



Integration Guide

Centrify® Identify Service (CIS)

About This Guide

Guide Type

Documented Integration — WatchGuard or a Technology Partner has provided documentation demonstrating integration.

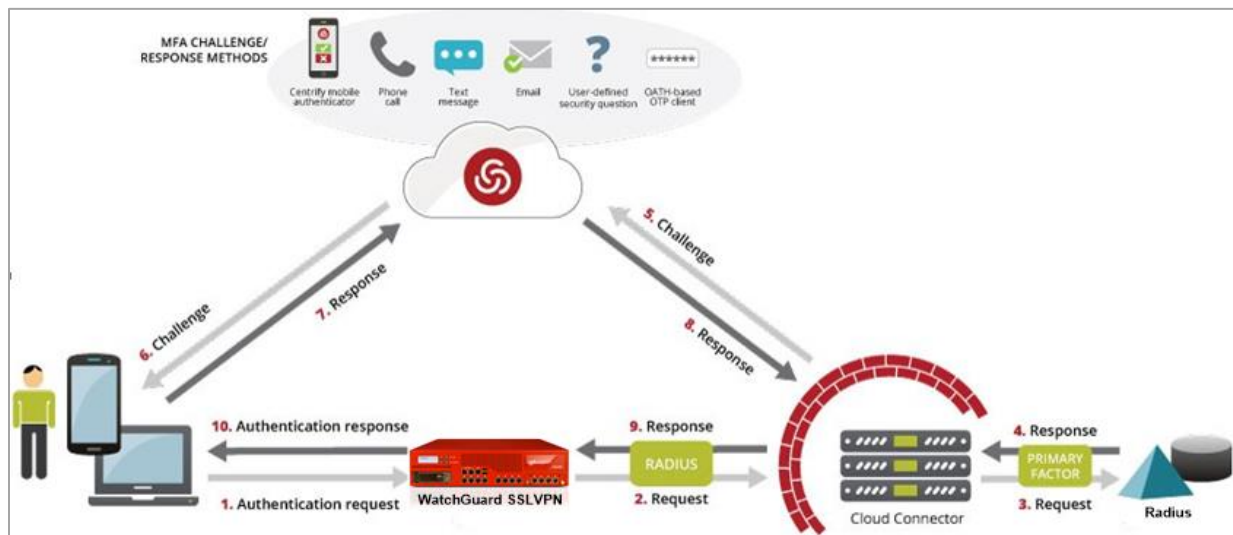
Guide Details

WatchGuard provides integration instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a third-party product, see the documentation and support resources for that product.

Centrify Identify Service Integration Overview

Centrify® Identify Service provides cloud-based authentication through the RADIUS protocol. This document describes how to integrate Centrify two-factor authentication with a WatchGuard Firebox and the WatchGuard Mobile VPN with SSL client.

This image shows the dataflow of a multi-factor authentication transaction with the WatchGuard Firebox.



Platform and Software

The hardware and software used to complete the steps outlined in this document include:

- Firebox with Fireware v11.11.x installed
- Centrify Identify Service (CIS)
- Centrify Cloud Connector installed on Windows Server 2012 R2

Configure Centrify Identify Service (CIS)

To configure CIS two-factor authentication to work with a Firebox and the Mobile VPN with SSL client, you must:

- Create user accounts in CIS
- Install a cloud connector on a host computer
- Configure Centrify RADIUS support
- Configure an authentication profile in CIS
- Configure a RADIUS client in CIS to use a WatchGuard Firebox
- Configure a security policy in CIS based on RADIUS
- Configure the Firebox to use RADIUS server authentication
- Add users to the Firebox who use RADIUS authentication

