



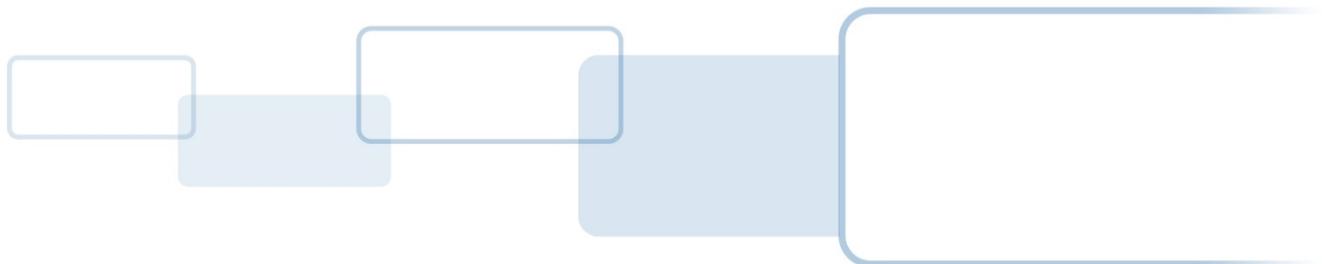
# **HID<sup>®</sup> ACTIVID<sup>®</sup> APPLIANCE WITH WALLIX<sup>®</sup> BASTION**

## **RADIUS TWO-FACTOR AUTHENTICATION CONFIGURATION GUIDE**

**DOCUMENT REFERENCE: APPL\_8.0\_WALLIX\_CG\_05.2019**

**PRODUCT VERSION: 8.0**

**MAY 2019**



## Copyright

© 2019 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

## Trademarks

HID, HID Global, the HID Blue Brick logo, the Chain Design and ActivID are trademarks or registered trademarks of HID Global, ASSA ABLOY AB, or its affiliates(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

## 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
<a href="#">blue</a>	Cross-references within the document.
<a href="#">blue, underline</a>	References to external web addresses.
<b>bold</b>	Action steps (paths, buttons, options); field and drop-down list labels; emphasis.
<i>italic</i>	File names, document titles, and file extensions.
Code snippets	Highlights <code>code snippets</code> within regular content.
Code samples	Highlights code samples
	<b>WARNING:</b> 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.
	<b>Important:</b> This symbol indicates something very important to the reader. Ignore this symbol at your own risk.
	<b>Note:</b> 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

Table of Contents .....	4
1.0 Introduction.....	5
1.1 Document Scope and Audience .....	5
2.0 Configuring the Wallix Bastion Host .....	6
2.1 Create an External Authentication Host.....	6
2.2 Create a Test User on the Wallix Bastion Host .....	8
3.0 Configuring ActivID Appliance .....	10
3.1 Configure the RADIUS Channel .....	10
3.2 Restart the RADIUS Front End.....	13
3.3 Create a New User on the ActivID Appliance.....	15
4.0 Testing the Deployment.....	22

## 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

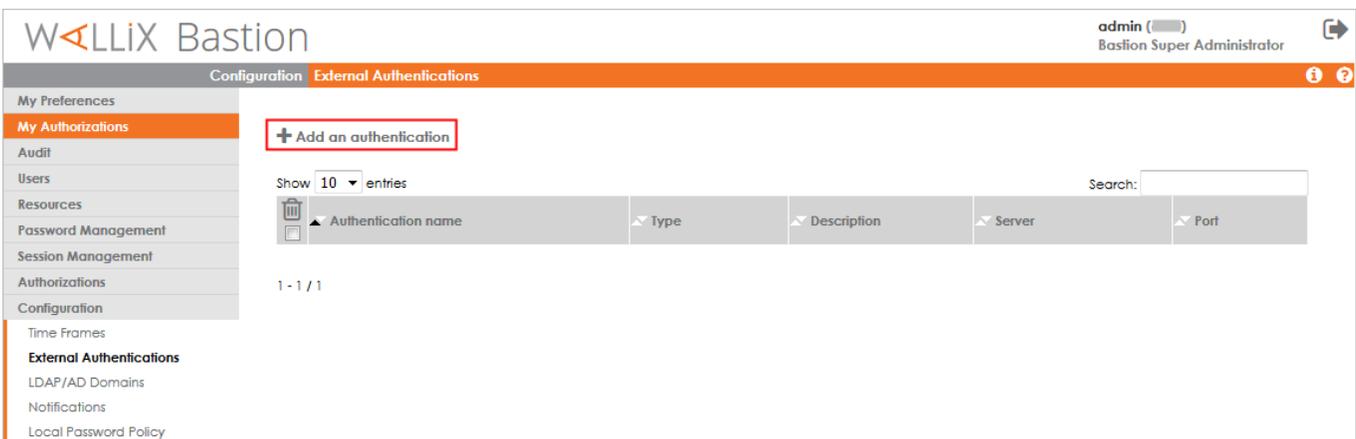
This section explains how to configure the Wallix Bastion host for external authentication with the ActivID Appliance.

- 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.

