HID® ActivID® Appliance with Wallix® Bastion

RADIUS Two-Factor Authentication Configuration Guide

Document Reference: APPL_8.0_WALLIX_CG_05.2019

Product Version: 8.0

May 2019

Copyright

Trademarks

Revision History

Date	Description	Document Version
May 2019	Initial release.	1.0

Contacts

Technical Support

If you purchased your product from a third party, then please contact that third party for Technical Support.

If you purchased your product directly from HID Global:

Americas
+1 800 670 6892

Europe, Middle East and Africa
+33 (0) 1 74 18 17 70

Asia Pacific
+852 3160 9873
+61 3 9111 2319

For further contact details, go to https://www.hidglobal.com/support

Customer Service

To contact HID Global Customer Service, go to https://www.hidglobal.com/customer-service

Typographic and Document Conventions

Typography	Description
blue	Cross-references within the document.
blue, underline	References to external web addresses.
bold	Action steps (paths, buttons, options); field and drop-down list labels; emphasis.
italic	File names, document titles, and file extensions.
`Code snippets`	Highlights `code snippets` within regular content.
`Code samples`	`Highlights code samples`
	**WARNING**: This symbol indicates a critical warning. It applies to actions that if taken or not taken will break the system. Read the warning carefully and follow it.
	**Important**: This symbol indicates something very important to the reader. Ignore this symbol at your own risk.
	**Note**: This symbol indicates a note that should be of interest to the reader. It is not critical. Nevertheless, the reader should pay attention.

Table of Contents

1.0 Introduction

The HID® ActivID® Appliance provides versatile multi-factor authentication to secure access to critical infrastructures and services. The solution is highly flexible, with easy-to-define policies designed to simplify user authentication and enable organizations to deploy tailored authentication solutions to their users.

The Wallix® Bastion® is a modular solution providing Privileged Access Management (PAM) to control access, monitor activity and securely manage passwords.

While the Wallix Bastion ensures the security of privileged accounts and target applications, the primary user still remains a potential source of compromise. Wallix and HID ActivID propose a joint solution remove the human factor as the weakest link within the security chain.

1.1 Document Scope and Audience

This guide explains how to configure RADIUS strong authentication access to a Wallix Bastion host with ActivID Appliance 8.0.

It is intended for system integrator and administrators.

Architecture-related topics are out of the scope of this guide. For further information, contact HID Global.

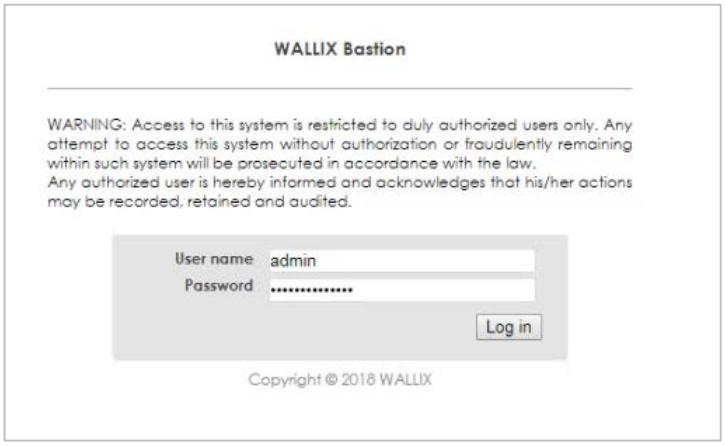
2.0 Configuring the Wallix Bastion Host

This section explains how to configure the Wallix Bastion host for external authentication with the ActivID Appliance.

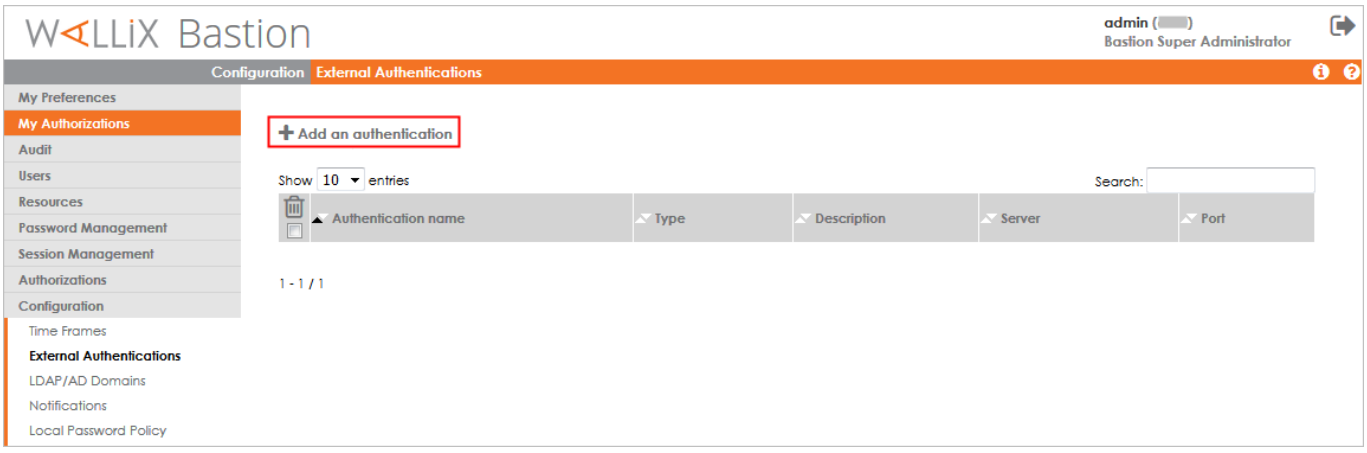
Prerequisites:

- You have installed and configured ActivID Appliance with the RADIUS Front End (RFE).
- You have installed and configured the Wallix Bastion host.
- You have configured the network connection and ports (RADIUS) between the Wallix Bastion host and the ActivID Appliance.

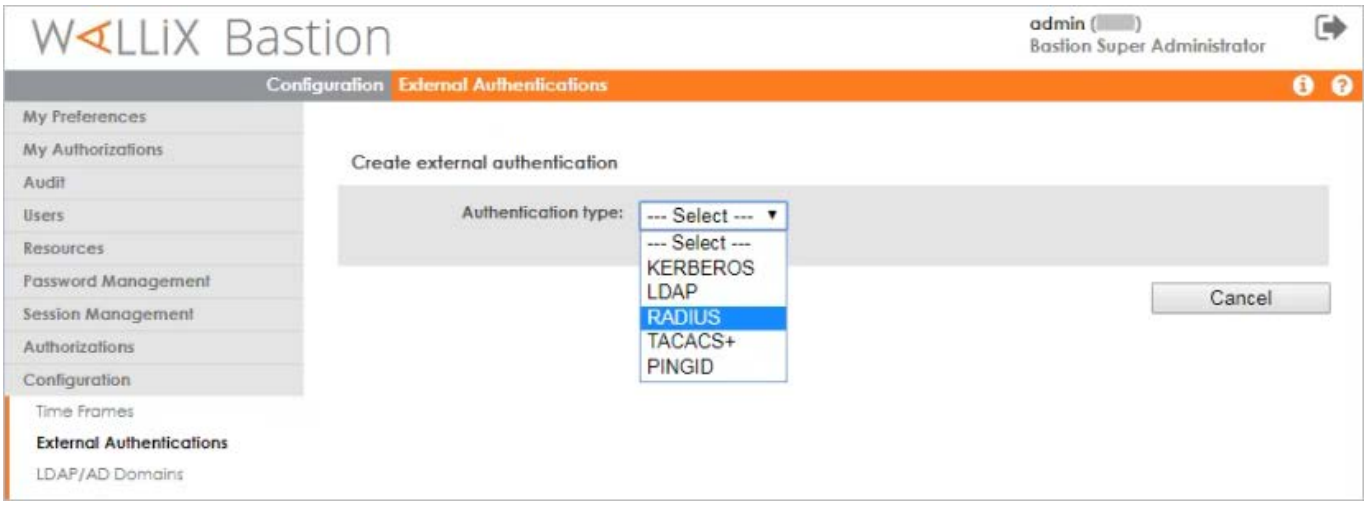
2.1 Create an External Authentication Host



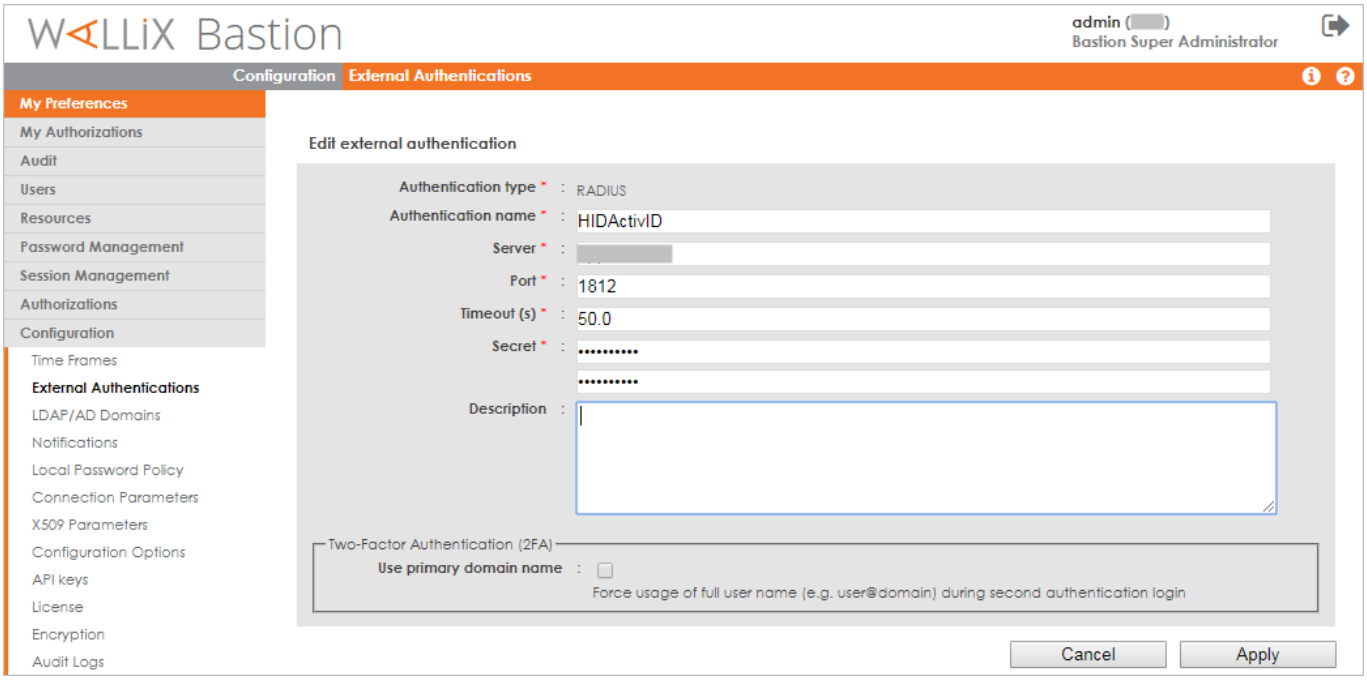
1. Using a browser, connect to the Wallix Bastion host portal and log on as an administrator.



