



CHAPTER 10

Managing Virtual Contexts

Virtual contexts enable you to create different management zones for users of the same VFrame system. For example, you could create a virtual context for the Finance department and another one for the Database Management department.

You are not required to create virtual contexts. Use them only if they make sense for your organization.

This chapter describes virtual contexts in further detail, and includes the following sections:

- [Understanding Virtual Contexts, page 10-1](#)
- [Working with Virtual Contexts, page 10-3](#)
- [Troubleshooting Virtual Contexts, page 10-9](#)
- [Virtual Contexts Reference, page 10-10](#)

Understanding Virtual Contexts

Virtual contexts enable you to partition a single VFrame system to create more limited administrative domains. This section describes contexts in more detail, and includes the following topics:

- [Virtual Context Overview, page 10-1](#)
- [Using an Access Control Server with Virtual Contexts, page 10-2](#)

Virtual Context Overview

A virtual context is a logically separate image of the VFrame system. If you create virtual contexts, users logged in to a virtual context can design and operate service networks without seeing any of the other functions of the product. A virtual context has its own resources, service networks, and user and role definitions that cannot be seen by users of any other context except the Admin context. Thus, virtual contexts enable you to create separate systems for different groups in your organization without requiring you to purchase separate physical equipment for each. The single VFrame system appears to each group as its own system.

By creating virtual contexts, you can limit the resources each group sees so that they do not have to search through the resources of their groups to find what they need to configure and manage. Limiting resource visibility also helps prevent accidents, such as one group changing the system configuration of another group by mistake.

All virtual contexts are created and managed in the Admin context. Administrators responsible for a specific virtual context cannot themselves create virtual contexts within that context. Thus, if you are responsible for creating virtual contexts, you should first understand how each group needs to have its resources and scope of control divided. For example, your Finance organization might require more than one context if it is necessary to maintain separation among various financial groups.

When creating a virtual context, you assign resource pools to the context. You should create pools so that only those resources allowed to the group are pooled, and assign only these pools to the context. You might also have some general-use pools that you can share among all (or a subset of) contexts. The pools you assign appear in the context (unless they are default pools), and their contents also appear in the context default pools.

The Admin context is a super user context. When logged in to the Admin context, you can see the objects available in and assigned to each virtual context defined in the system, as well as perform system-wide tasks unavailable in individual virtual contexts (such as resource discovery and management).

Users logged in to a virtual context are automatically logged out when one of the following happens:

- The user account is deleted.
- The role permissions are changed.
- The role permission is modified.
- The resource pool assignment is changed.

In all the preceding cases, you will see a pop up stating the reason why they were logged out. Once that pop up is acknowledged, you will see another pop up stating that the session is invalid. Once that pop up is acknowledged, you will have to log back in for the changes to take affect.

Using an Access Control Server with Virtual Contexts

You can control user access to a virtual context by using your access control server, such as a Cisco Access Control Server (ACS). When using an access control server, you create and manage users in the ACS instead of in VFrame. However, you can use VFrame local user authentication as a backup authentication scheme, so that if your ACS cannot respond (due to network or server problems), users can still log in to the virtual context.

If you want to use an ACS to control virtual context access, you must configure your ACS appropriately. This procedure describes the general steps for setting up a Cisco ACS as a RADIUS server for use with VFrame. For specific information about using Cisco Secure ACS, see that product online help.

Before You Begin

You cannot use the same ACS for more than one virtual context. Ensure that you configure users for only a single context in any one ACS.

Procedure

-
- Step 1** In Cisco Secure ACS, define the VFrame server as a AAA client in the Network Configuration section.
- For AAA Client IP Address, enter the IP address of the VFrame server. Typically, this should be the VFrame server management IP address, but it can be the IP address of any of the VFrame server interfaces whose traffic can be routed between the ACS and VFrame servers.
 - For Key, enter a valid key. When you configure the virtual context to use this RADIUS server, you will need to enter this same key in VFrame.