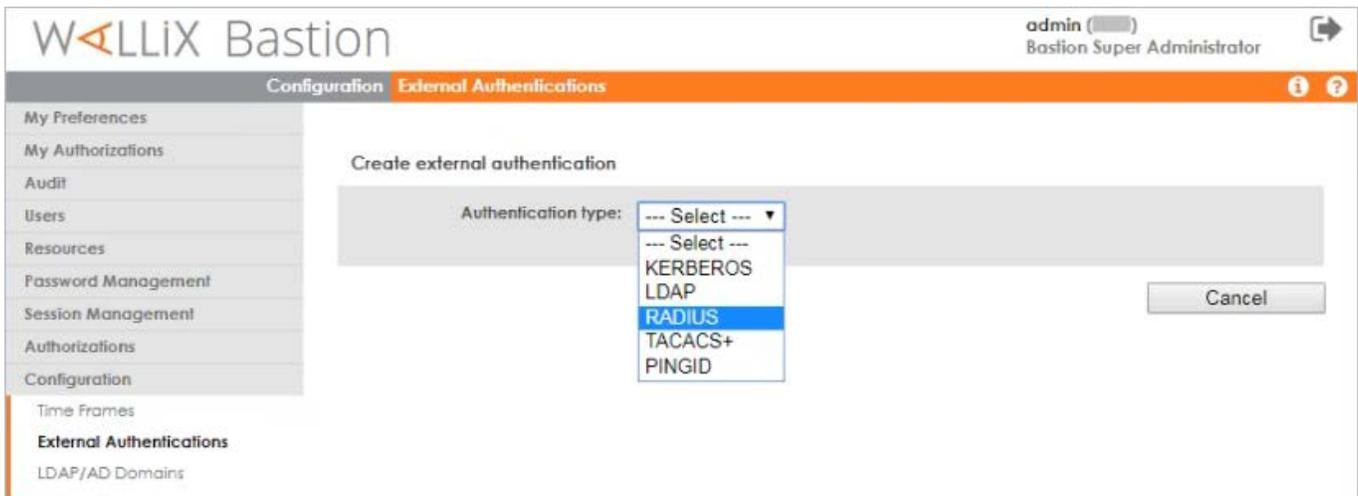
### 2.1 Create an External Authentication Host



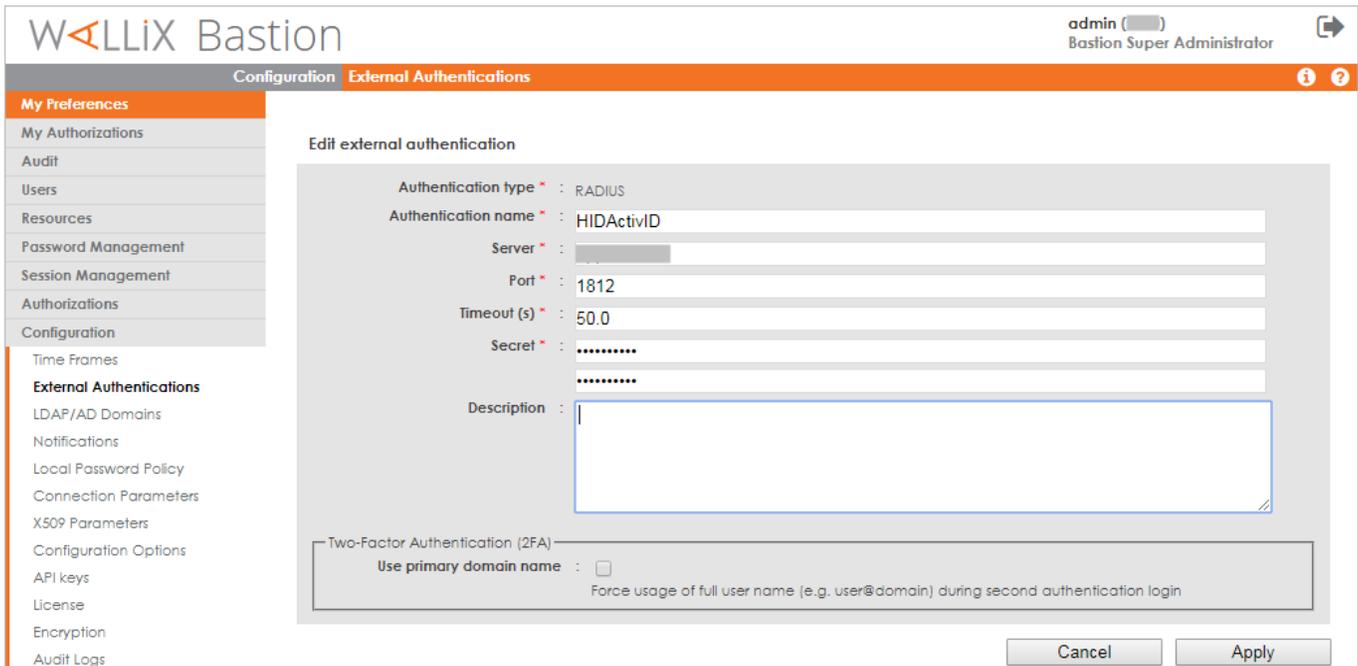
1. Using a browser, connect to the Wallix Bastion host portal and log on as an administrator.



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.

