



## CHAPTER 4

# Managing Device Credentials

---

VFrame requires device credentials for communicating with the devices it manages. This chapter describes device credentials, and includes the following sections:

- [Understanding Device Credentials, page 4-1](#)
- [Working with Device Credentials, page 4-5](#)
- [Troubleshooting Device Credentials, page 4-15](#)
- [Device Credentials Reference, page 4-16](#)

## Understanding Device Credentials

VFrame must know the credentials (such as CLI usernames and passwords, SNMPv1n2 community strings, or SNMPv3 usernames and authentication passwords) for any device you want it to manage. This section describes more about device credentials, describes how VFrame uses them, provides recommendations on how to define and organize them effectively, and includes the following topics:

- [Device Credentials Overview, page 4-1](#)
- [Understanding How VFrame Uses the Device Credential Lists, page 4-3](#)
- [Understanding IP Address Patterns, page 4-3](#)
- [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)

## Device Credentials Overview

Device credentials are simply the CLI username and password, SNMPv1n2 community strings, or SNMPv3 username and authentication password required to log in to a device and obtain the information VFrame requires to discover and manage the device. The CLI username and password is the same user account you would use to log in to the device CLI to perform system configuration.

You must configure the correct device credentials for any device you want VFrame to manage. VFrame encrypts passwords to keep them safe. As you change passwords on managed devices, ensure that you also change them in the VFrame credentials list.

VFrame separates credentials into the following categories:

- **Network**—For Ethernet switches. You must define a username and both a user EXEC mode and a privileged EXEC (enable) mode password for the device. You also must define the SNMPv1n2 read community string or SNMPv3 username and authentication password, which is required to discover the switch.




---

**Note** You are required to configure credentials for only one SNMP version (SNMPv1n2 or SNMPv3), but you can configure both if you want. VFrame checks the SNMPv3 credentials first and the SNMPv1n2 credentials are used only if no SNMPv3 credential match is found.

---

- Network Services—For service modules, such as FWSM and CSM, that reside in an Ethernet switch. You must define a username and both a user EXEC mode and a privileged EXEC (enable) mode password for the service module.
- Server—For the LOM managers that will control the servers, and the LOM interfaces on the servers:
  - LOM Managers—VFrame discovers servers by using a lights-out management (LOM) manager, which contains a server inventory and identifies the IP addresses for the LOM interfaces on those servers. The LOM managers log in to the LOM interfaces on the servers and power on and power off the servers. You must define the username and password required to log in to the LOM manager. For more information on LOM managers, see [LOM Managers, page 3-6](#).
  - LOM—The username and passwords for logging in to the LOM interfaces on servers. The LOM managers use these credentials.
- Storage—For storage devices. There are three categories of storage credential:
  - SNMP—If your storage network contains Cisco MDS Fibre Channel switches or Brocade Fibre Channel switches, you must define SNMPv1n2 community strings or the SNMPv3 username and authentication password for the device. For SNMPv1n2, both read and write community strings must be specified if your storage network is Cisco MDS-based; for Brocade-based storage networks only the read community string is required.




---

**Note** You are required to configure credentials for only one SNMP version (SNMPv1n2 or SNMPv3), but you can configure both if you want. VFrame checks the SNMPv3 credentials first and the SNMPv1n2 credentials are used only if no SNMPv3 credential match is found.

---

- NAS—If your storage network contains NAS filers, you must define a username and password for the device.
- SAN Manager (Storage Manager)—If you are using storage managers to manage storage arrays, you must define the username and password for the storage manager. During the VFrame installation, if you selected to manage your SAN in storage array mode (through an MDS switch and a storage manager), you must configure the storage manager credentials. For details, see [Storage Array Mode, page 3-4](#).
- Brocade CLI—If your storage network contains Brocade Fibre Channel switches you must define command line interface credentials for them. The user information that you specify must have zone modification privileges. In addition, we recommended that a separate account with zone privileges be created for exclusive use by VFrame.
- Virtual Machine Management—For Virtual Centers, If your storage network contains Virtual Centers, you must define a username and password for the device.

#### Related Topics

- [Understanding How VFrame Uses the Device Credential Lists, page 4-3](#)
- [Understanding IP Address Patterns, page 4-3](#)
- [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)

## Understanding How VFrame Uses the Device Credential Lists

Each category of device credential is a separate list of credentials. When VFrame needs the credential for a device, it searches the appropriate list from top to bottom looking for a match. Thus, it is important how you arrange your credential list.

This is how VFrame processes a credential list when trying to find the credentials for a device:

- 
- Step 1** VFrame starts at the top of the credentials list for the appropriate type of device, and compares the device IP address to the IP address pattern defined for each credential. (For more information about the IP address patterns used in credentials, see [Understanding IP Address Patterns, page 4-3](#).)
- Step 2** The following procedure details the necessary steps VFrame follows to process a credentials list:
- If the device IP address **does not** match the IP address pattern in the credential, VFrame moves to the next entry in the list.
  - If the device IP address **does** match the IP address pattern in the credential, VFrame tries the credential.
    - If the credential works, VFrame proceeds with its device management task and does not try any other credentials.
    - If the credential **does not** work, **and** there is a **stop flag** on the credential (Stop in the On Failure field), VFrame issues an error to the job log. If the device being processed is the only device in the job, the job fails; otherwise, the job continues with the next device.
    - If the credential **does not** work, **and** there is **no stop flag** on the credential (nothing in the On Failure field), VFrame continues to the next entry in the credentials list.
- Step 3** If VFrame gets to the end of the credentials list without finding a correct credential, VFrame issues an error message to the job log and continues to the next device (if there is one).
- 

### Related Topics

- [Device Credentials Overview, page 4-1](#)
- [Understanding IP Address Patterns, page 4-3](#)
- [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)

## Understanding IP Address Patterns

When you create a device credential, you must include one or more IP addresses of the devices that use the credential. When VFrame searches the credentials list, it looks for a match to the IP address of the device it is trying to manage.

Instead of entering credentials for every unique IP address used by your devices, you can create IP address patterns or variable expressions. Thus, you can match a set of IP addresses with a single credential entry or IP address definition.

You can define IP addresses in a credential entry in the following ways:

- Single IP address—A complete IP address, such as 10.100.30.10.
- IP address with wildcard—An IP address with wildcards used to represent any number within an octet. The wildcard is the asterisk (\*). For example, 10.100.10.\* matches any address from the 10.100.10.0 to 10.100.10.255 range.

To create a default credential, one that matches any IP address, you can create a credential for the \*.\*.\*.\* IP address. Place default credentials last in the credential list.

- IP address range—You can specify a range of IP addresses using the [x-y] characters, where x is the first value in the range, and y is the last value. For example, 10.100.10.[13-15] matches the IP addresses 10.100.10.13, 10.100.10.14, and 10.100.10.15.
- Combination of wildcards and ranges—You can include both \* and [x-y] expressions within a single IP address pattern. For example, 10.[10-12].\*.\*.

#### Related Topics

- [Device Credentials Overview, page 4-1](#)
- [Understanding How VFrame Uses the Device Credential Lists, page 4-3](#)
- [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)

## Understanding How to Organize a Credentials List and to Use Stop Flags

When you add a credential, VFrame places the new credential at the bottom of the list. However, this might not be the best placement for the credential you are adding. Use the up and down arrow keys to create your desired sequence of entries. You can also set stop flags to control whether VFrame tries additional entries after a credential fails.

In general, you should organize your credentials list so that more specific credentials are at the top of the list, and more general ones are at the bottom of the list. This ensures that VFrame will always first try a credential that most closely matches a device IP address.