- Configure Mobile VPN with SSL with RADIUS authentication in the Firebox

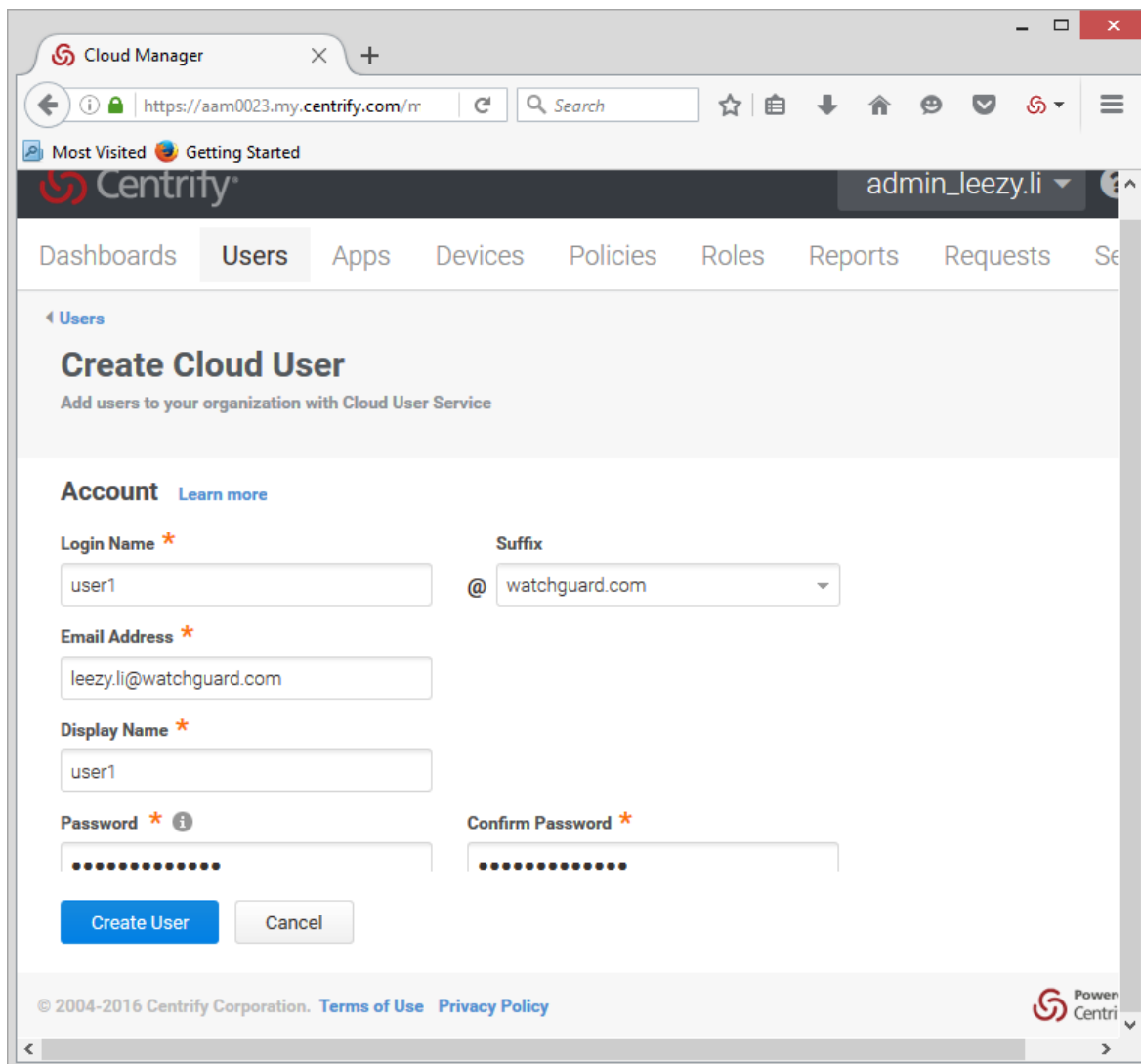
Create User Accounts in CIS

Before CIS can authenticate users, you must add a user store in CIS that reflects the users who need to use multi-factor authentication. Use one of these methods to add users to CIS:

- Manually: Add one user at a time with the *Add User* shortcut
- Automatically: Import up to 10,000 accounts from an Excel .xls or .xlsx spreadsheet or a .csv file

In this document, we show you how to use the Add User shortcut to manually create users. To learn more about how to add users, see the CIS documentation.

1. Log on to Centrify Cloud Manager with your administrator account.
2. Click **Users > Add User**.



The screenshot shows a web browser window with the Centrify Cloud Manager interface. The URL bar shows 'https://aam0023.my.centrixy.com/'. The user is logged in as 'admin_leezy.li'. The navigation menu includes 'Dashboards', 'Users', 'Apps', 'Devices', 'Policies', 'Roles', 'Reports', 'Requests', and 'Se'. The 'Users' section is active, and the 'Create Cloud User' form is displayed. The form has the following fields:

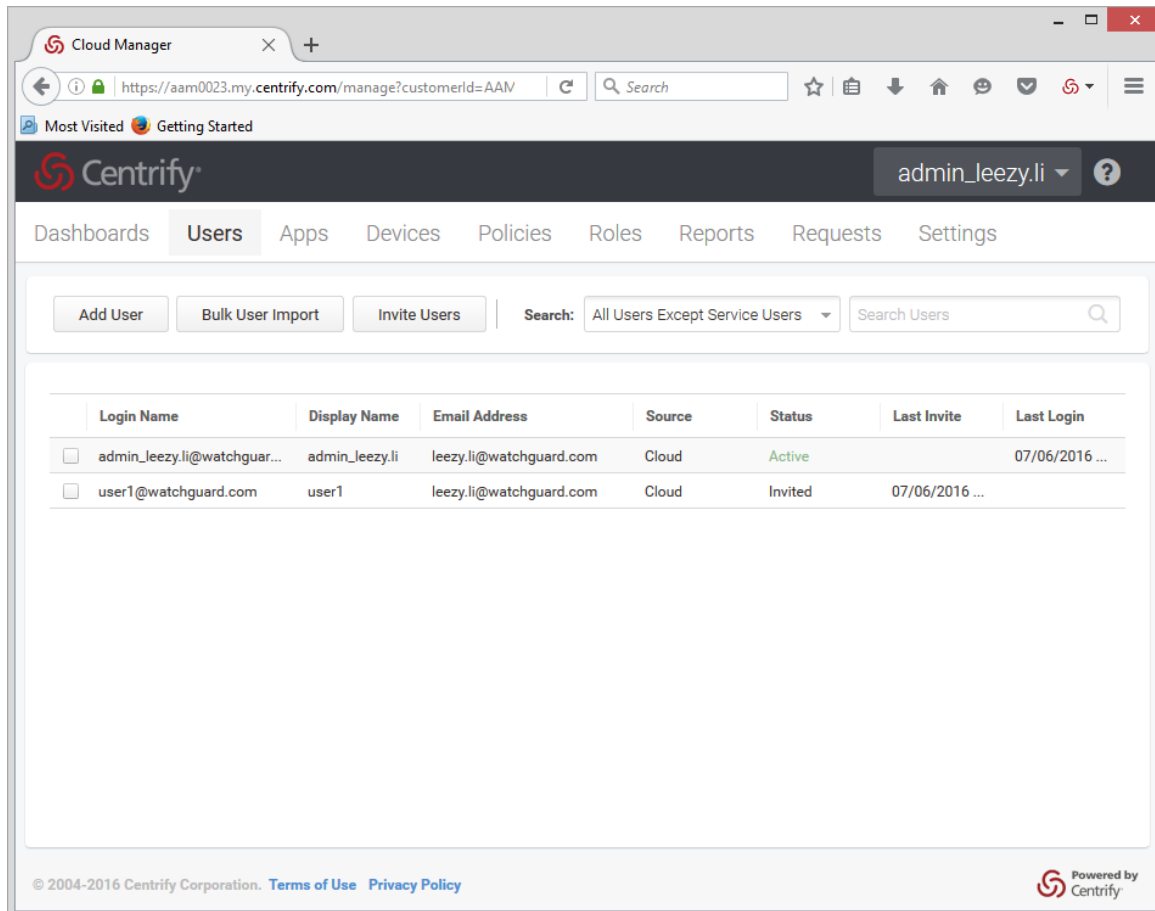
- Account** (with a 'Learn more' link)
- Login Name ***: Text input with 'user1' entered.
- Suffix**: Dropdown menu with '@ watchguard.com' selected.
- Email Address ***: Text input with 'leezy.li@watchguard.com' entered.
- Display Name ***: Text input with 'user1' entered.
- Password ***: Password input field with masked characters.
- Confirm Password ***: Password input field with masked characters.