**WALLIX Bastion** admin ( ) Bastion Super Administrator

Configuration External Authentication

My Preferences  
My Authorizations  
Audit  
Users  
Resources  
Password Management  
Session Management  
Authorizations  
Configuration

**Data successfully saved.**

+ Add an authentication

Show 10 entries Search:

Authentication name	Type	Description	Server	Port
HIDActivID	RADIUS		[redacted]	1812

1 - 1 / 1

## 2.2 Create a Test User on the Wallix Bastion Host

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

**WALLIX Bastion** admin ( ) Bastion Super Administrator

Users Accounts

My Preferences  
My Authorizations  
Audit  
Users  
**Accounts**  
Groups  
Profiles  
Resources  
Password Management

+ Add a user

Show 10 entries Search:

User name	Display name	Profile	Authentication	Groups	Status	Last connection
admin	Bastion Super Administrator	WA8_administrator	local		✓	--

1 - 1 / 1

2. Click **Add a user**.

User name: user01  
Display name:  
Email: user01  
GPG key: Choose File No file chosen  
Preferred language: English  
Profile: user  
Disabled:   
Account expiration date: YYYY-MM-DD hh:mm  
Groups: User's groups

Available Groups  
Selected Groups

Authentication and backup servers  
Available Authentications: local  
Selected Authentications: HIDActivID

IP restrictions: IP/Subnets

Cancel Apply

3. Enter the required user parameters (illustrated above as a minimum) and click **Apply**.  
The new user is displayed in the list of Accounts.

WALLIX Bastion admin Bastion Super Administrator

Users Accounts

+ Add a user

Show 10 entries Search:

User name	Display name	Profile	Authentication	Groups	Status	Last connection
admin	Bastion Super Administrator	WAB_administrator	local		✓	--
user01		user	HIDActivID		✓	--

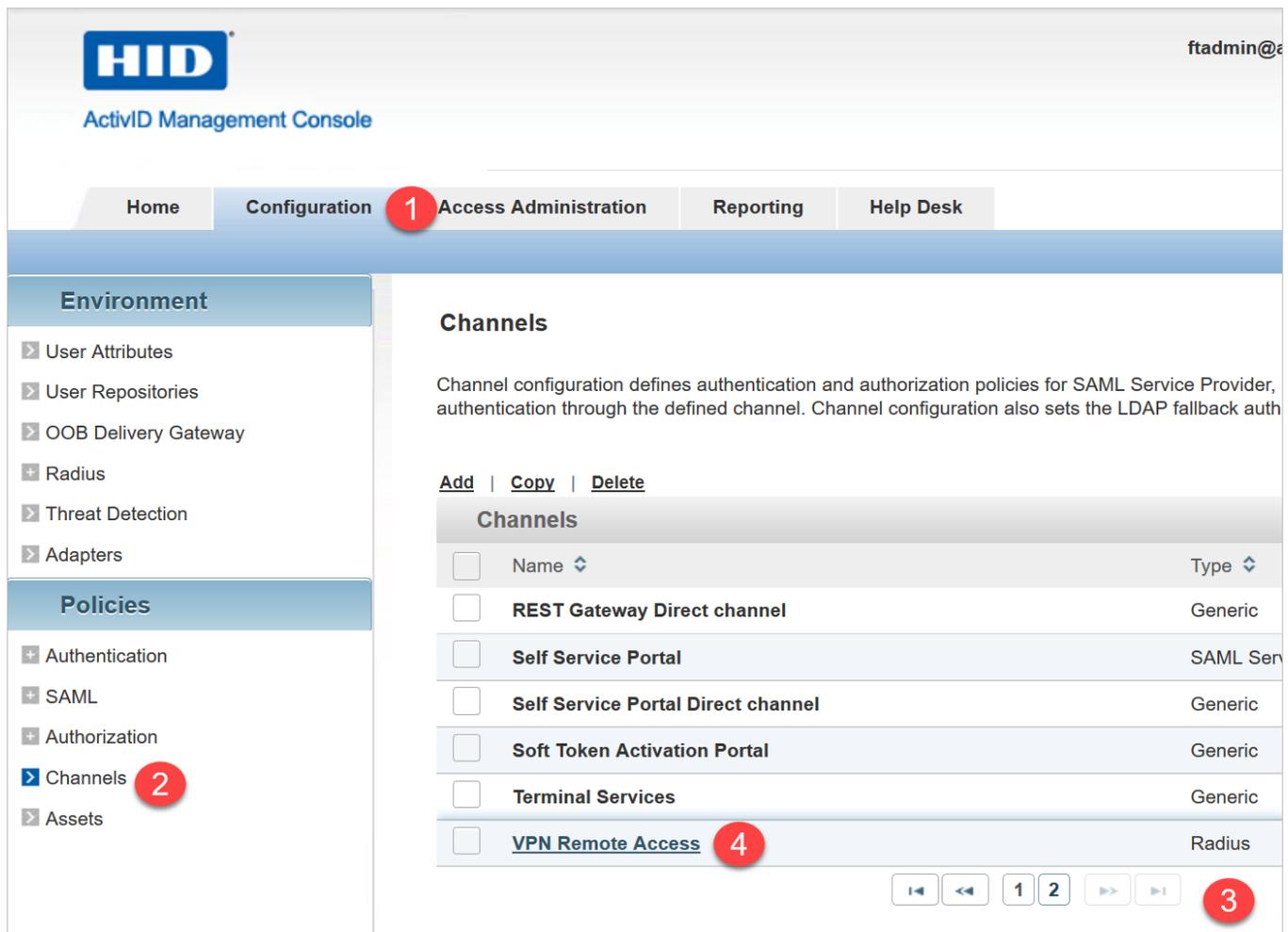
1 - 2 / 2

### 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

- 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*).



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

The screenshot shows the 'VPN Remote Access Details' configuration page in the ActivID Management Console. The 'Channel Policy' tab is selected. The 'Shared secret' field is highlighted with a red box. The 'User Identification' dropdown is set to 'User Centric'. The 'Add' section shows 'Authorized IP addresses or host names' with 'No result found' and '0 Listing'.

