



Configuring Group Authorization Using an Access Control List

This chapter explains how to configure group authorization using an access control list. It contains the following sections:

- [Configuring an Access Control List for Group Authorization, page 18-1](#)
- [Enabling the Access Control List, page 18-2](#)
- [Modifying an Access Control List, page 18-3](#)
- [Viewing Access Control List Settings, page 18-5](#)

In ACNS 5.x software, you can configure group authorization using an access control list (ACL) only after a user has been authenticated against an NTLM or LDAP HTTP-request authentication server. The use of this list configures a group privilege when members of the group are accessing content provided by the Content Engine. Using the ACL allows or prevents users belonging to certain groups from viewing specific content. This authorization feature offers more specific access control because that access is only allowed to certain groups.

In ACNS 5.x software, the access control list contains the following feature enhancements and limitations:

- A user can belong to several groups.
- A user can belong to an unlimited number of groups within groupname strings.
- A groupname string is a case-sensitive string with mixed-case alphanumeric characteristics.
- Each unique groupname string cannot exceed 128 characters.



Note If the unique groupname string is longer than 128 characters, the group is ignored.

Configuring an Access Control List for Group Authorization

To configure an ACL for group authorization, follow these steps:

-
- Step 1** From the Content Distribution Manager GUI, choose **Devices > Devices**.
 - Step 2** Click the **Edit** icon next to the Content Engine for which you want to configure group authorization.
 - Step 3** To display the entire table of contents, click the **Show All** button above the Contents pane.

- Step 4** In the Contents pane, choose **General Settings > Authentication > Access List > Configure Access Control List**. The Access List Settings for Content Engine window appears listing all configured ACL settings.
- Step 5** To configure a new access list setting, click the Create New Access List Setting icon in the taskbar. The Creating New Access List for Content Engine window appears.
- Step 6** Configure the Action parameter by choosing either **Permit** or **Deny**.
- Step 7** Configure the Group Name parameter.
- Specify any user group by choosing **Any Group Name**.
 - Specify a particular user group by choosing **Enter Group Name**. Enter a group name in the text field, such as, Marketing or Sales.
- Step 8** Click **Submit** to save the configuration. The Access List Settings for Content Engine window reappears.
- Step 9** To configure additional ACL settings, repeat [Step 5](#) through [Step 8](#).
- Step 10** Review the order of your ACL settings and reposition them in the list, if necessary.
- a. To change the position of the settings in the list that you are creating, click the **Change Position** button. A dialog box pops up.
 - b. In the Create Access List at position field, enter a position number.
 - c. In the dialog box, click the **Submit** button. The dialog box closes and the Access List Settings for Content Engine window reappears.
- Alternatively, see the [“Repositioning Settings in the Access Control List”](#) section on page 18-5.
- Step 11** To save the ACL, click **Submit**, and then proceed to the next section, [“Enabling the Access Control List,”](#) to enable the ACL.
-

Enabling the Access Control List

To enable the use of the ACL, follow these steps:

- Step 1** From the Content Distribution Manager GUI, choose **Devices > Devices**.
- Step 2** Click the **Edit** icon next to the Content Engine for which you want to enable the ACL.
- Step 3** In the Contents pane, choose **General Settings > Authentication > Access List > Enable Access Control List**. The Enable Access Control List window appears.
- Step 4** Check the **Enable Access Control List** check box.
- Step 5** Click **Submit**.
-

Using the CLI to Configure and Enable an ACL for Group Authorization

To configure an ACL from the CLI, use the **access-lists 300** global configuration command. This command allows you to permit or deny a group from accessing the Internet by using the Content Engine. For instance, use the **access-lists 300 deny groupname marketing** command to prevent any user from the marketing group from accessing content through the Content Engine.

Use the **access-lists enable** global configuration command to enable the use of the ACL.

You can display the configuration of the ACL by using the **show access-lists 300 EXEC** command, as shown in this example:

```
ContentEngine# show access-lists 300
Access Control List Configuration
-----
Access Control List is enabled
Groupname-based List (300)
1. permit groupname techpubs
2. permit groupname acme1
3. permit groupname engineering
4. permit groupname sales
5. permit groupname marketing
6. deny groupname any
```

To display statistical information for the access control list, use the **show statistics access-lists 300** command, as shown in this example:

```
ContentEngine# show statistics access-lists 300
Access Control Lists Statistics
-----
Groupname and username-based List (300)
Number of requests:      1
Number of deny responses: 0
Number of permit responses: 1
```

To reset the statistical information for the access control list, use the **clear statistics access-lists 300** command.

```
ContentEngine# clear statistics access-lists 300
```

```
ContentEngine(config)# access-lists 300 permit groupname acme1 position 2
```

Modifying an Access Control List

To modify an ACL, follow these steps:

-
- Step 1** From the Content Distribution Manager GUI, choose **Devices > Devices**.
 - Step 2** Click the **Edit** icon next to the Content Engine for which you want to modify the group authorization.
 - Step 3** In the Contents pane, choose **General Settings > Authentication > Access List > Configure Access Control List**. The Access List Settings for Content Engine window appears listing all configured settings.
 - Step 4** Click the **Edit Access List Setting** icon next to the ACL that you want to change. The Modifying Access List window appears.
 - Step 5** Change any of the configurable parameters that you want to modify.
 - Step 6** To save the new ACL setting, click **Submit**.
-

