



CHAPTER 2

Managing Roles and Users

VFrame Data Center provides you with the ability to define 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.

This chapter explains how to create roles for users, and local user accounts, for use with the product, and includes the following sections:

- [Understanding Roles and Local Users, page 2-1](#)
- [Managing Roles, page 2-5](#)
- [Managing Users, page 2-7](#)
- [Troubleshooting Roles and Users, page 2-9](#)
- [Role and User Reference, page 2-9](#)

Understanding Roles and Local Users

Users who use VFrame require a user account. If you are using VFrame to authenticate user logins instead of an ACS (Access Control 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. For information about setting up ACS authentication for a virtual context, see [Using an Access Control Server with Virtual Contexts, page 10-2](#).

This section describes roles and local users in more detail, and includes the following topics:

- [Roles Overview, page 2-2](#)
- [Users Overview, page 2-2](#)
- [Understanding Role Permissions, page 2-2](#)
- [Understanding Privileges in VirtualCenter, page 2-5](#)

Roles Overview

A role is a named set of permissions. These permissions are described in [Understanding Role Permissions, page 2-2](#). 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 limit what each user is allowed to do within the system.

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.

Creating roles is optional. If you choose, you can give every user full privileges to their virtual context.

In AdminContext there is a user called admin. It is a VFrame Data Center default account. The admin user has access to the whole VFrame Data Center feature set and access to all resources discovered and created. The role assignment for admin cannot be changed and the password for admin can only be changed in the CLI.

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 choosing **Tools > VFrame Administration > User > 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 in to the Admin context, you are creating a user account that can log in only to the Admin context.

When you are logged in to 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 on the Contexts tab by choosing **Tools > VFrame Administration > User > 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 to manage authentication for the context, you need to configure user accounts on the ACS, as described in [Using an Access Control Server with Virtual Contexts, page 10-2](#).

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 in to 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 any combination of these permissions based on the requirements of your organization. Before creating roles, determine what types of distinction you need to make 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 choose 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 choose a top-level permission folder to select all of the permissions within the folder.

Role Permissions

VFrame Data Center uses the following role permissions:

- Access Control—Permissions relating to roles, users and virtual contexts.
 - Roles—To create and manage roles, choose **Tools > VFrame Administration > User > Roles**.
 - Users—To create and manage users and assign them roles, choose **Tools > VFrame Administration > User > Users**.
 - Virtual Contexts—To create and manage virtual contexts, including the roles, users, and authentication schemes used in them, choose **Tools > VFrame Administration > User > Contexts**.
- Design—Permissions relating to template and network design.
 - Global Libraries—To use the global library, choose **View > Templates**, double-click a template, then choose **Properties > Macros & Variables > Global Libraries**.
 - LOM Managers—To create or use lights-out management templates on the LOM Managers tab, choose **Tools > LOM Managers**.
 - Service Networks—To create or use service network designs, choose **View > Service Networks**.
 - Storage Managers—To create or use storage manager templates on the Storage Managers tab, choose **Tools > Storage Managers**.
 - Templates—To create or use templates for service networks, choose **View > Templates**.
- Device Credentials—Permissions relating to the definition of the credentials required to log in to devices. To create credentials, choose **Tools > VFrame Administration > Network > 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.
 - Virtual Machine Managers—Define and manage the credentials needed to discover virtual machine managers.
- Discovery—Permissions related to discovering devices in the network and adding them to the Resources tab. To discover devices, choose **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 NAS filers, SAN fabrics, and storage managers.
 - Virtual Machine Manager—Create and run discovery jobs for virtual machine managers.
- Reports—Permissions relating to using reports.

- Logged-In Users—View a list of currently logged-in users. To view logged-in users, choose **Tools > VFrame Administration > User > Logged-In Users**.
- Logical Server Trend—Generate and view logical server trend reports. To view logical server trends, choose **Reports > Logical Server Report**.
- Resource Utilization—Generate and view resource usage reports. To view resource usage, choose **Reports > Resource Utilization**.
- Service Network Availability—Generate and view service network availability reports. To view available networks, choose **Reports > Service Network Availability**.
- User Audit—Generate and view the audit log. To view audit logs, choose **Tools > VFrame Administration > User > Audit**.
- Resource Health Monitoring—Permissions relating to configuring notification settings and other settings for physical device faults. To configure notification settings, choose **Tools > VFrame Administration > Network > 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.
 - Virtual Machine Managers—Configure physical fault settings for virtual machine managers.
- Service Network Operations—Permission relating to performing various actions while operating a service network. To perform commands, choose **View > Operations**.
 - Create/Image/Delete Servers—The ability to add servers to a server group in a service network, delete them, or add the server image to them.
 - Deploy/Verify Network—The ability to deploy, undeploy, and verify the service network, clear configuration and verification errors, put elements in to the maintenance state, and release resources.
 - Server LUN and 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 in to maintenance.
- System—Permissions relating to configuring system settings.
 - Device Manager Configuration—Configure device managers. To add device managers, choose **Tools > VFrame Administration > General > Device Managers**.

