ADTRAN®

NetVanta Unified Communications Technical Note

Creating Custom Authorization Roles

Introduction

This technical note describes how to create custom roles in ADTRAN's NetVanta Unified Communications Server using the Microsoft® Authorization Manager to suit specific organizational role requirements. The UC server authorization capabilities leverage the Authorization Manager Microsoft Management Console (MMC) snap-in. NetVanta Unified Communications has included many default roles that can be assigned to users.

When integrated with Active Directory, the UC server provides the following capabilities:

- Single sign-on

- Delegation of control

- Authorization and role assignment

The Server Configuration Wizard does not automatically create the advanced authentication roles. This technical note provides instructions on creating a custom authorization store that will be used to assign roles to UC server users.

Custom roles can reduce or increase the capabilities of users. For example, if a user needs personal business assistant (PBA) functions, but the administrator does not want the user to be able to manage announcements or services, the administrator can create a custom role for that user. Similarly, the administrator could create a custom role that includes the ability to request an outbound dialing request, a capability normally only associated with the administrator role.

Creating the Authorization Store

The authorization store should be created before running the Server Configuration Wizard, prior to adding users. If users have already been created, the administrator must assign a role to each preexisting configured Windows user. Subsequent users added after the authorization store has been created will have a default role (standard user) assigned to their user profile.

To create an authorization store:

1. Log in to the UC server computer as a domain administrator.

2. Select **Start > Run**. Enter **cmd** and select **OK**.

3. If the UC server was installed in the default directory, navigate to C:\Program Files\ADTRAN\NetVanta UC Server\bin.

4. Enter the following:

   manageazman +createxmlstore +admin <DOMAIN>\<UC SERVER SERVICE ACCOUNT>

5. Open the service control panel application and restart **NetVanta UC Server Application Services**.

You can also create an authorization store at any time after the initial installation and server configuration, but you will have to manage each of the existing users and configure their role.

Authorization Roles

You can enable Windows authentication, which allows you to assign a role to a Windows user. Authorization is the process that determines whether a user can perform a certain operation on an object or objects (for example, identities, profiles, ports, announcements, and faxes). You can add users to or remove users from specific roles. If you have created a custom authorization store on your system, you can choose from the following preconfigured roles:

Administrator	Users assigned this role have full access, for example, they are fully able to manage system objects like users and ports, and they can create, change, and delete objects in shared folders.
Read Only Administrator	Users assigned this role have similar capabilities as administrators, but they cannot create, change, or delete system objects.
Restricted User	Users assigned this role have capabilities typically associated with personal assistant (PA) and PBA users, except they cannot create or delete announcements, and can only read services.
Standard User	Users assigned this role have capabilities typically associated with PA and PBA users.
Executive Assistant	Users assigned this role have the same capabilities as standard users, but they can also manage objects that belong to other profiles to which they have access. For other profiles, their authorization does not allow them to create or delete announcements, and allows them to only read services.

Restricted Executive Assistant	Users assigned this role have restricted user capabilities for their own profile, and the same authorization for other profiles to which they have access.
Power User	Users assigned this role are similar in capability to executive assistant, except that they can also create or delete announcements for other profiles, and have full authorization for services.

A user's authorization for a specific profile depends on the following:

- The role associated with a user's authentication

- The user's profile type, for example, System, PBA, or PA.

NOTE: If there is no custom authorization store, then all Windows authentications will be able to manage any user profiles that have been given to that user.

Creating Custom Roles

CAUTION: *Errors in role definitions will have a negative impact on the behavior of the UC server. Take extreme caution when changing existing roles and when creating new roles.*

To manage custom roles:

1. Run the Microsoft Management Console. Select **Start > Run**. Enter **MMC** and select **OK**.

2. Select **File > Add/Remove Snap-in**.

3. Select **Add**.

4. Select **Authorization Manager**, select **Add**, and select **Close**.

5. Select **OK**.

6. Right-click on **Authorization Manager** and select **Open Authorization Store**.

7. Select **XML file** and, if the UC server was installed in the default directory, browse to C:\Program Files\ADTRAN\NetVanta UC Server\Data\System\OWStore_<COMPUTER NAME>.xml.

8. Select **OK**.

Authorization Manager

Authorization Manager is a flexible rights management tool that can assign individual rights to Windows user roles. For more information on Authorization Manager, refer to the Microsoft TechNet article titled *Role-Based Access Control for Multi-tier Applications Using Authorization Manager*, available online at *http://technet.microsoft.com/en-us/library/cc780256%28WS.10%29.aspx*.