Consider the entries shown in [Figure 4-1](#). If VFrame is looking for a credential for 10.100.90.15, it will use the test1 credential (username admin) because 10.100.90.15 fits the 10.100.90.[10-20] IP address pattern. If the credential fails, VFrame will try the test2 credential (user root) because the IP address also matches the 10.100.90.\* pattern. However, if that credential fails, VFrame will not try any additional credentials because there is a stop flag on the test2 credential, that is, **Stop** appears in the On Failure field.

On the other hand, if VFrame is looking for a credential for 10.100.70.8, it will first try the test1 credential. If that fails, it will skip test2 because the IP address does not match any IP address pattern defined in test2. Thus, the stop flag will not prevent VFrame from continuing down the list to the Default credential, which it will also try, because \*.\*.\*.\* matches all IP addresses.

**Figure 4-1** Example Network CLI Credentials List

Name	IP Ranges	User	On Failure
test1	10.100.90.[10-20],10.100.70.*	admin	
test2	10.100.30.*,10.100.90.*	root	Stop
test3	10.100.30.*	admin	
Default	*.*.*.*	admin	

<b>1</b>	Stop flag	<b>2</b>	Up and Down buttons
----------	-----------	----------	---------------------

Now consider the list shown in [Figure 4-2](#), where the test1 and test2 credentials are switched. This time when VFrame processes 10.100.90.15, it will try the test2 credential first. If the test2 credential fails, the test1 credential will **not** be tried because of the stop flag on the test2 credential. In this case, defining 10.100.90.[10-20] in the test1 credential is pointless, because all IP addresses in the 10.100.90.\* address space will either succeed using the test2 credential, or VFrame will stop looking for another credential.

**Figure 4-2** Example Network CLI Credential Reordered

Name	IP Ranges	User	On Failure
test2	10.100.30.*,10.100.90.*	root	Stop
test1	10.100.90.[10-20],10.100.70.*	admin	
test3	10.100.30.*	admin	
Default	*.*.*.*	admin	

### Related Topics

- [Device Credentials Overview](#), page 4-1
- [Understanding How VFrame Uses the Device Credential Lists](#), page 4-3
- [Understanding IP Address Patterns](#), page 4-3

## Working with Device Credentials

This section describes how to create and manage device credential lists, and includes the following topics:

- [Configuring Device Credentials](#), page 4-5
- [Editing or Modifying Device Credentials](#), page 4-13
- [Deleting Device Credentials](#), page 4-14
- [Rearranging the Device Credentials List and Using Stop Flags](#), page 4-14

## Configuring Device Credentials

This section describe how to configure credentials, and includes the following topics:

- [Configuring Network Credentials](#), page 4-6
- [Configuring Network Services Credentials](#), page 4-7
- [Configuring NAS Credentials](#), page 4-8
- [Configuring SNMP Credentials for Fibre Channel Switches](#), page 4-8
- [Configuring Storage Manager Credentials](#), page 4-10
- [Configuring Brocade CLI Credentials](#), page 4-10
- [Configuring Server Credentials](#), page 4-11
- [Configuring Virtual Machine Manager Credentials](#), page 4-12

## Configuring Network Credentials

You must configure CLI and SNMP credentials so that VFrame can communicate with Ethernet switches. CLI credentials are required for logging in to a switch. The SNMP credentials are required for discovering a switch.



### Note

You are required to configure credentials for only one SNMP version (SNMPv1n2 and SNMPv3), but you can configure both if you want. VFrame checks the SNMPv3 credentials first and the SNMPv1n2 credentials are used only if no matching IP Address pattern is found in the SNMPv3 credential list. If an IP Address pattern match is found in the SNMPv3 credential list but credential validation fails, VFrame does not try the SNMPv1n2 credentials.

### Before You Begin

Determine the following credentials for each of the switches that VFrame will manage:

- CLI usernames and passwords
- SNMPv1n2 read community strings
- SNMPv3 username, authentication password and protocol, security mode, and privacy password and protocol



### Note

Ethernet switches support the Data Encryption Standard (DES) privacy protocol, but not the Advanced Encryption Standard (AES) privacy protocol.

### Procedure

- Step 1** Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
- Step 2** In the Network dialog box, click the **Credentials** tab (see [Credentials Tab, page 4-16](#)).
- Step 3** Click the **Network** category. The CLI tab is selected by default.
- Step 4** Click **New** to open the CLI Credential dialog box for defining the username and passwords required to log in to the device and enter privileged EXEC (enable) mode. For more information on the fields on this dialog box, see [CLI Credential Dialog Box, page 4-20](#).

When you finish defining the credential, click **OK** to add it to the end of the credential table. Use the up and down arrows to reposition the credential in the list as desired. See the following topics for information on the importance of credential order and stop flag usage:

- [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)
- [Rearranging the Device Credentials List and Using Stop Flags, page 4-14](#)

- Step 5** Click the **SNMPv1n2** tab.
- Step 6** Click **New** to open the SNMPv1n2 Credential dialog box for defining the SNMPv1n2 read community string used to discover the device. For more information on the fields on this dialog box, see [SNMPv1n2 Credential Dialog Box, page 4-21](#).

When finished defining the credential, click **OK** to add it to the end of the credential table. Use the up and down arrows to reposition the credential in the list as desired.

- Step 7** Click the **SNMPv3** tab.

**Step 8** Click **New** to open the SNMPv3 Credential dialog box for defining the SNMPv3 authNoPriv (authentication only) or authPriv (authentication and privacy) security modes. For more information on the fields on this dialog box, see [SNMPv3 Credential Dialog Box, page 4-23](#).

When finished defining the credential, click **OK** to add it to the end of the credential table. Use the up and down arrows to reposition the credential in the list as desired.

---

#### Next Step

After you add the credentials, you can discover the Ethernet switch (see [Discovering Ethernet Switches and Service Modules, page 6-4](#)).

#### Related Topics

- [Understanding Device Credentials, page 4-1](#)
- [Editing or Modifying Device Credentials, page 4-13](#)
- [Deleting Device Credentials, page 4-14](#)

## Configuring Network Services Credentials

Network services credentials are the credentials required for logging in to service modules such as FWSM and CSM. These service modules reside in an Ethernet switch.

#### Before You Begin

Determine the usernames and passwords for each of the service modules that VFrame will manage.

#### Procedure

---

- Step 1** Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
- Step 2** In the Network dialog box, click the **Credentials** tab (see [Credentials Tab, page 4-16](#)).
- Step 3** Click the **Network Services** category. The Network Services CLI tab is selected by default.
- Step 4** Click **New** to open the CLI Credential dialog box for defining the username and passwords required to log in to the service module and enter privileged EXEC (enable) mode. For more information on the fields on this dialog box, see [CLI Credential Dialog Box, page 4-20](#).

When you finish defining the credential, click **OK** to add it to the end of the credential table. Use the up and down arrows to reposition the credential in the list as desired. See the following topics for information on the importance of credential order and stop flag usage:

- [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)
  - [Rearranging the Device Credentials List and Using Stop Flags, page 4-14](#)
- 

#### Next Step

After you add the credentials, you can discover the Ethernet switch and its service modules. (see [Discovering Ethernet Switches and Service Modules, page 6-4](#)).

**Related Topics**

- [Understanding Device Credentials, page 4-1](#)
- [Editing or Modifying Device Credentials, page 4-13](#)
- [Deleting Device Credentials, page 4-14](#)

## Configuring NAS Credentials

If you are using NAS filers, configure the NAS credentials so that VFrame can communicate with them.

**Before You Begin**

Determine the usernames and passwords for each of the NAS filers that VFrame will manage.

