

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



hidglobal.com



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	Europe, Middle East and Africa	Asia Pacific
+1 800 670 6892	+33 (0) 1 74 18 17 70	+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.
<u>blue, underline</u>	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
A	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

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

WADNING A.	and the lists with	teres is unabled and the shifts of the standard stress which it has
attempt to a	ccess this system	m without authorization or fraudulently remaining
within such sys	stem will be pro	secuted in accordance with the law.
Any authorize	d user is hereby	r informed and acknowledges that his/her actions
may be recor	ded, retained a	and audited.
	User name	admin
	Password	
	Password	······

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

W ∢ LLiX Bast	tion				admin () Bastion Super Administrator	۲
Confi	guration External Authentications					1 9
My Preferences						
My Authorizations	+ Add an authentication					
Audit						
Users	Show 10 👻 entries			s	iearch:	
Resources	m	Turne	Description	6	n-4	
Password Management		_ туре	∠ Description	Server	~ гоп	
Session Management						
Authorizations	1-1/1					
Configuration						
Time Frames						
External Authentications						
LDAP/AD Domains						
Notifications						
Local Password Policy						

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



W ∢ LLiX Bas	stion		admin (IIIII) Bastion Super Administrator	۲
Co	nfiguration External Authentications			0 0
My Preferences				
My Authorizations	Create external authentication			
Audit	cicale external admentication			
Users	Authentication type:	Select 🔻		
Resources		Select		
Password Management		LDAP	Canad	
Session Management		RADIUS	Cancel	
Authorizations		TACACS+		
Configuration		PINGID		
Time Frames				
External Authentications				
LDAP/AD Domains				

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

W ∢ LLiX Bast	ion	admin (Total) Bastion Super Administrator	•
Confi	guration External Authentications	6 6	ð
My Preferences			
My Authorizations	Edit external authentication		
Audit			
Users	Authentication type * :	RADIUS	
Resources	Authentication name * :	HIDActivID	
Password Management	Server * :	and the second se	
Session Management	Port * :	1812	
Authorizations	Timeout (s) * :	50.0	
Configuration	Secret * ·	50.0	
Time Frames	Sucrei .		
External Authentications			
LDAP/AD Domains	Description :		
Notifications			
Local Password Policy			
Connection Parameters			
X509 Parameters			
Configuration Options	Ivo-Factor Authentication (2FA) —		
API keys	use printing domain name	Force usage of full user name (e.g. user@domain) during second authentication login	
License			
Encryption		Consel A 1	
Audit Logs		Cancei Apply	

- 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.



W ∢ LLiX Bas	tion			admin (Bastion Supe) er Administrator	•
Con	figuration External Authentication:					00
My Preferences	A b b b b b b b b b b					
My Authorizations	U Data successfully saved.					
Audit	Add an authentication					
Users						
Resources	Show 10 T entries			Search:		
Password Management	<u>ا</u>					
Session Management	Authentication name	🔿 Туре	Description	Server	∠ Port	
Authorizations	HIDActivID	RADIUS			1812	
Configuration	1 - 1 / 1					

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

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

W ∢ LLiX Bas	tion	admin () Bastion Super Administrator
User	rs Accounts	() ()
My Preferences		
My Authorizations	+ Add a user	+ 1
Audit		
Users		
Accounts	Show 10 - entries	Search:
Groups	Iter name Dirplay name Profile Authentiagtion Crouns	Statur Last
Profiles		connection
Resources	admin Bastion Super Administrator WAB_administrator 🝳 local	 ✓
Password Management	1-1/1	

2. Click Add a user.



User name *:	user01	
Display name :		
Email * :	user01	
CBC have	User's email	
GPG Key :	Choose File No file chosen	
Preferred : language *	English	
Profile *:	user T	
Disabled :		
Account: expiration		
date	YYYY-MM-DD hh:mm	
Gloups	User's groups	
	Available Groups	Selected Groups
	Q	Q
		Select and click 🔊
	<u>ــــــــــــــــــــــــــــــــــــ</u>	▲
		0
		3
	.	
	Select all	Ø Delete all
Authentication :	List of authentication sources to validate this user passwo	ord
servers *		
	Available Authentications	Selected Authentications
	Q	0
		Select and click
	local	HIDActivID
		•
		•
- IP restrictions		
	IP/Subnets ▼	0
		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.

