



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.

These topics describe virtual contexts in further detail:

- [Understanding Virtual Contexts, page 10-1](#)
- [Working with Virtual Contexts, page 10-4](#)
- [Troubleshooting Virtual Contexts, page 10-12](#)
- [Virtual Contexts Reference, page 10-13](#)

Understanding Virtual Contexts

Virtual contexts enable you to partition a single VFrame system to create more limited administrative domains. These topics describe contexts in more detail:

- [Virtual Context Overview, page 10-2](#)
- [Using an Access Control Server with Virtual Contexts, page 10-3](#)

Virtual Context Overview

A virtual context is a logically separate image of the VFrame system. If you create virtual contexts, users logged into 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 everyone else's resources to find what they need to configure and manage. Limiting resource visibility also helps prevent accidents, such as one group changing the configuration of another group's system 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's default pools.

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

Using an Access Control Server with Virtual Contexts

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

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

Before You Begin

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

Procedure

-
- Step 1** In Cisco Secure ACS, define the VFrame server as an 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's management IP address, but it can be the IP address of any of the VFrame server's 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**, select **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** section. 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** section as a **cisco-av-pair** parameter. If you do not assign a role, the user can perform all tasks. The entry has this syntax:
shell: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 into the product. For example, to assign the role Designer, enter:
shell:roles=“Designer”
To assign the user two roles, Designer and Operator, enter:
shell:roles=“Designer Operator”
- Step 3** In VFrame, log into the Admin context and configure the virtual context to use the ACS server, as described in [Defining a Context’s Authentication Scheme](#), page 10-6.
-

Working with Virtual Contexts

These topics describe how to create and manage virtual contexts from the Admin context:

- [Creating or Modifying Virtual Contexts](#), page 10-4
- [Deleting Virtual Contexts](#), page 10-12

Creating or Modifying Virtual Contexts

This topic describes the overall process for creating or modifying a virtual context. For information on what a context is, see [Virtual Context Overview](#), page 10-2.

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** Select **Access Control > Virtual Contexts** to open the Virtual Contexts tab (see [Virtual Contexts Tab, page 10-13](#)).
- 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**.
Users must enter this context name when logging into the context.
 - To modify an existing context, select it from the list in the left pane. Its 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.
- See these topics for information on configuring the context's settings:
- [Defining a Context's Authentication Scheme, page 10-6](#)
 - [Managing Roles in a Context, page 10-8](#)
 - [Managing Users of a Context, page 10-9](#)
 - [Managing Resources Assigned to a Context, page 10-11](#)
- 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 10-12](#)

Defining a Context's Authentication Scheme

A context's authentication scheme determines how user access to the context is controlled. You can use these schemes:

- **Local**—User logins are controlled by the VFrame server. Each user who logs into the context must be defined with VFrame as a user of the context on the Users tab.
- **RADIUS**—User logins are controlled by your organization's 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 10-3](#).

Before You Begin

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

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.

Procedure

Step 1 If you are not already looking at the context's properties, select **Access Control > Virtual Contexts** to open the Virtual Contexts tab (see [Virtual Contexts Tab, page 10-13](#)), and then select the context from the list of contexts. The properties appear in the right pane.

Step 2 Click the **Authentication** tab.

The left pane of the authentication tab includes an Authentication Scheme folder, with subfolders for each authentication scheme defined for the context. These schemes 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** To add the RADIUS authentication scheme to the list of schemes:
- a. Select the **Authentication Schemes** folder.
 - b. Select **RADIUS** from the **Add Authentication Scheme** drop-down list. This adds a RADIUS Group folder to the Authentication Scheme folder.