At the bottom of the form are two buttons: 'Create User' (in blue) and 'Cancel' (in grey). The footer of the page shows '© 2004-2016 Centrify Corporation. Terms of Use Privacy Policy' and the Centrify logo.

3. Type the required information.
4. Click **Create User**.


In this example, we created a user named *user1*. An email message is sent to the email address that you defined for *user1*.

5. Click **Add**.
This page appears.



6. Open the email message you received at the email address defined for *user1*.
7. Click **Login Now** to access the user portal.

8. Click **Enroll Mobile Devices Now**. The device you choose to enroll uses the mobile authenticator to finish secondary authentication.



Welcome to Centrify Identity Service

Your system administrator has created a Centrify Identity Service account for you.

login name: [user1@watchguard.com](#)

If you need help or have any questions, please contact your system administrator.

We hope you enjoy using the service.

Centrify

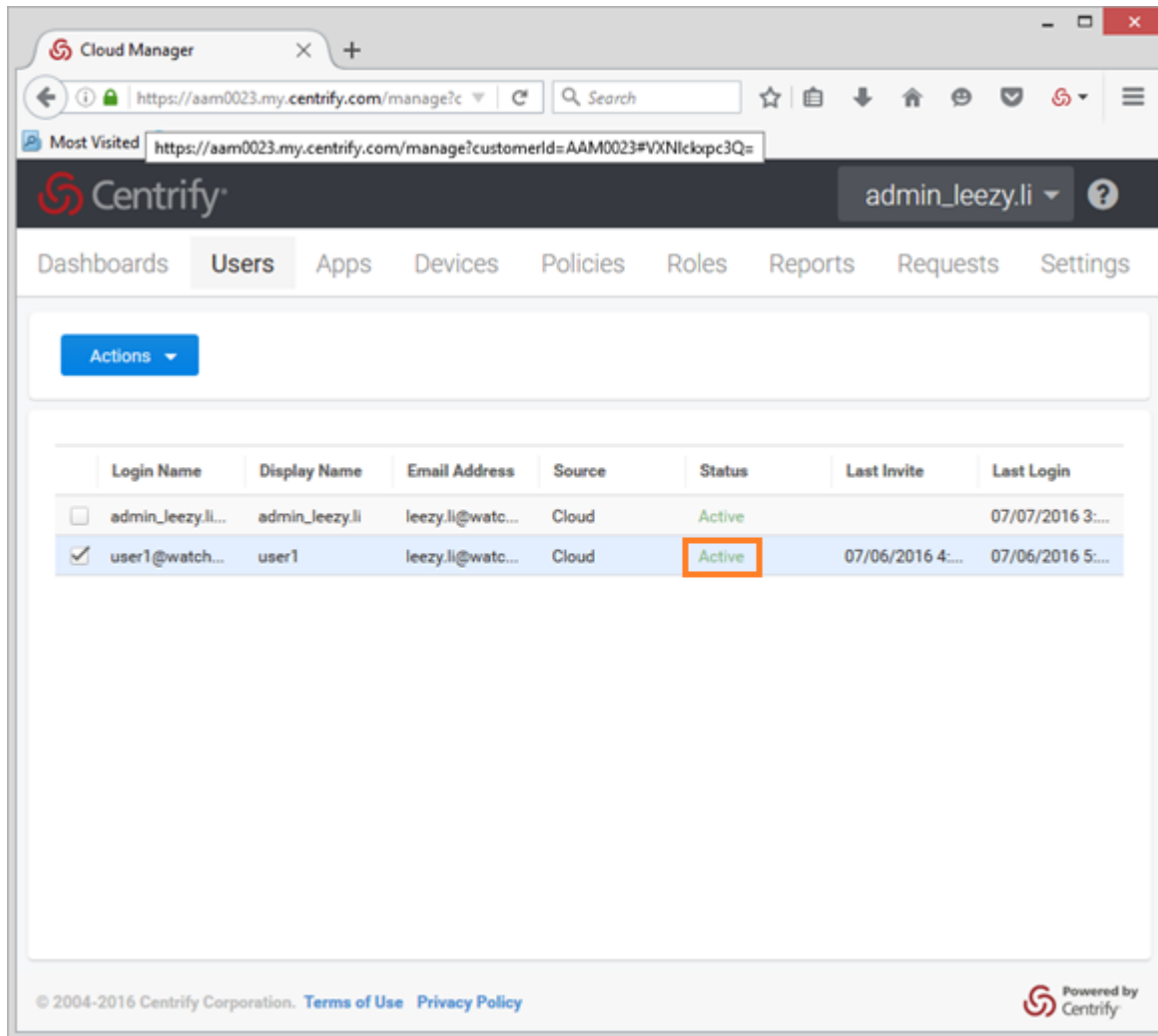
Access the User Portal and start using your applications and services.