W ∢ LLiX Bas	tion	admin (119) Bastion Super	Administrator
User	Accounts		i 😯
My Preferences			
My Authorizations	Add a user		+ L
Audit			
Users			
Accounts	Show 10 • entries	Search:	
Groups		uthentication Groups	Status
Profiles		one of our of ou	connection
Resources	admin Bastion Super Administrator WAB_administrator ${f Q}_{{f c}}$ lo	ocal	✓
Password Management	user01 user H	IDActivID	 ✓
Session Management	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

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

HID				ftadmin@a
ActivID Management Cor	sole			
Home Configur	tion 1 Access Administration	Reporting	Help Desk	
	-			
Environment	Ohannala			
User Attributes	Channels			
User Repositories	Channel configuration defines	s authentication ar	nd authorization po	licies for SAML Service Provider,
OOB Delivery Gateway	autrentication through the de	anned channel. Cha	annei comiguration	also sets the LDAP failback auth
🗄 Radius	Add Copy Delete			
Threat Detection	Channels			
Adapters	Name 🗘			Type ᅌ
Policies	REST Gateway Dire	ect channel		Generic
+ Authentication	Self Service Portal			SAML Serv
I SAML	Self Service Portal	Direct channel		Generic
Authorization	Soft Token Activati	on Portal		Generic
Channels 2	Terminal Services			Generic
Assets	VPN Remote Acces	<u>ss</u> 4		Radius
			14 <4	12 🕨 🖬 3

- 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.



ActivID Managemen	t Console						User :
Home Cor	nfiguration	Access Administration	Reporting	Help Desk			
Environment User Attributes User Repositories OOB Delivery Gateway Radius Threat Detection		VPN Remote Access Name* Description Type*	Details	VPN Remote Access Default RADIUS cha Radius	s annel		c
Adapters Policies Authentication SAML Authorization		Trusted Identity Provide Allowed Authentication Define Challenge Configur	Policies	rization Profiles Sele	ard Policy	Channel Policy	Fallbac
ChannelsAssets		Shared secret * Confirm Shared secret * User Identification *		User Centric			
		Add Authorized IP addresses of No result found 0 Listing Save Back to List	or host names				,

- 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.



Host name IP addre	ss (IPv4)	
IP address (IPv4)*	192.	
CIDR subnet mask	24	
required fields		

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

Name*	VPN Remote Access	Code CH_VPN
Description	Default RADIUS channel	
Type *	Radius	
Trusted Identity Providers	Authorization Profiles Selection Rules Cha	annel Policy Fallback Authentication
Allowed Authentication Poli	cies	
Shared secret*	••••••	
Shared secret*	••••••	
Confirm Shared secret*	•••••	
Lear Identification *	User Centric	User Identification Configuration
User identification		
Add Delete		
Add Delete Authorized IP addresse	s or host names	

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).

A Restart RADIUS Front End
Are you sure you want to restart RADIUS Front End?

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://<appliancehostname>/aiconsole) and log on as an operator with help desk privileges (for example, *ftadmin*).

m Dashboard — V	Vebmin X 📶	ActivID Management Conso	× +		
+ 🛈 🖌 https://	//aicons	sole/tap, 1 desk/helpDes	k.xhtml	G	Q Search
HID ActivID Mana	gement Console				
Home	Configuration	Access Administration	Reporting	Help Desk	2
Users					
Advanced User Sea	arch				
Register User			0	Help Desk	
Devices Advanced Device S Import Device	earch			The Help I or device advanced s access to s	Desk can summarize l management tasks. search criteria, you ca pecific users or device

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



Register User	×
Select User Admin Group	
Device Managers: ActivID Administrators with permissions for device management	^
Help Desk Operators: ActivID Administrators with permissions for help desk operations	
User Administrator: ActivID Administrators with permissions for user and group management	
🔻 😹 Systems User Type	
Soft Token Portal Administrators: Soft Token Portal Administrators Group	
System Users: Users allowing external systems authentication and authorization	
& ADFS Systems User Type	
💌 🚴 Employees User Type	
Seos Unbound: Anonymous users for Unbound Seos devices	
Business Partners: Sample for Business Partners	
Le Contractors: Sample for Contractors	
S Full Time Employees: Sample for Employees	v
Group Full Time Employees Select Group	

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

Register User					×
Configure User At	tributes				
User ID*	user01	 1			
First Name					
Last Name					
Title		7			
E-Mail Address					
*required fields			Back	Next	Cancel
				2	

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



Register User	×
User Registration Complete	
In the user user01 has been registered successfully.	
You can close the Wizard now or continue with Roles assignment and Credentials registration.	
Continue	