**Procedure**

- 
- Step 1** Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
  - Step 2** In the Network dialog box, click the **Credentials** tab (see [Credentials Tab, page 4-16](#)).
  - Step 3** Click the **Storage** category. The SNMPv1n2 tab is selected by default.
  - Step 4** Click the **NAS** tab.
  - Step 5** Click **New** to open the NAS Credential dialog box for defining the username and password required to log in to the device. For more information on the fields on this dialog box, see [NAS Credential Dialog Box, page 4-24](#).

When you finish defining the credential, click **OK** to add it to the end of the credential table. Use the up and down arrows to reposition the credential in the list as desired. See the following topics for information on the importance of credential order and stop flag usage:

- [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)
  - [Rearranging the Device Credentials List and Using Stop Flags, page 4-14](#)
- 

**Next Step**

After you add the credentials, you can discover the NAS filer and its volumes (see [Discovering NAS Filers and Their Components, page 6-7](#)).

**Related Topics**

- [Understanding Device Credentials, page 4-1](#)
- [Editing or Modifying Device Credentials, page 4-13](#)
- [Deleting Device Credentials, page 4-14](#)

## Configuring SNMP Credentials for Fibre Channel Switches

If you are using Fibre Channel switches, configure the SNMP credentials so that VFrame can communicate with them.

**Note**

You are required to configure credentials for only one SNMP version (SNMPv1n2 or SNMPv3), but you can configure both if you want. VFrame checks the SNMPv3 credentials first and the SNMPv1n2 credentials are used only if no SNMPv3 credential match is found.

**Before You Begin**

Determine the following credentials for each Fibre Channel switch that VFrame will manage:

- CLI usernames and passwords
- SNMPv1n2 read and write community strings
- SNMPv3 username, authentication password and protocol, security mode, and privacy password and protocol

**Procedure**

- 
- Step 1** Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
- Step 2** In the Network dialog box, click the **Credentials** tab (see [Credentials Tab, page 4-16](#)).
- Step 3** Click the **Storage** category. The SNMPv1n2 tab is selected by default.
- Step 4** Click **New** to open the SNMPv1n2 Credential dialog box for defining the SNMPv1n2 read and write community strings used to manage the switch. For more information on the fields on this dialog box, see [SNMPv1n2 Credential Dialog Box, page 4-21](#).

When finished defining the credential, click **OK** to add it to the end of the credential table. Use the up and down arrows to reposition the credential in the list as desired. See the following topics for information on the importance of credential order and stop flag usage:

- [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)
- [Rearranging the Device Credentials List and Using Stop Flags, page 4-14](#)

- Step 5** Click the **SNMPv3** tab.
- Step 6** Click **New** to open the SNMPv3 Credential dialog box for defining the SNMPv3 authNoPriv (authentication only) or authPriv (authentication and privacy) security modes. For more information on the fields on this dialog box, see [SNMPv3 Credential Dialog Box, page 4-23](#).

When you finish defining the credential, click **OK** to add it to the end of the credential table. Use the up and down arrows to reposition the credential in the list as desired.

---

**Next Step**

After you add the credentials, you can discover the Fibre Channel switches in your SAN fabric(s), along with connected host and target ports. In addition, if the SAN fabric being discovered is Cisco MDS-based, VSAN and related information is also discovered. For more information, see [Discovering SAN Fabric Devices and Their Components, page 6-6](#).

**Related Topics**

- [Understanding Device Credentials, page 4-1](#)
- [Editing or Modifying Device Credentials, page 4-13](#)
- [Deleting Device Credentials, page 4-14](#)

## Configuring Storage Manager Credentials

For SAN-based deployments a Storage Manager is required for Storage Array configuration. You must configure credentials for the Storage Manager to enable VFrame to communicate with it.

### Before You Begin

Determine the usernames and passwords for each of the storage managers that VFrame will manage.

### Procedure

- 
- Step 1** Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
  - Step 2** In the Network dialog box, click the **Credentials** tab (see [Credentials Tab, page 4-16](#)).
  - Step 3** Click the **Storage** category. The SNMPv1n2 tab is selected by default.
  - Step 4** Click the **SAN Manager** tab.
  - Step 5** Click **New** to open the SAN Manager Credential dialog box for defining the username and password required to log in to the storage manager. For more information on the fields on this dialog box, see [SAN Manager Credential Dialog Box, page 4-25](#).

When you finish defining the credential, click **OK** to add it to the end of the credential table. Use the up and down arrows to reposition the credential in the list as desired. See the following topics for information on the importance of credential order and stop flag usage:

- [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)
  - [Rearranging the Device Credentials List and Using Stop Flags, page 4-14](#)
- 

### Next Step

After you add the credentials, you can discover Storage Managers and the storage arrays associated with them (see [Discovering Storage Arrays and Their Components Through Storage Managers, page 6-8](#)).

### Related Topics

- [Understanding Device Credentials, page 4-1](#)
- [Editing or Modifying Device Credentials, page 4-13](#)
- [Deleting Device Credentials, page 4-14](#)

## Configuring Brocade CLI Credentials

You must configure CLI credentials so that VFrame can communicate with Brocade Fibre Channel switches.

### Before You Begin

Determine the CLI usernames and passwords for each Brocade Fibre Channel switch that VFrame will manage.

### Procedure

- 
- Step 1** Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
  - Step 2** In the Network dialog box, click the **Credentials** tab (see [Credentials Tab, page 4-16](#)).
  - Step 3** Click the **Storage** category, and then click the Brocade CLI tab.
  - Step 4** Click **New** to open the Brocade CLI Credential dialog box for defining the username and passwords required to log in to the device and enter privileged EXEC (enable) mode. For more information on the fields on this dialog box, see [Brocade CLI Credential Dialog Box, page 4-27](#).

When you finish defining the credential, click **OK** to add it to the end of the credential table. Use the up and down arrows to reposition the credential in the list as desired. See the following topics for information on the importance of credential order and stop flag usage:

- [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)
  - [Rearranging the Device Credentials List and Using Stop Flags, page 4-14](#)
- 

### Next Step

After you add the credentials, you can discover the Brocade Fibre Channel switch (see [Discovering SAN Fabric Devices and Their Components, page 6-6](#)).

### Related Topics

- [Understanding Device Credentials, page 4-1](#)
- [Editing or Modifying Device Credentials, page 4-13](#)
- [Deleting Device Credentials, page 4-14](#)

## Configuring Server Credentials

You must configure the LOM manager credentials so that VFrame can communicate with the LOM managers to run inventory and to power on and power off the servers. VFrame controls the power management of the servers through LOM managers. You must also configure the LOM interface credentials so that the LOM managers can log in to the interfaces.

### Before You Begin

Determine the usernames and passwords for each of the LOM managers that VFrame will use, and for the LOM interfaces on each application, and optionally, on each model server.



### Note

---

It is optional to provide the LOM manager username and password for VFrame-created default internal LOM managers. The macrouser account is internal to VFrame, and VFrame can bypass the standard logging mechanism and execute the LOM macros directly.

---

### Procedure

- 
- Step 1** Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
  - Step 2** In the Network dialog box, click the **Credentials** tab (see [Credentials Tab, page 4-16](#)).
  - Step 3** Click the **Servers** category. The LOM Manager tab is selected by default.

**Step 4** On the LOM Manager tab, click **New** to open the LOM Manager Credential dialog box for defining the username and password required to log in to the LOM manager. For more information on the fields on this dialog box, see [LOM Manager Credential Dialog Box, page 4-28](#).

When you finish defining the credential, click **OK** to add it to the end of the credential table. Use the up and down arrows to reposition the credential in the list as desired. See the following topics for information on the importance of credential order and stop flag usage:

- [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)
- [Rearranging the Device Credentials List and Using Stop Flags, page 4-14](#)

**Step 5** Click the **LOM** tab.

**Step 6** Click **New** to open the LOM Credential dialog box for defining the username and password required to log in to the LOM interfaces on application or model servers. For more information on the fields on this dialog box, see [LOM Credential Dialog Box, page 4-29](#).

