

Deployment Guide

NIOS Integration with RADIUS



Table of Contents

Overview	2
Authentication	2
Authentication Prerequisites	2
Workflow	2
Enabling Radius Authentication	3
Configuring Remote RADIUS Servers	3
Configuring a RADIUS Authentication Server Group	3
Defining the Authentication Policy	6
Configuring a List of Remote Admin Groups	8
Test the configuration	9

Overview

Infoblox NIOS supports the following authentication methods: local database, RADIUS, Active Directory, LDAP, and TACACS+. NIOS can use any combination of these authentication methods.

Depending on where admin user credentials are stored, you can configure the NIOS appliance to authenticate admins locally or remotely. When you configure the authentication type as "local," NIOS authenticates admins against its local database. When you configure the authentication type as "remote," NIOS authenticates admins whose user credentials are stored remotely on authentication servers, such as RADIUS servers, AD domain controllers, LDAP servers, or TACACS+ servers.

This deployment guide covers remote authentication for Administrators using supported RADIUS Servers.

Authentication

NIOS can authenticate admins whose user credentials are stored remotely on RADIUS servers. It requires authentication server groups to be configured. For example, you can create a server group for RADIUS servers. Then in the admin authentication policy, you can list which authentication server groups to use and in what order.

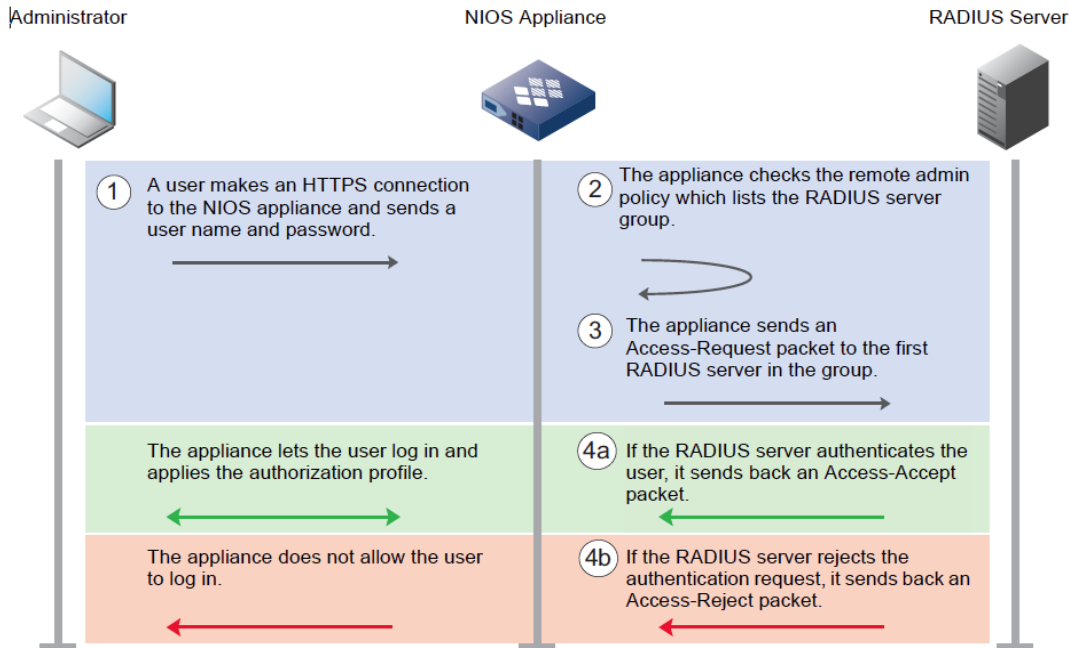
Authentication Prerequisites

A RADIUS Server (FreeRadius is used in the examples provided in this guide) configured to accept Access Request packets from NIOS. The following options must be configured for NIOS to communicate with the RADIUS Server:

- RADIUS server FQDN or IP address
- Authentication Port
- Authentication Type
- Shared Secret
- Accounting Port

Workflow

1. User connects to NIOS via https and sends in the username and password.
2. NIOS checks the remote admin policy which lists the Radius Server group.
3. NIOS sends an Access Request packet to the server ordered first in the Radius Server group.
4. Either of the following two possibilities will occur next:
 - a. If NIOS receives an Access Accept packet from the Radius server and can match the user to a group configured in NIOS, it lets the user log in and applies the authorization profile.
 - b. NIOS does not allow the user to log in if it receives an Access Reject packet from the Radius Server.



