User Interface

Administration Console

Unified Intelligence Center is installed on a Cisco Unified Operating System platform as a cluster with a maximum of eight nodes: one Controller node and up to seven Member nodes.

The Controller node is mandatory and provides both the Administration and the Unified Intelligence Center Reporting web applications. A cluster can consist of the Controller node only.

Member nodes are optional and have the Unified Intelligence Center Reporting application only. (Unified Intelligence Center Administration is not available on a Member node.)

The Administration console manages all components in a unified deployment and also provides links to:

- Cisco Unified Serviceability and SNMP
- Disaster Recovery System
- Real Time Monitoring Tool (RTMT)

Related Topics

Configure SNMP-Associated Settings
Real Time Monitoring Tool
Disaster Recovery System

Access Administration Console

The System Application User who is defined during the installation is by default the initial Super User who can sign in to the Administration Application.

This initial Super User can then create other Super Users in the **Admin Users** page. For more information, see *Manage All Super Users*.

Note When you log in to the Admin Console site and you do not have any scheduled backup configured and enabled, Unified Intelligence Center returns the message "No active backup schedule is available. Set up a new schedule now." Unified Intelligence Center displays this message only for the administrator.

To access the Administration console:

Procedure

Step 1 Direct your browser to the URL *https://<HOST ADDRESS>/oamp* where *HOST ADDRESS* is the IP Address or Hostname of your server.

Step 2 Sign in using your Super User (system application user) ID and password. A successful sign-in launches the OAMP application.

What to do next

See *Home Page*.

The session timeout for inactivity is thirty minutes. It is not configurable.

See also: *Users in the Administration Console*.

Related Topics

System Application User, on page 3
Home Page, on page 2
Users in the Administration Console, on page 3
Manage All Super Users

Home Page

The Home page appears by default after a successful sign-in.

Table 1: Actions From This Page

To	Do this
Display the values for a function	Click a menu in the left navigation pane.
Open the Unified Intelligence Center reporting interface on a member node	• Open a new browser window and enter this URL: *https://<HOST ADDRESS>:8444/* where *HOST ADDRESS* is the IP Address or Hostname of your server.
Verify your signed on identity	This shows as protected text after *Signed on as*. Displays **Administrator** on the top-right corner of your screen.

To	Do this
Sign Out	Click **Administrator** > **Sign Out** on the top-right corner of your screen.
Return to this Home page	Click **Home** in the left navigation pane.

Users in the Administration Console

There are three user accounts that have access to the Administration console:

- Super Users
- System Application User
- System Administration User

Super Users

This user role is defined in the Administration console. It is the only user role for Administration.

The initial and default Super User is the *System Application User* who is configured during installation.

The initial Super User (the System Application User) can sign in to the Unified Intelligence Center Reporting console and has *all* User Roles and *full permissions* for all drawers in Unified Intelligence Center Reporting. Those credentials cannot be removed from the initial Super User.

Additional Super Users who are added in the Administration Console can also sign in to Unified Intelligence Center Reporting and are considered to be IMS users. They have limited Login User role only, until the Unified Intelligence Center Reporting security administrator gives them additional roles and flags them as Active users.

Local users can log in using their IMS username and password. After logging in for the first time, the users are listed on the User List Page. The username is not case sensitive, but the password is case sensitive.

System Application User

This user role is defined during installation. Although it is possible to define unique application user names and passwords during the installation of each node, you must use the same credentials for all installations.

The application user defined during the installation of the *Controller* is the only System Application User recognized by Unified Intelligence Center.

This user has full rights to all functions in the Administration and Unified Intelligence Center Reporting applications, as described below:

- Can log in to the Administration application and becomes the initial Super User for Administration.
- Can create additional Super Users in the Administration application.
- Can log in to Unified Intelligence Center and has full rights to all functions in Unified Intelligence Center.
- Is the initial Security Administrator user in the Unified Intelligence Center Reporting application.

- Can create additional Security Administrator users in the Unified Intelligence Center Reporting application.
- Cannot have any role taken away from them.
- Cannot take any role away from himself.
- This user can log in to the Reporting application and is the initial System user.

System Administration User

The System Administrator account User ID and password are configured at installation for each node. You must enter the same user name and password for all nodes.

The System Administrator for the *Controller* can access:

- The Cisco Systems tools on the Navigation drop-down menu in the Administration console: Disaster Recovery System, Cisco Unified Serviceability, and Cisco Unified OS Administration interfaces.
- The CLI for the Controller.

The System Administrator has no access to functions in the Unified Intelligence Center Reporting application.

Note If you configure unique System Administrator credentials for Member nodes, use those credentials to access the CLI for those Member servers.

Unified Intelligence Center Cluster

Unified Intelligence Center is installed as a cluster of at least one and up to eight nodes.

Nodes in the Unified Intelligence Center Cluster

The first node in the Unified Intelligence Center cluster is the Controller. For database replication, this node is referred to as the “publisher”. This means that it *publishes* or replicates, its databases to Member nodes.

The Member nodes are referred to as *subscribers* of the database replication. Members receive data from the publisher.

Each node on which reporting functionality is processed (the Controller node and each member node) has a Unified Intelligence Center database which is constantly accumulating and removing records; for example, when a dashboard is added or a user record is removed.

When all nodes are up, changes to the Unified Intelligence Center databases replicate synchronously among the Controller/publisher and all Member/subscribers by means of an “update anywhere” model. For more information, see *Database Replication*.

The Disaster Recovery System performs the database maintenance. For more information, see *Disaster Recovery System*.

Related Topics

utils dbreplication

utils disaster_recovery

Unified Intelligence Center Cache

Unified Intelligence Center uses a cache to optimize access to the local Cisco Unified Intelligence Center database and it is built on top of the local configuration database. Unified Intelligence Center is designed to provide a highly scalable cluster in which every node manages its own local cache independently of other nodes.

When an item stored in the local cache (such as a report template or a dashboard) is modified, a message is sent to other nodes in the cluster indicating that the item has been modified and that their version of that item is stale. On receipt of this message, each node invalidates its own references to the stale item in the local cache. In this manner, all nodes remain synchronized.

In a few exceptional cases where, stale data can be re-cached or become out of synch in the cluster. Therefore, the Unified Intelligence Center System Configuration administrator has access to the **Synchronize Cluster** link below the username on the top-right corner of your user interface screen.

Click and confirm. This action notifies all nodes in the cluster to clear their local cache, and it synchronizes and empties all caches in the cluster. Clearing the locale cache forces each node to go directly to the database for the requested information.

Each node gets fresh data from the database. The data is automatically put into the local cache and accessed during future requests. Data will be consistent in the database, and there will be no loss of information.

Note It is best to perform this action during off-hours.