5. Click Continue.

Select User Role(s) Roles Name Description Audit Viewer Grants permissions to search and view audit records. Configuration Allows configuring User Repositories, OOB Delivery Gateways, Channels, and Authorization Profiles. Configuration Allows access to management console configuration functions	Register User		×
Roles Name Description Audit Viewer Grants permissions to search and view audit records. Configuration Allows configuring User Repositories, OOB Delivery Gateways, Channels, and Authorization Profiles. Configuration Allows access to management console configuration functions	Select User Role(s)		
Roles Name Description Audit Viewer Grants permissions to search and view audit records. Configuration Allows configuring User Repositories, OOB Delivery Gateways, Channels, and Authorization Profiles. Configuration Allows access to management console configuration functions			
Name Description Audit Viewer Grants permissions to search and view audit records. Configuration Allows configuring User Repositories, OOB Delivery Gateways, Channels, and Authorization Profiles. Configuration Allows access to management console configuration functions	Roles		
Audit Viewer Grants permissions to search and view audit records. Configuration Allows configuring User Repositories, OOB Delivery Gateways, Channels, and Authorization Profiles. Configuration Allows access to management console configuration functions	Name	Description	
Configuration Allows configuring User Repositories, OOB Delivery Gateways, Channels, and Authorization Profiles. Configuration Manager Allows access to management console configuration functions	Audit Viewer	Grants permissions to search and view audit records.	
Configuration Manager Allows access to management console configuration functions	Configuration	Allows configuring User Repositories, OOB Delivery Gateways, Channels, and Authorization Profiles.	
	Configuration Manager	Allows access to management console configuration functions	
Device Administration Grants permissions to search, import, manage devices and credentials.	Device Administration	Grants permissions to search, import, manage devices and credentials.	
Help Desk Grants permissions to manage user assets.	Help Desk	Grants permissions to manage user assets.	
9 Listings	9 Listings	I 2 De De Cancel	

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



Re	gister	User	×
R	egiste	er User for Authentication	
		Register One-Time Password	
1		Create Password	
	\bigcirc	Register Out of Band	
	\bigcirc	Set up Security Questions	
	\bigcirc	Register PKI	
		2 Next Cancel	

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

Register User			х
Select Authentication P	olicy		
Authentication Policy	Employee Static Password	1	-
			2 Next Cancel

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



Page 19

Register User			×
Set New Password			
Alias User ID* Password*	user01		
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		×
Configure Authe	ntication Policy	
Status	Enabled	
Valid From	2017/07/25 14:51 To 2022/07/24 14:51	
Maximum num	er of successful authentications allowed:	
	Unlimited	
	Maximum number of successful authentications allowed	
	Back Save Cancel	

10. Leave all default validity parameters and click Save.



Register User		×
0	Creation successful	
	Close	

- 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 Conso	× +					
e/tab/help-desk/user/sea	rch/userEdit.xhtn	nl C'	Q Search	☆ 自	↓ ⋒ ♥	2
			ftadmin@	D Hom	ne Profile Log	g Off
				upper04		a
				User Search	b Device Search	
Access Administration	Reporting	Help Desk				
user01's details						
Summary						
User Information		Authentic	ation Records	Devices		
First Name:		🗹 Em	ployee Static Password	None		
Last Name:						
User Type: Employ	ees User Type					
Admin Group: Full Tim	e Employees					
Verify Identity Del	ete Enable En	nergency Access				
user01's Identity	allet 2 s	Permissions	Permissions Inherited from	Admin Group and	d User Role	
Register One-Time Passw	ord Create Pa	ssword <u>Regis</u>	ter Out of Band <u>Set up Sec</u>	urity Questions	Register PKI	
			and device a			
A Oser wallet gathers all use	er authentication re	cords, credentials,	, and devices.			
Authentication Re	cords					
Authentication Poli	CV	Last Login	Davs before Expiry	Failure Ra	te Status	
Employee Static F	Password	2.01209.11	1824	0/8		
				5,5		
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.