- For Authenticate Using, click **RADIUS (Cisco IOS/PIX)**. You must use this scheme because it includes an attribute value used by VFrame.
- Step 2** In Cisco Secure ACS, configure users in the **User Setup** area. For each user:
- Define the user account name and password.
 - Optionally, define the VFrame role you want to assign to the user in the Cisco IOS/PIX RADIUS Attributes area as a cisco-av-pair parameter. If you do not assign a role, the user can perform all tasks. The entry has this syntax:
vframe:roles=role-name-list
where *role-name-list* is a space-delimited list of the names of roles defined for the virtual context in VFrame. These roles must exist when the user tries to log in to the product. For example, to assign the role Designer, enter:
vframe:roles=Designer
To assign the user two roles, Designer and Operator, enter:
vframe:roles=Designer Operator
- Step 3** In VFrame, log in to the Admin context and configure the virtual context to use the ACS, as described in [Defining a Context Authentication Scheme, page 10-4](#).
-

Working with Virtual Contexts

This section describes how to create and manage virtual contexts from the Admin context, and includes the following topics:

- [Creating or Modifying Virtual Contexts, page 10-3](#)
- [Deleting Virtual Contexts, page 10-8](#)

Creating or Modifying Virtual Contexts

This section describes the overall process for creating or modifying a virtual context. For information about what a context is, see [Virtual Context Overview, page 10-1](#).

Before You Begin

Create the resource pools you will assign to the context, and gather the information required to create the authentication scheme and the user accounts and roles for the context.

Procedure

- Step 1** Choose **Tools > VFrame Administration > User > Contexts** to open the Contexts tab.
- Step 2** Do one of the following:
- To create a new context, click **New**. When prompted, enter the name of the context and click **OK**. You use this context name when logging in to the context.
 - To modify an existing context, click the context in the Virtual Contexts selector. The properties appear in the right pane.

- Step 3** Modify the properties of the context. To create a usable context, you must assign some resource pools to the context, including an IP Address Range pool, and create at least one user account. It can also be helpful to enter a description of the context to help you remember its purpose.

This section describes how to configure context settings, and includes the following topics:

- [Defining a Context Authentication Scheme, page 10-4](#)
- [Managing Roles in a Context, page 10-5](#)
- [Managing Users of a Context, page 10-6](#)
- [Managing Resources Assigned to a Context, page 10-7](#)

- Step 4** When you are finished making changes, click **Save** to save them.
-

Related Topics

- [Understanding Virtual Contexts, page 10-1](#)
- [Troubleshooting Virtual Contexts, page 10-9](#)

Defining a Context Authentication Scheme

A context authentication scheme determines how user access to the context is controlled. Each user who logs in to the context must be defined in VFrame Data Center as a user of the context irrespective of whether local or remote authentication is used. When authentication is done against the remote server and the roles are received from the remote server, the user still needs to be defined in the VFrame context. You can use the following schemes:

- **Local**—User logins are controlled by the VFrame server. User passwords and roles are defined locally and are stored in the database.
- **LDAP**—User logins are controlled by your LDAP server. Each user who log in must be defined in the LDAP server. A user is defined locally, but authentication and authorization is done based on values configured on the LDAP server.
- **RADIUS**—User logins are controlled by your RADIUS server, such as Cisco Secure ACS. Each user who logs in must be defined in the RADIUS server, as described in [Using an Access Control Server with Virtual Contexts, page 10-2](#). The user is defined locally, but authentication and authorization is done based on the values configured on the RADIUS server.

Before You Begin

If you want to use only local authentication, you do not have to configure anything on the Authentication tab. Local authentication is the default authentication method.

If you want to use your LDAP server to authenticate users of the context, configure your LDAP server before you create the context.

If you want to use your RADIUS server to authenticate users of the context, configure your RADIUS server before you create the context.

Procedure

- Step 1** Choose **Tools > VFrame Administration > User > Contexts** to open the Contexts tab (see [Contexts Tab, page 10-10](#)).
- Step 2** Click a context in the Virtual Contexts selector.

The Authentication, Roles, Users and Resources tabs appear in the right pane. The Authentication tab is clicked, and the Authentication Scheme folder is opened to show the authentication type subfolders.

These subfolders are used in order, top to bottom, to authenticate user logins. If an authentication server does not respond to a login request, VFrame asks the next server in the list to authenticate the user. Authentication failures (for example, wrong username or password) end the authentication attempt. When VFrame tries local authentication (represented by the Local folder), the attempt either passes or fails, and no subsequent authentication schemes are tried.

Step 3 Add servers to a sub folder:

- a. Choose the appropriate sub folder.
- b. Click **Add Authentication Server**.

The Input dialog box appears.

- c. Enter an IP address in the Enter Server IP field.

The IP address you entered appears below the folder. The right pane shows the various server settings.

- d. Configure server settings.