When finished defining the credential, click **OK** to add it to the end of the credential table. Use the up and down arrows to reposition the credential in the list as desired.

### Next Step

After you add the credentials, you can discover LOM managers and the servers they control (see [Discovering Servers, page 6-10](#)).

### Related Topics

- [Understanding Device Credentials, page 4-1](#)
- [Editing or Modifying Device Credentials, page 4-13](#)
- [Deleting Device Credentials, page 4-14](#)

## Configuring Virtual Machine Manager Credentials

Configure the Virtual Machine Manager credentials so that VFrame can communicate with the Virtual Center.

### Before You Begin

Determine the usernames and passwords for each Virtual Center that VFrame will manage.

### Procedure

**Step 1** Choose **Tools > VFrame Administration > Network** to open the Network dialog box.

**Step 2** In the Network dialog box, click the **Credentials** tab (see [Credentials Tab, page 4-16](#)).

**Step 3** Click the **Virtual Machine Management** category. The Virtual Machine Managers tab is selected by default.

**Step 4** Click **New** to open the Virtual Machine Manager Credential dialog box for defining the username and password required to log in to the Virtual Center. For more information on the fields on this dialog box, see [Virtual Machine Manager Credential Dialog Box, page 4-31](#).

When you finish defining the credential, click **OK** to add it to the end of the credential table. Use the up and down arrows to reposition the credential in the list as desired. See the following topics for information on the importance of credential order and stop flag usage:

- [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)
  - [Rearranging the Device Credentials List and Using Stop Flags, page 4-14](#)
- 

### Next Step

After you add the credentials, you can discover the NAS filer and its volumes.

### Related Topics

- [Understanding Device Credentials, page 4-1](#)
- [Editing or Modifying Device Credentials, page 4-13](#)
- [Deleting Device Credentials, page 4-14](#)

## Editing or Modifying Device Credentials

If a credential is no longer correct, you can modify it. You can change the IP address range, usernames, passwords, or SNMP community strings.

### Procedure

---

- Step 1** Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
- Step 2** In the Network dialog box, click the **Credentials** tab (see [Credentials Tab, page 4-16](#)).
- Step 3** Select the category and tab that contains the credential you want to modify.
- Step 4** Double-click the desired credential. Alternatively, you can select the credential and click **Edit** or choose **Edit** from the right-click shortcut menu.

Doing so opens one of the following dialog boxes:

- [CLI Credential Dialog Box, page 4-20](#)
- [SNMPv1n2 Credential Dialog Box, page 4-21](#)
- [SNMPv3 Credential Dialog Box, page 4-23](#)
- [NAS Credential Dialog Box, page 4-24](#)
- [SAN Manager Credential Dialog Box, page 4-25](#)
- [Brocade CLI Credential Dialog Box, page 4-27](#)
- [LOM Manager Credential Dialog Box, page 4-28](#)
- [LOM Credential Dialog Box, page 4-29](#)
- [Virtual Machine Manager Credential Dialog Box, page 4-31](#)

After making your modifications, click **OK**.

---

### Related Topics

- [Understanding Device Credentials, page 4-1](#)
- [Configuring Device Credentials, page 4-5](#)
- [Deleting Device Credentials, page 4-14](#)

## Deleting Device Credentials

If you no longer need a credential, you can delete it. Make sure that the credential is not needed by any VFrame-managed device.

### Procedure

- 
- Step 1** Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
  - Step 2** In the Network dialog box, click the **Credentials** tab (see [Credentials Tab, page 4-16](#)).
  - Step 3** Select the category and tab that contains the credential you want to delete.
  - Step 4** Select the credential and click **Delete**. Alternatively, you can choose **Delete** from the right-click shortcut menu.
- 

### Related Topics

- [Understanding Device Credentials, page 4-1](#)
- [Configuring Device Credentials, page 4-5](#)
- [Editing or Modifying Device Credentials, page 4-13](#)

## Rearranging the Device Credentials List and Using Stop Flags

The order in which device credentials appear in a credentials list matters. When searching for the credential for a specific device, VFrame starts from the top of the credentials list and searches down, looking for a credential with an IP address pattern that matches the IP address of the device. If the credential does not work, VFrame continues to search the list. If a credential matches, a stop flag prevents VFrame from trying additional entries in the list in case a credential does not work.

For a complete explanation, with examples, of how VFrame processes a credentials list and handles credential order and stop flags, see the following topics:

- [Understanding How VFrame Uses the Device Credential Lists, page 4-3](#)
- [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)

### To rearrange the credentials and modify stop flag settings:

- To move a credential up or down in the list, select the credential and click the up or down arrows as appropriate ([Figure 4-3](#)).

**Figure 4-3** Up and Down Buttons for Credentials

Name	IP Ranges	User	On Failure
test1	10.100.90.[10-20],10.100.70.*	admin	
test2	10.100.30.*,10.100.90.*	root	Stop
test3	10.100.30.*	admin	
Default	*.*.*.*	admin	

<b>1</b>	Stop flag	<b>2</b>	Up and Down buttons
----------	-----------	----------	---------------------

- To set a stop flag on a credential, select a credential, click **edit**, and from the If credentials fail drop-down list choose **Stop Trying Credentials**.
- To remove a stop flag, select a credential that has a stop flag (Stop appears in the On Failure field), click **edit**, and from the If credentials fail drop-down list choose **Try Additional Credentials**.

#### Related Topics

- [Understanding Device Credentials, page 4-1](#)
- [Credentials Tab, page 4-16](#)

## Troubleshooting Device Credentials

This section describes some problems you might encounter when working with device credentials and their solutions, and includes the following topics:

- [Problem The correct credential is in the credentials list, but VFrame cannot log in to a device.](#)
- [Problem The server credentials are in the list, but VFrame cannot discover the servers.](#)
- [Problem VFrame used to be able to log in to a device, but now it cannot.](#)

**Problem** The correct credential is in the credentials list, but VFrame cannot log in to a device.

**Solution** First, check that the credential is defined in the correct list. For example, FWSM credentials must appear in the Network Services CLI list, not the Network CLI list. Next, check to see if there is a stop flag set on a credential above the correct credential (that is, Stop appears in the On Failure field). If the IP address of the failing device matches the IP address pattern in the credential with the stop flag, that flag is preventing VFrame from trying the correct credential. Either remove the stop flag, or move the correct credential above the credential with the stop flag. If none of these are the problem, carefully check the IP address pattern of the credential to ensure that it actually matches the IP address of the failing device. Also, check the username, password, or SNMP configuration on the device itself.

**Problem** The server credentials are in the list, but VFrame cannot discover the servers.

**Solution** The credentials list for the Server category contains the credentials for the LOM managers, not the servers themselves. The LOM manager is the device that manages connections to the servers. Although VFrame can act as a LOM manager, you must set it up to do so. You will still have to define the VFrame LOM manager credentials in this list rather than the server credentials. For more information, see [Device Credentials Overview, page 4-1](#).

**Problem** VFrame used to be able to log in to a device, but now it cannot.

**Solution** Check to see if the passwords or SNMP community strings on the device were changed. You must update the credential list in VFrame whenever you change passwords or community strings on the devices.

If you changed the credentials on the device to something which is already in the VFrame credential list, you must still move the credential up and back down the device credential list. On successful validation, the credential is cached in VFrame and this cache is invalidated only on some actions, such as adding, modifying, and deleting credentials, setting and removing stop flags, and re-order credentials.

