



CHAPTER 2

Managing Roles and Local Users

VFrame gives you the ability to define limited roles for users. This ability lets you control what users can see and configure in the product, for example, storage experts will not be distracted by server-specific features.

These topics explain how to create roles for users, and local user accounts, for use with the product:

- [Understanding Roles and Local Users, page 2-1](#)
- [Managing Roles, page 2-7](#)
- [Managing Users, page 2-9](#)
- [Troubleshooting Roles and Users, page 2-11](#)
- [Role and User Reference, page 2-12](#)

Understanding Roles and Local Users

Every person who will use VFrame requires a user account. If you are using VFrame to authenticate user logins (instead of an ACS server), you must define these accounts locally on the VFrame server. You can assign to each user a role that restricts access to only specific parts of the product. You can assign roles to both local users and ACS users.

These sections describe roles, and local users, in more detail. For information about setting up ACS authentication for a virtual context, see [Using an Access Control Server with Virtual Contexts, page 10-3](#).

- [Roles Overview, page 2-2](#)
- [Users Overview, page 2-3](#)
- [Understanding Role Permissions, page 2-3](#)

Roles Overview

A role is a named set of permissions. These permissions are described in [Understanding Role Permissions, page 2-3](#). For example, you could create a role that allows only configuring and monitoring servers, and another role that allows only configuring and monitoring storage devices. The roles you create depend solely on the needs of your organization and on how specifically you want to delimit what each user is allowed to do within the system. VFrame comes with several predefined roles you can use.

Each user account can be assigned a role. If the user has accounts for more than one virtual context, you can assign a different role for each context. For example, a user might have accounts for both the Admin context and a specific virtual context and have only limited privileges in the Admin context but full privileges in the virtual context.

You have a choice when creating roles: create a set of system-wide roles in the Admin context and share them with all virtual contexts, or create roles in each context. You can do both: create some common roles in the Admin context, and allow virtual context users to create additional roles for user types unique to their organization.

In either case, creating roles is optional. If you choose, you can give every user full privileges to their virtual context.

Users Overview

A local user account defines a username and password and can be associated with a role that defines the permissions the user has to the VFrame system. The account is also associated to a virtual context.

When you use the Users tab to create users (by selecting **Access Control > Users**), you are creating a user account only for use in the context to which you are logged in. For example, if you are logged into the Admin context, you are creating a user account that can log in only to the Admin context.

When you are logged into the Admin context, you have the additional ability to create users for specific virtual contexts. You do this when you are creating or managing the virtual context from the Virtual Contexts tab (by selecting **Access Control > Virtual Contexts**). The method for creating the user account, and the account attributes, are the same as when you are using the Users tab, but the user you create is only for that virtual context. However, if you are using an ACS server to manage authentication for the context, you need to configure user accounts in the ACS server, as described in [Using an Access Control Server with Virtual Contexts, page 10-3](#).

When you send the account names to your users, you also need to send them their passwords and the names of the virtual contexts for which their user accounts are defined. All three pieces of information are needed to successfully log into the system. All of these items are case-sensitive, so make sure that you provide the exact values.

Understanding Role Permissions

When you create a role, you assign the role permissions or authorities to perform certain tasks in the product. You can assign to a role any combination of these permissions based on the requirements of your organization. Before creating roles, determine what types of distinction you need between your users.

For the most part, tasks relate to specific tabs or windows in the interface. However, they can also relate to different actions within a window or tab, so that different users might see different things on the same tab based on their permissions. This level of permissions gives you more detailed control over user rights.

When you define a role, the tasks you can select depend on whether the role is for the Admin context or for a virtual context. For example, many tasks cannot be performed in a virtual context. The following list of permissions covers all tasks. You can select a top-level permission folder to select all of the permissions within the folder.

- Access Control
 - Roles—Create and manage roles (select **Access Control > Roles**).
 - Users—Create and manage users and assign them roles (select **Access Control > Users**).
 - Virtual Contexts—Create and manage virtual contexts, including the roles, users, and authentication schemes used in them (select **Access Control > Virtual Contexts**).
- Design
 - Global Libraries—Permissions related to using the global variables library (select **Design > Global Library**).
 - LOM Managers—Create or use lights-out management templates on the LOM Managers tab (select **Design > LOM Managers**).
 - Service Networks—Create or use service network designs (select **Design > Service Networks**).
 - Storage Managers—Create or use storage manager templates on the Storage Managers tab (select **Design > Storage Managers**).
 - Templates—Create or use templates for service networks (select **Design > Templates**).
- Device Credentials—Permissions relating to the definition of the credentials (user names, passwords, SNMP community strings, and so forth) required to log into devices (select **Tools > Device Credentials**).
 - Network—Define and manage the credentials needed to discover network devices such as switches and their modules.
 - Network Services—Define and manage the credentials for the modules included in Catalyst switches, such as the Firewall Services Module (FWSM).

