Authenticating Using RADIUS

RADIUS provides authentication, accounting, and authorization functions. The appliance supports authentication using the following RADIUS servers: FreeRADIUS, Microsoft, Cisco, and Funk.

You must be a superuser to configure admin accounts and RADIUS server properties on the appliance.

When you configure the appliance to authenticate administrators using a RADIUS server, the appliance acts similarly to a network access server (NAS), which is a RADIUS client that sends authentication and accounting requests to the RADIUS server. Figure 4.3 illustrates the authentication process.

**Figure 4.3 Authentication using a RADIUS server**

![Authentication process diagram]

**Remote RADIUS Authentication**

When you configure the appliance for remote authentication with a RADIUS server, you must specify the authentication method of the RADIUS server. Specify PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol).

With PAP, the client sends the user name and password in clear text to the appliance. The appliance uses a shared secret to encrypt the password and sends it to the RADIUS server in an Access-Request packet. The RADIUS server uses the shared secret to decrypt the password. If the decrypted password matches a password in its database, the user is successfully authenticated and allowed to log in.

With CHAP, when the client tries to log in, it sends its user name and password to the appliance. The appliance then creates an MD5 hash of the password together with a random number that the appliance generates. It then sends the random number, user name, and hash to the RADIUS server in an Access-Request package. The RADIUS server takes the password that matches the user name from its database and creates its own MD5 hash of the password and random number that it received. If the hash that the RADIUS server generates matches the hash that it received from the appliance, then the user is successfully authenticated and allowed to log in.

To configure the appliance to authenticate administrators using a RADIUS server, you must configure admin accounts and groups for these administrators on the RADIUS server. Then, on the appliance, you must do the following:

- Configure an authentication server group for RADIUS.
- Define admin groups and specify their privileges and settings. The names must match admin group names defined on the RADIUS server. The appliance applies these privileges and settings to users that belong to those groups on the RADIUS server. See About Admin Groups for information about defining admin groups.
- If there are no admin groups defined on the RADIUS server, designate an admin group as the default group. See About Admin Groups for information about defining a default admin group.
- Add the RADIUS service to the list of admin authentication services in the admin policy, and add the admin groups that match those on the RADIUS server. See Defining the Authentication Policy for more information about configuring admin policy.

**Configuring a RADIUS Authentication Server Group**

You can add multiple RADIUS servers to the group for redundancy. When you do, the appliance tries to connect to the first RADIUS server on the list and if the server does not respond within the maximum retransmission limit, then it tries the next RADIUS server on the list.

After you add a RADIUS server to the appliance, you can validate the configuration. The appliance uses a pre-defined username and password when it tests the connection to the RADIUS server. The pre-defined user name is "Infoblox_test_user" and the password is "Infoblox_test_password". Do not use these as your administrator username and password.

To configure a RADIUS authentication server group on the appliance:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Click the Add icon in the RADIUS Services subtab.
3. In the Add RADIUS Authentication Service wizard, complete the following:
   - Name: Enter the name of the server group.
• **RADIUS Servers**: Click the Add icon and enter the following:
  - **Server Name or IP Address**: Enter the FQDN or the IP address of the RADIUS server that is used for authentication.
  - **Comment**: Enter additional information about the RADIUS server.
  - **Authentication Port**: The destination port on the RADIUS server. The default is 1812. This field is required only if you do not enable accounting on the RADIUS server. This field is not required if you enable accounting to configure an accounting-only RADIUS server.
  - **Authentication Type**: Select the authentication method of the RADIUS server from the drop-down list. You can specify either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol). The default is PAP.
  - **Shared Secret**: Enter the shared secret that the appliance and the RADIUS server use to encrypt and decrypt their messages. This shared secret is a value that is known only to the appliance and the RADIUS server.
  - **Enable Accounting**: Select this to enable RADIUS accounting for the server so you can track an administrator’s activities during a session. When you enable accounting, you must enter a valid port number in the **Accounting Port** field.
  - **Accounting Port**: The destination port on the RADIUS server. The default is 1813.
  - **Connect through Management Interface**: Select this so that the appliance uses the MGMT port for administrator authentication communications with just this RADIUS server.
  - **Disable server**: Select this to disable the RADIUS server if, for example, the connection to the server is down and you want to stop the appliance from trying to connect to this server.
  - **Click Test** to test the configuration. If the appliance connects to the RADIUS server using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the RADIUS server, the appliance displays a message indicating an error in the configuration.

  • **Authentication**: Optionally, modify the authentication settings. These settings apply to all RADIUS servers that you configure on the appliance.
    - **Timeout(s)**: Specify the number of seconds that the appliance waits for a response from the RADIUS server.
    - **Retries**: Specify how many times the appliance attempts to contact an authentication RADIUS server. The default is 5.
    - If you have configured multiple RADIUS servers for authentication and the appliance fails to contact the first server in the list, it tries to contact the next server, and so on.

