:** IP address of the AAA server.
- **Shared Secret:** Key for device authentications. The shared secret can be up to 128 characters in length.

Step 4 To configure a AAA server (not Cisco ISE), leave the **Cisco ISE Server** toggle to **Off** and proceed to the next step. To configure a Cisco ISE server, set the **Cisco ISE server** toggle to **On** and enter information in the following fields:

- **Username:** Name that is used to log into the Cisco ISE CLI.
 - Note** This user must be a Super Admin.
- **Password:** Password for the Cisco ISE CLI username.
- **FQDN:** Fully qualified domain name (FQDN) of the Cisco ISE server.
 - Note**
 - We recommend that you copy the FQDN that is defined in Cisco ISE (**Administration > Deployment > Deployment Nodes > List**) and paste it directly into this field.
 - The FQDN that you enter must match the FQDN, Common Name (CN), or Subject Alternative Name (SAN) defined in the Cisco ISE certificate.

The FQDN consists of two parts, a hostname and the domain name, in the following format:

hostname.domainname.com

Example: The FQDN for a Cisco ISE server can be ise.cisco.com.

- **SSH Key:**

The SSH key is a Diffie-Hellman crypto key in base64 encoded format. This key provides security for SSH connections to the Cisco ISE Administration console. You can retrieve the key with the Cisco ISE CLI command **show crypto authorized_keys** and **show crypto host_keys**.

Cisco ISE.

- **Virtual IP Address(es):** Virtual IP address of the load balancer behind which the Cisco ISE policy service nodes (PSNs) are located. If you have multiple PSN farms behind different load balancers, you can enter a maximum of six virtual IP addresses.

Note After the required information is provided, Cisco ISE is integrated with Cisco DNA Center in two phases. It takes few minutes for the integration to complete. The phase-wise integration status is shown in the **Authentication and Policy Servers** page and **System 360** page as follows:

Cisco ISE server registration phase:

- **Authentication and Policy Servers** page: "In Progress"
- **System 360** page: "Primary Available"

pxGrid subscriptions registration phase:

- **Authentication and Policy Servers** page: "Active"
- **System 360** page: "Primary Available" and "PXGRID Available"

If the status of the configured ISE server is "FAILED" due to password change, click **Retry**, and update the password to re-sync the ISE connectivity.

Step 5 Click **View Advanced Settings** and configure the settings:

- **Protocol:** TACACS and RADIUS. RADIUS is the default. You can select both protocols.

Attention If you do not enable TACAS for a Cisco ISE server here, you cannot configure the Cisco ISE server as a TACACS server under **Design > Network Settings > Network** when configuring a AAA server for network device authentication.

- **Authentication Port:** Port used to relay authentication messages to the AAA server. The default is UDP port 1812.
- **Accounting Port:** Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. The default UDP port is 1813.
- **Port:** Port used by TACAS. The default port is 49.
- **Retries:** Number of times that Cisco DNA Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 3.
- **Timeout:** Length of time the device waits for the AAA server to respond before abandoning the attempt to connect. The default timeout is 4 seconds.

Step 6 Click **Add**.


Step 7 To add a secondary server, repeat Step 2 through Step 6.

Configure SNMP Properties

You can configure the retry and timeout values for SNMP.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see the [Cisco DNA Center Administrator Guide](#).

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Settings > Device Settings > SNMP**

Step 2 Configure the following fields:

- **Retries:** Number of attempts allowed to connect to the device. Valid values are from 1 to 3. The default is 3.
- **Timeout (in Seconds):** Number of seconds Cisco DNA Center waits for when trying to establish a connection with a device before timing out. Valid values are from 1 to 300 seconds, in intervals of 5 seconds. The default is 5 seconds.

Step 3 Click **Save**.

Note To return to the default settings, click **Reset and Save**.