Login Now

Enroll a mobile device for on-the-go, secure access to your apps.

Enroll Mobile Devices Now

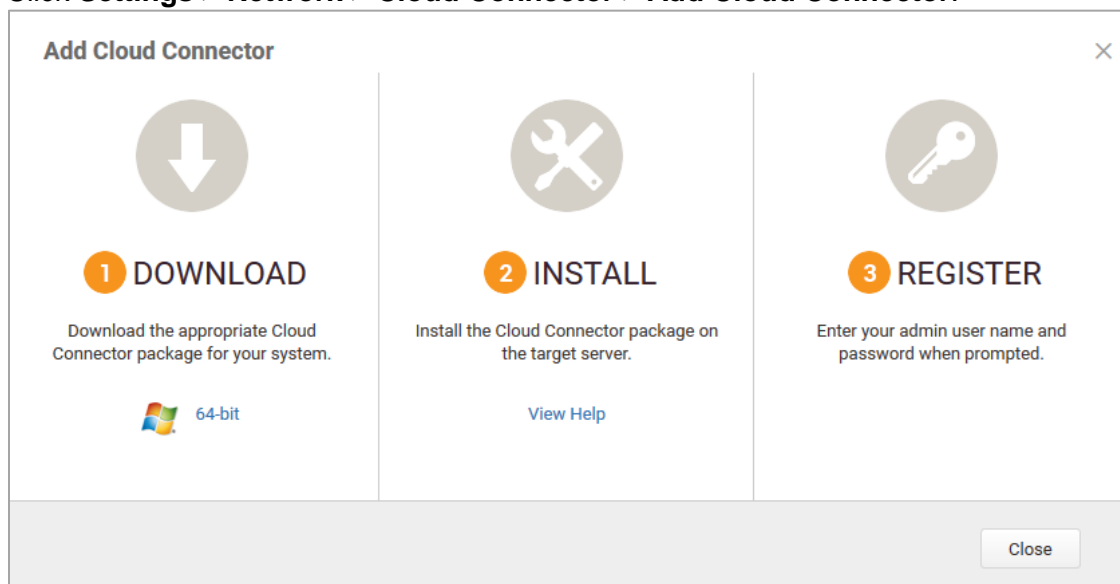
9. After the User Portal setup is finished, the user status is active.



Install a Cloud Connector on a Host Computer

1. Log on to the host computer with an account that has sufficient permissions to install the cloud connector. In our example, we use a host computer installed with Windows Server 2012 R2.
2. Log on to Centrify Cloud Manager with your administrator account.

3. Click **Settings > Network > Cloud Connector > Add Cloud Connector**.



4. From the **Download** pane, click **64-bit** to download the Cloud Connector installation program.
5. Follow the installation wizard to install the program.

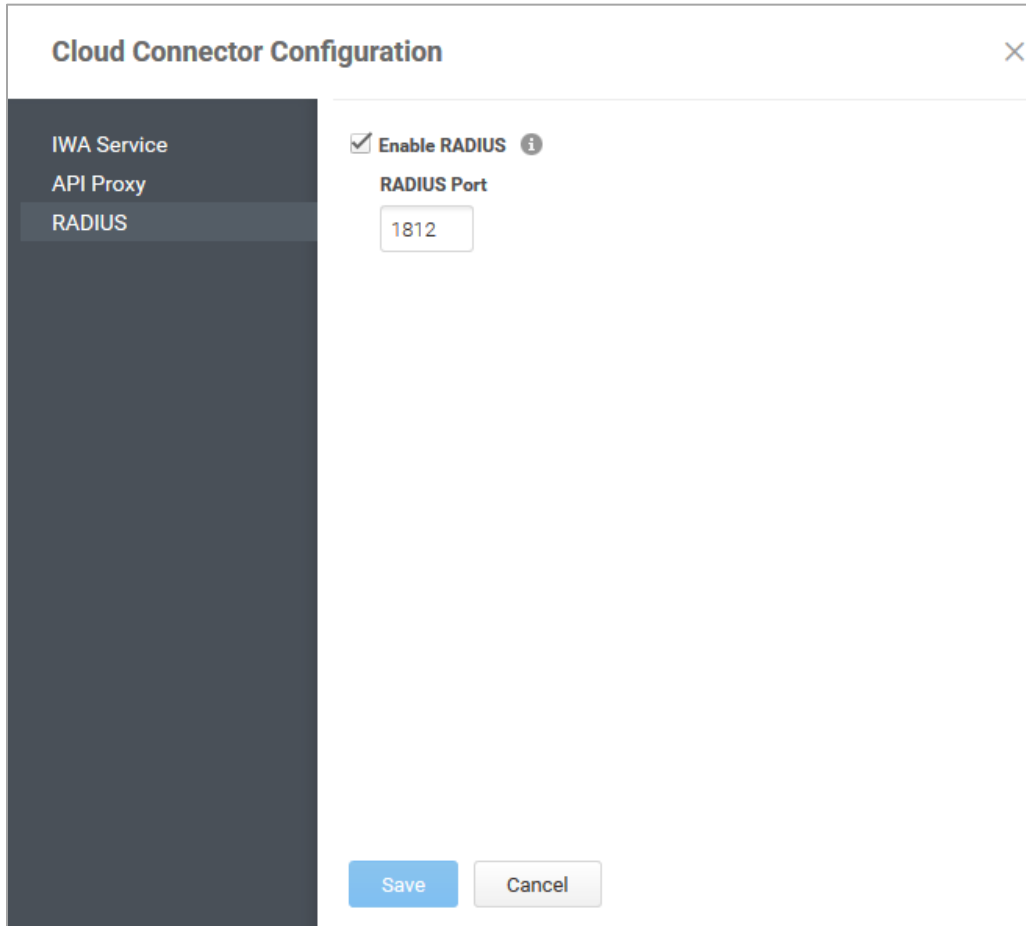
This page appears which shows the added cloud connector.