The server settings for a RADIUS server are Timeout, Authentication Port and Shared Key. The server settings for an LDAP server are Timeout, Authentication Port, Use Secure Sockets Layer, Logon Information, User Name and Role Definition.

Step 4 Change the order of servers to match your authentication requirements:

- a. Click the server.
- b. Use the up or down arrows to position it as desired. Servers at the top of the list are tried first.

Step 5 Delete a server:

- a. Click the appropriate server.
- b. Click **Delete**.

Step 6 Click **Apply**.

Step 7 Click **OK**.

Related Topics

- [Understanding Virtual Contexts, page 10-1](#)
- [Troubleshooting Virtual Contexts, page 10-9](#)

Managing Roles in a Context

Roles are groups of authorization permissions that you can assign to users. They are optional, and you need to create them only if the users of the context require them. Besides creating roles within the context properties, you can also create roles using the Roles tab and share them, in which case they are available to all contexts. The ones that you create in a specific context are available only to that context.

For more information about roles, see the following topics:

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

Before You Begin

Determine whether the roles you are creating are unique to this context or whether they should be shared by many contexts. If a role should be shared, create it as a shared role on the Roles tab by choosing **Tools > VFrame Administration > User > Contexts**.

This procedure explains how to create roles that are used only within a single context.

If you are using an authentication server to control user logins, you must assign these roles to users in the ACS. For information about configuring user roles in the ACS, see [Using an Access Control Server with Virtual Contexts, page 10-2](#).

Procedure

-
- Step 1** Choose **Tools > VFrame Administration > User > Contexts** to open the Contexts tab (see [Contexts Tab, page 10-10](#)).
- Step 2** Click a context in the Virtual Contexts selector.
- The Authentication, Roles, Users and Resources tabs appear in the right pane. The Authentication tab is selected, and the Authentication Scheme folder is opened to show the authentication type subfolders.
- Step 3** Click the **Roles** tab.
- Step 4** Do any of the following:
- To create a role, click **New**, and check the privileges you want to assign to the role. For information about privileges, see [Understanding Role Permissions, page 2-2](#).
 - To change a role, click it and make your modifications.
 - To delete a role, click it and then click **Delete**. Before deleting a role, ensure that it is not assigned to any users.
- Step 5** Click **Apply**.
- Step 6** Click **OK**.
-

Related Topics

- [Managing Users of a Context, page 10-6](#)

Managing Users of a Context

If you are using local user authentication, only the users you create for the context can log in to it.

For more information about users, see the following topics:

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

Before You Begin

If you are defining these user accounts so that local authentication can be used as a fall-back method (if the ACS cannot reply to login requests), get the list of usernames and passwords from your ACS. The names and passwords must be the same as those defined in the ACS.

Procedure

-
- Step 1** Choose **Tools > VFrame Administration > User > Contexts** to open the Contexts tab (see [Contexts Tab, page 10-10](#)).
- Step 2** Click a context in the Virtual Contexts selector.
- The Authentication, Roles, Users and Resources tabs appear in the right pane. The Authentication tab is selected, and the Authentication Scheme folder is opened to show the authentication type subfolders.
- Step 3** Click the **Users** tab.
- Step 4** To create a new user:
- Click **New**.
 - Enter the username.
The name cannot include spaces and is case-sensitive.
 - Click **OK** to add the user.
 - Enter the password for the user in the Local Password and Confirm Password fields.
The password is case-sensitive. For security, the password is not displayed. You only see asterisks. This password is used for local authentication, not for ACS authentication.
 - On the **Roles** tab, click the roles that define the permissions you want the user to have. You can click more than one role, or click **All Tasks** if the user is permitted to do all tasks in the context.
 - If you want to limit the user to have the ability to work only with specific service networks, click the **Service Networks** tab and click the desired networks. These networks must exist (be defined in the context) before you can assign them to user accounts.
- Step 5** To change an existing user, click the user in the drop-down list and make your changes.
- Step 6** Click **Apply**.
- Step 7** Click **OK**.
-

Related Topics

- [Defining a Context Authentication Scheme, page 10-4](#)
- [Managing Roles in a Context, page 10-5](#)

Managing Resources Assigned to a Context

A virtual context can use only the resources that you assign to it. Thus, if the context needs Firewall Services Modules (FWSM), you must assign it at least one FWSM resource pool. The pools you assign appear in the context (unless they are default pools), and their contents also appear in the context default pools.