- Server—Define and manage the credentials needed to discover servers.
 - Storage—Define and manage the credentials needed to discover storage devices such as logical units (LUNs) and network attached storage (NAS) filers.
- Discovery—Permissions related to discovering devices in the network and adding them to the Resources tab (select **Tools > Discovery**).
 - Network—Create and run discovery jobs for network devices.
 - Server—Create and run discovery jobs for servers and LOM managers.
 - Storage—Create and run discovery jobs for storage devices (NAS filers and SAN fabric devices) and storage managers.
- Reports
 - Logged-In Users—View a list of currently logged in users (select **Reports > Logged-In Users**).
 - Logical Server Trend—Generate and view logical server trend reports (select **Reports > Logical Server Trend**).
 - Resource Utilization—Generate and view resource usage reports (select **Reports > Resource Utilization**).
 - Service Network Availability—Generate and view service network availability reports (select **Reports > Service Network Availability**).
 - User Audit—Generate and view the audit log (select **Reports > User Audit**).
- Resource Health Monitoring—Permissions relating to configuring notification settings and other settings for physical device faults (**Tools > Resource Health Monitoring**).
 - Network—Configure physical fault settings for network devices.
 - Network Services—Configure physical fault settings for network service modules.
 - Server—Configure physical fault settings for servers.
 - Storage—Configure physical fault settings for storage devices.

- Service Network Operations—Perform various actions while operating a service network (select **Operations > Operations**). The permissions in this category relate to commands performed from the Operations tab.
 - Create/Image/Delete Servers—The ability to add servers to a server group in a service network, delete them, or add the golden image to them.
 - Deploy/Verify Network—The ability to deploy, undeploy, and verify the service network, clear configuration and verification errors, put elements into the maintenance state, and release resources.
 - Server LUN Path Selection—The ability to define the LUN path for the service network, if using SAN-based storage.
 - Policy—The ability to configure the policies for a service network.
 - Start/Stop/Maintain Servers—The ability to start or stop servers or to put them into maintenance.
- System—Permissions relating to configuring system settings (select **File > System Settings**).
 - Device Manager Configuration—Configure device managers.
 - SMTP—Configure e-mail settings.
 - Syslog—Configure system log setting.
 - System Preferences—Configure the system preferences.
 - VFrame Routing Table—Configure static routes in the routing table.
- Tools
 - Device Manager Launch—The ability to open a connection to a device from within VFrame, for example, an SSH command-line session with a switch.
 - Pools—Create and manage resource pools (select **Tools > Pools**).
 - Server Images—Create and manage golden images for application servers (select **Tools > Server Images**).

- View
 - Alarms—View and manage fault alarms (select **View > Alarms**).
 - Jobs—View jobs in the consolidated jobs viewer on the Jobs tab (select **View > Jobs**).
 - Resources—View and manage physical resources (select **View > Resources**).

Managing Roles

These topics explain how to create and manage roles:

- [Creating or Modifying Roles, page 2-7](#)
- [Deleting Roles, page 2-8](#)

Creating or Modifying Roles

Roles define a set of permissions to use various product features. You assign roles to users when you create user accounts. Although you are not required to create roles, they can help you limit what a user can do and see within the product, helping you implement a workflow and security policy.

This procedure explains how to create or modify a role defined for the virtual context into which you are logged. If you are an administrator using the Admin context and need to create or modify a role defined solely for another virtual context, use the Virtual Contexts tab (select **Access Control > Virtual Contexts**).

Before You Begin

Review the list of permissions you can assign to a role, and determine what types of roles and permission combinations you require for your workflow and security requirements. For information on the various permissions, see [Understanding Role Permissions, page 2-3](#).

Procedure

-
- Step 1** Select **Access Control > Roles** to open the Roles tab (see [Roles Tab, page 2-12](#)).
- Step 2** Do one of the following:
- To create a new role, click **New**, and select the permissions you want assigned to the role. You can also enter a description for the role.

If you are creating a role in the Admin context, you can select **Shared** to make the role appear in all virtual contexts. Shared roles allow you to create roles for all virtual contexts, not just the Admin context.
 - To modify an existing role, select it from the list of roles, and make your changes. Any users that are assigned the role and who are logged in are logged out after you save your changes.
- Step 3** Click **Save** to save your changes.
-

Related Topics

- [Understanding Roles and Local Users, page 2-1](#)
- [Troubleshooting Roles and Users, page 2-11](#)

Deleting Roles

If you are no longer using a role, and do not need it anymore, you can delete it.