Cloud Connectors Learn more										
Add Cloud Connector										
	Cloud Connector Configuration	Forest	Version	Last Ping	Hostname	AD Proxy	LDAP Proxy	App Gateway	RADIUS	Status
<input type="checkbox"/>	WIN-Q93520CGJPU		16.6.155	07/07/2016 05:02 PM	WIN-Q93520CGJPU	Disabled	Enabled	Enabled	Enabled	Active

Configure Centrify RADIUS Support

1. Log on to Cloud Manager with your administrator account.
2. Click **Settings > Network > Cloud Connectors**.
3. Select the cloud connector that you previously added.

4. Click **RADIUS**.



The image shows a 'Cloud Connector Configuration' dialog box. On the left is a dark sidebar with three menu items: 'IWA Service', 'API Proxy', and 'RADIUS'. The 'RADIUS' item is highlighted. The main area of the dialog is white and contains the following elements: a checked checkbox labeled 'Enable RADIUS' with an information icon to its right; a label 'RADIUS Port' above a text input field containing the value '1812'; and at the bottom, two buttons: a blue 'Save' button and a grey 'Cancel' button. A close button (X) is located in the top right corner of the dialog's title bar.

5. Select the **Enable RADIUS** check box.
6. Type the port number that the Centrify Cloud Connector uses to talk to the Centrify Cloud Service. The default port number is 1812.
7. Click **Save**.

Configure an Authentication Profile

1. Click **Settings > Authentication > Authentication Profile**.
2. Click **Add profile** to add a new profile or use the **Default New Device Login Profile**. In our example, we use **Default New Device Login Profile** as the authentication profile.

If you select an option other than **Email confirmation code** for secondary authentication, you must enroll a device with the user.

Authentication Profile ✕

Profile Name *

Authentication Mechanisms

Challenge 1	Challenge 2 (optional)
<input checked="" type="checkbox"/> Password	<input type="checkbox"/> Password
<input type="checkbox"/> Mobile Authenticator	<input type="checkbox"/> Mobile Authenticator
<input type="checkbox"/> Phone call	<input type="checkbox"/> Phone call
<input type="checkbox"/> Text message (SMS) confirmation code	<input type="checkbox"/> Text message (SMS) confirmation code
<input type="checkbox"/> Email confirmation code	<input checked="" type="checkbox"/> Email confirmation code
<input type="checkbox"/> User-defined Security Question	<input type="checkbox"/> User-defined Security Question
<input type="checkbox"/> OATH OTP Client	<input type="checkbox"/> OATH OTP Client

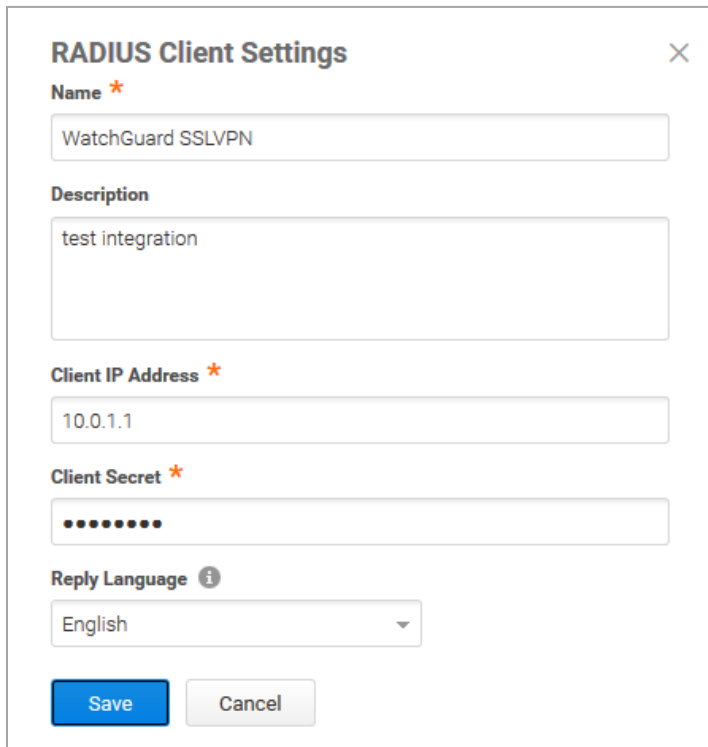
Challenge Pass-Through Duration ⓘ

To learn more about how to use authentication mechanisms, see the CIS documentation.

Configure a RADIUS Client to Use a WatchGuard Firebox

To configure a RADIUS client:

1. Click **Settings > Authentication > RADIUS Clients > Add** to configure your RADIUS client.



The screenshot shows a 'RADIUS Client Settings' dialog box with a close button (X) in the top right corner. The dialog contains the following fields and controls:

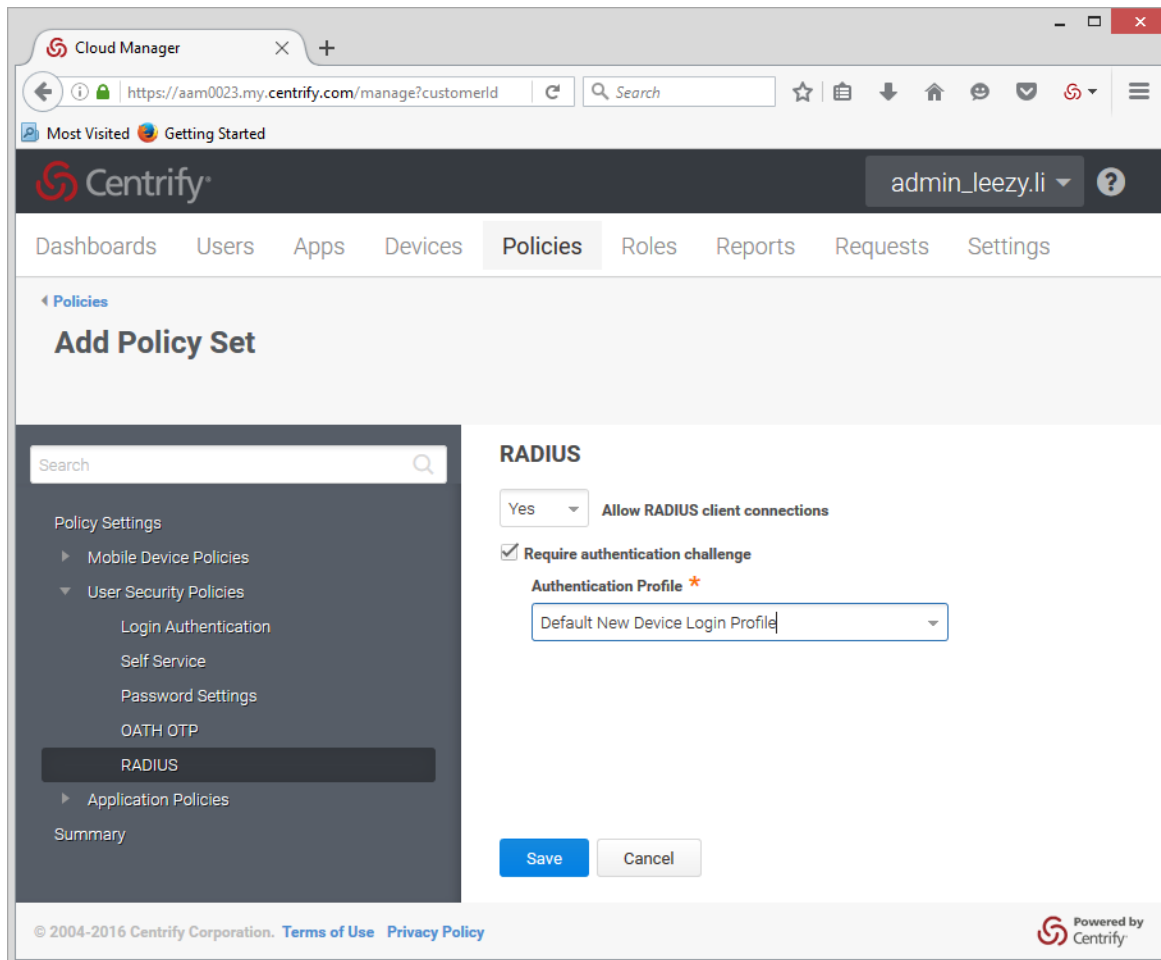
- Name ***: A text input field containing 'WatchGuard SSLVPN'.
- Description**: A text input field containing 'test integration'.
- Client IP Address ***: A text input field containing '10.0.1.1'.
- Client Secret ***: A text input field filled with ten dots, representing a masked secret.
- Reply Language**: A dropdown menu with an information icon (i) to its right, currently set to 'English'.
- Buttons**: 'Save' and 'Cancel' buttons at the bottom left.

2. In **Name** and **Description** text boxes, type a name and description for your RADIUS client. In our example, we use the WatchGuard Firebox as a RADIUS client.
3. In the **Client IP Address** text box, type the IP address of the RADIUS client.
4. In the **Client Secret** text box, type a shared secret key for the RADIUS client and Centrify cloud. If you entered a secret key on your RADIUS client, type the same key here.
5. Click **Save**.

Configure a Security Policy Based on RADIUS

To configure a security policy:

1. Click **Policies > Add Policy Set > User Security Policies > RADIUS**.



The screenshot shows the Centrify Cloud Manager web interface. The browser address bar displays 'https://aam0023.my.centify.com/manage?customerid'. The user is logged in as 'admin_leezy.li'. The navigation menu includes 'Dashboards', 'Users', 'Apps', 'Devices', 'Policies', 'Roles', 'Reports', 'Requests', and 'Settings'. The 'Policies' section is active, and the 'Add Policy Set' page is shown. On the left, a sidebar lists 'Policy Settings' with sub-items: 'Mobile Device Policies', 'User Security Policies' (expanded), 'Login Authentication', 'Self Service', 'Password Settings', 'OATH OTP', 'RADIUS' (selected), 'Application Policies', and 'Summary'. The main content area is titled 'RADIUS' and contains the following configuration options: 'Allow RADIUS client connections' set to 'Yes', 'Require authentication challenge' checked, and 'Authentication Profile' set to 'Default New Device Login Profile'. 'Save' and 'Cancel' buttons are at the bottom. The footer includes copyright information and the Centrify logo.

2. From the **Allow RADIUS client connections** drop-down list, select **Yes**.
3. Select the **Require authentication challenge** check box to require that users provide a secondary authentication mechanism to log on through the RADIUS client.
4. From the **Authentication Profile** drop-down list, select **Default New Device Login Profile**.
5. Click **Save**.

Configure the Firebox

In this example, we use Fireware Web UI to configure our Firebox. You can also use Policy Manager to complete these steps.

Configure the Firebox to Use RADIUS Server Authentication

To authenticate with CIS, you must enable the RADIUS server on the Firebox.

1. Log on to Fireware Web UI at *https://<IP address of Firebox>:8080*.
2. Click **Authentication > Servers > RADIUS**.
3. Select the **Enable RADIUS Server** check box.