Environment

- User Attributes
- User Repositories
- OOB Delivery Gateway
- Radius
- Threat Detection
- Adapters

Policies

- Authentication
- SAML
- Authorization
- Channels
- Assets

VPN Remote Access Details

Name \* VPN Remote Access

Description Default RADIUS channel

Type \* Radius

Trusted Identity Providers | Authorization Profiles Selection Rules | Channel Policy | Fallback

Allowed Authentication Policies

Define Challenge Configuration | Set Authentication Forward Policy | Define Push-based Authentication

Shared secret \* [Redacted]

Confirm Shared secret \* [Redacted]

User Identification \* User Centric

Add

Authorized IP addresses or host names

No result found

0 Listing

Save Back to List

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.

**Add Authorized Host name or IP Address/CIDR subnet mask**

Host name  IP address (IPv4)

IP address (IPv4) \*

CIDR subnet mask

\*required fields

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

**VPN Remote Access Details**

Name \*  Code

Description

Type \*

[Define Challenge Configuration](#) | [Set Authentication Forward Policy](#) | [Define Push-based Authentication Configuration](#)

Shared secret \*

Confirm Shared secret \*

User Identification \*  [User Identification Configuration](#)

**Add** | **Delete**

Authorized IP addresses or host names

192. ....

---

1 Listing

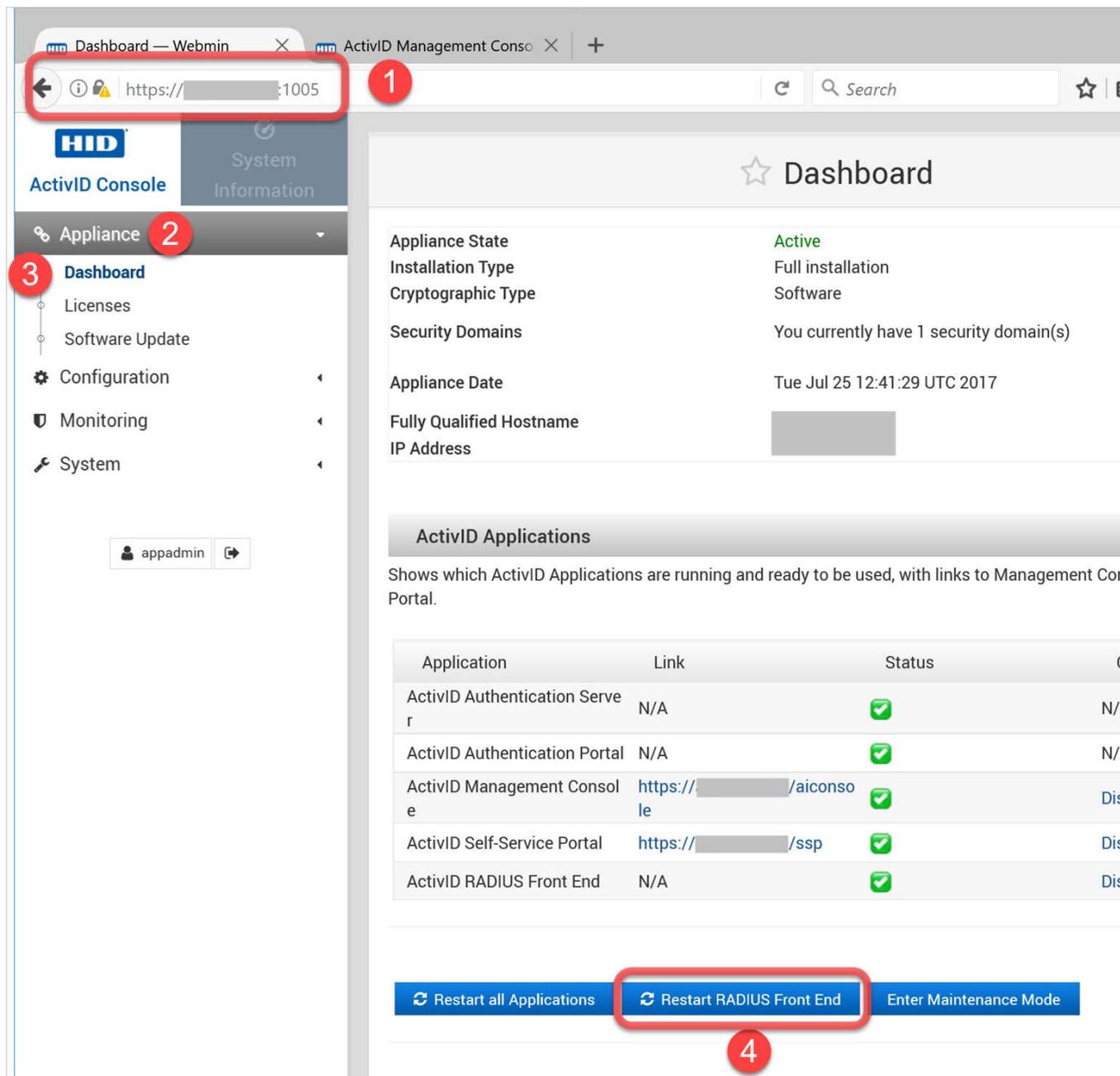
\*required fields

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

### 3.2 Restart the RADIUS Front End

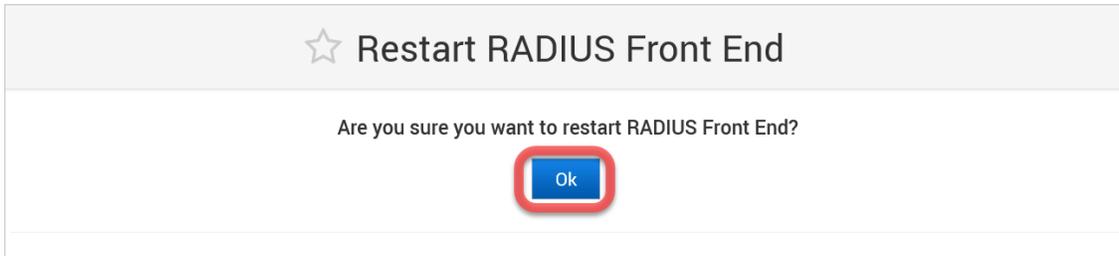
In order to apply the RADIUS configuration, you must restart the RADIUS Front End application.