Enabling Radius Authentication

To enable authentication of user logins in NIOS with Radius, common configuration steps are provided in the sections below.

Configuring Remote RADIUS Servers

The remote RADIUS server must also be configured to communicate with NIOS. In the following example, we set the RADIUS server to allow access-request packets from RADIUS clients in 10.0.0.0/8 subnet with shared secret "infoblox". In order to achieve this, edit the **clients.conf** file and add the following:

```
client anybody {
  ipaddr = 10.0.0.0
  netmask = 8
  secret = infoblox
  require_message_authenticator = no
  nastype = other
}
```

Save the file.

User names and passwords are stored in the **Users** file, which the RADIUS server uses to authenticate users. In our example we have added a user named **user1** with password **test** in the **Users** file.

This is accomplished by editing the **Users** file and adding the following content:

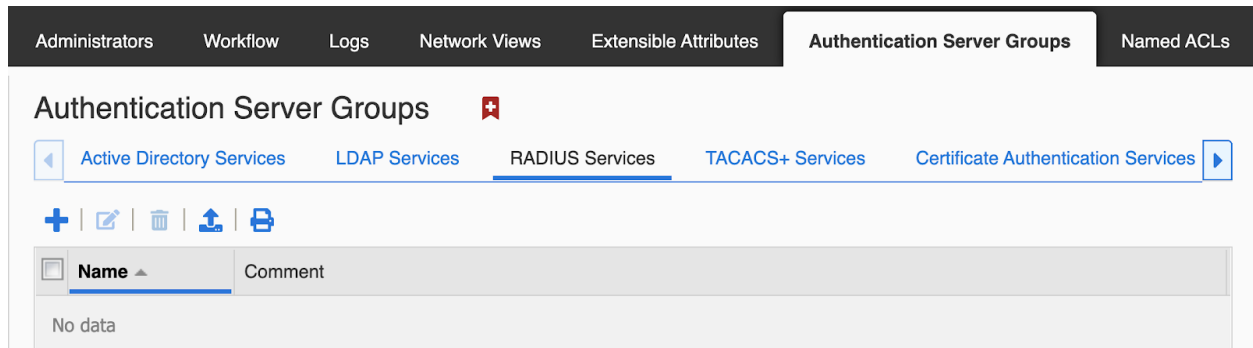
```
user1 Cleartext-Password := "test"
```

Configuring a RADIUS Authentication Server Group

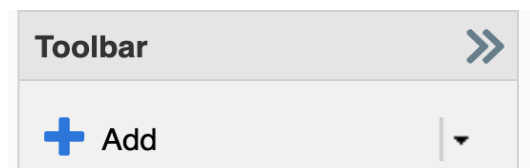
RADIUS servers used by NIOS to authenticate users login are configured under Administration -> Authentication Server Groups in the NIOS Grid Manager GUI. For redundancy, multiple RADIUS servers can be added to an authentication group. NIOS attempts to use the servers in the order that they have been configured.

To add a RADIUS Authentication Server Group:

Go to **Administration > Authentication Server Groups > RADIUS Services**.



Click the **Add > RADIUS Service** from **Toolbar**.




- Active Directory Service
- LDAP Service
- RADIUS Service
- TACACS+ Service
- Certificate Authentication Service
- SAML Authentication Service

Type a name for the group in the Name field. In our example we used **Radius-Group**. Click **+**.