Changing the Currently Applied Settings

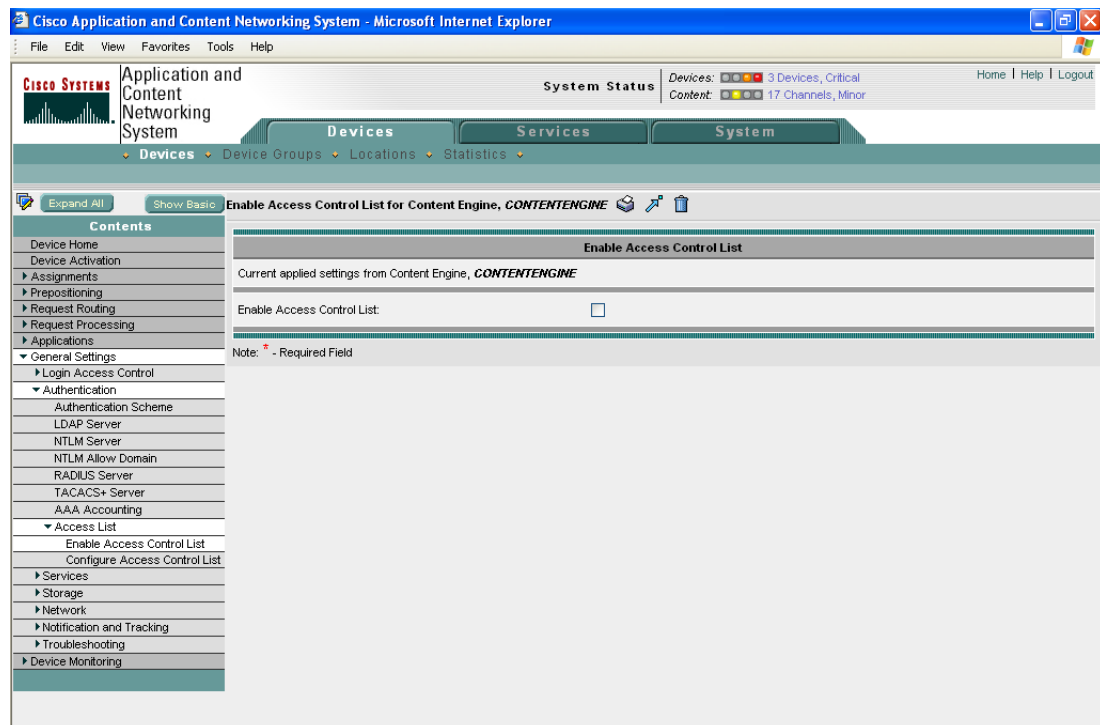
Access list settings can be applied from the Content Engine or from a device group. The source of the currently applied settings is shown in the Access List Settings window (**Devices > General Settings > Authentication > Access List > Configure Access Control List**) for any chosen Content Engine. You can change the source of the currently applied settings from the Content Engine to a device group, provided that the following conditions are met:

- You have configured a device group.
- The Content Engine is assigned to the device group.
- The access list is configured in the device group.

To change the current applied settings, follow these steps:

-
- Step 1** From the Content Distribution Manager GUI, choose **Devices > Devices**.
- Step 2** Click the **Edit** icon next to the Content Engine for which you want to enable the ACL.
- Step 3** In the Contents pane, choose **General Settings > Authentication > Access List > Enable Access Control List**. The Enable Access Control List for Content Engine window appears. (See [Figure 18-1](#).)

Figure 18-1 Enable Access Control List for Content Engine Window



- Step 4** From the drop-down list in the taskbar, chose a device group. (In the example in [Figure 18-1](#), the device group *dgl* has been chosen.)
- Step 5** To save the changes, click **Submit**.
-

Repositioning Settings in the Access Control List

To reposition the settings in the ACL, follow these steps:

-
- Step 1** From the Content Distribution Manager GUI, choose **Devices > Devices**.
 - Step 2** Click the **Edit** icon next to the Content Engine for which you want to reposition the ACL settings.
 - Step 3** In the Contents pane, choose **General Settings > Authentication > Access List > Configure Access Control List**. The Access List Settings for Content Engine window appears listing all configured settings.
 - Step 4** To move a setting up or down in the list order, click the **Up** or **Down** arrow in the Move column. The setting shifts one position up or down. The list is saved in the new order.
-

Viewing Access Control List Settings

To view the ACL settings, follow these steps:

-
- Step 1** From the Content Distribution Manager GUI, choose **Devices > Devices**.
 - Step 2** Click the **Edit** icon next to the Content Engine for which you want to reposition the ACL settings.
 - Step 3** In the Contents pane, choose **General Settings > Authentication > Access List > Configure Access Control List**. The Access List Settings for Content Engine window appears listing all configured settings.

Columns display the position, action, and group name of each setting configured in the ACL.