You can change the retransmit and timeout values. These values control how many times VFrame tries to get a response from a server before moving to the next server or authentication method, and the time to wait for a response.
 - c. With the RADIUS Group folder selected, click **Add Authentication Server**. A dialog box opens asking for the IP address of the server.
 - d. Enter the IP address of the RADIUS server and click **OK**. The server is added to the RADIUS group as a folder.
 - e. With the server's folder selected, enter the shared key that is defined in the RADIUS server to communicate with the VFrame server, and select whether the key should be sent in clear text or encrypted. You can also change other server communications settings, but entering the shared key is the only required one.
 - f. Click **Save** to save your changes.
 - g. If you want to define more than one server, select the RADIUS Group folder and repeat the process of defining a server.
- Step 4** Change the order of authentication schemes and servers to match your authentication requirements:
- To change the order of an authentication scheme, select the scheme and click the up or down arrows to the left of the folder tree. Schemes at the top of the list are tried first.
 - To change the order of a server within a group, select the server and use the up or down arrows to position it as desired. Servers at the top of the list are tried first.
- Step 5** Click **Save** to save your changes.
-

Tips

- To delete a server, or a scheme, select it and click **Delete**. If you are completely removing a scheme, ensure that users are defined in VFrame (local users) or that you are adding a replacement scheme; otherwise, users will not be able to log into the context.

Related Topics

- [Understanding Virtual Contexts, page 10-1](#)
- [Troubleshooting Virtual Contexts, page 10-12](#)

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 on roles, read these topics:

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

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 (select **Access Control > Roles**).

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 server. For information on configuring user roles in the ACS server, see [Using an Access Control Server with Virtual Contexts, page 10-3](#).

Procedure

- Step 1** If you are not already looking at the context's properties, select **Access Control** > **Virtual Contexts** to open the Virtual Contexts tab (see [Virtual Contexts Tab, page 10-13](#)), and then select the context from the list of contexts. The properties appear in the right pane.
- Step 2** Click the **Roles** tab.
- Step 3** Do any of the following:
- To create a role, click **New**, and select the privileges you want to assign to the role. For information on privileges, see [Understanding Role Permissions, page 2-3](#).
When finished, click **Save**.
 - To change a role, select it and make your modifications. When finished, click **Save**.
 - To delete a role, select it and click **Delete**. Before deleting a role, ensure that it is not assigned to any users.
- Step 4** If you make any changes, be sure to click **Save**.
-

Related Topics

- [Managing Users of a Context, page 10-9](#)

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.

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 users, read these topics:

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

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 server cannot reply to login requests), get the list of usernames and passwords from your ACS server. The names and passwords must be the same as those defined in the ACS server.

Procedure

-
- Step 1** If you are not already looking at the context's properties, select **Access Control > Virtual Contexts** to open the Virtual Contexts tab (see [Virtual Contexts Tab, page 10-13](#)), and then select the context from the list of contexts. The properties appear in the right pane.
- Step 2** Click the **Users** tab.
- Step 3** To create a new user:
- Click **New**. You are prompted for a user name.
 - 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, 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 want to limit the user to have the ability to work only with specific service networks, click the **Service Networks** tab and select the desired networks. These networks must exist (be defined in the context) before you can assign them to user accounts.
 - Click **Save** to save your changes.
- Step 4** To change an existing user, select the user in the list of users, make your changes, and click **Save**.
-

Related Topics

- [Defining a Context's Authentication Scheme, page 10-6](#)
- [Managing Roles in a Context, page 10-8](#)

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's default pools.

You can assign default pools, or you can create pools specifically for the virtual context. To create pools, select **Tools > 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** If you are not already looking at the context's properties, select **Access Control > Virtual Contexts** to open the Virtual Contexts tab (see [Virtual Contexts Tab, page 10-13](#)), and then select the context from the list of contexts. The properties appear in the right pane.
- Step 2** Click the **Resources** tab.
- Step 3** Select the pools that contain the resources the context is allowed to use. If you want to assign all managed devices, select **Select All Default Resource Pools**.
- Step 4** Click **Save**.
-

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 select 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** Select **Access Control > Virtual Contexts** to open the Virtual Contexts tab (see [Virtual Contexts Tab, page 10-13](#)).
 - Step 2** Select the context you want to delete.
 - Step 3** Click the **Users** tab.
 - Step 4** In the **Users** tab, select each user and click the **Delete** button on the tab. You cannot delete the context if any user is defined for it.
 - Step 5** Click **Delete** at the top of the Virtual Contexts tab to delete the context.
-

Related Topics

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

Troubleshooting Virtual Contexts

These are some problems you might have with virtual contexts and their solutions. These problems assume that you are managing the virtual contexts, and the user does not have authorization to modify virtual context settings:

- [User cannot log into the context.](#)
- [User cannot see the required resources.](#)

Problem User cannot log into the context.