# Device Credentials Reference

This section describes the tabs and dialog boxes you use when managing device credentials, and includes the following topics:

- [Credentials Tab, page 4-16](#)
- [CLI Credential Dialog Box, page 4-20](#)
- [SNMPv1n2 Credential Dialog Box, page 4-21](#)
- [SNMPv3 Credential Dialog Box, page 4-23](#)
- [NAS Credential Dialog Box, page 4-24](#)
- [SAN Manager Credential Dialog Box, page 4-25](#)
- [LOM Manager Credential Dialog Box, page 4-28](#)
- [LOM Credential Dialog Box, page 4-29](#)
- [Virtual Machine Manager Credential Dialog Box, page 4-31](#)
- [Credentials Shortcut Menu Options, page 4-32](#)

## Credentials Tab

Use the Credentials tab to define and manage the credentials (such as usernames, passwords, SNMP community strings) for the devices you want VFrame to manage. You must keep this list up-to-date as you change passwords on the devices.

### How to Get to This Tab

Choose **Tools > VFrame Administration > Network** to open the Network dialog box. In the Network dialog box, click the **Credentials** tab.

### Related Topics

- [Understanding Device Credentials, page 4-1](#)
  - [Device Credentials Overview, page 4-1](#)
  - [Understanding How VFrame Uses the Device Credential Lists, page 4-3](#)
  - [Understanding IP Address Patterns, page 4-3](#)
  - [Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4](#)
- [Configuring Device Credentials, page 4-5](#)
- [Editing or Modifying Device Credentials, page 4-13](#)
- [Deleting Device Credentials, page 4-14](#)
- [Rearranging the Device Credentials List and Using Stop Flags, page 4-14](#)

## Field Reference

Table 4-1 Credentials Tab




Element	Description
New button	<p>Click this button to add a credential to the credentials list displayed in the tab below this button. A different dialog box opens for you to enter the credential information depending on the type of credential you are defining:</p> <ul style="list-style-type: none"> <li>• Network CLI, Network Services CLI—See <a href="#">CLI Credential Dialog Box, page 4-20</a>.</li> <li>• Network SNMPv1n2—See <a href="#">SNMPv1n2 Credential Dialog Box, page 4-21</a>.</li> <li>• Network SNMPv3—See <a href="#">SNMPv3 Credential Dialog Box, page 4-23</a>.</li> <li>• Network Services CLI—See <a href="#">CLI Credential Dialog Box, page 4-20</a>.</li> <li>• LOM Manager—See <a href="#">LOM Manager Credential Dialog Box, page 4-28</a>.</li> <li>• LOM—See <a href="#">LOM Credential Dialog Box, page 4-29</a>.</li> <li>• Storage SNMPv1n2 (for SAN fabric devices)—See <a href="#">SNMPv1n2 Credential Dialog Box, page 4-21</a>.</li> <li>• Storage SNMPv3 (for SAN fabric devices)—See <a href="#">SNMPv3 Credential Dialog Box, page 4-23</a>.</li> <li>• NAS—See <a href="#">NAS Credential Dialog Box, page 4-24</a>.</li> <li>• SAN Managers (Storage Managers)—See <a href="#">SAN Manager Credential Dialog Box, page 4-25</a>.</li> <li>• Brocade CLI—See <a href="#">Brocade CLI Credential Dialog Box, page 4-27</a>.</li> <li>• Virtual Machine Manager—See <a href="#">Virtual Machine Manager Credential Dialog Box, page 4-31</a>.</li> </ul>
Edit button	Click this button to modify the selected credential.
Delete button	Click this button to delete the selected credential.
Up and Down arrows (on the right side of the window)	<p>Click the up or down arrows to move the selected row up or down in the credentials list. When searching for a device credential, VFrame searches the list from top to bottom. Therefore, the order of the credentials is important and affects processing. For an explanation of how credential ordering affects processing, see <a href="#">Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4</a>.</p> 

Table 4-1 Credentials Tab (continued)

Element	Description
<b>Categories (left pane) and Associated Credential Tabs (right pane)</b>	
<p>When you select a category from the left pane, tabs appear in the right pane. Each tab represents a separate credentials list. When searching for device credentials, VFrame only searches the list appropriate for the type of device it is accessing, and the type of action it needs to take. The following information describes these credential lists and their usage.</p> <p>The table column headings are explained after the categories.</p>	
Network category	<p>The credentials required for Ethernet switches:</p> <ul style="list-style-type: none"> <li>• CLI—Credentials for logging in to the device. Define a username and both a user EXEC mode and a privileged EXEC (enable) mode password for the device.</li> <li>• One or both of the following SNMP credentials, which are required to discover the switch: <ul style="list-style-type: none"> <li>– SNMPv1n2—The SNMPv1n2 read community string.</li> <li>– SNMPv3—The SNMPv3 authNoPriv (authentication only) or authPriv (authentication and privacy) security modes.</li> </ul> </li> </ul> <p> <b>Note</b> You are required to configure credentials for only one SNMP version (SNMPv1n2 or SNMPv3), but you can configure both if you want. VFrame checks the SNMPv3 credentials first and the SNMPv1n2 credentials are used only if no SNMPv3 credential match is found.</p>
Network Services category	<p>The credentials required for Ethernet services modules such as FWSM and CSM.</p> <ul style="list-style-type: none"> <li>• Network Services CLI—Credentials for logging in to the service module. Define a username and both a user EXEC mode and a privileged EXEC (enable) mode password for the module.</li> </ul>
Server category	<p>The credentials for the lights-out management (LOM) managers that will control the servers.</p> <ul style="list-style-type: none"> <li>• LOM Manager—Credentials for logging in to the LOM manager. These are not the credentials for logging in to the servers. The LOM manager contains a server inventory and the usernames and passwords required to log in to the LOM interfaces on the servers to power on and power off the servers.</li> </ul> <p>Define the username and password required to log in to the LOM manager. For more information on LOM managers, see <a href="#">LOM Managers, page 3-6</a>.</p> <ul style="list-style-type: none"> <li>• LOM—Credentials for logging in to the LOM interfaces on servers. Define the username and password required for logging in to the LOM interface. The LOM managers use these credentials.</li> </ul>

**Table 4-1** *Credentials Tab (continued)*

Element	Description
Storage category	<p>The credentials required for the storage devices.</p> <ul style="list-style-type: none"> <li>One or both of the following SNMP credentials for Fibre Channel switches: <ul style="list-style-type: none"> <li>SNMPv1n2—The SNMPv1n2 Read Community String and, depending on the switch Vendor, Write Community string. For Cisco MDS switches, VFrame requires both SNMP Read And Write Community strings to be provided. For Brocade switches, only the Read Community string is required.</li> <li>SNMPv3—The SNMPv3 authNoPriv (authentication only) or authPriv (authentication and privacy) security levels.</li> </ul> </li> </ul> <p> <b>Note</b> You are required to configure credentials for only one SNMP version (SNMPv1n2 or SNMPv3), but you can configure both if you want. VFrame checks the SNMPv3 credentials first and the SNMPv1n2 credentials are used only if no SNMPv3 credential match is found.</p> <ul style="list-style-type: none"> <li>NAS—Credentials for NAS filers. Define a username and password for logging in to the device.</li> <li>Storage Manager—Credentials for storage managers. If you are using storage managers to manage storage arrays, define the username and password for logging in to the storage manager.</li> <li>Brocade CLI—If your storage network contains Brocade Fibre Channel switches you must define command line interface (CLI) credentials for them. The user information that you specify must have zone modification privileges. In addition, we recommend that a separate account with zone privileges be created for exclusive use by VFrame.</li> </ul>
Virtual Machine Management	The credentials required for Virtual Centers. Define the username and password required to log in to the Virtual Center.

**Credential Tables (right pane)**

The following information describes the table columns for the credential lists. There are essentially two types of lists: CLI credentials and SNMP credentials. Most attributes are common to both types of lists; differences are noted.