2. In the left menu, under **Configuration**, select **External Authentication** and click **Add an authentication**.

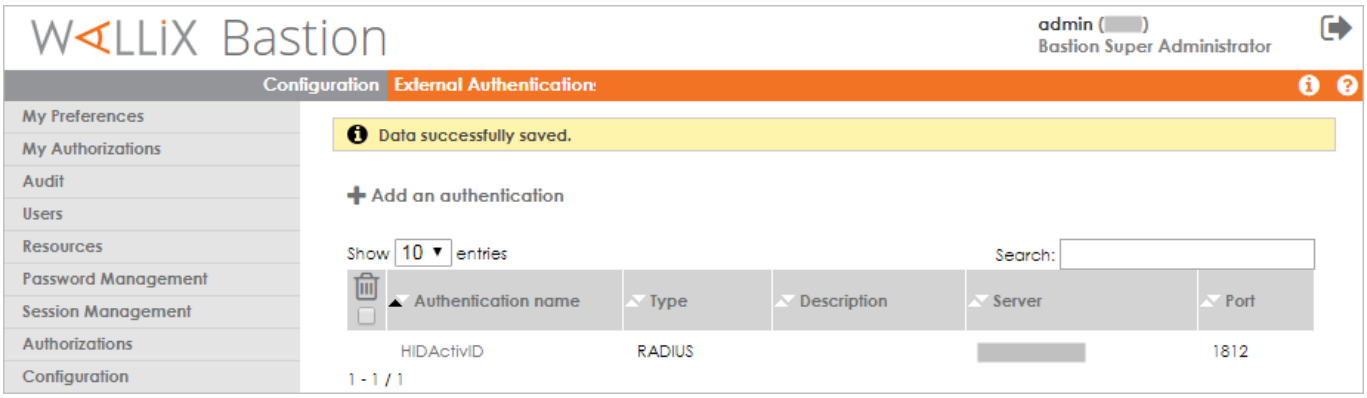


3. From the **Authentication type** drop-down list, select **RADIUS**.



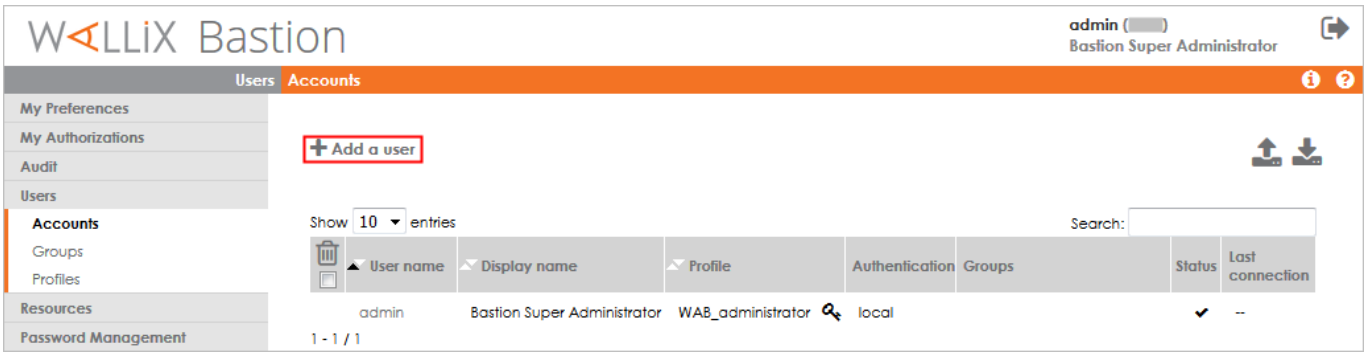
4. Enter the required RADIUS server parameters (as defined on the ActivID Appliance).
5. If you are deploying HID Approve™ mobile push-based authentication, increase the **Timeout** to at least 45-50 seconds.
6. Click **Apply**.

   The ActivID Appliance RFE is listed in the External authentication configuration.

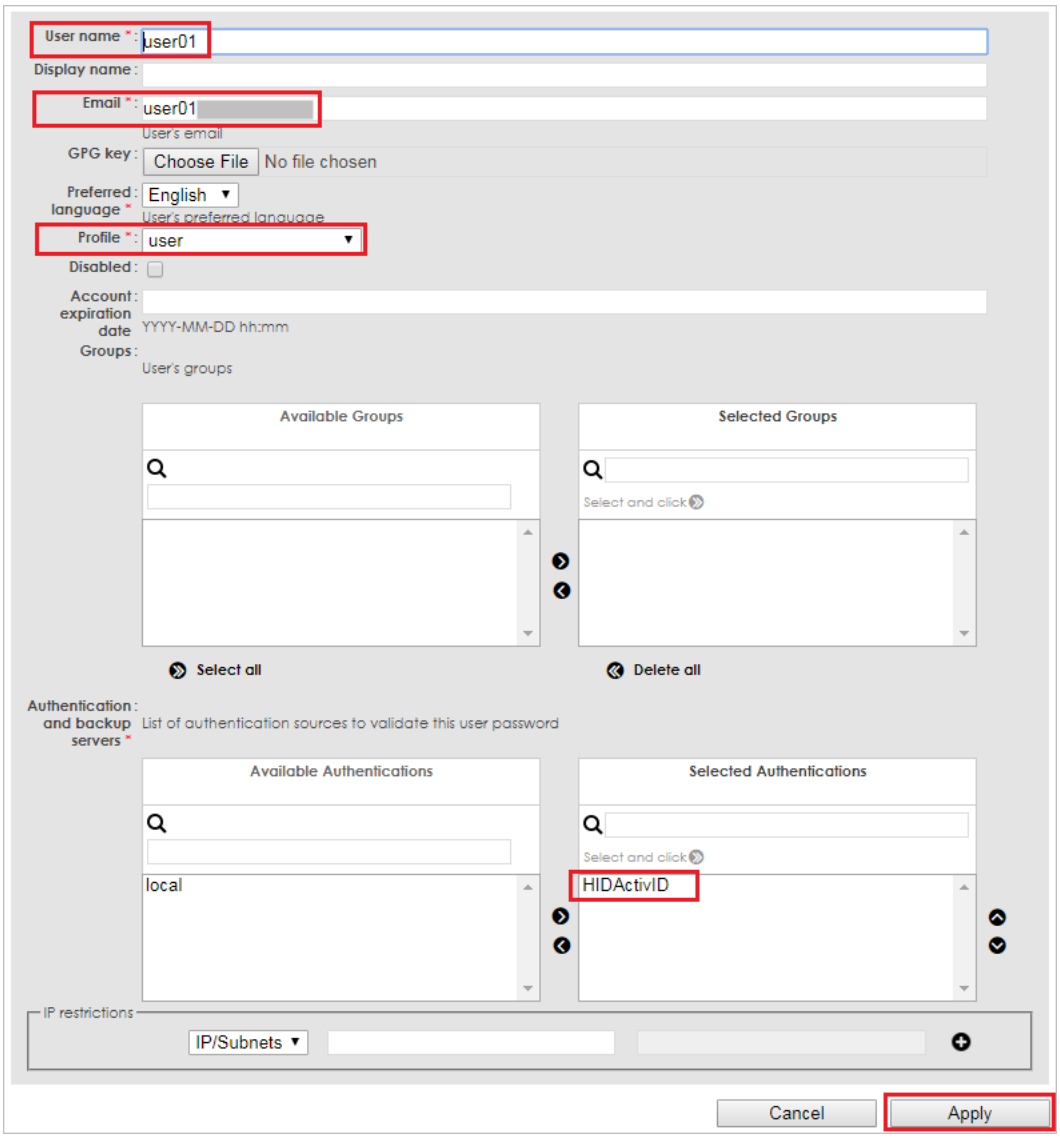


2.2 Create a Test User on the Wallix Bastion Host

1. In the left menu, under **Users**, select **Accounts**.

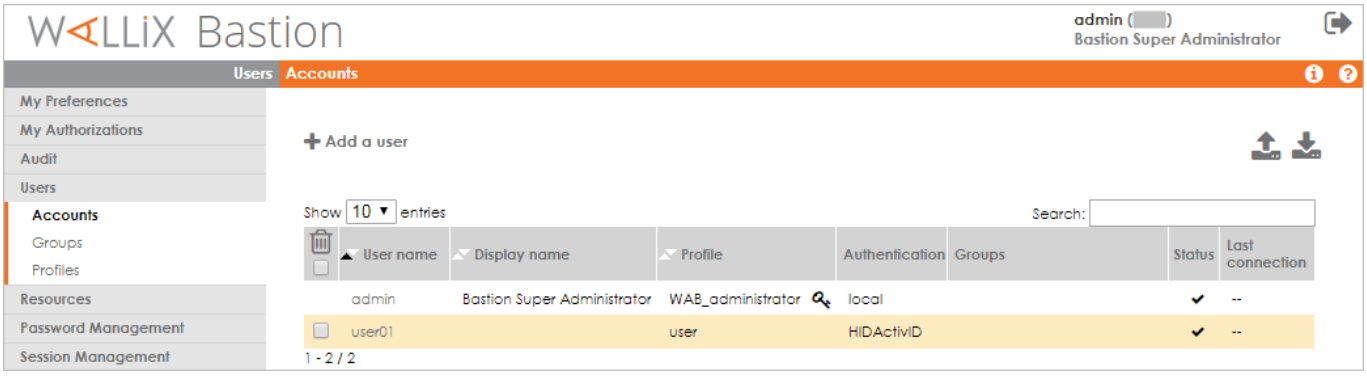


2. Click **Add a user**.



3. Enter the required user parameters (illustrated above as a minimum) and click **Apply**.

   The new user is displayed in the list of Accounts.