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



- 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).



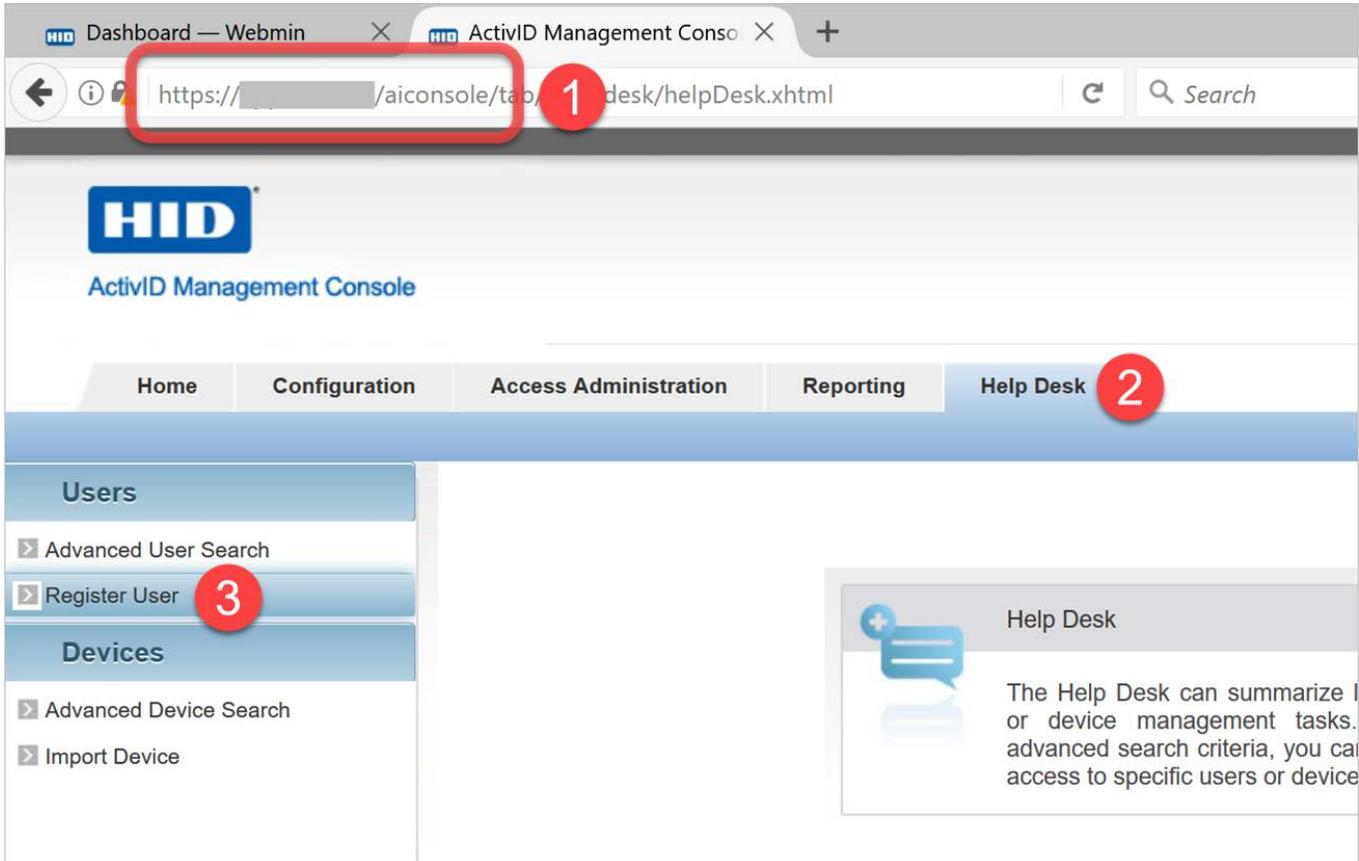
4. Click **OK**.

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.

- 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*).