  • **Accounting**: Optionally, modify the Accounting settings.
    - **Timeout(s)**: Specify the number of seconds that the appliance waits for a response from the RADIUS server.
    - **Retries**: Specify how many times the appliance attempts to contact an accounting RADIUS server. The default is 1000.
    - **Mode**: Specifies how the appliance contacts the RADIUS servers. The default is Ordered List. Do not change this value; Ordered List is the only mode that the appliance uses when it uses a RADIUS server group to authenticate remote admins. In this mode, the appliance always selects the first RADIUS server in the list when it sends an authentication request. It queries the next server only when the first server is considered down.
    - **Comment**: Enter useful information about the RADIUS service.
    - **Disable**: Select this to disable RADIUS authentication for the servers listed in the table.

4. **Save the configuration.**

### Managing the RADIUS Server List

When you add multiple RADIUS servers, the appliance lists the servers in the order you added them. This list also determines the order in which the appliance attempts to contact a RADIUS server. You can change the order of the list, as follows:

1. From the **Administration** tab, click the **Authentication Server Groups** tab -> **RADIUS Services** subtab, select the **server_group** check box and click the **Edit** icon.
2. In the **RADIUS Servers** table, do the following:
   - To move a server up the list, select it and click the up arrow.
   - To move a server down the list, select it and click the down arrow.
   - You can also delete a RADIUS server by selecting a RADIUS server from the RADIUS Servers table and clicking the Delete icon.
3. **Save the configuration.**

### Disabling RADIUS Servers on Multi-Grid Master

You can disable a RADIUS server if, for example, the connection to the server is down and you want to stop the appliance from trying to connect to this server.

To disable a RADIUS server:

1. From the **Administration** tab, click the **Authentication Server Groups** tab -> **RADIUS Services** subtab, select the **server_group** check box and click the **Edit** icon.
2. In the **RADIUS Service** editor, select the check box of the server you want to disable in the RADIUS Servers section, and then click the **Edit** icon.
3. In the RADIUS Servers section, select **Disable**.
4. **Save the configuration.**
Configuring Remote RADIUS Servers

In addition to setting up the appliance to communicate with a RADIUS server, you must also set up the remote RADIUS server to communicate with the appliance.

**Note:** If you have two Infoblox appliances in an HA pair, enter both the members of the HA pair as separate access appliances and use the LAN or MGMT IP address of both appliances (not the VIP address), if configured.

Depending on your particular RADIUS server, you can configure the following RADIUS server options to enable communication with the appliance:

- Authentication Port
- Accounting Port
- Domain Name/IP Address of the appliance
- Shared Secret Password
- Vendor Types

**Configuring Admin Groups on the Remote RADIUS Server**

Infoblox supports admin accounts on one or more RADIUS servers.

To set up admins and associate them with an admin group on a remote RADIUS server, do the following:

- Import Infoblox VSAs (vendor-specific attributes) to the dictionary file on the RADIUS server
- For third-party RADIUS servers, import the Infoblox vendor file (the Infoblox vendor ID is 7779)
- Define a local admin group on the appliance (or use an existing group)
- Define a remote admin group—with the same name as the group defined on the appliance—on the RADIUS server
- Associate one or more remote admin accounts on the RADIUS server with the remote admin group

Refer to the documentation for your RADIUS server for more information.

**Configuring Admin Accounts on the Remote RADIUS Server**

To set up remote admin accounts on a RADIUS server and apply the privileges and properties of the admin group on the appliance, do the following:

- Define the admin group on the appliance, and then add it to the admin policy. Note that the names of the remote admin group and the admin group on the appliance must match. You can also define a default admin group. See Defining the Authentication Policy for more information on configuring admin policies and remote admin group lists.
- On the RADIUS server:
  - Create one or more admin accounts.
  - Add and activate a policy for the admin accounts, but do not associate the policy with a policy group that contains an infoblox-group-info attribute.

When an administrator whose account is stored on a RADIUS server attempts to log in to a appliance, the appliance forwards the user name and password for authentication to the RADIUS server. When the server successfully authenticates the administrator and it responds to the appliance without specifying an admin group, the appliance applies the privileges and properties of the default admin group to that administrator. Refer to the documentation for your RADIUS server for more information.

**Authorization Groups Using RADIUS**

You can specify authorization privileges for an admin group on the appliance only. The appliance ignores authorization settings from the RADIUS server. Therefore, you must configure all admin groups on the appliance, regardless of where the admin accounts that belong to those groups are stored—on the appliance or on the RADIUS server. For information about specifying superuser and limited-access authorization privileges, see Creating Superuser Admin Groups and Creating Limited-Access Admin Groups.

Then you must add those admin groups to the authentication policy. For more information, see Defining the Authentication Policy.

**Accounting Activities Using RADIUS**

You can enable the accounting feature on the RADIUS server to track whether an administrator has initiated a session. After an administrator successfully logs in, the appliance sends an Accounting-Start packet to the RADIUS server. For information, see Managing the RADIUS Server Li
st.