**Note**

When you add a device manager, you can right-click a device in the resources selector on the Resources tab and then choose **Device Manager**. For more information see [Chapter 7, “Managing Devices.”](#)

- SMTP—Configure e-mail settings. To configure e-mail settings, choose **Tools > VFrame Administration > General > SMTP**.
- Syslog Notification—Configure system log setting. To configure syslog notification, choose **Tools > VFrame Administration > General > Notification**.
- System Preferences—Configure the system preferences. To configure system preferences, choose **Tools > VFrame Administration > General > General**.

- VFrame Routing Table—Configure static routes in the routing table. To configure static routes, choose **Tools > VFrame Administration > Network > Routing**.
- Tools—Permissions relating to manage devices, pools and golden images.
 - 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. To manage devices, choose **General > Device Managers**.
 - Pools—Create and manage resource pools. To create and manage pools, choose **Tools > Resource Pools**.
 - Golden Images—Create and manage golden images for application servers To create and manage golden images, choose **Tools > Golden Images**.
- View—Permissions relating to viewing and managing alarms, jobs and resources.
 - Alarms—View and manage alarms. To view and manage alarms, choose **Tools > Alarms**.
 - Jobs—View jobs. To view jobs, choose **Tools > Job Logs**.
 - Resources—View and manage physical resources. To view and manage physical resources, choose **View > Resources**.

Understanding Privileges in VirtualCenter

VFrame can manage VMware VirtualCenter. To manage VirtualCenter using VFrame you have to enable the following privileges in VirtualCenter:

- Global
 - Manage Custom Attributes
 - Set Custom Attributes
 - Licenses
- Host—Inventory
 - Add Standalone Host
 - Add Host to Cluster
 - Remove Host
- Host—Configuration
 - Connection
 - Storage Partition Configuration
 - Network Configuration
- Host—Local Operations
 - Add Host to VirtualCenter

Managing Roles

This section describes roles in VFrame Data Center, and includes the following topics:

- [Creating or Modifying Roles, page 2-6](#)
- [Deleting Roles, page 2-6](#)

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 Contexts tab by choosing **Tools > VFrame Administration > User > 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 2-2](#).

Procedure

-
- Step 1** Choose **Tools > VFrame Administration > User > Roles** to open the Roles tab (see [Roles Tab, page 2-9](#)).
- Step 2** Do one of the following:
- To create a new role, click **New**, and check 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 check the **Shared** check box 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, click it 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 **Apply**.
- Step 4** Click **OK**.
-

Related Topics

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

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 Contexts tab by choosing **Tools > VFrame Administration > User > Contexts**.

Before You Begin

Ensure that the role is not assigned to any user accounts. If you are using an ACS to control access to the software, the roles are assigned to users on the ACS. For more information, see [Using an Access Control Server with Virtual Contexts, page 10-2](#). If you delete a role that is assigned to a user, the user can log in to 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** Choose **Tools > VFrame Administration > User > Roles** to open the Roles tab (see [Roles Tab, page 2-9](#)).
- Step 2** Click the role in the **Roles** selector.
- Step 3** Click **Delete**.
-

Related Topics

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

Managing Users

The following topics explain how to create and manage user accounts:

- [Creating and Modifying Users, page 2-7](#)
- [Deleting Users, page 2-8](#)

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 in to a virtual context, and local authentication is used for access control, then only those users defined on the Users tab can log in to the system. If you are using an ACS, you do not have to define users as described in this section. 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 on your ACS. Passwords for the account must be the same on the ACS and in VFrame for local authentication to work as a fall-back method. For more information on setting up an ACS, see the following topics:

- [Using an Access Control Server with Virtual Contexts, page 10-2](#)
- [Defining a Context Authentication Scheme, page 10-4](#)

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 Contexts tab by choosing **Tools > VFrame Administration > User > 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 2-6](#).