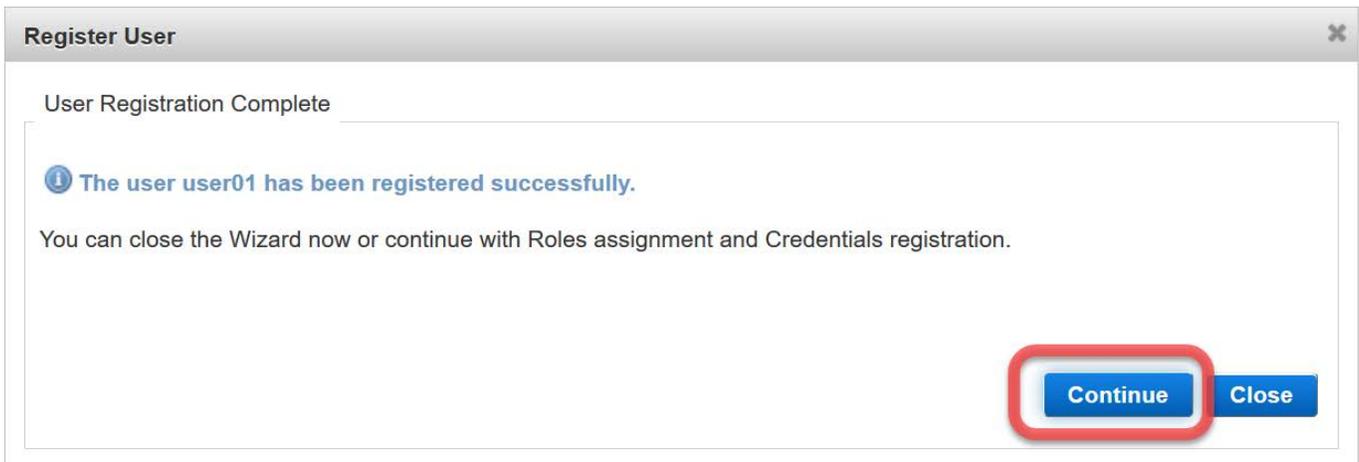
- Select the **Help Desk** tab (2) and, under **Users**, select **Register User** (3).

The screenshot shows the 'Register User' dialog box with the 'Select User Admin Group' section. A list of user groups is displayed, including 'Device Managers', 'Help Desk Operators', 'User Administrator', 'Systems User Type' (with sub-groups 'Soft Token Portal Administrators' and 'System Users'), 'ADFS Systems User Type', and 'Employees User Type' (with sub-groups 'Seos Unbound', 'Business Partners', 'Contractors', and 'Full Time Employees'). The 'Full Time Employees' group is highlighted with a red circle and the number '1'. Below the list, a text box contains 'Full Time Employees' and a 'Select Group' button is highlighted with a red circle and the number '2'.

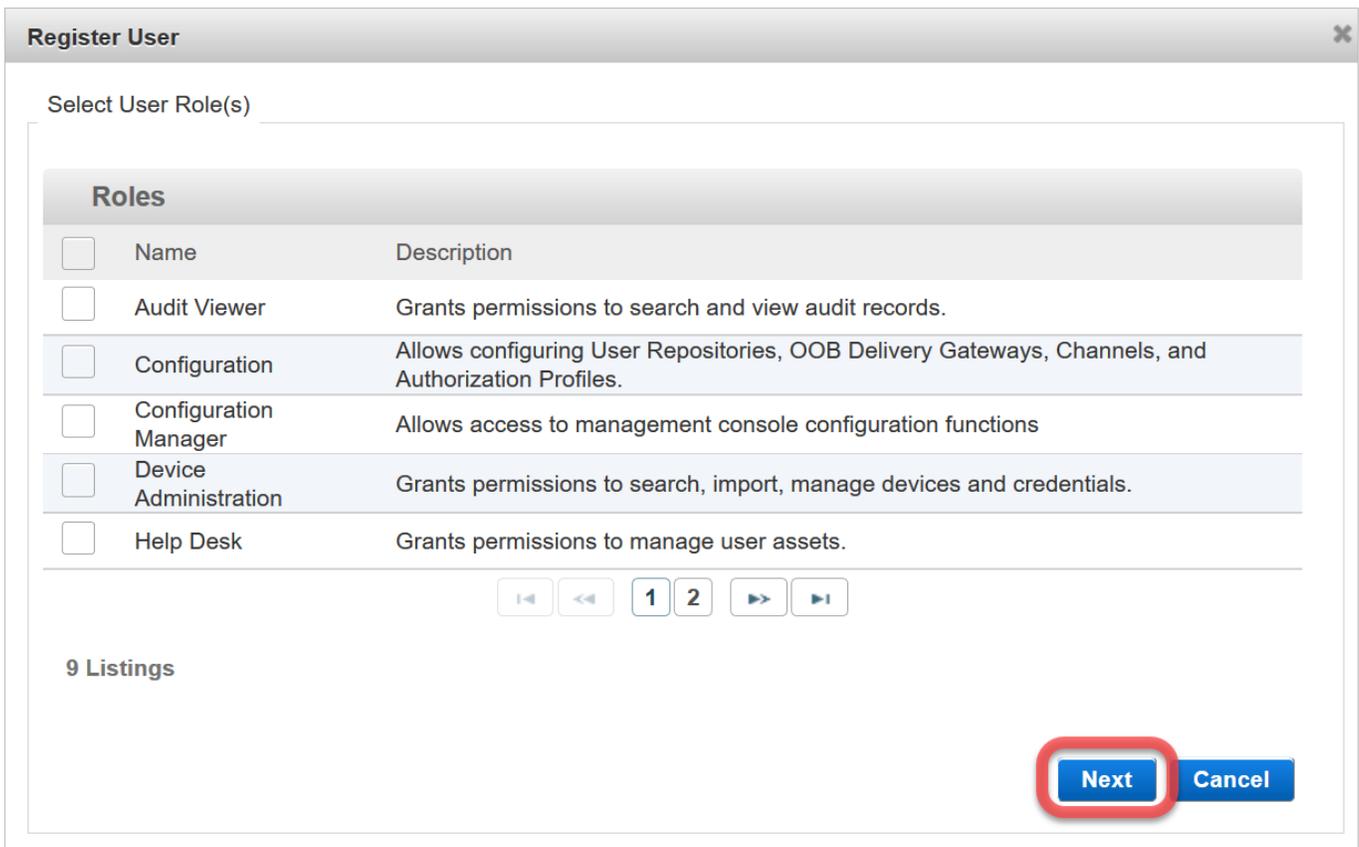
- Under **Employees User Type**, select **Full Time Employees** (1) and then click **Select Group** (2)

The screenshot shows the 'Register User' dialog box with the 'Configure User Attributes' section. It contains five input fields: 'User ID \*' (with 'user01' entered and a red circle '1' next to it), 'First Name', 'Last Name', 'Title', and 'E-Mail Address'. At the bottom left, there is a note '\*required fields'. At the bottom right, there are three buttons: 'Back', 'Next' (with a red circle '2' next to it), and 'Cancel'.