This procedure explains how to delete a role defined for the virtual context into which you are logged. If you are an administrator using the Admin context and need to delete a role defined for another virtual context, use the Virtual Contexts tab (select **Access Control > Virtual Contexts**).

Before You Begin

Ensure that the role is not assigned to any user accounts. If you are using an ACS server to control access to the software, the roles are assigned to users in the ACS server. (For more information, see [Using an Access Control Server with Virtual Contexts, page 10-3](#).) If you delete a role that is assigned to a user, the user can log into the system but cannot do anything. If the user is logged in, the user is logged out after you delete the role.

Procedure

-
- Step 1** Select **Access Control > Roles** to open the Roles tab (see [Roles Tab, page 2-12](#)).
- Step 2** Select the role from the list, and click **Delete**.
-

Related Topics

- [Understanding Roles and Local Users, page 2-1](#)
- [Troubleshooting Roles and Users, page 2-11](#)

Managing Users

These topics explain how to create and manage user accounts:

- [Creating and Modifying Users, page 2-9](#)
- [Deleting Users, page 2-11](#)

Creating and Modifying Users

If you are creating users in the Admin context, only those users you define on the Users tab can log in to the Admin context.

If you are logged into a virtual context, and local authentication is used for access control, then only those users defined on the Users tab can log into the system. If you are using an access control server (ACS), you do not have to define users as described in this topic. However, if you want to use local authentication as a fall-back authentication method, you must define each user in the context as well as in your ACS server. Passwords for the account must be the same in the ACS server and in VFrame for local authentication to work as a fall-back method. For more information on setting up ACS control, see these topics:

- [Using an Access Control Server with Virtual Contexts, page 10-3](#)
- [Defining a Context's Authentication Scheme, page 10-6](#)

This procedure explains how to create or modify a user account defined for the virtual context into which you are logged. If you are an administrator using the Admin context and need to create or modify a user account defined for another virtual context, use the Virtual Contexts tab (select **Access Control > Virtual Contexts**).

Before You Begin

If you are assigning a specific role to the user, create the role before creating the user account. However, you can modify the user account later to assign roles. For more information, see [Creating or Modifying Roles, page 2-7](#).

Procedure

- Step 1** Select **Access Control > Users** to open the Users tab (see [Users Tab, page 2-14](#)).
- Step 2** To create a new user:
- Click **New**. You are prompted for the username.
 - Enter the username. The name cannot include spaces and is case-sensitive. Click **OK** to add the user.
 - Enter the password in the **Local Password** and **Confirm Password** fields. The password is case-sensitive. For security, the password is not displayed: you only see asterisks.
 - On the **Roles** tab, select the roles that define the permissions you want the user to have. You can select more than one role, or select **All Tasks** if the user is permitted to do all tasks in the context.
 - If you are logged into a virtual context, you can limit the user to work only with specific service networks. Click the **Service Networks** tab and select the desired networks. These networks must be defined in the context before you can assign them to user accounts.
 - Click **Save** to save your changes.
- Step 3** To change an existing user, select the user in the list of users, make your changes, and click **Save**.
-

Related Topics

- [Understanding Roles and Local Users, page 2-1](#)
- [Troubleshooting Roles and Users, page 2-11](#)

Deleting Users

If you are no longer using a user account and do not need it anymore, you can delete it.

This procedure explains how to delete a user defined for the virtual context into which you are logged. If you are an administrator using the Admin context, and need to delete a user defined for another virtual context, use the Virtual Contexts tab (select **Access Control > Virtual Contexts**).

You cannot delete the Admin context user named **admin**.

Do not delete all users of a context, unless you intend to delete the context.

Procedure

-
- Step 1** Select **Access Control > Users** to open the Users tab (see [Users Tab, page 2-14](#)).
- Step 2** Select the user from the list, and click **Delete**.
-

Related Topics

- [Users Overview, page 2-3](#)

Troubleshooting Roles and Users

Role and user troubleshooting is closely related to the virtual context that the user is using. For more information on troubleshooting user accounts and roles, see [Troubleshooting Virtual Contexts, page 10-12](#).

Role and User Reference

These topics describe the main tabs and dialog boxes you use when managing roles and users:

- [Roles Tab, page 2-12](#)
- [Users Tab, page 2-14](#)

Roles Tab

Use the Roles tab to create authorization roles that you can assign to users to control the tasks they can perform.