W∢LLiX	Bastion
	WALLIX Bastion
	WARNING: Access to this system is restricted to duly authorized users only. Any attempt to access this system without authorization or fraudulently remaining within such system will be prosecuted in accordance with the law. Any authorized user is hereby informed and acknowledges that his/her actions may be recorded, retained and audited.
	User name user01 Password Log in
	Copyright © 2018 WALLIX

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: ٠

W ∢ LLiX Bas	tion
Syste	system Logs
My Preferences	
My Authorizations	
Audit	
Users	
Resources	Most recent events
Password Management	Mar 12 18:48:41 ip-10-0-0-35 wabengine[25165]: [-] Authentication succeeded for user 'admin'
Session Management	Mar 12 18:47:02 ip-10-0-0-35 wabengine[25165]: [-] Authentication succeeded for user 'admin' Mar 12 18:45:05 ip-10-0-0-35 WAB(root)[28716]: WABSendDelavedNotifications: Not allowed by License
Authorizations	Mar 12 18:45:01 ip-10-0-0-35 CRON[28657]: (root) CMD (/opt/wab/sbin/WABRunIfNotSlave /usr/bin/flock -v /opt/wab/bin/WABSendDelavedNotifications)
Configuration	Mar 12 18:45:01 ip-10-0-0-35 CRON[28653]: (root) CMD (/opt/wab/sbin/WABRunIfNotSlave /usr/bin/flock
System	Mar 12 18:45:01 ip-10-0-0-35 CRON[28652]: (root) CMD (/opt/wab/sbin/WABRunIfNotSlave /usr/bin/flock
Status	Mar 12 18:45:01 ip-10-0-0-35 CRON[28650]: (root) CMD (/usr/bin/flock -w 0 /run/WABRaidSendNotification
Network	Mar 12 18:43:08 ip-10-0-0-35 wabengine[25165]: [-] Authentication succeeded for user 'user01'
Time Service	Mar 12 18:42:24 ip-10-0-0-35 wabengine[25165]: [-] Authentication succeeded for user 'admin'
Remote Storage	Mar 12 18:41:56 ip-10-0-0-35 wabengine[25165]: [-] Authentication failed for user 'user01' Mar 12 18:41:56 ip-10-0-0-35 wabengine[25165]: [-] Error when trying to authenticate user 'user01' aga

- Check the Audit entry on ActivID Appliance: ٠
- Log on to the ActivID Management Console and search for the test user. 1.

HID					ftadmin@l	Home Profile Log Off
ActivID Managemen	t Console				user01	Search Device Search
Home Con	figuration A	ccess Administration	Reporting	Help Desk		
Users		user01's details				
 Advanced User Search Register User 	S	Summary				
Devices		User Information		Authen	tication Records	Devices
 Advanced Device Search Import Device 		First Name: Last Name: User Type: Employ Admin Group: Full Tir <u>Verify Identity</u> <u>Delet</u>	yees User Type ne Employees <u>e</u> <u>Enable Emer</u>	gency Access	Employee Static Password	None
	2	user01's Identity V Change User ID Move	Vallet Roles	Permissions	Permissions Inherited from	n Admin Group and User Role
		User ID	user01		User Repository	Local Database
		User Type First Name	Employees Us	er Type	Admin Group Last Name	Full Time Employees



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

H	ID İ						ftadmin@	Home	Profile Log Off
ActivID	D Manage	ment Console					user01		<u>२</u>
							🖲 User Sear	ch Oevic	e Search
Ho	ome	Configuration	Access Administratio	n Reporting	Help Desk				
Users			View Audit						
Advanced U	Jser Searc	n	Destrict search to Der	od					
Negister Us	ser	_							
Devices	s		🔵 loday 🔵 Las	t/days 🔵 Last:	3U days				
Advanced D	Device Sea	rch	Within the last	3 🌲 days					
🛯 Import Devi	ice		During the day	, bet	ween	and			
			Between 2019/0	13/12 13:54 🛛 🗂	and 2019/03	12 18:54			
			Audit Log Search Crite	ria					
			Over Channel Any		•				
			Audit Records	;					
			Record Id 🗢	Timestamp ᅌ	Message ≎	Action 🗢	Response ≎	Status ᅌ	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 Mar 12, 2010		indirectPrimaryAuthenticateDevice	SUCCESS	SUCCESS	VPN Remote Access

- 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.



Home Configuration	Access Administration Rep	porting Help Desk	
Audit Report Details Unchec	ked		
Record ID	_1.1.77	Timestamp	Mar 12, 2019 06:44:55 PM
Session			
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	
Action			
Event Type			
Action	indirectPrimaryAuthenticateDevi	ice	
Parameters	"ATC"="DYNMC_AUTH" "DAI "Action"="indirectPrimaryAuthe "ARP"="RFE-V[30.13],RFE-H[CV[1551785716],RLM-V[8.2.0.44],	M"="1" enticateDevice" "ANS"="true" .com],RFE- ,NAS-IP[]]"	ID address of the Mallin Destion
Correlation ID			IP address of the Wallix Bastion
Correlation Type			
Response - SUCCESS			
Action Response	SUCCESS		
Message			

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





hidglobal.com