[Servers](#) / RADIUS

Before you configure your Firebox device to use a RADIUS authentication server, make Primary Server Settings

☒ Enable RADIUS Server

IP Address

Port

Passphrase

Confirm

Timeout seconds

Retries

Group Attribute

Dead Time Minutes

4. In the **IP Address** text box, type the IP address of CIS.
5. In the **Port** text box, type the port used in CIS for RADIUS authentication. The default is port 1812.
6. In the **Passphrase** and **Confirm** text boxes, type the shared secret you configured for the RADIUS client on CIS.
7. Click **Save**.

Add Users

On the Firebox, add a new user to log on to the RADIUS server.

1. Select **Authentication > Users and Groups**.
2. Click **Add**.
3. Select **User**.
4. In the **Name** text box, type the same user name you created in CIS.
5. From the **Authentication Server** drop-down list, select **RADIUS**.
6. Click **OK**.

The user is added to the Users and Groups list on the Firebox.

Users and Groups		
Define users and groups to use in policies and aliases. Make sure the user or group name you add matches a user or group already configured on your authentication server.		
<input type="checkbox"/> NAME	TYPE	AUTHENTICATION SERVER
<input type="checkbox"/> SSLVPN-Users	Group	
<input type="checkbox"/> user1@watchguard.com	Group	RADIUS

7. Click **Save**.

Configure Mobile VPN with SSL with RADIUS Authentication

To use RADIUS authentication for user connections with the Mobile VPN with SSL client, enable Mobile VPN with SSL on the Firebox and configure it to use RADIUS for authentication.

1. Select **VPN > Mobile VPN with SSL**.
2. Select the **Activate Mobile VPN with SSL** check box.

Mobile VPN with SSL	
When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN"	
<input checked="" type="checkbox"/> Activate Mobile VPN with SSL	
<div><div>General</div><div>Authentication</div><div>Advanced</div></div>	
Firebox IP Addresses or Domain Names	
Type a firebox IP or domain name for SSL VPN users to connect to.	
Primary	<input type="text" value="220.248.145.23"/>
Secondary	<input type="text"/>

3. In the **Primary** text box, type the IP address to which Mobile VPN with SSL clients connect.
This is the IP address of the Firebox.
4. Select the **Authentication** tab.

5. Select the check box next to **RADIUS (Default)** to use the RADIUS authentication server.

Mobile VPN with SSL

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

☒ Activate Mobile VPN with SSL

General Authentication Advanced

Authentication Server Settings

Select one or more authentication servers. The first server in the list is the default authentication server.

SELECT	AUTHENTICATION SERVER
<input checked="" type="checkbox"/>	RADIUS (Default)
<input checked="" type="checkbox"/>	Firebox-DB
<input checked="" type="checkbox"/>	eco.cdc.com

DEFAULT

☐ Auto reconnect after a connection is lost

☐ Force users to authenticate after a connection is lost

☐ Allow the Mobile VPN with SSL client to remember password

Define users and groups to authenticate with Mobile VPN with SSL. The users and groups you define are automatically included in the "SSLVPN-Users" group.

NAME	TYPE	AUTHENTICATION SERVER
<input type="checkbox"/> SSLVPN-Users	Group	Any
<input type="checkbox"/> user1@watchguard.com	User	RADIUS

ADD REMOVE

SAVE

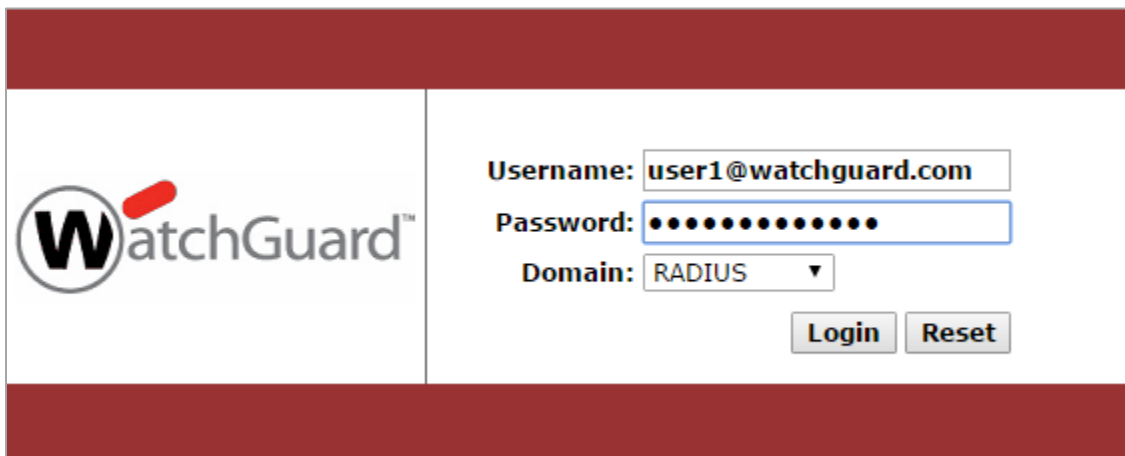
6. Click **Save**.

Test the Integration

To test the integration, we use Mobile VPN with SSL to test user authentication.