- 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.

**Register User**

Register User for Authentication

- Register One-Time Password
- 1** Create Password
- Register Out of Band
- Set up Security Questions
- Register PKI

**2** **Next** **Cancel**

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

**Register User**

Select Authentication Policy

Authentication Policy **1** Employee Static Password

**2** **Next** **Cancel**

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

**Register User** [Close]

Set New Password

Alias User ID \*

Password \*

Confirm Password \*

Password Policy

The password must

- contain only alphanumeric characters
- contain at maximum 20 characters
- contain at least 6 characters
- contain at least 3 different characters
- not be a user attribute
- not be in dictionary

\*required fields

**Back** **Next** **Cancel**

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

**Register User** [Close]

Configure Authentication Policy

Status

Valid From   To

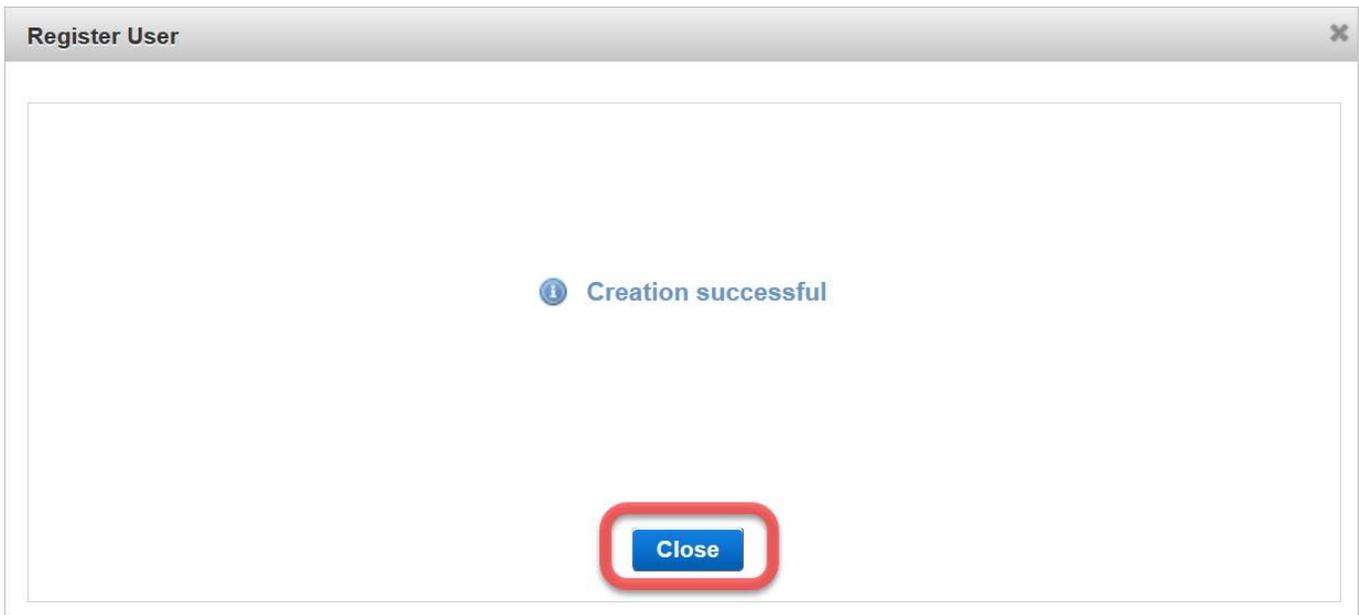
Maximum number of successful authentications allowed:

Unlimited

Maximum number of successful authentications allowed

**Back** **Save** **Cancel**

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.

ActivID Management Console

ftadmin@ Home | Profile | Log Off

1 user01

User Search Device Search

Access Administration Reporting Help Desk

### user01's details

#### Summary

User Information	Authentication Records	Devices
First Name: Last Name: User Type: Employees User Type Admin Group: Full Time Employees <a href="#">Verify Identity</a>   <a href="#">Delete</a>   <a href="#">Enable Emergency Access</a>	<input checked="" type="checkbox"/> Employee Static Password	None

user01's Identity **Wallet** 2 s Permissions Permissions Inherited from Admin Group and User Role

[Register One-Time Password](#) | [Create Password](#) | [Register Out of Band](#) | [Set up Security Questions](#) | [Register PKI](#)

A User wallet gathers all user authentication records, credentials, and devices.