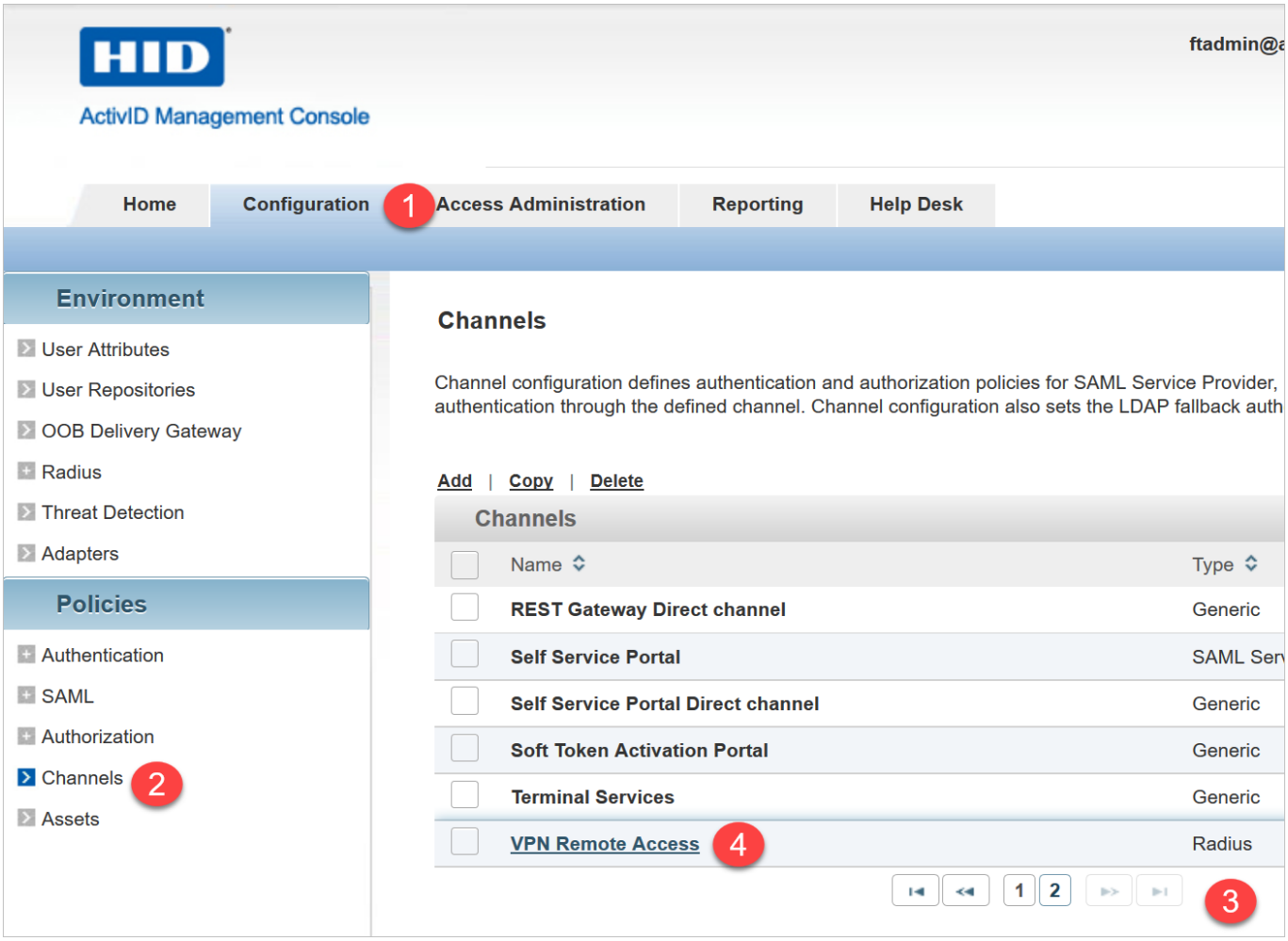


3.0 Configuring ActivID Appliance

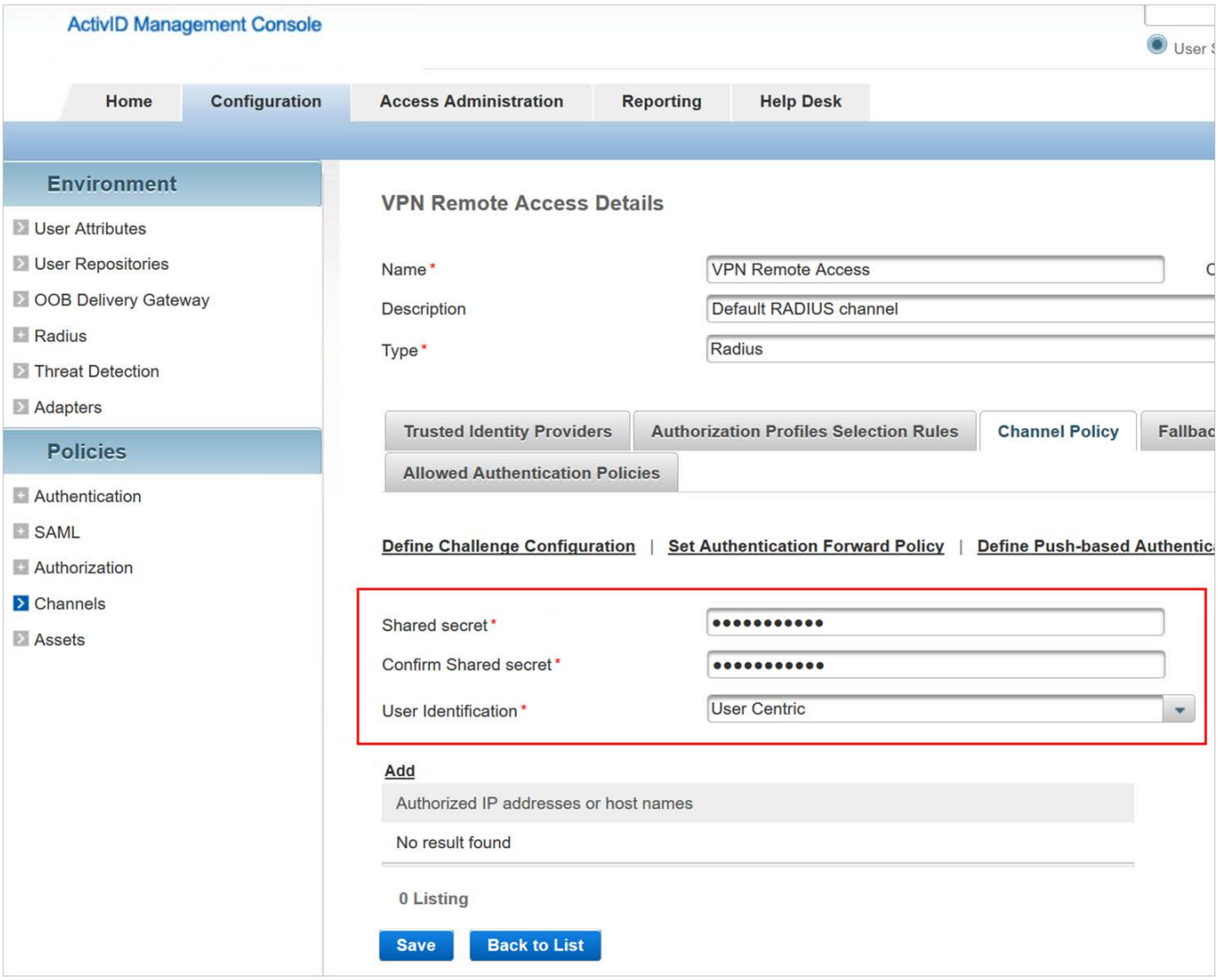
This section explains how to configure a RADIUS channel on the ActivID Appliance and create the ActivID Appliance user.

3.1 Configure the RADIUS Channel

1. Using a browser, connect to the ActivID Management Console (https://<appliance-hostname>/aiconsole) and log on as an administrator with privileges allowing channel configuration (for example, *ftadmin*).

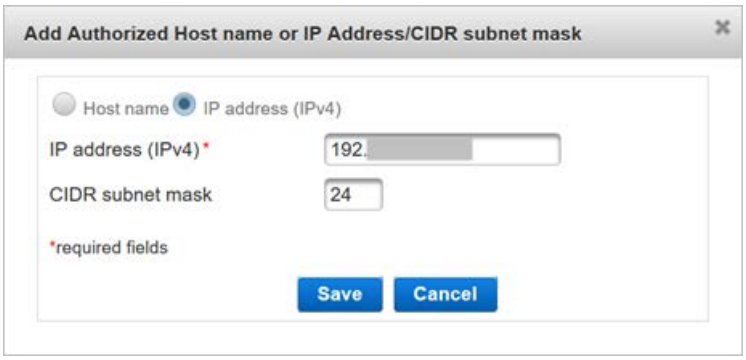


2. Select the **Configuration** tab (1) and, under **Policies**, select **Channels** (2).
3. Go to the end of the channel list (3) and click on the **VPN Remote Access** (4) channel to access the configuration.

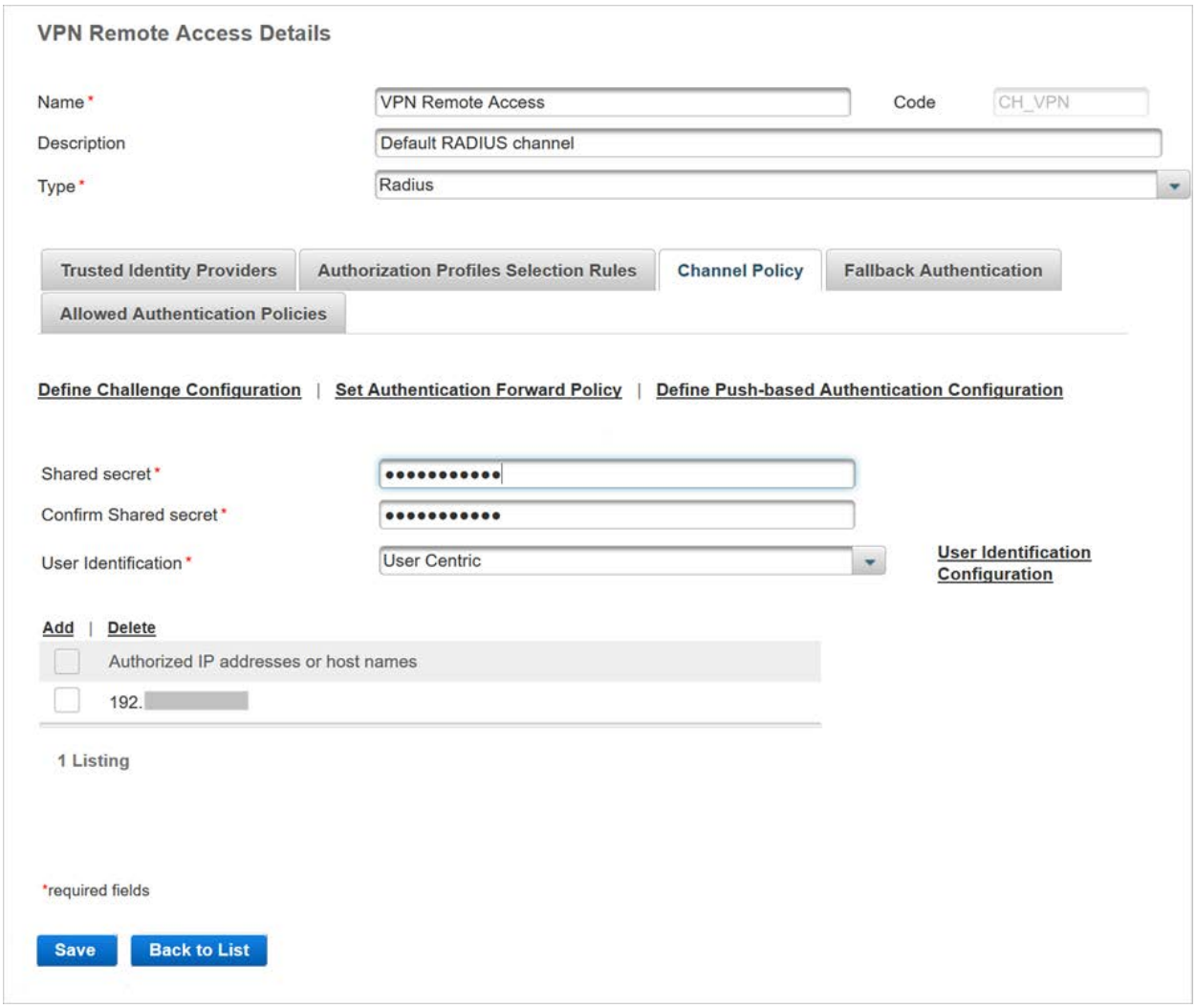


4. Select the **Channel Policy** tab.
5. Enter and confirm a **Shared secret** for the RADIUS channel.

   Your RADIUS Client on the Wallix Bastion host must use the same Shared secret.
6. Click **Add** to enter the IP address of the Wallix Bastion host as an IP authorized to access the RADIUS channel for RADIUS authentication.