You can assign default pools, or you can create pools specifically for the virtual context. To create pools, choose **Tools > Resource Pools**.

Before You Begin

Determine the resource requirements of the service networks that will be defined in the context. Create the resources pools the context requires.

Procedure

-
- Step 1** Choose **Tools > VFrame Administration > User > Contexts** to open the Contexts tab (see [Contexts Tab, page 10-10](#)).
- Step 2** Click a context in the Virtual Contexts selector.
- The Authentication, Roles, Users and Resources tabs appear in the right pane. The Authentication tab is selected, and the Authentication Scheme folder is opened to show the authentication type subfolders.
- Step 3** Click the **Resources** tab.
- Step 4** Do one of the following:
- Check the pools that contain the resources the context is allowed to use.
 - Assign all managed devices by clicking **Select All Default Resource Pools**.
- Step 5** Click **Apply**.
- Step 6** Click **OK**.
-

Related Topics

- [Understanding Virtual Contexts, page 10-1](#)

Deleting Virtual Contexts

If you no longer need a virtual context, you can delete it. When you delete a context, everything defined in the context is also deleted.

Before You Begin

Ensure that you choose the right context before deleting it. After you delete it, you cannot retrieve the context.

You cannot delete a context if it includes a service network, even if that network is not currently running.

Procedure

-
- Step 1** Choose **Tools > VFrame Administration > User > Contexts** to open the Contexts tab (see [Contexts Tab, page 10-10](#)).
- Step 2** Click a context in the Virtual Contexts selector.
- The Authentication, Roles, Users and Resources tabs appear in the right pane. The Authentication tab is selected, and the Authentication Scheme folder is opened to show the authentication type subfolders.
- Step 3** Click the **Users** tab.
- Step 4** On the **Users** tab, click each user and then click **Delete**.
- You cannot delete the context if any user is defined for it.
- Step 5** Click **Delete** at the top of the Contexts tab to delete the context.
- Step 6** Click **Apply**.
- Step 7** Click **OK**.
-

Related Topics

- [Understanding Virtual Contexts, page 10-1](#)

Troubleshooting Virtual Contexts

Assuming that you are managing the virtual contexts, and the user does not have authorization to modify virtual context settings, this section describes some problems you might encounter when working with virtual contexts and their solutions, and includes the following topics:

- **Problem** [User cannot log in to the context.](#)
- **Problem** [User cannot see the required resources.](#)

Problem User cannot log in to the context.

Solution If a user cannot log in to a context, first verify that the user is selecting the correct context name during login. If you are using local authentication (VFrame manages user authentication), ensure that the user name, including correct capitalization, is defined as a user of the context. If you are using ACS for authentication, verify that the user is defined in the ACS and that the ACS is configured correctly (that is, log in to the context using an account you know should work). If none of these are the problem, reset the user password on the Contexts tab.

Problem User cannot see the required resources.

Solution If a user can log in to a context but cannot see the resources that the user is supposed to manage, check the user role. If it does not include the required permissions, assign a more appropriate role to the user. (If you are using ACS authentication, you must do this in the ACS.) If the role is not the problem, check the service network assigned to the user, and change it if it does not reflect the user range of control; you must make a resource scope assignment for the user to see any resource pools. If fixing the scope still does not resolve the problem, check the resource pools assigned to the context: Do they include all the devices the context is expected to use? You might need to add resources to existing pools, create new ones, or perhaps assign some additional existing pools to the context.

Virtual Contexts Reference

Contexts Tab

Use the Contexts tab to create and manage virtual contexts. Virtual contexts are logically separate images of the VFrame system. A virtual context allows you to create a separate system for different groups in your organization without requiring you to purchase separate systems. The single VFrame system appears to each group as its own system.

You are not required to create virtual contexts. Use them only if they make sense for your organization.

How to Get to This Tab

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

Related Topics

- [Understanding Virtual Contexts, page 10-1](#)
- [Creating or Modifying Virtual Contexts, page 10-3](#)
- [Deleting Virtual Contexts, page 10-8](#)
- [Troubleshooting Virtual Contexts, page 10-9](#)

Field Reference

Table 10-1 *Contexts tab*

Element	Description
New button	Click this button to create a new virtual context.
Delete button	Click this button to delete the selected virtual context. Deleting a context deletes everything defined in that context. You cannot delete a context that has a service network, even if it is not in operation. You also must first delete any user defined for the context (click the Users tab for the virtual context to delete users).
Virtual Contexts selector	The list of virtual contexts defined for this system. The list does not include the Admin context, because you cannot modify or delete the Admin context.