To download and configure the Mobile VPN with SSL client software from the Firebox:

1. Go to the SSL VPN web portal at <https://<IP of Firebox>:4100/sslvpn.html>.

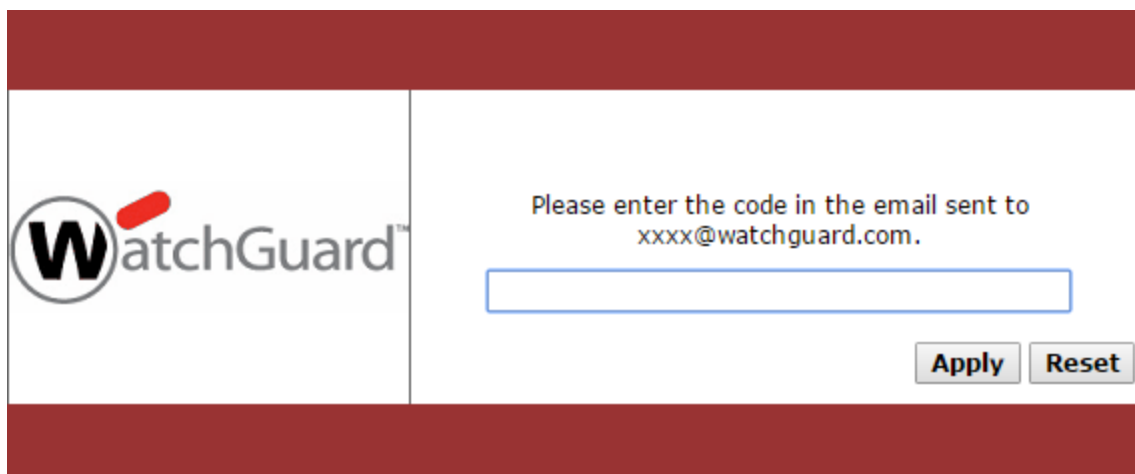


The image shows the WatchGuard SSL VPN web portal login screen. On the left is the WatchGuard logo. On the right, there are three input fields: 'Username:' with the value 'user1@watchguard.com', 'Password:' with masked characters, and 'Domain:' with a dropdown menu showing 'RADIUS'. Below these fields are 'Login' and 'Reset' buttons.

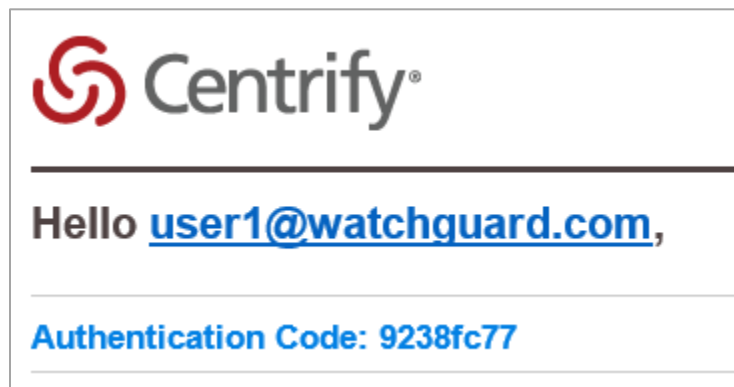
2. In the **Username** text box, type a user name defined in CIS.

3. In the **Password** text box, type the password defined in CIS.
4. From the **Domain** drop-down list, select **RADIUS** if it does not already appear.
5. Click **Login**.

This authentication page appears if the user is authenticated:

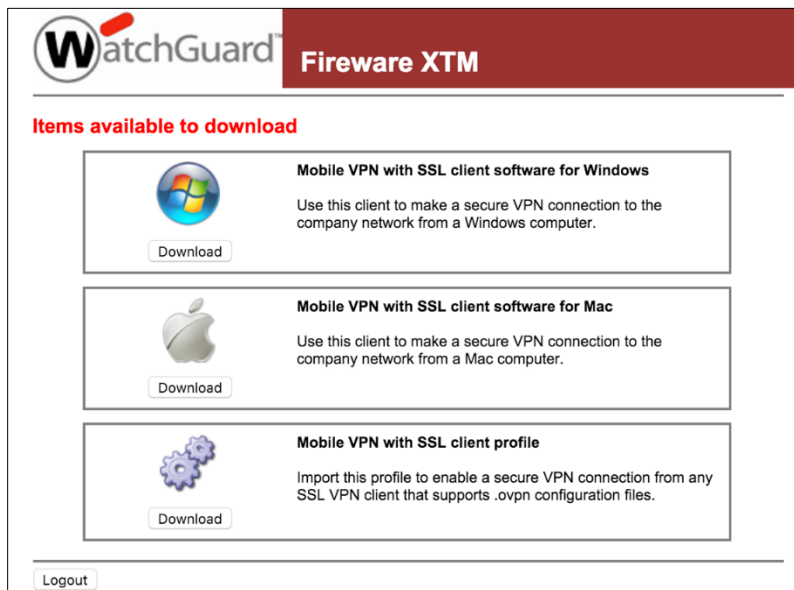
The image shows a web interface for WatchGuard authentication. It features a red header and footer. On the left, there is a logo with a stylized 'W' inside a circle, followed by the text 'atchGuard™'. On the right, there is a text prompt: 'Please enter the code in the email sent to xxxx@watchguard.com.' Below this prompt is a single-line text input field. At the bottom right of the input area, there are two buttons: 'Apply' and 'Reset'.

6. Type the Authentication code that you received in an email message.

The image shows a web interface for Centrify authentication. It features a white background with a red header. On the left, there is a logo with a stylized 'C' inside a circle, followed by the text 'Centrify®'. Below the logo, there is a horizontal line. Under the line, there is a text prompt: 'Hello user1@watchguard.com,'. Below this prompt, there is another horizontal line. Under the line, there is a text prompt: 'Authentication Code: 9238fc77'.

7. Click **Apply**.

After successful authentication, the download page appears.



8. Download the appropriate version of the VPN client for your operating system.

Mobile VPN with SSL Client Authentication

After you download and install the Mobile VPN with SSL client on your computer, you can use the same authentication process to connect to the Firebox with the SSL VPN client.