Each row in the table is a separate credential.

Name	The name of the credential. This name is a label for your use in identifying the purpose of a credential. It is not used when accessing a device.
IP Ranges	The IP address patterns defined for this credential. VFrame compares a device IP address to the IP address patterns in this list to find a match. For more information about IP address patterns, see <a href="#">Understanding IP Address Patterns, page 4-3</a> .
User	The username defined for the credential.  The User field only appears for CLI, SNMPv3, Network Services CLI, LOM manager, NAS, or SAN Manager (Storage Manager) credentials.

Table 4-1 Credentials Tab (continued)

Element	Description
Read Community	The SNMP read community string for the credential. Even if the credential requires a write community string, only the read string is shown in the table. The Read Community field only appears for SNMPv1n2 credentials.
On Failure	Whether there is a stop flag defined for this credential.  When <b>Stop</b> appears in this field, if VFrame tries to use this credential when accessing a specific device and the credential fails, no additional credentials are tried. The stop flag takes effect only if VFrame tries the credential, that is, if the IP address of the device fits an IP address pattern in the credential.  If the field is blank, VFrame continues to the next credential if the credential fails.

## CLI Credential Dialog Box

Use the CLI Credential dialog box to create or modify credentials for logging in to an Ethernet switch or its service modules.

### How to Get to This Dialog Box

1. Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
2. In the Network dialog box, click the **Credentials** tab.
3. Click the **Network** or **Network Services** category, and then click the **CLI** or **Network Services CLI** tab.
4. Do one of the following:
  - Click **New** to create a new credential.
  - Choose a credential and click **Edit**, or double-click a credential.

### Related Topics

- [Configuring Network Credentials, page 4-6](#)
- [Configuring Network Services Credentials, page 4-7](#)
- [Understanding Device Credentials, page 4-1](#)
- [Troubleshooting Device Credentials, page 4-15](#)

## Field Reference

Table 4-2 CLI Credential Dialog Box

Element	Description
Name	<p>A name assigned to the credential. This name is to help you identify the purpose of a credential. It is not used when accessing a device.</p> <p>The name must be unique within the credentials list to which you are adding the credential.</p> <p>You cannot modify the name after you create the credential.</p>
IP Ranges	<p>A comma-separated list of IP address patterns. When VFrame searches for a credential for a device, it compares the device IP address to the IP address patterns entered here, and uses the credential if there is a match. You can use an asterisk (*) as a wildcard to match any number in an octet (for example, 10.100.10.*), or [x-y] to match a range of numbers (from x to y, for example, 10-20).</p> <p>For a more thorough explanation of IP address patterns, see <a href="#">Understanding IP Address Patterns, page 4-3</a>.</p>
User	The username configured on the switch.
Password Confirm Password	The user EXEC mode password configured for the username. Enter the password in both fields.
Enable Password Confirm Enable Password	The privileged EXEC (enable) mode password configured on the switch, if any. Enter the password in both fields.
If Credentials Fail	<p>Adds or removes a stop flag from the credential. From the drop-down list, you can:</p> <ul style="list-style-type: none"> <li>Choose the <b>Stop Trying Credentials</b> option to add a stop flag to the credential. When a stop flag is added to a credential, <b>Stop</b> appears in the On Failure field.</li> <li>Choose the <b>Try Additional Credentials</b> option to remove the stop flag from the credential.</li> </ul> <p>For information on how stop flags affect credential processing, see <a href="#">Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4</a>.</p>

## SNMPv1n2 Credential Dialog Box

Use the SNMPv1n2 dialog box to create or modify the SNMPv1/2 community strings for Ethernet switches or SAN fabric devices.

### How to Get to This Dialog Box

1. Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
2. In the Network dialog box, click the **Credentials** tab.
3. Click the **Network** or **Category** category, and then click the **SNMPv1n2** tab.
4. Do one of the following:

- Click **New** to create a new credential.
- Choose a credential and click **Edit**, or double-click a credential.

### Related Topics

- [Configuring Network Credentials, page 4-6](#)
- [Configuring SNMP Credentials for Fibre Channel Switches, page 4-8](#)
- [Understanding Device Credentials, page 4-1](#)
- [Troubleshooting Device Credentials, page 4-15](#)

### Field Reference

**Table 4-3** *SNMPv1n2 Credential Dialog Box*

Element	Description
Name	<p>A name assigned to the credential. This name is to help you identify the purpose of a credential. It is not used when accessing a device.</p> <p>The name must be unique within the credentials list to which you are adding the credential.</p> <p>You cannot modify the name after you create the credential.</p>
IP Ranges	<p>A comma-separated list of IP address patterns. When VFrame searches for a credential for a device, it compares the device IP address to the IP address patterns entered here, and uses the credential if there is a match. You can use an asterisk (*) as a wildcard to match any number in an octet (for example, 10.100.10.*), or [x-y] to match a range of numbers (from x to y, for example, 10-20).</p> <p>For a more thorough explanation of IP address patterns, see <a href="#">Understanding IP Address Patterns, page 4-3</a>.</p>
Read Community	The SNMP read community string. This is used for Ethernet device discovery and Fibre Channel switch inventory management.
Write Community (Storage only)	The SNMP write community string. This is required for Cisco MDS switch inventory management.
If Credentials Fail	<p>Adds or removes a stop flag from the credential. From the drop-down list, you can:</p> <ul style="list-style-type: none"> <li>• Choose the <b>Stop Trying Credentials</b> option to add a stop flag to the credential. When a stop flag is added to a credential, <b>Stop</b> appears in the On Failure field.</li> <li>• Choose the <b>Try Additional Credentials</b> option to remove the stop flag from the credential.</li> </ul> <p>For information on how stop flags affect credential processing, see <a href="#">Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4</a>.</p>

## SNMPv3 Credential Dialog Box

Use the SNMPv3 dialog box to create or modify the SNMPv3 authentication or privacy credentials for Ethernet switches or SAN fabric devices.

### How to Get to This Dialog Box

1. Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
2. In the Network dialog box, click the **Credentials** tab.
3. Click the **Network** or **Storage** category, and then click the **SNMPv3** tab.
4. Do one of the following:
  - Click **New** to create a new credential.
  - Choose a credential and click **Edit**, or double-click a credential.

### Related Topics

- [Configuring Network Credentials, page 4-6](#)
- [Configuring SNMP Credentials for Fibre Channel Switches, page 4-8](#)
- [Understanding Device Credentials, page 4-1](#)
- [Troubleshooting Device Credentials, page 4-15](#)

### Field Reference

**Table 4-4** *SNMPv3 Credential Dialog Box*

Element	Description
Name	<p>A name assigned to the credential. This name is to help you identify the purpose of a credential. It is not used when accessing a device.</p> <p>The name must be unique within the credentials list to which you are adding the credential.</p> <p>You cannot modify the name after you create the credential.</p>
IP Ranges	<p>A comma-separated list of IP address patterns. When VFrame searches for a credential for a device, it compares the device IP address to the IP address patterns entered here, and uses the credential if there is a match. You can use an asterisk (*) as a wildcard to match any number in an octet (for example, 10.100.10.*), or [x-y] to match a range of numbers (from x to y, for example, 10-20).</p> <p>For a more thorough explanation of IP address patterns, see <a href="#">Understanding IP Address Patterns, page 4-3</a>.</p>
User	The username configured on the Ethernet switch or Fibre Channel switch.
Authentication Password	The authentication password configured for the Ethernet switch or Fibre Channel switch. Enter the authentication password in both fields.
Authentication Confirm Password	