7. Select the **IP address** option, enter the **IP** and **CIDR subnet mask** of the Wallix Bastion host, and then click **Save**.

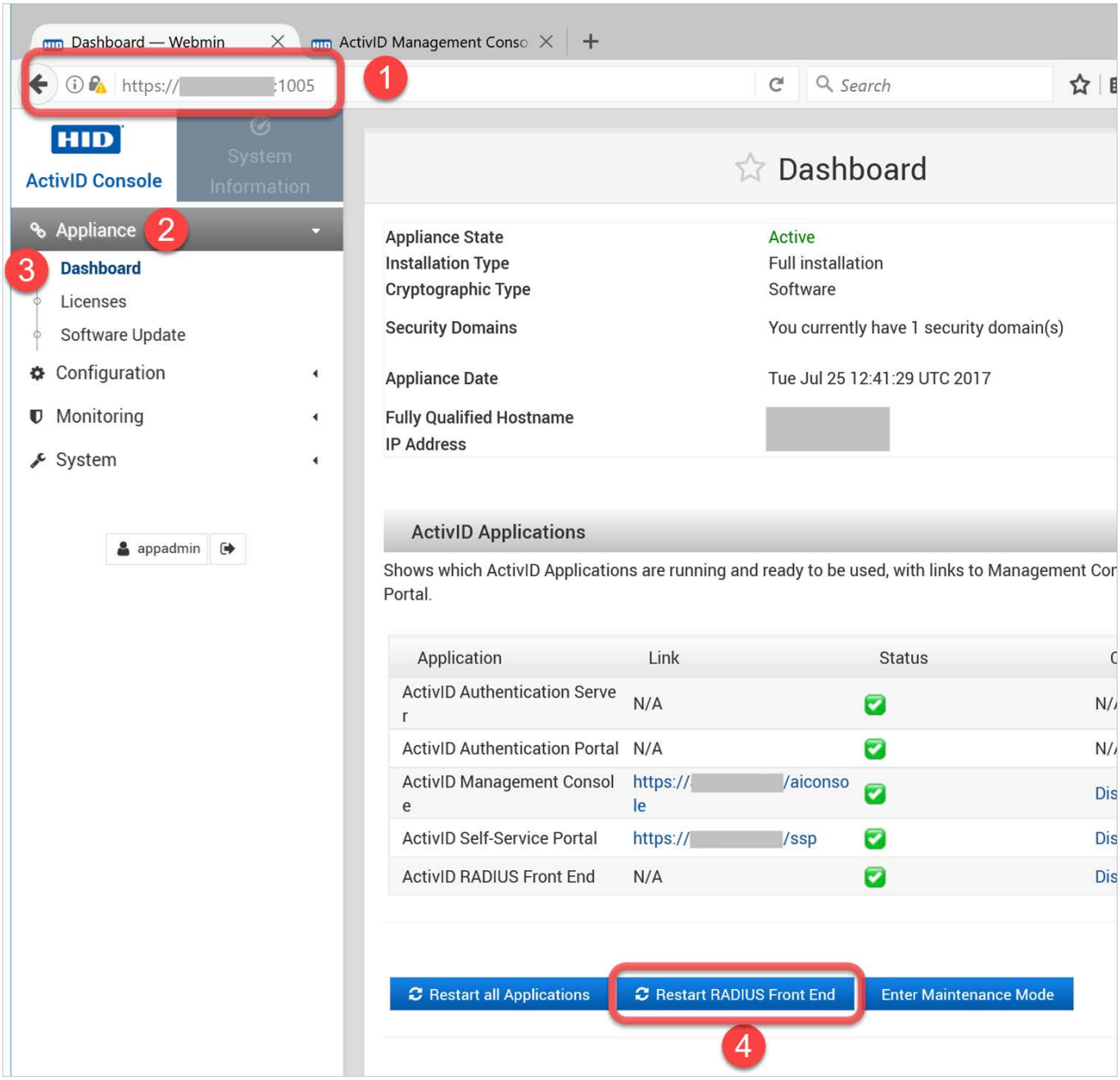


8. In the channel configuration page, click **Save**.

3.2 Restart the RADIUS Front End

In order to apply the RADIUS configuration, you must restart the RADIUS Front End application.

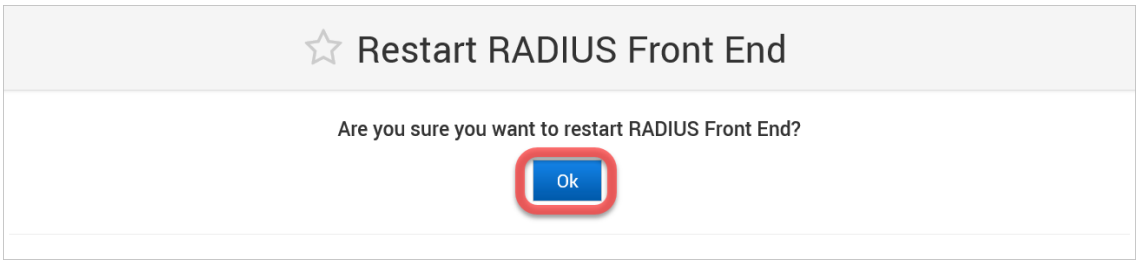
1. Using a browser, go to the ActivID Console (https://<appliance-hostname>:1005) and log on as *appadmin* (the ActivID Appliance administrator).



2. Under **Appliance** (2) in the left menu, select **Dashboard** (3).

   Or, under **Configuration** in the left menu, select **Applications**.

3. Under the list of **ActivID Applications**, click **Restart RADIUS Front End** (4).



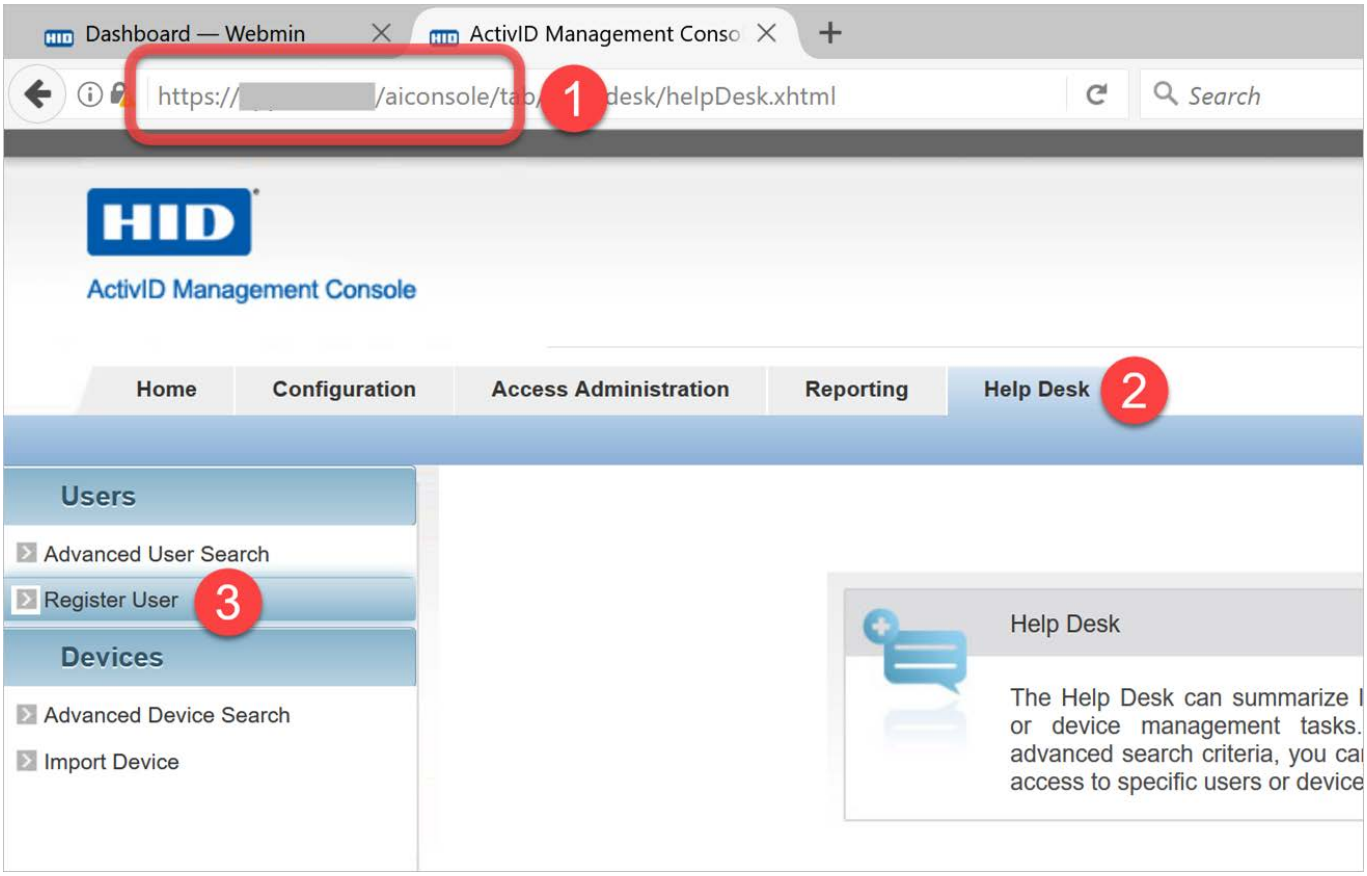
4. Click **OK**.

   The ActivID Appliance RFE is restarted and the status returns to the green check mark.