Authorization Manager includes:

Roles　　　A collection of task definitions. It can also include role definitions.

Tasks　　　A collection of operations.

Operations　Primitive actions.

You can combine roles, tasks, and operations into a role assignment. However, it is recommended for management simplicity to group lower level operations into higher level management groups, such as roles.

High-level role assignments include the following:

- Display

- Display Own

- Handle Events

- Manage

- Manage Own

- Modify

- Modify Own

- Read

- Read Own

- Update

- Submit

Tasks and operations include the following:

**Own**　　　　　The user's own greetings.

Other　　　　If the administrator has delegated control to another user's profile, the rights assigned will apply to those other profiles.

Administrative　Some rights only apply to the administrator managing the system. If a user has been granted rights to the administrator profile, they can be limited to managing only certain aspects of the administrative capabilities. An example of this would be to allow a designee to manage announcements, but not be allowed to manage services.

Creating a Role Definition

To create a role definition:

1. Run the Microsoft Management Console. Select **Start > Run**. Enter **MMC** and select **OK**.

2. Right-click on **Authorization Manager** and select **Open Authorization Store**.

3. Select **XML file** and, if the UC server was installed in the default directory, browse to C:\Program Files\ADTRAN\NetVanta UC Server\Data\System\OWStore_<COMPUTER NAME>.xml.

4. Select **OK**.

5. Select **OWStore_<computername>.xml > UC Server > Definitions > Role Definitions**.

6. In the console tree, right-click **Role Definitions**, and then select **New Role Definition**.

7. In the **New Role** dialog box, in the **Name** field, enter a name for the role (for example, **User with Outbound Dialing**).

8. In **Description**, enter a description of the role (for example, **Users who can send outbound call requests**).

9. Specify a combination of roles and tasks that you want to include. For example:

   - Power User Defn – Role Definition

   - Submit Outbound Call Request - Task
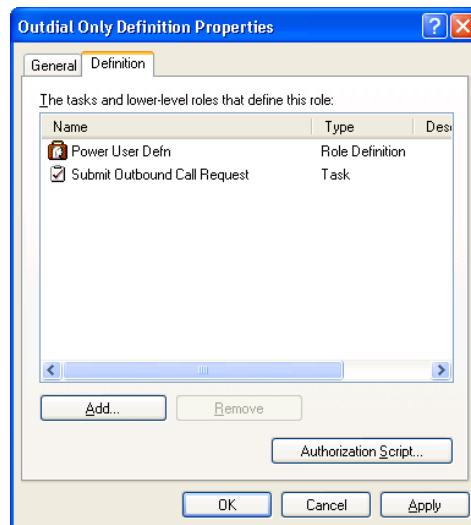
TIP: *ADTRAN recommends choosing a role that is close to what is required, and then adding individual tasks that you want to include with the role definition.*

Creating an Authorization Role

The roles that are managed in the role assignment tree view can be assigned to users in the UC server.

To create a role assignment within an application:

1. Open **Authorization Manager**.

2. In the console tree, right-click **Role Assignments**, and then select **Assign Roles**.

3. In the **Add Role** dialog box, enable the role that was created in *Creating a Role Definition* (for example, **Outdial only definition**).
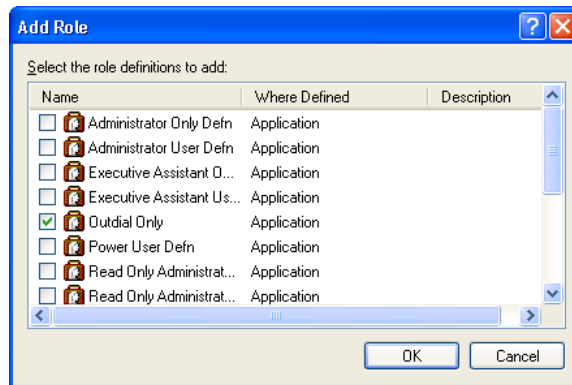
Associating a Role with a UC Server Windows Authentication User

The roles that are included with the UC server or are added to the UC server can be associated with a Windows user. The default role is standard user when you create a new user.

To change a role:

1. Open the UC client administrator application and select the **Users** pane.

2. From the content pane, select a Windows user, right-click and select **Open**.

3. Select the **Authentications** tab.

4. Select a role from the **Role** drop-down list.

5. Select **OK**.