Add RADIUS Authentication Service > Step 1 of 1

*Name

radius-group 

*RADIUS Servers



<input type="checkbox"/>	Server	Comment	Accounting	Disabled
No data				

Enter IP address or FQDN of your RADIUS server and authentication port. By default the RADIUS server port **1812** is used for authentication.

Select the Authentication type from the list as **PAP** or **CHAP**. Default is PAP.

Enter Shared secret as defined in the **clients** file in **Shared Secret** field.

Click **Test** to see if NIOS can establish successful connection with the RADIUS server. A message in blue is displayed upon successful connection.

Add RADIUS Authentication Service > Step 1 of 1

*RADIUS Servers



Add RADIUS Server

*Server Name or IP Address: 1.2.3.4

Comment:

*Authentication Port: 1812

Authentication Type: PAP

*Shared Secret:

Enable Accounting Accounting Port: 1813

Connect through Management Interface

Disable Server

Click **Add**.

Optionally, modify the Authentication settings and Accounting settings

Optionally, modify the Recovery Interval settings.

Add RADIUS Authentication Service > Step 1 of 1

*Name

*RADIUS Servers

Server	Comment	Accounting	Disabled
<input type="checkbox"/> 1.2.3.4		No	No

Authentication *Timeout(s) Seconds *Retries

Accounting *Timeout(s) Seconds *Retries

Note: Timeouts and Retries are per server

Mode

*Recovery Interval Seconds

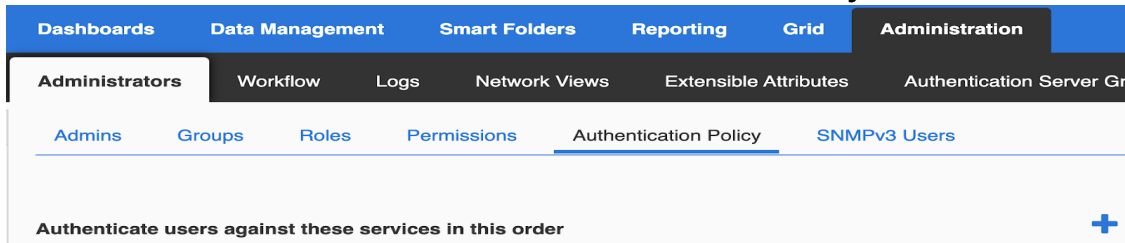
Click **Save & Close**.

Defining the Authentication Policy

The authentication policy defines which Authentication Server Groups the appliance uses to authenticate users and lists the local admin groups that the remote admin groups map to. By default, the appliance provides the “Local Admin” service for authenticating users against the local database. You cannot modify or delete this default service.

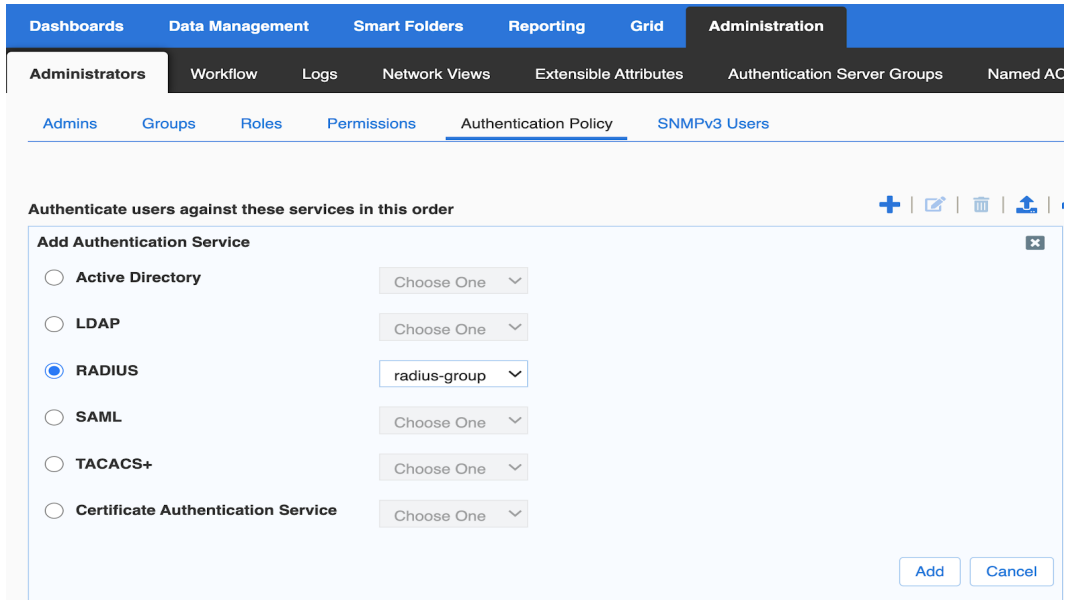
To create remote authentication policy:

Go to **Administration > Administrators > Authentication Policy**.

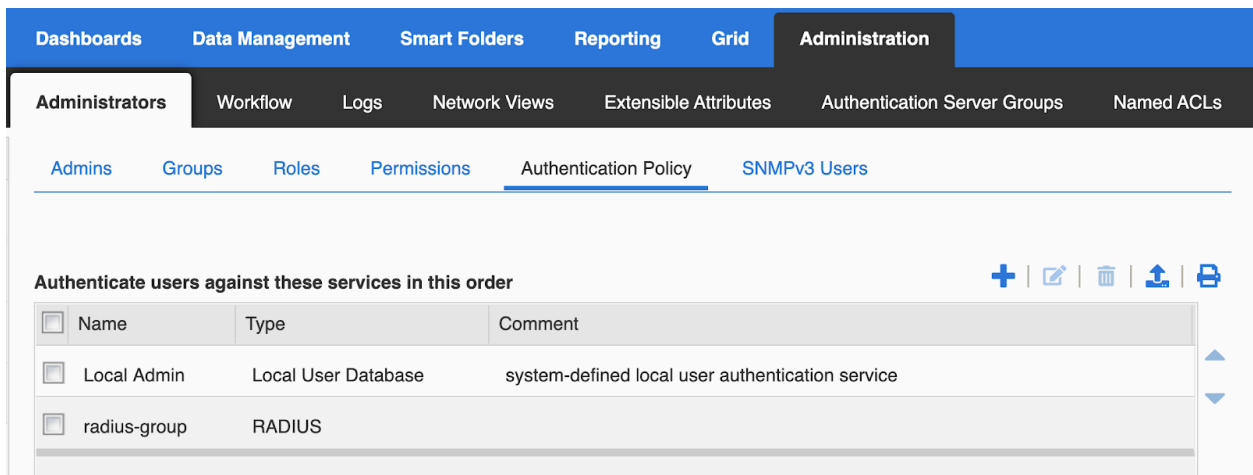


Click **+**.

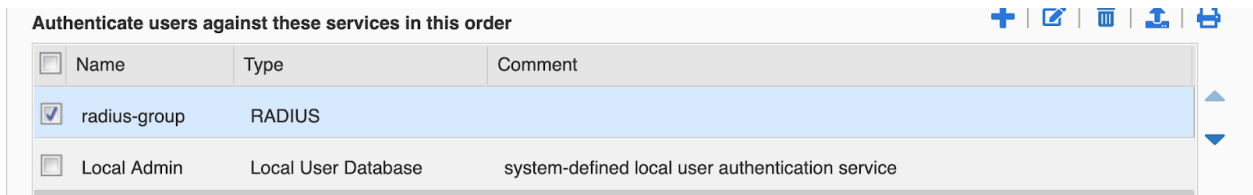
Under the **Add Authentication Service** section, select **RADIUS** and choose the appropriate RADIUS authentication Server Group from the drop-down menu.



Click **Add**.
The newly created policy will be ordered after the default **Local Admin** policy.