**Table 4-4** SNMPv3 Credential Dialog Box (continued)

Element	Description
Authentication Protocol	One of the following authentication protocols: <ul style="list-style-type: none"> <li>MD5—Provides authentication based on the HMAC-MD5 algorithm.</li> <li>SHA—Provides authentication based on the HMAC-SHA algorithm.</li> </ul>
AuthPriv security mode	Enables security mode, which provides encryption in addition to authentication.
Privacy Password Privacy Confirm Password	The privacy password configured for the Ethernet switch or Fibre Channel switch. Enter the privacy password in both fields.
Privacy Protocol	One of the following privacy protocols: <ul style="list-style-type: none"> <li>DES<sup>1</sup>—Provides encryption in addition to authentication based on the Data Encryption Standard.</li> <li>AES<sup>2</sup>—Provides encryption in addition to authentication based on the Advanced Encryption Standard.</li> </ul>
Validate Write Permission	Determines whether write permission for the user must be validated. When the check box is checked, validation is required. This check box applies only to storage credentials.
If Credentials Fail	Adds or removes a stop flag from the credential. From the drop-down list, you can: <ul style="list-style-type: none"> <li>Choose the <b>Stop Trying Credentials</b> option to add a stop flag to the credential. When a stop flag is added to a credential, <b>Stop</b> appears in the On Failure field.</li> <li>Choose the <b>Try Additional Credentials</b> option to remove the stop flag from the credential.</li> </ul> <p>For information on how stop flags affect credential processing, see <a href="#">Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4</a>.</p>

1. SAN fabric devices and Ethernet switches both support DES.

2. SAN fabric devices support AES, but Ethernet switches do not.

## NAS Credential Dialog Box

Use the NAS Credential dialog box to create or modify the NAS filer credentials.

### How to Get to This Dialog Box

1. Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
2. In the Network dialog box, click the **Credentials** tab.
3. Click the **Storage** category, and then click the **NAS** tab.
4. Do one of the following:
  - Click **New** to create a new credential.
  - Choose a credential and click **Edit**, or double-click a credential.

**Related Topics**

- [Configuring NAS Credentials, page 4-8](#)
- [Understanding Device Credentials, page 4-1](#)
- [Troubleshooting Device Credentials, page 4-15](#)

**Field Reference****Table 4-5 NAS Credential Dialog Box**

Element	Description
Name	<p>A name assigned to the credential. This name is to help you identify the purpose of a credential. It is not used when accessing a device.</p> <p>The name must be unique within the credentials list to which you are adding the credential.</p> <p>You cannot modify the name after you create the credential.</p>
IP Ranges	<p>A comma-separated list of IP address patterns. When VFrame searches for a credential for a device, it compares the device IP address to the IP address patterns entered here, and uses the credential if there is a match. You can use an asterisk (*) as a wildcard to match any number in an octet (for example, 10.100.10.*), or [x-y] to match a range of numbers (from x to y, for example, 10-20).</p> <p>For a more thorough explanation of IP address patterns, see <a href="#">Understanding IP Address Patterns, page 4-3</a>.</p>
User	(Optional) The username configured on the NAS filer.
Password Confirm Password	The password configured for the username. Enter the password in both fields.
If Credentials Fail	<p>Adds or removes a stop flag from the credential. From the drop-down list, you can:</p> <ul style="list-style-type: none"> <li>• Choose the <b>Stop Trying Credentials</b> option to add a stop flag to the credential. When a stop flag is added to a credential, <b>Stop</b> appears in the On Failure field.</li> <li>• Choose the <b>Try Additional Credentials</b> option to remove the stop flag from the credential.</li> </ul> <p>For information on how stop flags affect credential processing, see <a href="#">Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4</a>.</p>

## SAN Manager Credential Dialog Box

Use the SAN Manager Credential dialog box to enter the Storage Manager credentials.

**How to Get to This Dialog Box**

1. Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
2. In the Network dialog box, click the **Credentials** tab.
3. Click the **Storage** category, and then click the **SAN Manager** tab.

4. Do one of the following:
  - Click **New** to create a new credential.
  - Choose a credential and click **Edit**, or double-click a credential.

#### Related Topics

- [Configuring Storage Manager Credentials, page 4-10](#)
- [Understanding Device Credentials, page 4-1](#)
- [Troubleshooting Device Credentials, page 4-15](#)

#### Field Reference

**Table 4-6 SAN Manager Credential Dialog Box**

Element	Description
Name	<p>A name assigned to the credential. This name is to help you identify the purpose of a credential. It is not used when accessing a device.</p> <p>The name must be unique within the credentials list to which you are adding the credential.</p> <p>You cannot modify the name after you create the credential.</p>
IP Ranges	<p>A comma-separated list of IP address patterns. When VFrame searches for a credential for a device, it compares the device IP address to the IP address patterns entered here, and uses the credential if there is a match. You can use an asterisk (*) as a wildcard to match any number in an octet (for example, 10.100.10.*), or [x-y] to match a range of numbers (from x to y, for example, 10-20).</p> <p>For a more thorough explanation of IP address patterns, see <a href="#">Understanding IP Address Patterns, page 4-3</a>.</p>
User	(Optional) The username configured on the storage manager.
Password	The password configured for the username. Enter the password in both fields.
Confirm Password	
If Credentials Fail	<p>Adds or removes a stop flag from the credential. From the drop-down list, you can:</p> <ul style="list-style-type: none"> <li>• Choose the <b>Stop Trying Credentials</b> option to add a stop flag to the credential. When a stop flag is added to a credential, <b>Stop</b> appears in the On Failure field.</li> <li>• Choose the <b>Try Additional Credentials</b> option to remove the stop flag from the credential.</li> </ul> <p>For information on how stop flags affect credential processing, see <a href="#">Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4</a>.</p>

## Brocade CLI Credential Dialog Box

Use the Brocade CLI Credential dialog box to enter the Brocade SAN switch credentials.

### How to Get to This Dialog Box

1. Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
2. In the Network dialog box, click the **Credentials** tab.
3. Click the **Storage** category, and then click the **Brocade CLI** tab.
4. Do one of the following:
  - Click **New** to create a new credential.
  - Choose a credential and click **Edit**, or double-click a credential.

### Related Topics

- [Configuring Storage Manager Credentials, page 4-10](#)
- [Understanding Device Credentials, page 4-1](#)
- [Troubleshooting Device Credentials, page 4-15](#)

### Field Reference

**Table 4-7** Brocade CLI Credential Dialog Box

Element	Description
Name	<p>A name assigned to the credential. This name is to help you identify the purpose of a credential. It is not used when accessing a device.</p> <p>The name must be unique within the credentials list to which you are adding the credential.</p> <p>You cannot modify the name after you create the credential.</p>
IP Ranges	<p>A comma-separated list of IP address patterns. When VFrame searches for a credential for a device, it compares the device IP address to the IP address patterns entered here, and uses the credential if there is a match. You can use an asterisk (*) as a wildcard to match any number in an octet (for example, 10.100.10.*), or [x-y] to match a range of numbers (from x to y, for example, 10-20).</p> <p>For a more thorough explanation of IP address patterns, see <a href="#">Understanding IP Address Patterns, page 4-3</a>.</p>
User	The username configured on the Brocade SAN switch.

**Table 4-7 Brocade CLI Credential Dialog Box (continued)**

Element	Description
Password Confirm Password	The password configured for the username. Enter the password in both fields.
If Credentials Fail	<p>Adds or removes a stop flag from the credential. From the drop-down list, you can:</p> <ul style="list-style-type: none"> <li>Choose the <b>Stop Trying Credentials</b> option to add a stop flag to the credential. When a stop flag is added to a credential, <b>Stop</b> appears in the On Failure field.</li> <li>Choose the <b>Try Additional Credentials</b> option to remove the stop flag from the credential.</li> </ul> <p>For information on how stop flags affect credential processing, see <a href="#">Understanding How to Organize a Credentials List and to Use Stop Flags</a>, page 4-4.</p>

## LOM Manager Credential Dialog Box

Use the LOM Manager Credential dialog box to create or modify the LOM manager credentials.