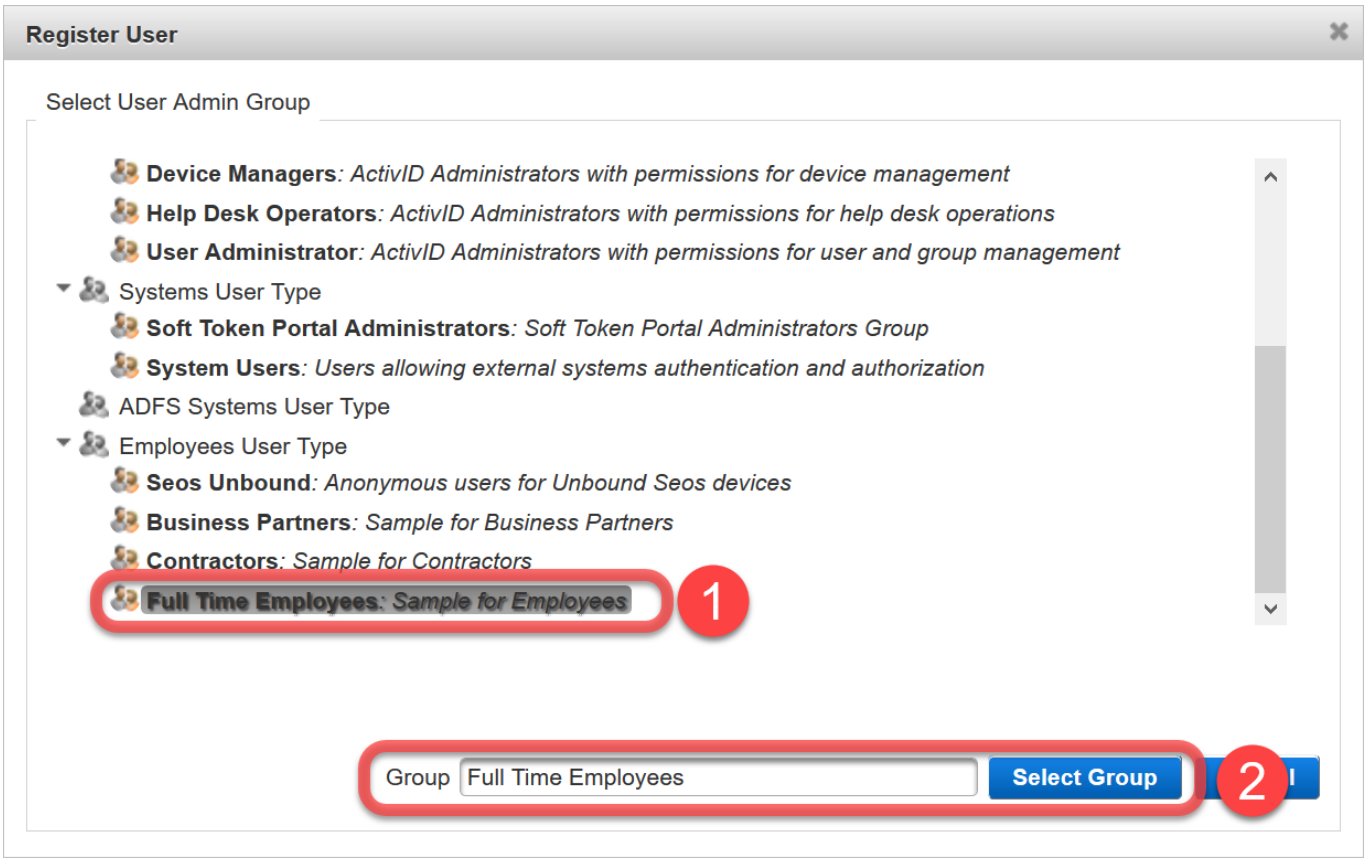
3.3 Create a New User on the ActivID Appliance

Prerequisites: You have created a new user on the Wallix Bastion host as described in section 2.2 Create a Test User on the Wallix Bastion Host on page 8.

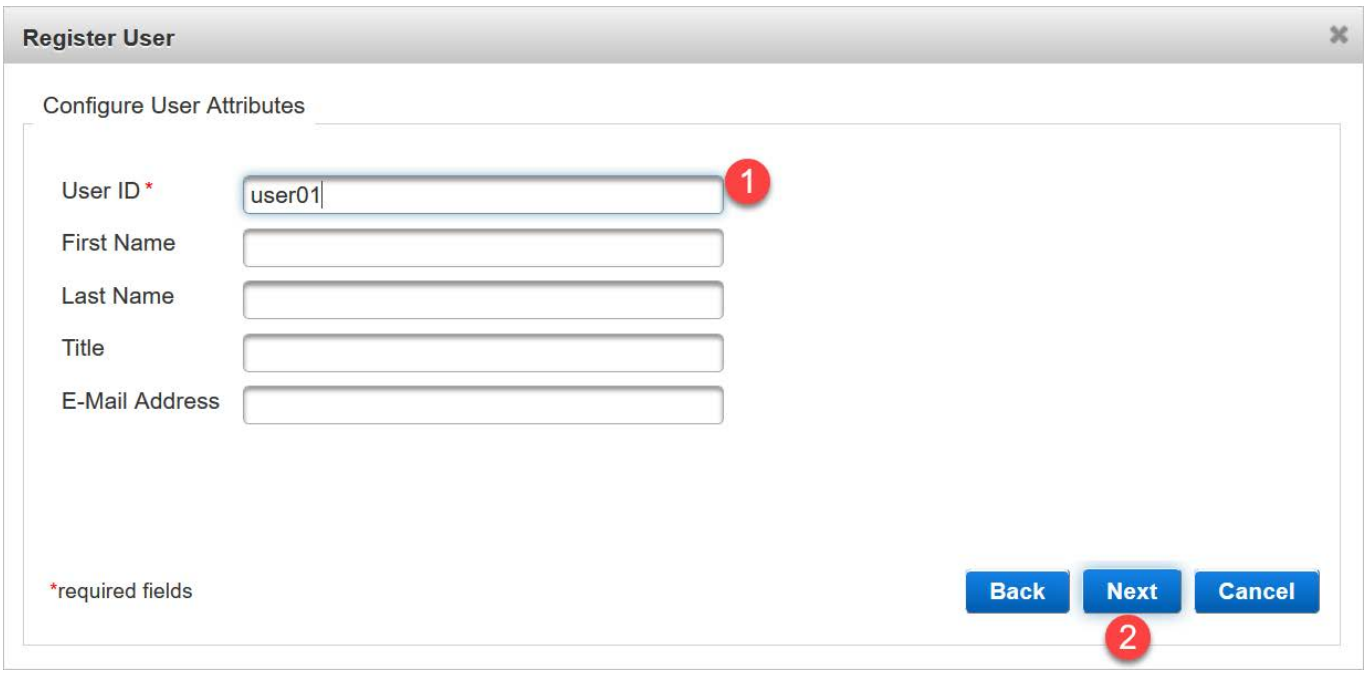
1. Using a browser, connect to the ActivID Management Console (https://<appliance-hostname>/aiconsole) and log on as an operator with help desk privileges (for example, *ftadmin*).



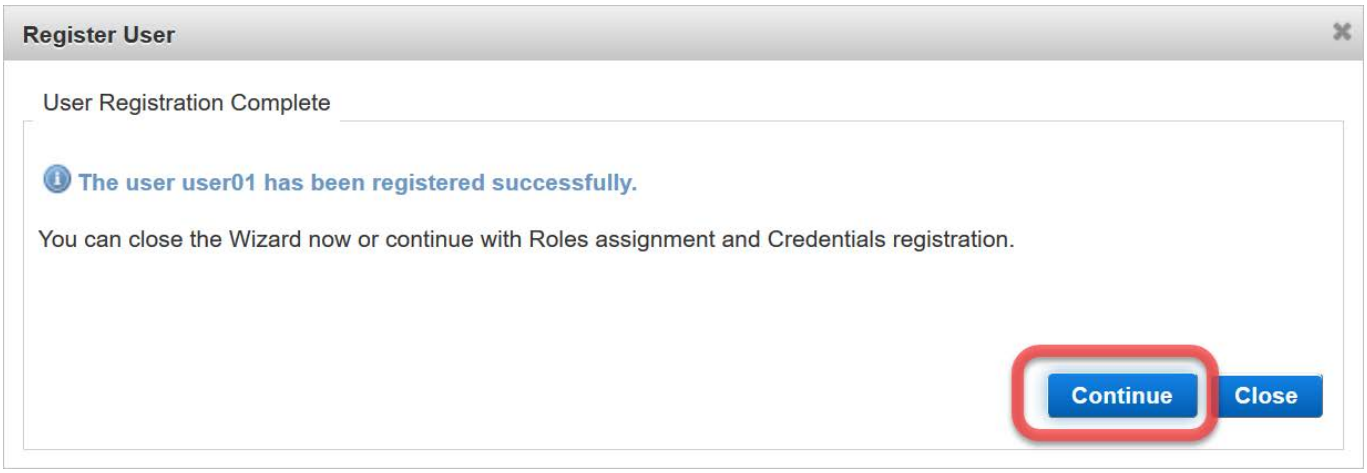
2. Select the **Help Desk** tab (2) and, under **Users**, select **Register User** (3).



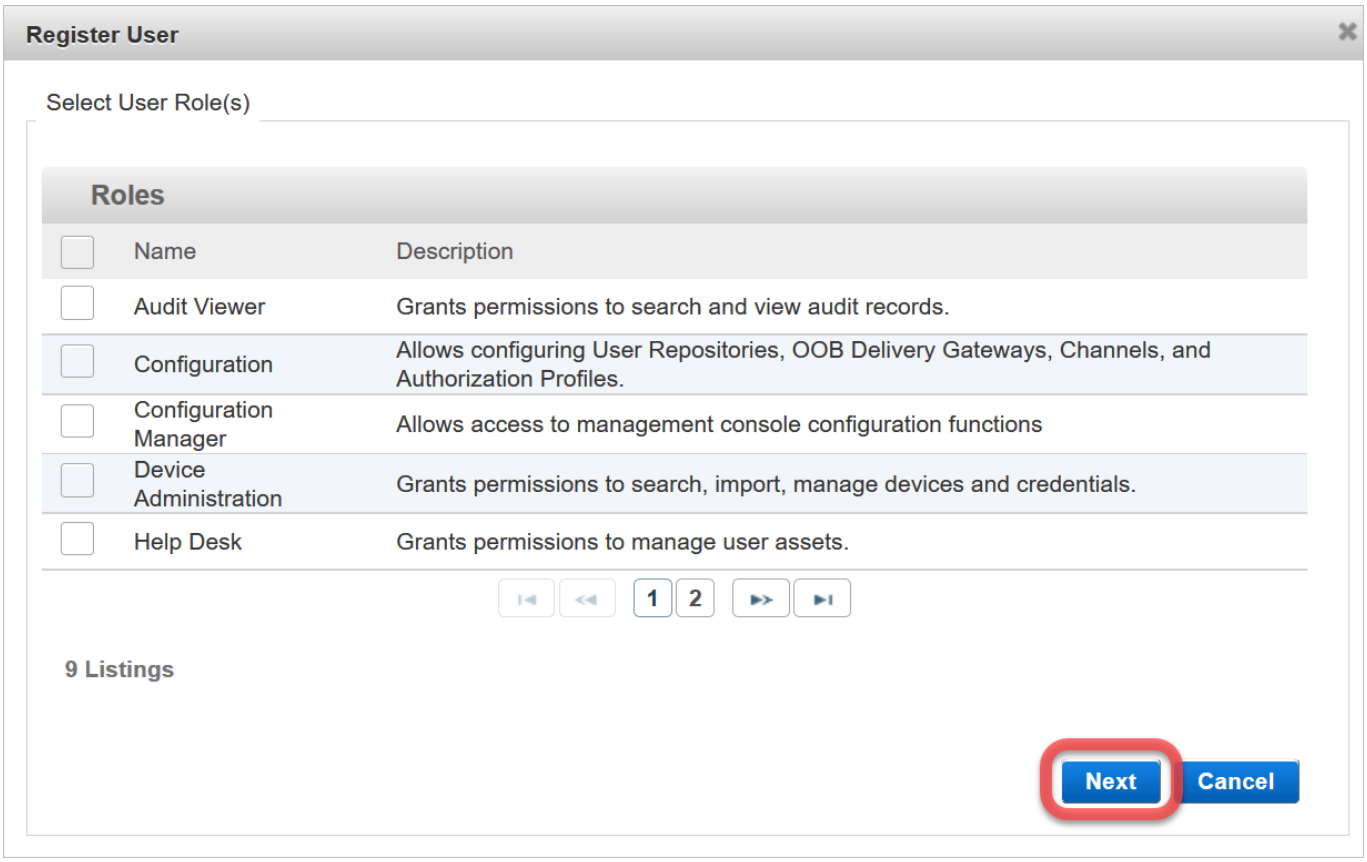
3. Under **Employees User Type**, select **Full Time Employees** (1) and then click **Select Group** (2)