The order can be customized as required. If you want NIOS to always authenticate users via the RADIUS Server first, please move the RADIUS policy above the Local Admin policy, you can reorder the list by selecting a group and using the arrow keys to move it up or down the list.



As a best practice, Local Admin policy may be placed before Radius policy.

Configuring a List of Remote Admin Groups

Users authenticated via RADIUS are considered remote admins. In order for NIOS to assign a remote admin to the correct group, you must list the admin groups in the local database, which match the remote admin groups. You can also define a default admin group to which NIOS assigns remote users to if no matches are found.

The appliance matches a remote admin to a group in the order the groups are listed. When the appliance receives information that an admin belongs to one or more groups, the appliance assigns the user to the first group in the list that matches. It assigns the admin to the default group, if specified, if the authentication server returns no groups, or if the appliance does not find a group in the local database that matches the group returned by the authentication server.

To configure the remote admin group list go to **Administration > Administrators > Authentication Policy**. In the **Authentication Server Groups is the authority for** section, keep the default selection **(Remote users, their passwords and their groups ownership)**.

In order for the appliance to assign a remote admin to the correct group, you must list the admin groups in the local database that match the remote admin groups. The appliance matches a remote admin to a group in the order the groups are listed.

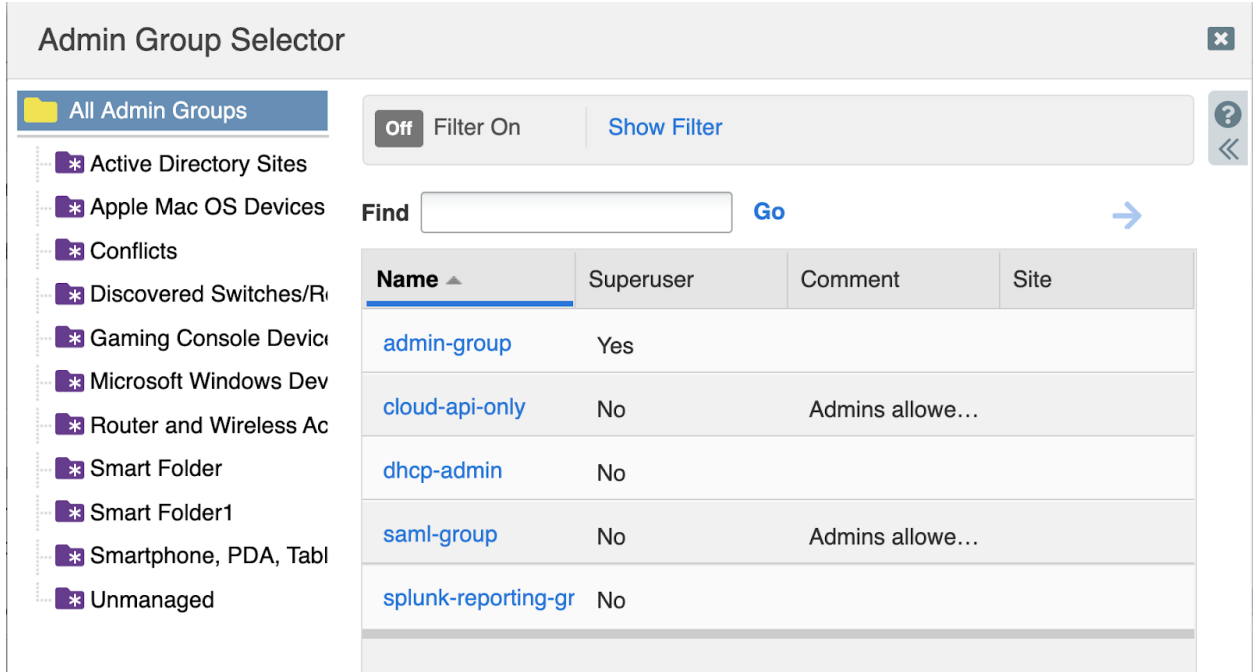
Note: The group you are going to add must already be there under **Administration > Administrators > Groups** tab.

