Defining the Authentication Policy

The authentication policy defines which authentication server groups the appliance uses to authenticate admins and lists the local admin groups that map to the remote admin groups.

By default, the appliance provides the "Local Admin" service for authenticating users against the local database. You cannot modify or delete this default service.

Configuring a List of Authentication Server Groups

To enable NIOS to use multiple authentication server groups, define a prioritized list as follows:

1. From the Administration tab, select the Administrators tab -> Authentication Policy tab.
2. From the Authenticate users against these services in this order section, click the Add icon to add an authentication server group.
3. Select one of the following in the Add Authentication Service section:
   - Active Directory: Select this to add an AD authentication server group, and then select a group from the drop-down list.
   - RADIUS: Select this to add a RADIUS authentication server group, and then select a group from the drop-down list.
   - TACACS+: Select this to add the TACACS+ authentication server group, and then select a group from the drop-down list.
   - LDAP: Select this to add the LDAP authentication server group, and then select a group from the drop-down list.
   - Certificate Authentication Service: Select this to add a certificate authentication service, and then select a service from the drop-down list.
4. Click Add.
   You can reorder the list by selecting an authentication server group and moving it up or down the list using the arrow keys.

Configuring a List of Remote Admin Groups

In order for NIOS to assign a remote admin to the correct group, you must list the admin groups in the local database that match the remote admin groups. You can also define a default admin group to which NIOS assigns remote users with no admin groups listed.

The appliance assigns a remote admin to a group in the order the groups are listed. When the appliance receives information that an admin belongs to one or more groups, the appliance assigns the user to the first group in the list that matches. It assigns the admin to the default group, if specified, if no groups are returned by the authentication server, or if the appliance does not find a group in the local database that matches the group returned by the authentication server.

To configure the remote admin group list:

1. From the Administration tab, select the Administrators tab -> Authentication Policy tab.
2. In the Authentication Server Groups is the authority for section, select one of the following:
   - Remote users, their passwords and their groups ownership: Select this to use the authentication server groups to define the list of remote users, their passwords and their group ownerships. This is selected by default. You can add the list of admin groups to map the remote admin group to a local group in the Map the remote admin group to the local group in this order section.
   - Passwords of Local users: Select this to authenticate a remote user when you do not know to which remote admin group the user belongs.
   - Map the remote admin group to the local group in this order: In order for the appliance to assign a remote admin to the correct group, you must list the admin groups in the local database that match the remote admin groups. The appliance matches a remote admin to a group in the order the groups are listed. You can also define a default admin group to which NIOS assigns remote users with no admin groups listed. This section is disabled when you select Passwords of Local users in the Authentication Server Groups is the authority for section.

When the appliance receives information that the admin belongs to one or more groups, the appliance selects the first group in the list that matches, and assigns that group to the admin. If no groups are returned by the authentication server, the default group is assigned (if specified).

Complete the following to configure the remote admin group list:

- Click the Add icon to add an admin group to the list. In the Admin Group Selector dialog box, select an admin group. Use Shift+click and Ctrl+click to select multiple admin groups.
- You can reorder the list by selecting an admin group and using the arrow keys to move it up or down the list.
- Assign user to this group if remote admin group cannot be found: Click Select to assign a user to a specific admin group if the remote admin group is not found. In the Admin Group Selector dialog box, select an admin group. You can also click Clear Selection to clear the displayed member and select a new one.