Multi-tenancy within Cisco Unified Communications Domain Manager

Data Partitioning

Data in the multitenant system is "partitioned" by a means of fully configurable hierarchy nodes.

The system can model the hierarchical nature of various businesses and manage the allocation of infrastructure. This infrastructure includes network devices, users, and other entities in the system. Hierarchy rules can be applied to various models in the system including creating hierarchy nodes, hierarchy node types (for example: provider, reseller, customer).

Devolved administration is enabled by creating administrators with different roles for different types of hierarchy nodes. For example:

- An administrator is responsible for the setup of the overall system.
- Provider administrators own and manage infrastructure and define services available to resellers or customers.
- Resellers offer the infrastructure and services to customers or enterprises.
- Customers and enterprises are grouped into various groupings.
- Groupings such as divisions or branches belong to customers.
- Physical locations hold users and phones.
- Users consume services and manage their own configurable settings.

The flexible mechanism is used to define as many levels as needed. Hierarchy node instances of different types can be created and the required business rules can be defined.

Parent-Child Relationships

All entities in the system reside at a specific hierarchy and the data displayed is within the scope of the specified hierarchy. Every entity in the system - including users, device models, and network components - has a parent hierarchy defined. A user is for example provisioned with a specific hierarchy node in a parent-child relationship. Usernames must be unique within a specific hierarchy.

The hierarchy at which an entity resides is always displayed in the list view of the item. For example, to see at which hierarchy users are defined in the system, sign in to the system as a provider, reseller, customer, or site administrator and navigate to **User Management** > **Users**. The resulting list view shows the hierarchy at which each user resides. Furthermore, the users displayed are scoped by the setting of the hierarchy bar at the top of the UI. Only users that reside at the current setting of the hierarchy bar and below are displayed in the list view.

Security

The system defaults to a self-signed web certificate.

- A unique web certificate can be copied onto the host using **scp** or **system download**.
- The web certificate is installed using **web cert add <certificate file>**.

SSH keys are used for sftp, passwordless ssh, and scp.

- Keys can be created using **keys createkey**.
- The public key copied to a remote host using **keys sendkey <user@host>**.
- A host can be authorized for incoming connections using **keys add <host>**.

The system uses an internal repository to check whether security package updates are available.

More repositories can be added with:

security repos add <repo-name> <url> <distro> <section> <categories>

For example, **security repos mymirror add http://archive.ubuntu.com/ubuntu/ precise-updates main universe multiverse**

In order to check whether there are security updates available, use:

security check

The system can be updated using:

security update