Procedure

-
- Step 1** Choose **Tools > VFrame Administration > User > Users** to open the Users tab (see [Users Tab, page 2-11](#)).
- Step 2** To create a new user:
- a. Click **New**.
 - b. Enter the user name. The name cannot include spaces and is case-sensitive.
 - c. Click **OK** to add the user.
 - d. Enter the password in the **Local Password** and **Confirm Password** fields. The password is case-sensitive.
 - e. On the **Roles** tab, check all the roles check boxes that define the permissions you want the user to have. You can check multiple check boxes, or check the **All Tasks** check box if the user is permitted to do all tasks in the context.
 - f. Click the **Service Networks** tab and click the appropriate service networks. These networks must be defined in the context before you can assign them to user accounts.
 - g. Click **Apply**.
 - h. Click **OK**.
- Step 3** To change an existing user:
- a. Click the user in the Users selector and make your changes.
 - b. Click **Apply**.
 - c. Click **OK**.
-

Related Topics

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

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 Contexts tab by choosing **Tools > VFrame Administration > User > 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** Choose **Tools > VFrame Administration > User > Users** to open the Users tab (see [Users Tab](#), page 2-11).
- Step 2** Click the role in the Users selector.
- Step 3** Click **Delete**.
-

Related Topics

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

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 10-9.

Role and User Reference

This section describes the tabs you use when managing roles and users, and includes the following topics:

- [Roles Tab](#), page 2-9
- [Users Tab](#), page 2-11

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 in to 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 Contexts tab to create the role by choosing **Tools > VFrame Administration > User > Contexts**.

How to Get to This Tab

Choose **Tools > VFrame Administration > User > Users** to open the Roles tab.

Related Topics

- [Understanding Roles and Local Users](#), page 2-1
- [Managing Roles](#), page 2-5
- [Troubleshooting Roles and Users](#), page 2-9

Field Reference

Table 2-1 Roles Tab

Element	Description
New button	<p>Click this button to create a role. When you click this button, the Input dialog box appears:</p> <ul style="list-style-type: none"> • Role Name—Enter a role name. The maximum number of characters is 64.
Delete button	Click this button to delete the selected role.
Roles selector	<p>This selector lists the roles directories:</p> <ul style="list-style-type: none"> • All Admin • Network Admin • Resource Allocator • Server Admin • Service Network Designer • Service Network Operator • Storage Admin • Template Designer <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 Contexts tab by choosing Tools > VFrame Administration > User > Contexts.</p>

Table 2-1 Roles Tab (continued)

Element	Description
Right pane	<p>Use this pane to choose roles:</p> <ul style="list-style-type: none"> • Shared—Check the Shared check box to share the roles with other contexts. This attribute can be configured only for roles created in the Admin context. If you are logged in to 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 check the Shared check box, the role can be used only within the context in which it is defined.</p> <ul style="list-style-type: none"> • Description—Enter a description of the role. • Permissions—Lists the permissions assigned to the role, based on tasks you will perform: <ul style="list-style-type: none"> – Access Control – Design – Device Credentials – Discovery – Reports – Resource Health Monitoring – Service Network Operations – System Settings – Tools – View <p>Choose the ones appropriate 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 choose a category, all permissions within the category are selected. For an explanation of these permissions, see Understanding Role Permissions, page 2-2.</p>

Users Tab

Use the Users tab to create and manage local user accounts for the context you are logged in to. 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 to control access to another virtual context, you need to create and manage users on the ACS. For more information, see [Using an Access Control Server with Virtual Contexts, page 10-2](#).

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 Contexts tab to create the user by choosing **Tools > VFrame Administration > User > Contexts**.

How to Get to This Tab

Choose **Tools > VFrame Administration > User > Users** to open the Users tab.

Related Topics

- [Understanding Roles and Local Users, page 2-1](#)
- [Managing Users, page 2-7](#)
- [Troubleshooting Roles and Users, page 2-9](#)

Field Reference**Table 2-2 Users Tab**

Element	Description
New button	Click this button to create a user. When you click this button, the Input dialog box appears: <ul style="list-style-type: none"> • User Name—Enter a user name. The maximum number of characters is 64.
Delete button	Click this button to delete the selected user.
Users selector	This selector lists the users. 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 Contexts tab by choosing Tools > VFrame Administration > User > Contexts .
Local Password field	Enter a password.
Confirm Password field	Reenter the password.
Description field	Enter a description of the user account.
Roles tab	The roles assigned to the user. Choose all roles that apply. Choose 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, 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 that the user is allowed access. The list includes only those networks created within the context into which you are logged. Choose All to not apply service network restrictions.