Organizational Hierarchy And Access Control

- Introduction
  - What is the Hierarchy?
  - Hierarchy versus Architecture
  - What is Role Based Access Control?
  - Resources, Permissions and Roles
    - View
    - Create
    - Edit
    - Delete
  - How is individual access controlled?
- Organizational Hierarchy

This article was updated to describe the following Contact Expert version:

Contact Expert v5.10 for Skype for Business Server 2015

Introduction

Contact Expert provides the means to set up an organizational hierarchy reflecting a typical customer’s corporate structure in an effort to provide more tightly defined security schemes following real life situations. This allows the configuration of user accounts into various organizational units that - together with the Role Based Access Control feature - establish elaborate control on who has access to what and to what extent within the system. For example supervisors limited by hierarchy to a certain organizational level can be configured to be unable to report on agents registered in other organizational units in an entirely different branch of the hierarchy.

What is the Hierarchy?

Contact Expert's Hierarchy concept means the entire organizational structure of a single CE deployment containing various levels and number of organizational units with defined relationships between them.

Hierarchy versus Architecture

The architecture of a Contact Expert deployment means the individual components including the agent workstations and server computers. The architecture can be a single-server setup where the server components are deployed onto a single computer, or distributed where more than one server computer provide the server functionalities of the entire CE deployment.

Do not confuse architecture with the Hierarchy. The former refers to the physical deployment while the latter is the sum of the organizational structure.

What is Role Based Access Control?

Access control is the means to restrict access to system resources to authorized users with proper permissions only. Users (Administrators, Supervisors, etc.) of the portal are granted access and certain privileges to resources and information via access control.

Contact Expert has a role-based access control, which means that instead of assigning individual permissions to specific users, roles are defined with predefined permission sets, therefore users need to be assigned to a specific role to obtain all permissions defined by the role. On top of the default roles, administrators have the ability to set up new roles hand-picking the permissions required.

To view the list of user roles created in the system, navigate to Organization & AccessPortal UsersUser Roles.

Resources, Permissions and Roles

A resource is any kind of entity (configurable object) in Contact Expert accessible in Contact Expert Portal – for example a human agent config, an outbound campaign, an email gateway, a contact, etc. A resource type is a class containing all the equal types of objects (resources) – e.g. Agents represent all the human agents in the contact center organization, Queues & Campaigns refers to all
A permission is a formal assignment of one particular privilege to a single resource for portal users by authorized persons. In effect users will be able to view different pages and perform different actions on the portal. End users are always granted permissions via the roles, and never directly.

A user can have more than one role assigned and therefore many different permissions provided. An effective permission set is the union of all privileges (permissions) assigned via all of the roles. Such privileges can be viewed by certain people.

To view the effective permission set of a user, navigate to Organization & Access Portal Users User Accounts Edit Effective Permissions.

When having sufficient privileges, you can access the role management options by navigating to Organization & Access Portal Users User Roles.

There are 4 types of permissions available for the role management over the portal, please see the following sections for a description of these.

The List permission
Actually, there is an additional – but hidden – permission that is granted to every single role automatically: the ability to list resource types on any part of the portal that needs a reference to the given object. For example, in case an administrator revokes all permissions to the Dial Rules resource type for a user because that user will have no business deleting, changing, adding or even viewing the details of the dial rules, that user might still need the ability to select a dial rule for the campaign she does have permissions to control.

View
Provides the ability to view all properties of a resource. For example, if a user is granted the right to view campaigns, he or she is able to retrieve all campaign properties like ID, display name, campaign status, assigned dial rule, business tags, etc.

Create
Provides the ability to create new resources. For example, if a user is granted the right to create campaigns, he or she is able to add a new campaign to Contact Expert including all its properties like ID, display name, campaign status, assigned dial rule, business tags, etc.

The Create permission does not implicitly provide the View permission! If a user is granted the Create right to a resource without also adding the View permission, then the user will effectively have no access to the resource!

Edit
Provides the ability to modify an existing resource. For example, if a user is granted the right to edit campaigns, he or she is able to update an existing campaign's every property like display name, campaign status, assigned dial rule, business tags, etc.

The Edit permission does not implicitly provide the View permission! If a user is granted the Edit right to a resource without also having the View permission, then the user will effectively have no access to the resource!

Delete
Provides the ability to remove irrelevant resources. For example, if a user is granted the delete campaign permission, he or she is able to remove an existing campaign from Contact Expert.

The Delete permission does not implicitly provide the View permission! If a user is granted the Delete right to a resource without also having the View permission, then the user will effectively have no access to the resource!

How is individual access controlled?
Putting all of the above together, when a user wishes to access a resource – e.g. campaigns, agents, other configuration – over the Contact Expert Portal, then the system will always combine the user's and the resource's organizational level within the Hierarchy with the
permissions provided by his/her roles and will evaluate whether access to any particular resource can be allowed or not based on the union of these two. When the Hierarchy is not blocking access, then the permission set in the associated Role will define the level of access.

Organizational Hierarchy

In CE the Hierarchy is founded on the Teams of agents. Many Teams can be created but each can only be assigned to a single Business Unit of which many can be created as well. Business Units are then organized into Tenants. There are many resources defined in CE, the business related items like skills, agents, dial rules, campaigns, etc. are all separated on the Tenant level while configurations dealing with connecting to the surrounding infrastructure are such as the telephony backend, email and data storage, etc. are established on a Deployment level.

For detailed description of every resource and the available permissions that can be assigned to these please visit the Administration of Roles and Permissions page in this documentation.