### How to Get to This Dialog Box

1. Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
2. In the Network dialog box, click the **Credentials** tab.
3. Click the **Server** category, and then click the **LOM Manager** tab.
4. Do one of the following:
  - Click **New** to create a new credential.
  - Choose a credential and click **Edit**, or double-click a credential.

### Related Topics

- [Configuring Server Credentials](#), page 4-11
- [Understanding Device Credentials](#), page 4-1
- [Troubleshooting Device Credentials](#), page 4-15

## Field Reference

Table 4-8 LOM Manager Credential Dialog Box

Element	Description
Name	<p>A name assigned to the credential. This name is to help you identify the purpose of a credential. It is not used when accessing a device.</p> <p>The name must be unique within the credentials list to which you are adding the credential.</p> <p>You cannot modify the name after you create the credential.</p>
IP Ranges	<p>A comma-separated list of IP address patterns. When VFrame searches for a credential for a device, it compares the device IP address to the IP address patterns entered here, and uses the credential if there is a match. You can use an asterisk (*) as a wildcard to match any number in an octet (for example, 10.100.10.*), or [x-y] to match a range of numbers (from x to y, for example, 10-20).</p> <p>For a more thorough explanation of IP address patterns, see <a href="#">Understanding IP Address Patterns, page 4-3</a>.</p>
User	<p>The username configured on the LOM manager.</p> <p>If you are using VFrame as the LOM manager, the username is <b>macrouser</b>.</p>
Password Confirm Password	<p>The password configured for the username. Enter the password in both fields.</p>
If Credentials Fail	<p>Adds or removes a stop flag from the credential. From the drop-down list, you can:</p> <ul style="list-style-type: none"> <li>Choose the <b>Stop Trying Credentials</b> option to add a stop flag to the credential. When a stop flag is added to a credential, <b>Stop</b> appears in the On Failure field.</li> <li>Choose the <b>Try Additional Credentials</b> option to remove the stop flag from the credential.</li> </ul> <p>For information on how stop flags affect credential processing, see <a href="#">Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4</a>.</p>

## LOM Credential Dialog Box

Use the LOM Credential dialog box to create or modify the credentials for server LOM interfaces. You can enter credentials for both application and model servers.

### How to Get to This Dialog Box

1. Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
2. In the Network dialog box, click the **Credentials** tab.
3. Click the **Server** category, and then click the **LOM** tab.

4. Do one of the following:
  - Click **New** to create a new credential.
  - Choose a credential and click **Edit**, or double-click a credential.

#### Related Topics

- [Configuring Server Credentials, page 4-11](#)
- [Understanding Device Credentials, page 4-1](#)
- [Troubleshooting Device Credentials, page 4-15](#)

#### Field Reference

**Table 4-9 LOM Credential Dialog Box**

Element	Description
Name	<p>A name assigned to the credential. This name is to help you identify the purpose of a credential. It is not used when accessing a device.</p> <p>The name must be unique within the credentials list to which you are adding the credential.</p> <p>You cannot modify the name after you create the credential.</p>
IP Ranges	<p>A comma-separated list of IP address patterns. When VFrame searches for a credential for a device, it compares the device IP address to the IP address patterns entered here, and uses the credential if there is a match. You can use an asterisk (*) as a wildcard to match any number in an octet (for example, 10.100.10.*), or [x-y] to match a range of numbers (from x to y, for example, 10-20).</p> <p>For a more thorough explanation of IP address patterns, see <a href="#">Understanding IP Address Patterns, page 4-3</a>.</p>
User	The username configured on the LOM interface, for example, root.
Password	The password configured for the username. Enter the password in both fields.
Confirm Password	
If Credentials Fail	<p>Adds or removes a stop flag from the credential. From the drop-down list, you can:</p> <ul style="list-style-type: none"> <li>• Choose the <b>Stop Trying Credentials</b> option to add a stop flag to the credential. When a stop flag is added to a credential, <b>Stop</b> appears in the On Failure field.</li> <li>• Choose the <b>Try Additional Credentials</b> option to remove the stop flag from the credential.</li> </ul> <p>For information on how stop flags affect credential processing, see <a href="#">Understanding How to Organize a Credentials List and to Use Stop Flags, page 4-4</a>.</p>

## Virtual Machine Manager Credential Dialog Box

Use the Virtual Machine Manager Credential dialog box to create or modify the Virtual Center credentials.

### How to Get to This Dialog Box

1. Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
2. In the Network dialog box, click the **Credentials** tab.
3. Click the **Virtual Machine Management** category, and then click the **Virtual Machine Managers** tab.
4. Do one of the following:
  - Click **New** to create a new credential.
  - Choose a credential and click **Edit**, or double-click a credential.

### Related Topics

- [Understanding Device Credentials, page 4-1](#)
- [Troubleshooting Device Credentials, page 4-15](#)

### Field Reference

**Table 4-10** *Virtual Machine Manager Credential Dialog Box*

Element	Description
Name	<p>A name assigned to the credential. This name is to help you identify the purpose of a credential. It is not used when accessing a device.</p> <p>The name must be unique within the credentials list to which you are adding the credential.</p> <p>You cannot modify the name after you create the credential.</p>
IP Ranges	<p>A comma-separated list of IP address patterns. When VFrame searches for a credential for a device, it compares the device IP address to the IP address patterns entered here, and uses the credential if there is a match. You can use an asterisk (*) as a wildcard to match any number in an octet (for example, 10.100.10.*), or [x-y] to match a range of numbers (from x to y, for example, 10-20).</p> <p>For a more thorough explanation of IP address patterns, see <a href="#">Understanding IP Address Patterns, page 4-3</a>.</p>

**Table 4-10** Virtual Machine Manager Credential Dialog Box (continued)

Element	Description
User	The username configured on the Virtual Center.
Password Confirm Password	The password configured for the username. Enter the password in both fields.
If Credentials Fail	<p>Adds or removes a stop flag from the credential. From the drop-down list, you can:</p> <ul style="list-style-type: none"> <li>Choose the <b>Stop Trying Credentials</b> option to add a stop flag to the credential. When a stop flag is added to a credential, <b>Stop</b> appears in the On Failure field.</li> <li>Choose the <b>Try Additional Credentials</b> option to remove the stop flag from the credential.</li> </ul> <p>For information on how stop flags affect credential processing, see <a href="#">Understanding How to Organize a Credentials List and to Use Stop Flags</a>, page 4-4.</p>

## Credentials Shortcut Menu Options

Use the credentials shortcut menu options to perform tasks such as modifying or deleting a selected device credential, or adding or removing a stop flag on a selected device credential.

### How to Open the Shortcut Menu

1. Choose **Tools > VFrame Administration > Network** to open the Network dialog box.
2. In the Network dialog box, click the **Credentials** tab.
3. Choose a credential and right-click to display the menu options.

### Related Topics

- [Understanding Device Credentials](#), page 4-1
- [Understanding How to Organize a Credentials List and to Use Stop Flags](#), page 4-4
- [Editing or Modifying Device Credentials](#), page 4-13
- [Deleting Device Credentials](#), page 4-14
- [Rearranging the Device Credentials List and Using Stop Flags](#), page 4-14

### Field Reference

**Table 4-11** Device Credentials Shortcut Menu Options

Element	Description
Edit	Modify the selected credentials.
Delete	Delete the selected credentials.
Up arrow	Move the row up in the credentials list.
Down arrow	Move the row down in the credentials list.