Virtual context properties (right pane)

The properties for the selected virtual context. Individual fields are described below.

Description scroll list	A description of the purpose of the virtual context.
-------------------------	--

Table 10-1 Contexts tab (continued)

Element	Description
Authentication Scheme tab	<p>The authentication scheme is used for managing user access to the virtual context. For information about how to define an authentication scheme, see Defining a Context Authentication Scheme, page 10-4. Use the up and down arrows on the left side of the tab to change the order in which VFrame tries authentication servers.</p> <ul style="list-style-type: none"> • Add Authentication Server—Click to add an authentication server. • Delete—Click to delete an authentication server. <p>You see the following settings if you choose a RADIUS server:</p> <ul style="list-style-type: none"> • Timeout—The time, in seconds, VFrame should wait before retransmitting the authentication request to the server. • Authentication Port—The port to use for authentication traffic, as configured for your ACS. • Shared Key—The key defined in the AAA client settings in the ACS for authenticating communications between VFrame and the ACS. You must enter the key exactly as it is configured in the ACS. <p>You see the following settings if you choose an LDAP server:</p> <ul style="list-style-type: none"> • Timeout—The time, in seconds, VFrame should wait before retransmitting the authentication request to the server. • Authentication Port—The port to use for authentication traffic, as configured for your ACS. • Use Secure Sockets Layer—Check the Use Secure Sockets Layer check box to make the connection to the server a secure socket connection. • Logon Requires Authentication—Check the Logon Requires Authentication check box to require authentication at login. • User Name—The user ID. • Role Definition—The user role. • User Name—The name of the LDAP attribute within the user record which contains the user ID. • Role Definition—Contains the list of groups which will be cross-referenced with the VFrame roles to determine the user role.

Table 10-1 *Contexts tab (continued)*

Element	Description
Roles tab	<p>The roles defined for the selected context and those shared in the Admin context. You assign these roles to users to define the authorization privileges for each user.</p> <ul style="list-style-type: none"> • New—Click to create a new role. • Delete—Click to delete a role. • Roles selector and right pane—The Roles selector lists the default roles and any roles you created. The right pane lists the privileges for each role: <ul style="list-style-type: none"> – Service Network Designer (default role)—Design > Service Networks. – Service Network Operator (default role)—Reports > Logical Server Trend, Resource Utilization, Service Network Availability, Service Network Operations > Create/Delete Image Servers, Deploy/Verify Networks, Policy, Server LUN and Path Selection, Start/Stop/Maintain Servers, and Tools > Device Manager Launch. – Template Designer (default role)—Design > Global Libraries, Templates. • Role Name—The name of the role. • Shared—Click to share the role.

Table 10-1 *Contexts tab (continued)*

Element	Description
Users tab	<p>The users defined for the selected context. If you are using local authentication, these are the only users that can log in to the virtual context. If you are using an ACS to control user logins, you must define the accounts in the ACS. However, you can define the same accounts here to use local authentication as a backup method.</p> <ul style="list-style-type: none"> • New—Click to create a new user. • Delete—Click to delete a user. • Users selector and right pane—The Users selector does not list any default users, but it lists the users you create. The right pane lists the roles and service networks for each user: <ul style="list-style-type: none"> – All Tasks—Click to assign all privileges. – Roles tab—Lists individual privileges: <ul style="list-style-type: none"> Service Network Designer (default role)—Design > Service Networks Service Network Operator (default role)—Reports > Logical Server Trend, Resource Utilization, Service Network Availability, Service Network Operations > Create/Delete Image Servers, Deploy/Verify Networks, Policy, Server LUN and Path Selection, Start/Stop/Maintain Servers, and Tools > Device Manager Launch Template Designer (default role)—Design > Global Libraries, Templates – Service Networks tab—Lists service networks available. • Local Password—Enter the local password. • Confirm Password—Re-enter the local password to confirm it. • Description—Enter a description of the user.
Resources tab	<p>The resource pools assigned to the virtual context:</p> <ul style="list-style-type: none"> • Description—Enter a description of the selected resource pool. • Select All Default Resource Pools—Check the Select All Default Resource Pools check box to choose all resource pools. • Right pane—Contains a list of all the resource pools.
Apply button	Click this button to apply your changes to the virtual context.