[Delete](#)

Authentication Records					
<input type="checkbox"/>	Authentication Policy	Last Login	Days before Expiry	Failure Rate	Status
<input type="checkbox"/>	Employee Static Password		1824	0/8	<input checked="" type="checkbox"/>

1 Listing

[Save](#) [Back to List](#)

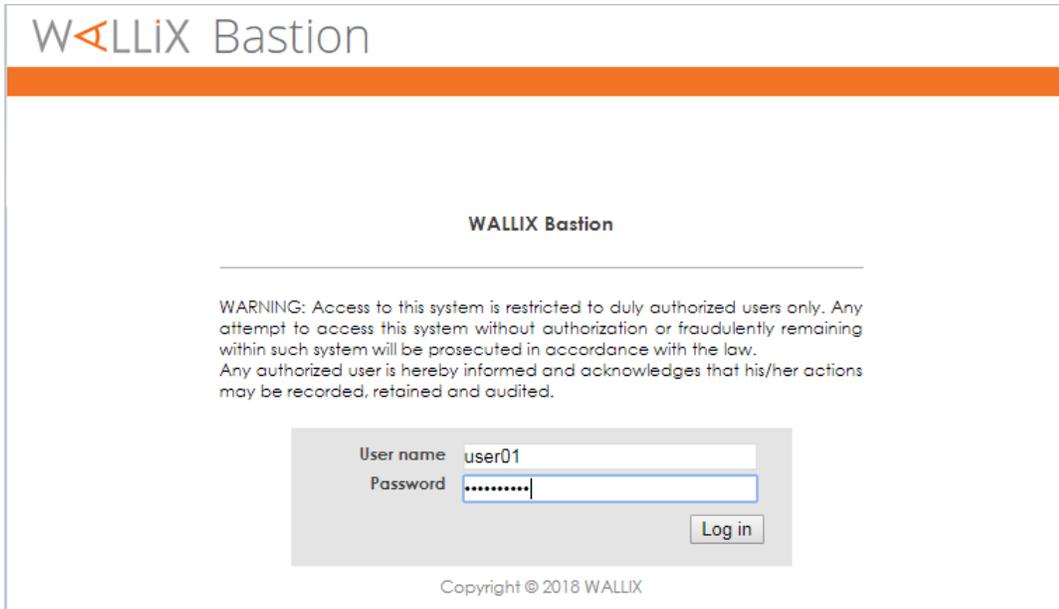
13. Select the **Wallet** tab (2).

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:

The screenshot shows the Wallix Bastion interface with the 'System Logs' tab selected. The left sidebar contains navigation options like 'My Preferences', 'My Authorizations', 'Audit', 'Users', 'Resources', 'Password Management', 'Session Management', 'Authorizations', 'Configuration', and 'System'. The main area displays 'Most recent events' as a list of syslog entries. One entry is highlighted with a red box: 'Mar 12 18:43:08 ip-10-0-0-35 wabengine[25165]: [-] Authentication succeeded for user 'user01''. Other entries show successful logins for 'admin' and failed attempts for 'user01'.

- Check the Audit entry on ActivID Appliance:

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

The screenshot shows the ActivID Management Console interface. At the top right, there is a search bar with 'user01' entered and a search icon. Below the search bar are 'User Search' and 'Device Search' radio buttons. The main navigation bar includes 'Home', 'Configuration', 'Access Administration', 'Reporting', and 'Help Desk'. The 'Users' section is active, showing 'user01's details'. The 'Summary' section includes 'User Information' (First Name, Last Name, User Type: Employees User Type, Admin Group: Full Time Employees), 'Authentication Records' (Employee Static Password checked), and 'Devices' (None). At the bottom, there are fields for 'user01's Identity', 'Wallet', 'Roles', 'Permissions', and 'Permissions Inherited from Admin Group and User Role'. A 'View Audit' button is highlighted with a red box. At the bottom of the details section, there are input fields for User ID (user01), User Repository (Local Database), User Type (Employees User Type), Admin Group (Full Time Employees), First Name, and Last Name.

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

**HID**  
ActivID Management Console

ftadmin@ Home | Profile | Log Off

user01 🔍  
 User Search  Device Search

Home Configuration Access Administration Reporting Help Desk

**Users**  
Advanced User Search  
Register User

**Devices**  
Advanced Device Search  
Import Device

### View Audit

Restrict search to Period

Today  Last 7 days  Last 30 days

Within the last  days

During the day  , between  and

Between  and

Audit Log Search Criteria

Over Channel

Record ID	Timestamp	Message	Action	Response	Status	Channel
1.1.77	Mar 12, 2019 06:44:55 PM		indirectPrimaryAuthenticateDevice	SUCCESS	SUCCESS	VPN Remote Access
1.5.74	Mar 12, 2019 06:43:07 PM		indirectPrimaryAuthenticateDevice	SUCCESS	SUCCESS	VPN Remote Access

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

<b>Home</b>	<b>Configuration</b>	<b>Access Administration</b>	<b>Reporting</b>	<b>Help Desk</b>
<b>Audit Report Details Unchecked</b>				
Record ID	1.1.77	Timestamp	Mar 12, 2019 06:44:55 PM	
<b>Session</b>				
Direct User Code	sys30862629231057377	Session ID	7dd9c95add	
Indirect User Code	user01	Indirect Session ID		
Authentication Policy	Employee Static Password	Channel	VPN Remote Access	
Device Serial Number		Host Address		
<b>Action</b>				
Event Type				
Action	indirectPrimaryAuthenticateDevice			
Parameters	"ATC"="DYNMC_AUTH" "DAM"="1" "Action"="indirectPrimaryAuthenticateDevice" "ANS"="true" "ARP"="RFE-V[3.0.13],RFE-H[.com],RFE- CV[1551783716],RLM-V[8.2.0.44],NAS-IP[ ]"			
Correlation ID				
Correlation Type				
<b>Response - SUCCESS</b>				
Action Response	SUCCESS			
Message				

IP address of the Wallix Bastion

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