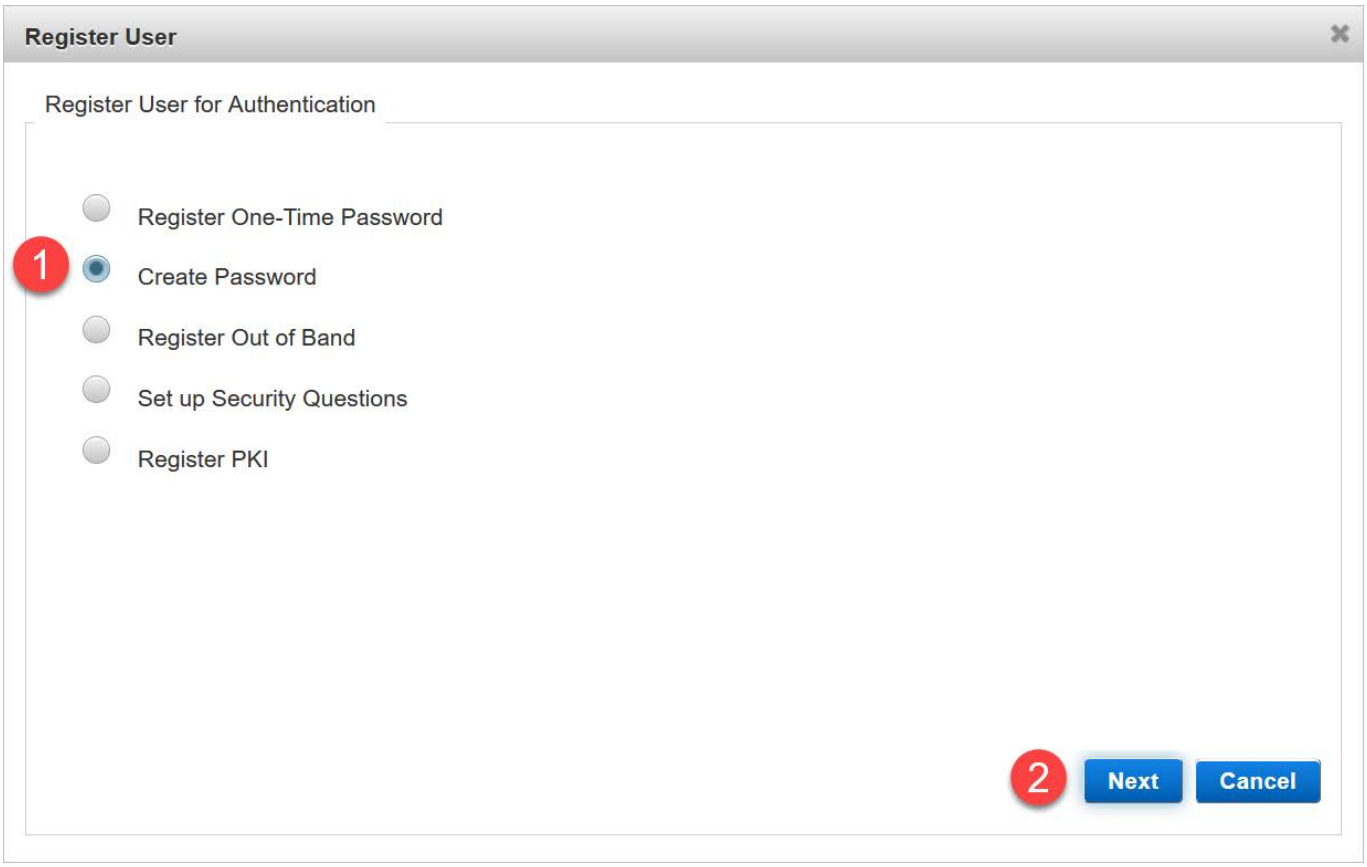
4. Enter a **User ID** (1) (this is the only mandatory field) and click **Next** (2).



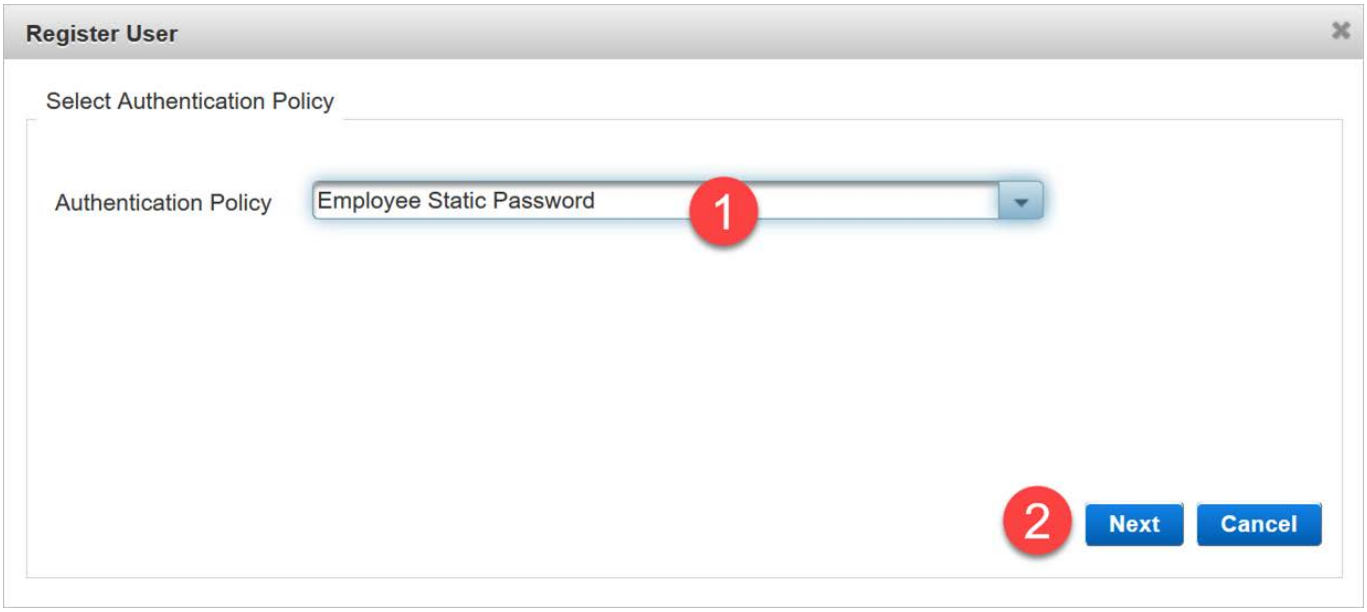
5. Click **Continue**.



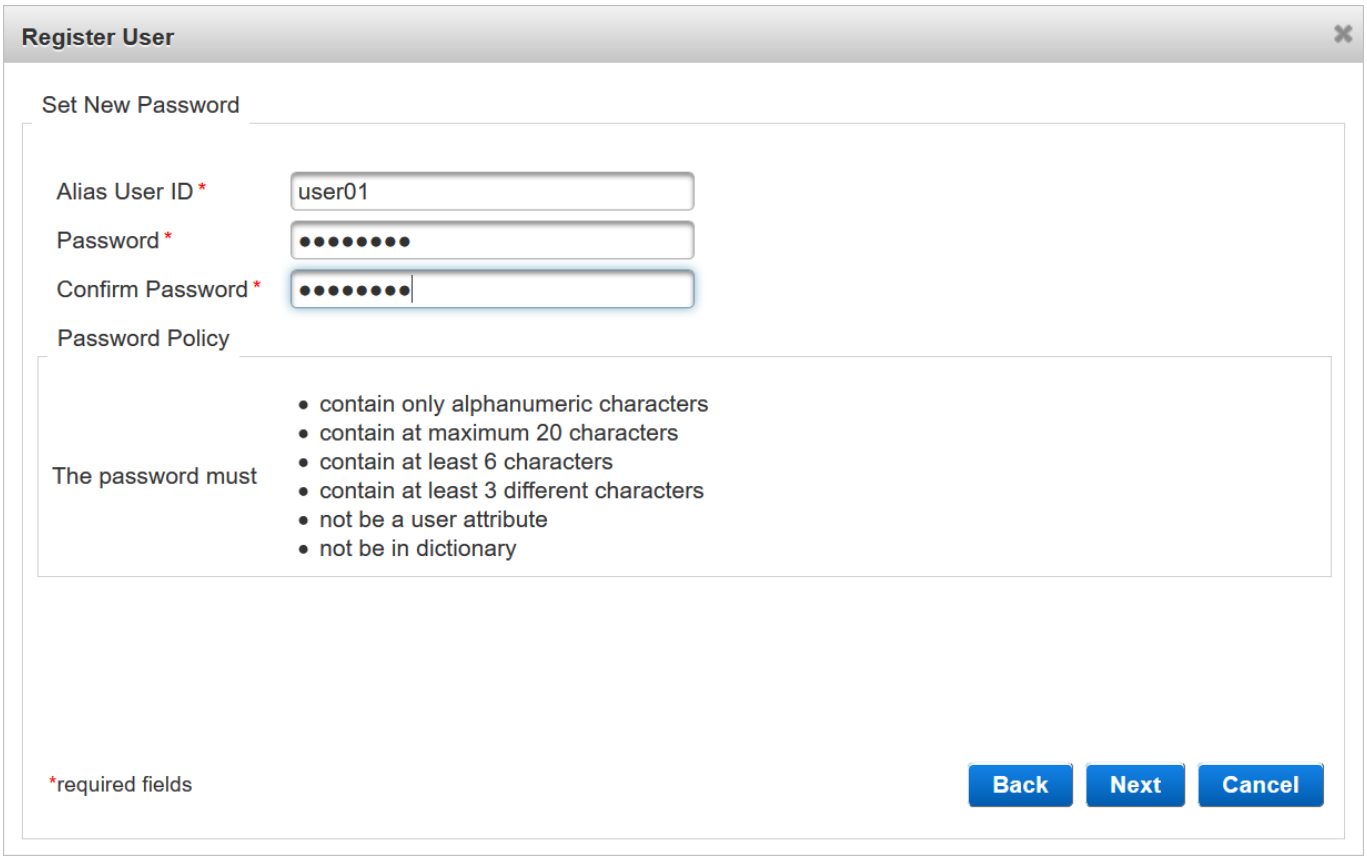
6. Click **Next** without assigning a role to the user.