Solution If a user cannot log into 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 server and that the ACS server is configured correctly (that is, log into the context using an account you know should work). If none of these are the problem, reset the user's password on the Virtual Contexts tab.

Problem User cannot see the required resources.

Solution If a user can log into a context but cannot see the resources that the user is supposed to manage, check the user's 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 server.) 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's 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

These topics describe the fields available for managing virtual contexts and reference information on using the various GUI features:

- [Virtual Contexts Tab, page 10-13](#)

Virtual Contexts Tab

Use the Virtual 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

Select **Access Control > Virtual Contexts** to open the Virtual Contexts tab.

Related Topics

- [Understanding Virtual Contexts, page 10-1](#)
- [Creating or Modifying Virtual Contexts, page 10-4](#)
- [Deleting Virtual Contexts, page 10-12](#)
- [Troubleshooting Virtual Contexts, page 10-12](#)

Field Reference

Table 10-1 Virtual Contexts Tab

Element	Description
New button	Click this button to create a new virtual context.
Save button	Click this button to save your changes to the 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 list (left pane)	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	A description of the purpose of the virtual context.

Table 10-1 Virtual Contexts Tab (continued)

Element	Description
Authentication tab	<p>The authentication scheme to use for managing user access to the virtual context. For information on how to define an authentication scheme, see Defining a Context's Authentication Scheme, page 10-6. Use the up and down arrows on the left side of the tab to change the order in which VFrame tries authentication schemes.</p> <p>If you define a RADIUS group, you see these attributes if you select the RADIUS Group folder:</p> <ul style="list-style-type: none"> • Retransmit Count—The number of times VFrame should try to get a response from a server in the group before trying the next server or authentication method. • Timeout—The time, in seconds, VFrame should wait before retransmitting the authentication request to the server. <p>Individual RADIUS servers have these attributes:</p> <ul style="list-style-type: none"> • IP—The IP address of the RADIUS server. • Retransmit Count, Timeout—These fields have the same meaning as those for the RADIUS group, but they only apply to this server. • Shared Key—The key defined in the AAA client settings in the ACS server for authenticating communications between VFrame and the ACS server. You must enter the key exactly as it is configured in the ACS server. <p>You must also select whether to send the key in clear text or encrypted. If you send it in clear text, a network snooper might be able to pick it up.</p> <ul style="list-style-type: none"> • Authentication Port—The port to use for authentication traffic, as configured for your ACS server.

Table 10-1 Virtual Contexts Tab (continued)

Element	Description
Roles tab	<p>The roles defined for the selected context and those shared from the Admin context. You assign these roles to users to define the authorization privileges for each user.</p> <ul style="list-style-type: none"> To add a role, click New. You are prompted for a name. After creating the role, select the privileges to assign to the role, and optionally enter a description. For information on authorization privileges, see Understanding Role Permissions, page 2-3. To delete a role, select it and click Delete. Ensure that the role is not assigned to a user before you delete it.
Users tab	<p>The users defined for the selected context. If you are using local authentication, these are the only users that can log into the virtual context. If you are using an ACS server to control user logins, you must define the accounts in the ACS server. However, you can define the same accounts here to use local authentication as a backup method.</p> <ul style="list-style-type: none"> To add a user, click New. You are prompted for a user account name. After creating the user, select the roles that define the user's authorization level (or All Tasks to create a super user), enter the user's password in the Local Password and Confirm Password fields, and optionally enter a description of the user. <p>To further control the scope of the user's privileges, click the Service Network tab and select the service networks that the user is allowed to operate. Select All to allow the user to operate any service network defined in the virtual context.</p> <ul style="list-style-type: none"> To delete a user, select the user and click Delete.
Resources tab	<p>The resource pools assigned to the virtual context. Select all pools that contain resources that should be available for use within the context. (To create pools, select Tools > Pools.) The pools you assign appear in the context (unless they are default pools), and their contents also appear in the context's default pools.</p> <p>To assign all managed devices to the virtual context, select Select All Default Resource Pools.</p>