Complete the following to configure the remote admin group list:

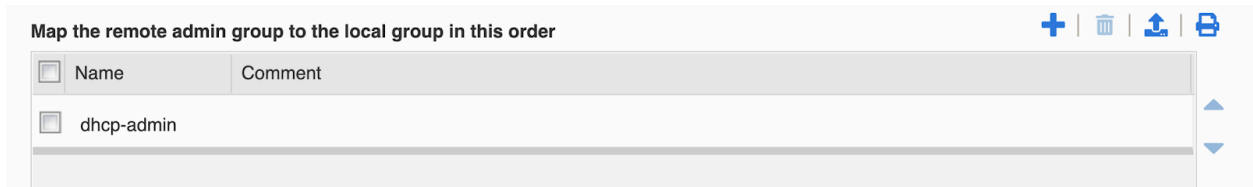
Click the + icon in **Map the remote admin group to the local group in this order** to add an admin group to the list.



In our example we added group **dhcp-admin** by selecting it in **Admin Group Selector**.

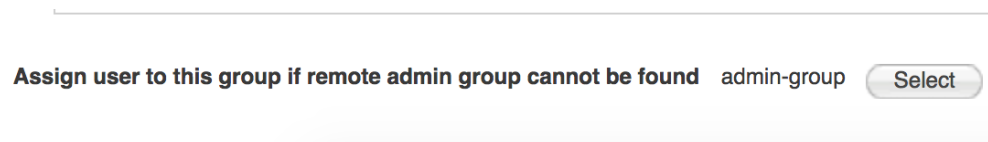


Once selected the group appears in the **Map the remote admin group to the local group in this order** section:



You can also define a default admin group to which NIOS assigns remote users with no admin groups listed. In order to select a default admin group, click **Select** next to **Assign user to this group if remote admin group cannot be found**.

In our example we selected **admin-group** from **Admin Group Selector**:

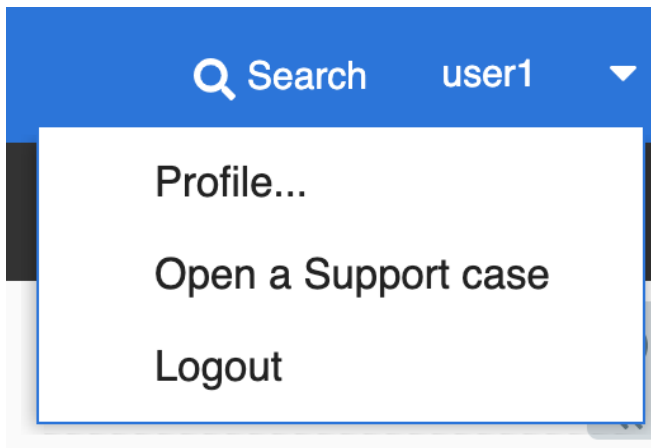


Test the configuration

To verify if the remote authentication via RADIUS Server is working, login using the username and password that is in the **users** file on the RADIUS Server.

In our example the username is user1 with password test.

Once logged in, go to the user profile:



Once you click on **Profile** under the active username, the **User Profile** window pops up.

A screenshot of the 'User Profile' window. The window title is 'User Profile'. It contains the following fields and values:

- Name: user1
- Type: Remote
- Group: admin-group
- Email Address: (empty text box with an '@' icon)
- Table Size: 20
- Default Dashboard: Tasks (dropdown menu)
- Maximum Widgets per Dashboard: 10
- Time Zone: Auto-detect time zone (dropdown menu)

There is also a 'Last Login' box showing '2020-12-30 10:50:55 PST'. At the bottom, there are 'Cancel' and 'Save & Close' buttons.

The **User Profile** window shows the user to be of type **Remote** along with its group membership. This verifies the user is authenticated remotely via RADIUS Server.

Users that are authenticated against the local database are of type Local.



Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com



© 2021 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).