When creating roles on this tab, you are only creating roles for the context to which you are logged in. If you are logged into the Admin context, you can also define these roles as shared, so that they are available in other virtual contexts. However, if you are an administrator with the permissions required to define virtual contexts, and you want to create roles just for a specific context, use the Virtual Contexts tab to create the role (select **Access Control > Virtual Contexts**).

How to Get to This Tab

Select **Access Control > Roles** to open the Roles tab.

Related Topics

- [Understanding Roles and Local Users, page 2-1](#)
- [Managing Roles, page 2-7](#)
- [Troubleshooting Roles and Users, page 2-11](#)

Field Reference

Table 2-1 Roles Tab

Element	Description
New button	Click this button to create a new role. You are prompted for a name for the role. You cannot rename the role after you create it.

Table 2-1 Roles Tab (continued)

Element	Description
Save button	Click this button to save your changes.
Delete button	Click this button to delete the selected role. Before deleting a role, ensure that no users are currently assigned the role.
Roles list (left pane)	<p>The roles currently defined for this virtual context.</p> <p>If you are in a context other than the Admin context, some roles might be shared from the Admin context. You cannot modify shared roles if you view them from a virtual context.</p> <p>If you are an administrator using the Admin context, the roles you create here are only for the Admin context unless you create them as shared roles. To create roles for a virtual context that are only for use in that context, use the Virtual Contexts tab (select Access Control > Virtual Contexts).</p>
Role properties (left pane)	<p>The properties of the selected role and the permissions assigned to it. The pane is empty until you select a role. The fields on the pane are:</p> <ul style="list-style-type: none"> • Shared—Whether the role is shared with other contexts. This attribute can be configured only for roles created in the Admin context. If you are logged into a virtual context, this attribute is displayed for roles shared from the Admin context, but you cannot change the setting. <p>If you are creating a role in a virtual context, or if you do not select Shared, the role can be used only within the context in which it is defined.</p> <ul style="list-style-type: none"> • Description—A description of the purpose of the role. • Permissions—The permissions assigned to the role, based on tasks you can perform in the interface. Select the ones desired for the role you are creating. For example, you can create roles specifically for storage administrators, network administrators, security administrators, or other specialized functions. If you select a category, all permissions within the category are selected. For an explanation of these permissions, see Understanding Role Permissions, page 2-3.

Users Tab

Use the Users tab to create and manage local user accounts for the virtual context you are logged into. Local user accounts are required if you are using VFrame to control access to the system. They are always used for the Admin context, but if you are using an ACS server to control access to another virtual context, you need to create and manage users in the ACS server. For more information, see [Using an Access Control Server with Virtual Contexts, page 10-3](#).

If you are an administrator with the permissions required to define virtual contexts, and you want to create users just for a specific context, use the Virtual Contexts tab to create the user (select **Access Control > Virtual Contexts**).

How to Get to This Tab

Select **Access Control > Users** to open the Users tab.

Related Topics

- [Understanding Roles and Local Users, page 2-1](#)
- [Managing Users, page 2-9](#)
- [Troubleshooting Roles and Users, page 2-11](#)

Field Reference

Table 2-2 Users Tab

Element	Description
New button	Click this button to create a new user account. You are prompted for a name for the user. This is the name the user will use to log into the product. The name cannot include spaces, and is case-sensitive. You cannot rename the user account after you create it.
Save button	Click this button to save your changes to the user properties.
Delete button	Click this button to delete the selected user.
Users list (left pane)	The user accounts defined for the virtual context. If you are an administrator using the Admin context, the users you create here are only for the Admin context. To create user accounts for a virtual context, use the Virtual Contexts tab (select Access Control > Virtual Contexts).

Table 2-2 Users Tab (continued)

Element	Description
User properties (right pane)	
The properties for the user account. Individual fields are described below.	
Description	A description of the user account.
Local Password Confirm Password	The user's password entered in each field. Only asterisks (*) display in this field to protect passwords. Asterisks display even if there is no password. This password is for local authentication, that is, where VFrame authenticates logins. It does not define ACS-authenticated passwords if you are using an ACS server.
Roles tab	The roles assigned to the user. Select all roles that apply. Select All Tasks if you want the user to be able to use all product features. The list of roles includes only those roles defined on the Roles tab (select Access Control > Roles), roles that were created in the Admin context and shared with all virtual contexts, or roles created by the administrator specifically for this virtual context on the Virtual Contexts tab.
Service Networks tab (virtual contexts only)	The service networks to which the user is allowed access. The list includes only those networks created within the context into which you are logged. Select All to not apply service network restrictions. If you restrict users to specific service networks, they cannot see any resource pools in the virtual context; they can see only the resources that were actually acquired by the service network.