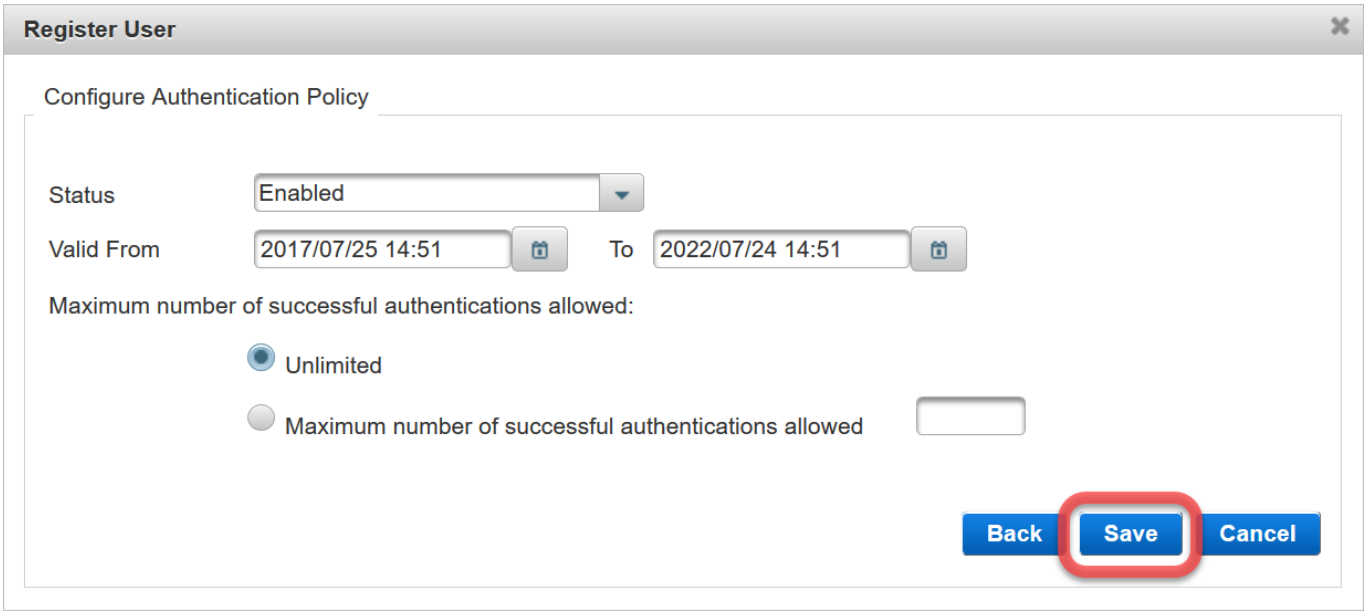
7. Select **Create Password** (1) (to create a static password authenticator) and click **Next** (2).



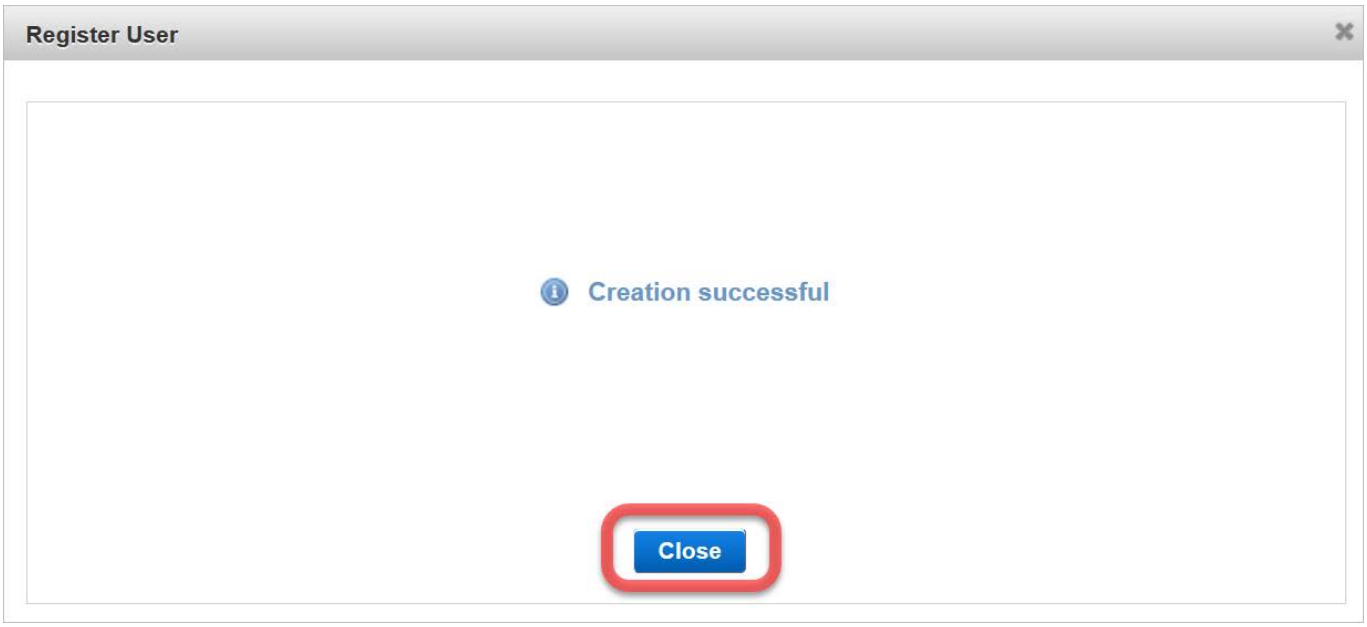
8. From the **Authentication Policy** drop-down list, select **Employee Static Password** (1) and click **Next** (2).



9. Enter and confirm a password for the user (for testing purposes, use *activ123*) and click **Next**.

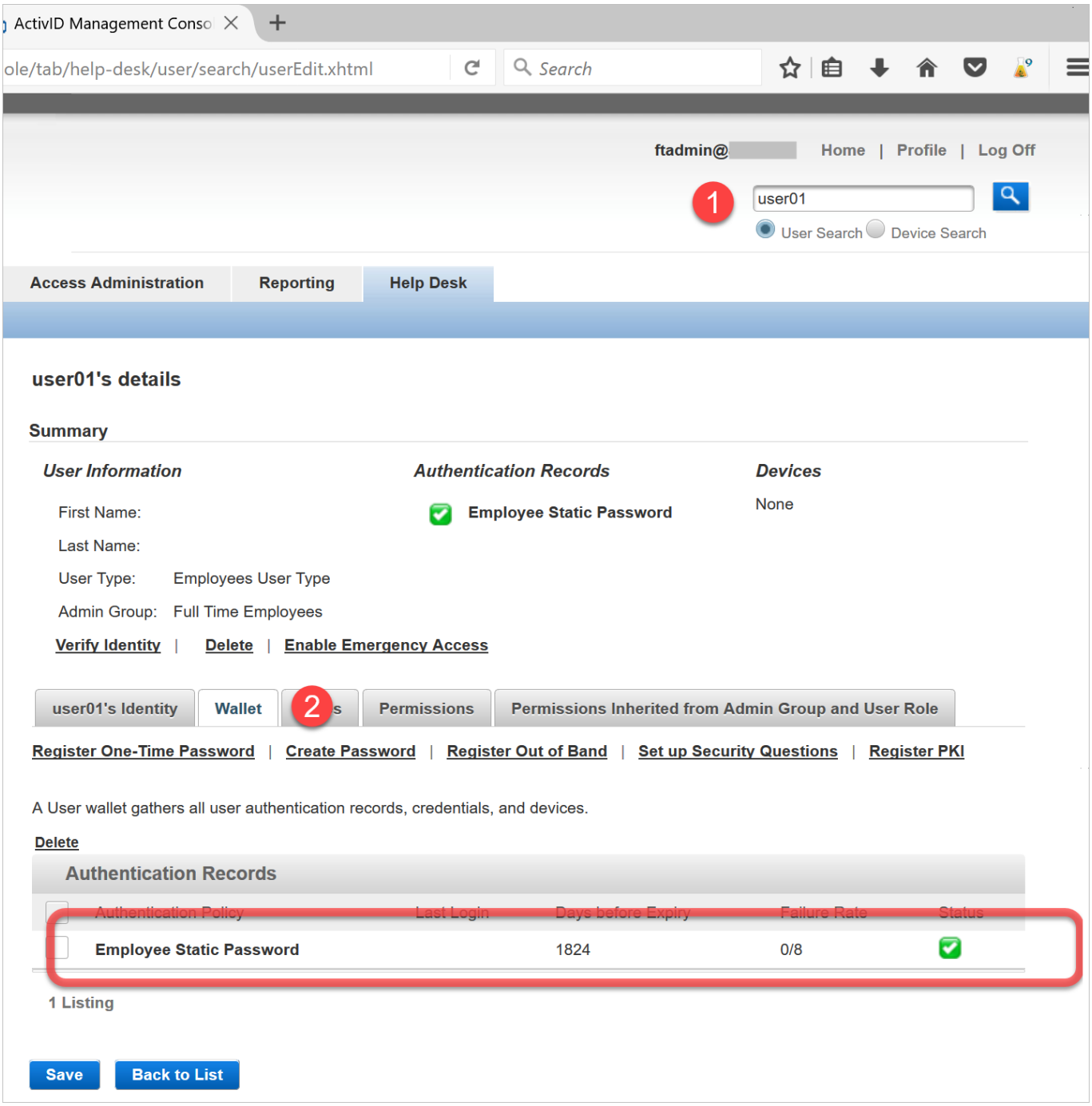


10. Leave all default validity parameters and click **Save**.



11. Click **Close**.
12. To verify that the password was created, search for the user (1).

    The user's details page is displayed.



13. Select the **Wallet** tab (2).

    In the Authentication Records list, the Employee Static Password authenticator is displayed and the active status is indicated by a green check mark.

4.0 Testing the Deployment

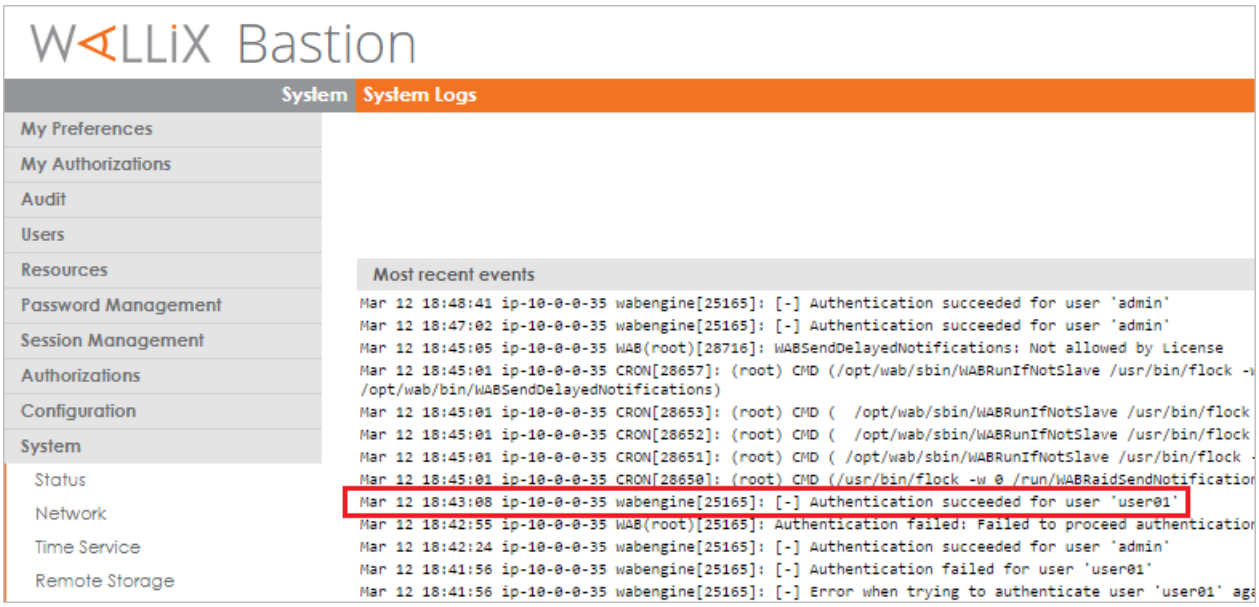
This section explains how to test the ActivID Appliance RADIUS authentication with the Wallix Bastion host.

