Manage User Access and Permissions

September 2014

- About User Accounts, Role Assignment, and Access, page 3-1
- About User Role Privileges, page 3-3
- Procedures, page 3-4

About User Accounts, Role Assignment, and Access

Cisco Show and Share user accounts are not created within Cisco Show and Share. Instead, they are created in (or imported to) Cisco Digital Media Manager. By default, those accounts are given the visitor role when the user logs in to Cisco Show and Share until you assign them a role with additional privileges.

However, you cannot assign different Cisco Show and Share roles to user accounts from within Cisco Digital Media Manager. To assign elevated privileges, you must use the Cisco Show and Share administration pages.

Table 3-1 describes the Cisco DMS roles in assigning user access to Cisco Show and Share.

<table>
<thead>
<tr>
<th>Use</th>
<th>When You Must</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Cisco Digital Media Manager  | Choose a framework to provide user directory services and authentication for all Cisco DMS products. | We support three such frameworks and you must choose one\(^1\).  
  - Import and synchronize query-filtered user account records from a Microsoft Active Directory (LDAP) server. Later, when anyone tries to log in to Cisco Show and Share, Active Directory checks that the username exists and authenticates that the password is valid.  
  - Use native features of DMS-Admin to create and edit user account records manually. Later, when anyone tries to log in to Cisco Show and Share, DMS-Admin checks that the username exists and authenticates that the password is valid.  
  - Integrate with your SAML v. 2.0 compatible federation IDP server (SSO server). |
| Create user groups.          |                                                    | —                                                                  |
| Assign users to user groups. |                                                    | —                                                                  |
### About User Accounts, Role Assignment, and Access

1. See the “Assign or Remove User Roles” section on page 3-4.
2. See the “Search for Users by Their Role Assignments” section on page 3-6.
3. When you turn On the approvals workflow, each author is forbidden to publish his or her own files. Instead, the author must submit all drafts to a designated “author approver,” who then decides whether to publish what the author submitted.
4. Users cannot see or use any features that you disable sitewide and cannot expose disabled features to any other users.
5. When you enable the forced login feature it is active only on the Show and Share portal—not the embedded player, mobile devices, or APIs. See the “Disable Access by Anonymous Visitors” section on page 7-8 for more information.

---

#### Table 3-1  Tasks Related to User Access (continued)

<table>
<thead>
<tr>
<th>Use</th>
<th>When You Must</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Show and Share</td>
<td>Assign roles to users.</td>
<td>See the “Assign or Remove User Roles” section on page 3-4.</td>
</tr>
<tr>
<td></td>
<td>Search for users who match a particular role.</td>
<td>See the “Search for Users by Their Role Assignments” section on page 3-6.</td>
</tr>
<tr>
<td></td>
<td>Turn an approvals workflow On or Off for publishing.</td>
<td>When you turn On the approvals workflow, each author is forbidden to publish his or her own files. Instead, the author must submit all drafts to a designated “author approver,” who then decides whether to publish what the author submitted.</td>
</tr>
<tr>
<td></td>
<td>Assign approvers to authors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Choose sitewide which features authors may turn on for their own videos.</td>
<td>Users cannot see or use any features that you disable sitewide and cannot expose disabled features to any other users.</td>
</tr>
<tr>
<td></td>
<td>Disable access by anonymous visitors.</td>
<td>When you enable the forced login feature it is active only on the Show and Share portal—not the embedded player, mobile devices, or APIs. See the “Disable Access by Anonymous Visitors” section on page 7-8 for more information.</td>
</tr>
</tbody>
</table>
About User Role Privileges

There are six Cisco Show and Share user roles that you can assign explicitly, while two additional user roles are implicit. Each role assignment supposes that its members share a set of rights and responsibilities in common. However, you can assign multiple roles to any given user.

Table 3-2 describes the effect that each role imposes on its constituent users.

**Key**
- Green tint—Yes.
- Red tint—No.
- Yellow tint—Limited or conditional.

**Table 3-2 User Roles**

<table>
<thead>
<tr>
<th>Roles</th>
<th>Levels of Access</th>
<th>Administration Roles</th>
<th>Media Roles</th>
<th>Implicit Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Basic Navigation</td>
<td>Categories</td>
<td>Playback</td>
<td>Content Creation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use</td>
<td>Drafts</td>
<td>Published</td>
</tr>
<tr>
<td>Administrator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visitor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. You cannot assign these roles. The superuser role is a default administrator role that you configure when you first set up Cisco Show and Share. The visitor role is the default role assigned to users who are not logged in.
Procedures

- Prerequisites, page 3-4
- Assign or Remove User Roles, page 3-4
- Search for Users by Their Role Assignments, page 3-6

Prerequisites

- Create or import user accounts in Cisco Digital Media Manager.
- Log in to Cisco Show and Share with administrative privileges.

Assign or Remove User Roles

You can assign one or more roles to Cisco Show and Share users. If you do not assign a specific role to a user, the user is given the visitor role by default.

You can assign roles individually or you can select multiple users to assign the same set of roles to.

Procedure

Step 1  Access the user role management screen:

a. Choose Administration from the global navigation.

b. Choose Manage > User Roles.
   The Show and Share User Roles table appears.
Step 2  Select one or more users:
   a. To navigate the table:
      – Browse—Use the pagination controls at the bottom of the table to browse through the list.
      – Sort—Click on the User Name, User ID, or User E-mail column heading to sort the table by that column. Clicking on the column again reverses the search.
      – Search—Use the search field to match a partial name, ID, or e-mail address. Do not use phrases with spaces.
      – Filter—Filter the table by role, group, or both.
   b. If using the search or filters, click Go to apply your filter or search. You can combine filtering and searching. To clear the filter or the search, clear the search field and filter lists and click Go again.
   c. For each user you want to select, check the check box to the left of the user name. You can select multiple users and assign them the same set of roles as a batch.

Step 3  Assign or remove roles:
   a. Click Edit User Role.

   The Edit User Roles dialog appears.
b. To review the users you have selected, click **See selected users**.
A dialog box appears, listing all of the users you have selected. You can remove selected users by clicking the X to the right of their name. Click **Done** to close the dialog box.

c. Check the check box next to the roles that you want to assign or remove from the user(s). You can assign or remove more than one role.

d. Choose **Add selected roles** to add the roles to the users. Choose **Remove selected roles** to remove the roles.

**Step 4** Click **Save** to save your changes.

---

**Search for Users by Their Role Assignments**

You can quickly identify all users who share a user role in common.

**Procedure**

**Step 1** Choose **Administration** from the global navigation.
**Step 2** Choose **Manage > User Roles**.
**Step 3** Choose an option from the Filter By list. You can filter the list by user role, by group, or by both.
**Step 4** *(Optional)* Enter all or part of a username in the Find a User field.
**Step 5** Click **Go**.

---