1. Using a browser, connect to the Wallix Bastion host portal.

2. Log on as the test user.

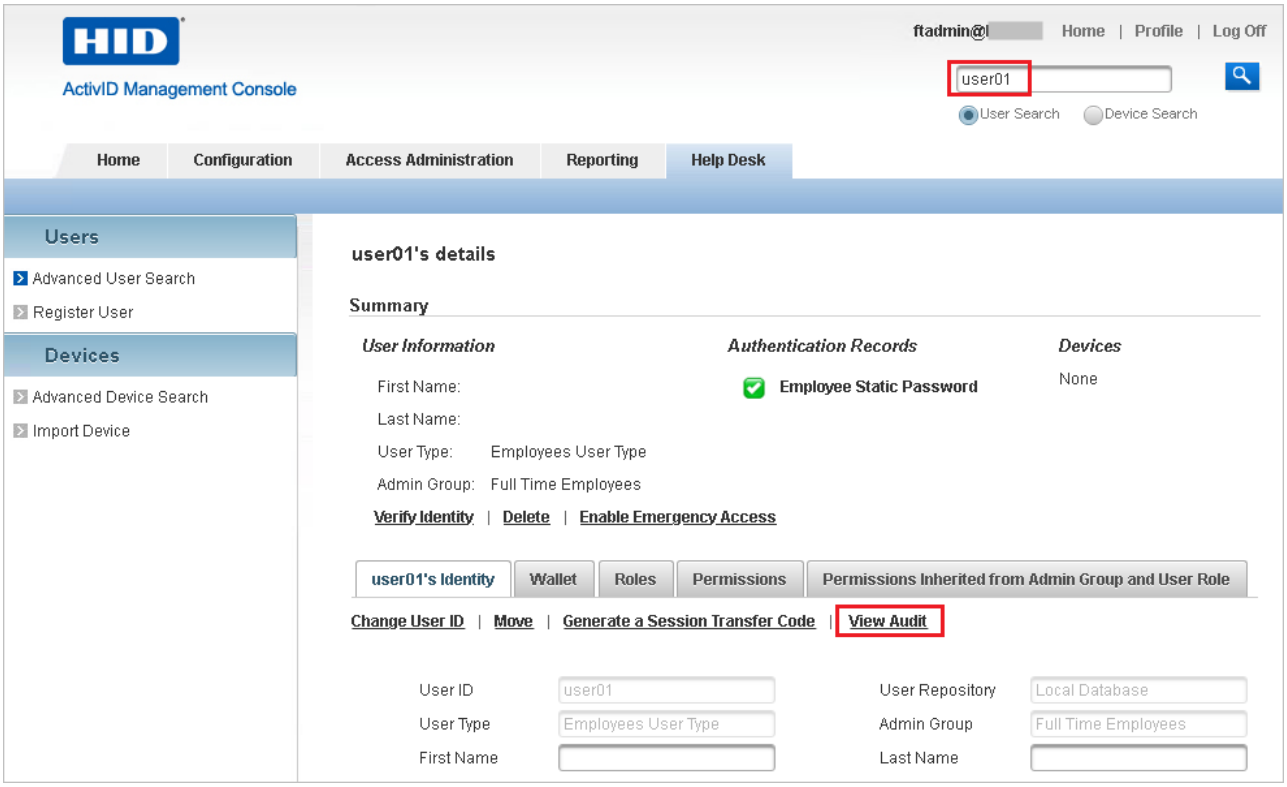
   The Welcome page is displayed (the options and layout might vary depending on the user's privileges).

- Verify the Syslog entry on the Wallix Bastion host for the successful user logon:

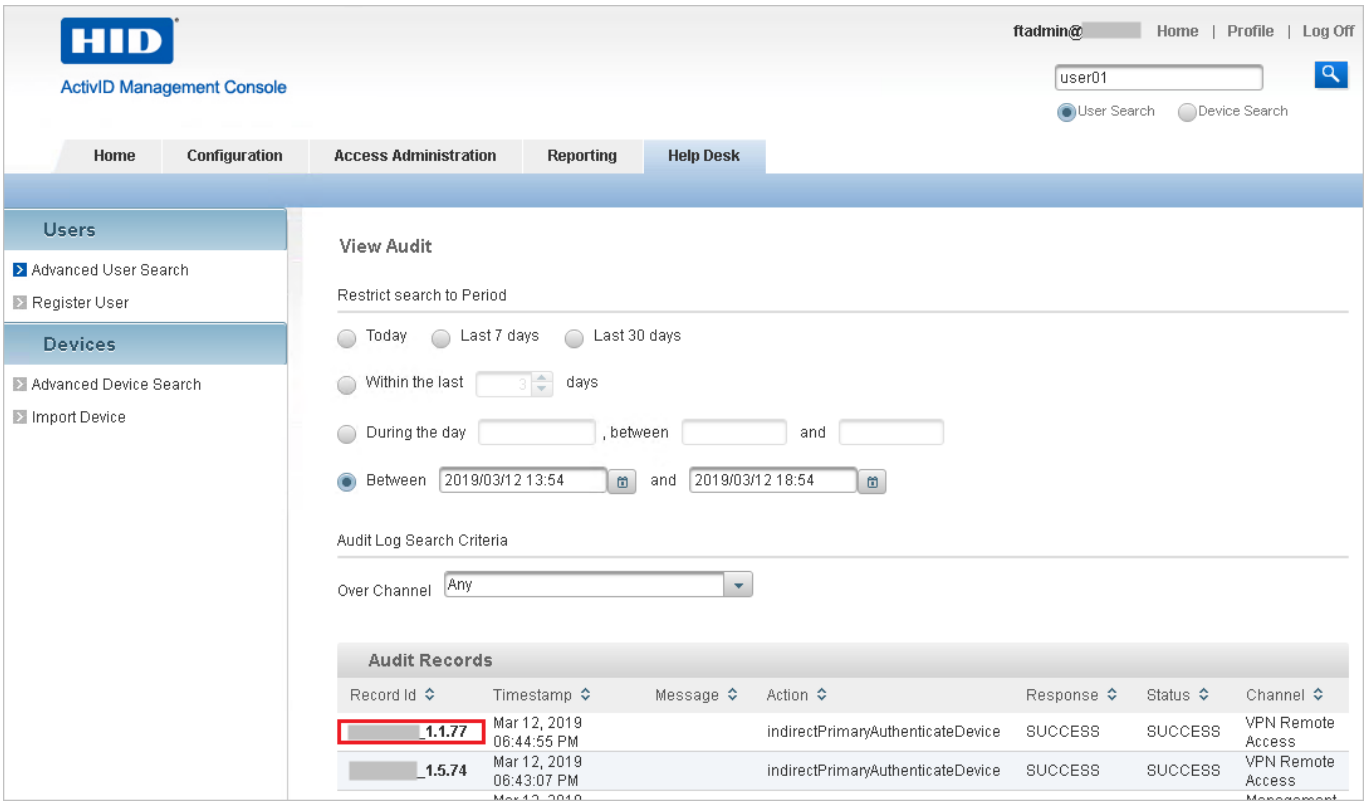


- Check the Audit entry on ActivID Appliance:

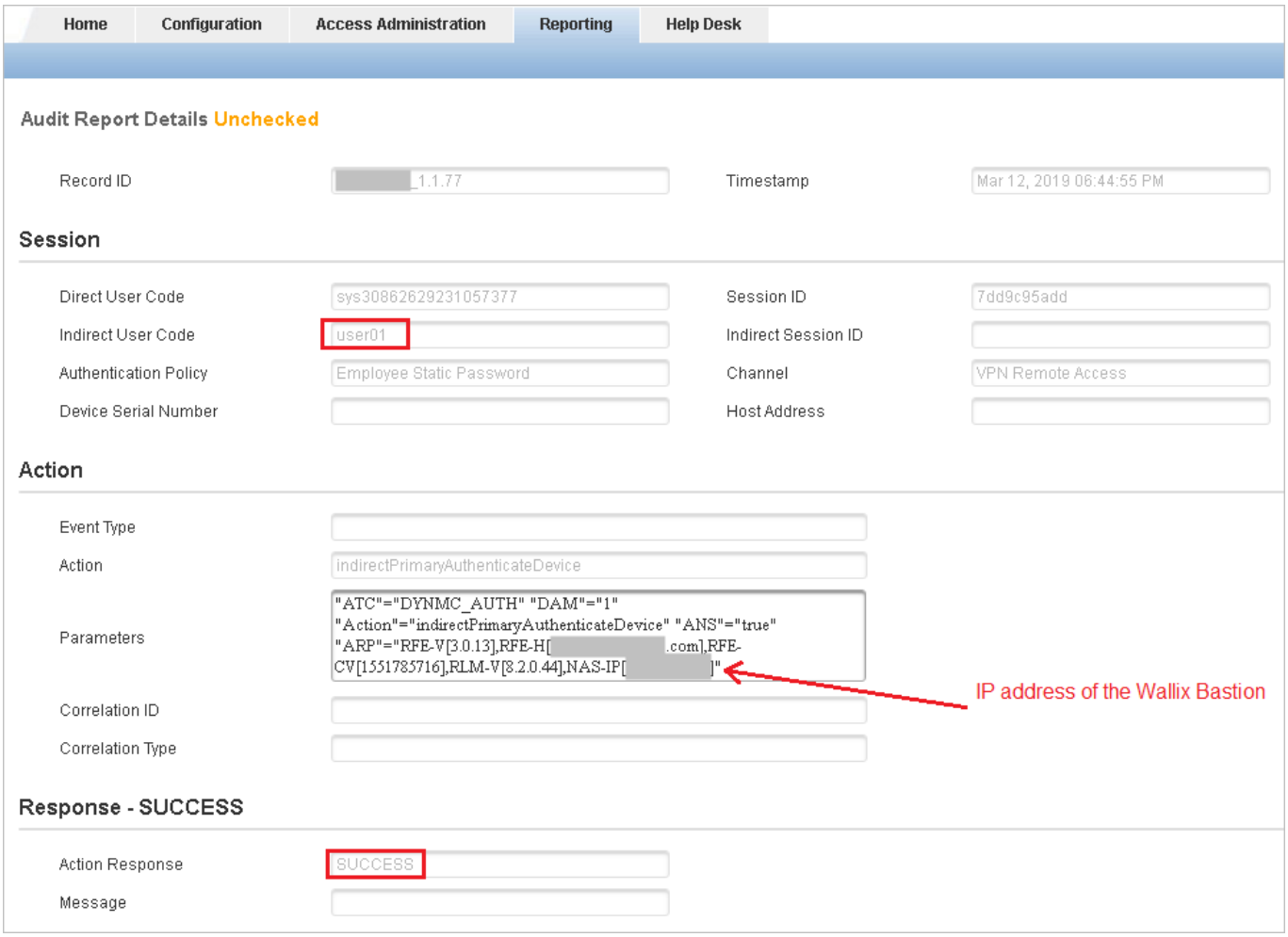
1. Log on to the ActivID Management Console and search for the test user.



2. In the user's **Identity** tab, click **View Audit** to list audit entries associated with the test user.



3. Select the audit record entry corresponding to the successful logon to the Wallix Bastion host. The SUCCESS status indicates the positive authentication.
4. Click the entry name in the **Record ID** column to view audit entry details.



The IP address of the Wallix Bastion host is displayed in the audit entry details.