

4TRESS[™] FT2011 Out-of-Band Authentication and Juniper[®] Secure Access

RADIUS Channel Integration Handbook

Document Version 2.2 | Released | May 2013



Table of Contents

List of Figures	3
 1.0 Introduction 1.1 Scope of Document	4 4 4
 2.0 Juniper Secure Access Configuration 2.1 Procedure 1: Create New LDAP Server Instance	5 7 10 10 13 15 16
 3.0 4TRESS AS Configuration	17 17 20 22 23 25 26
 4.0 Assign SMS Token(s)	26 26
5.0 Sample Authentication Using Out-of-Band Authentication	27



List of Figures

FIGURE 1: Sample Juniper Sign-In Page Before Customization	15
FIGURE 2: Sample Juniper Sign-In Page After Customization	15



1.0 Introduction

The Juniper® Networks SA Series SSL VPN Appliances enable remote and mobile employees, customers, and partners to gain secure access to corporate Virtual Private Network resources and applications. Providing secure access via a VPN over existing Internet connections requires strong, two-factor authentication to protect resources. The HID Global Identity Assurance[™] solutions that work with Juniper Networks incorporate SSL VPN solutions with versatile, strong authentication that is flexible, scalable, and simple to manage. HID Global Identity Assurance offers two solutions:

- 4TRESS[™] AAA Server for Remote Access—Addresses the security risks associated with a mobile workforce remotely accessing systems and data.
- 4TRESS Authentication Server (AS)—Offers support for multiple authentication methods that are useful for diverse audiences across a variety of service channels (SAML, RADIUS, etc.), including user name and password, mobile and PC soft tokens, one-time passwords, and transparent Web soft tokens.

1.1 Scope of Document

This document explains how to set up 4TRESS FT2011 RADIUS out-of-band (OOB) authentication with the Juniper Networks Secure Access (SA) Series of appliances. Use this handbook to enable authentication via OOB short message service (SMS) and Email for use with a Juniper VPN.

1.2 Prerequisites

- 4TRESS FT2011.
- User phone numbers and Email addresses are stored in the LDAP server.
- Juniper SA version 7.1.x installed and configured.
- Users have static LDAP passwords.
- There is an existing Short Message Peer-to-Peer Protocol / Simple Mail Transfer Protocol (SMPP/SMTP) gateway to send one-time-password OOB codes to users.
- The Juniper login page has been customized.
- Ability to manage double authentication (LDAP, RADIUS) sequentially from the same sign-in page on the Juniper network.



Note: Using Juniper double authentication (an LDAP password plus an out-of-band, one-time password) is optional. You can configure the sign-in page so that users do not have to use static LDAP passwords.



2.0 Juniper Secure Access Configuration

This chapter describes how to manage Juniper Secure Access. When a user signs into a Juniper SA Series appliance, the user specifies an authentication realm, which is associated with a specific authentication server. The Juniper SA Series appliance forwards the user's credentials to this authentication server to verify the user's identity.

You will create two authentication servers:

- LDAP Server to validate network passwords, and
- 4TRESS AAA RADIUS Server to validate one-time-passwords and the SMS activation code.

2.1 Procedure 1: Create New LDAP Server Instance

To define the LDAP Server instance, perform the following steps (this will create a new LDAP server instance on the SA Series SSL VPN appliance).



Getting Started

 In the Admin console, expand the Authentication menu, and then click Auth. Servers.

Auth	entication Server	s	
New:	LDAP Server	•	New Server

2. From the **New** drop-down list, select LDAP Server, and then click **New Server**.

The following dialog is displayed.



Settings Users			
Name:	LDAP-SRV	Label to reference this	s server.
LDAP Server:	10.16.72.131	Name or IP address	
LDAP Port:	389		
Backup LDAP Server1:		Name or IP address	
Backup LDAP Port1:			
Backup LDAP Server2:		Name or IP address	
Backup LDAP Port2:			
LDAP Server Type:	Active Directory	•	
Connection:	Unencrypted	🔿 LDAPS 🕥 Start T	TLS
Connection Timeout:	15	Seconds to wait for co	nnection to LDAP server
Search Timeout:	60	Seconds to wait for se	earch results, excluding connection time
	Test Connection		
Authentication required?			
In order to use Pa	ssword Manageme	nt, you may need to se	lect the 'Authentication required to
Authentication	required to searcl	h LDAP	
Admin DN:	cn=Administrate	or,cn=users,dc=commande	er0-
Password:			
Finding user entries			
Specify how to fin	id a user entry		
Base DN:	dc=commander	r04.dc=com	example: dc=sales.dc=com
Filter:	samaccountrar	mand ISED	

- **Name**—Specify a name to identify the server instance.
- LDAP Server—Specify the name or IP address of the LDAP server that the SA Series SSL VPN Appliance uses to validate your users.
- LDAP Port—Specify the port on which the LDAP server listens.
- Backup servers and ports—OPTIONAL—Specify parameters for backup LDAP servers.
- LDAP Server Type—Specify the type of LDAP server against which you want to authenticate users.
- Connection, Connection Timeout, Search Timeout—Accept the defaults.
- 3. Click **Test Connection** to verify the connection between the SA Series SSL VPN appliance and the specified LDAP server(s).
- 4. Select the option, Authentication required to search LDAP, and enter the appropriate Admin DN and Password.



New Server..

-

- 5. In the Finding user entries section, specify a Base DN from which to begin searching for user entries, and make sure that the Filter is correct (for example: samaccountname=<USER>).
- 6. At the bottom of the dialog, click Save Changes (not illustrated).

2.2 **Procedure 2: Create New RADIUS Authentication Server**

When using an external RADIUS server to authenticate Juniper SA users, you must configure the server to recognize the Juniper SA as a client and specify a shared secret for the RADIUS server to use to authenticate the client request. To configure a connection to the RADIUS server on an SA Series SSL VPN appliance, perform the following steps.





Auth Servers > 4TRESS AS			
Settings Users		-	
Name:	4TRE	SS AS	Label to reference this server.
NAS-Identifier:			Name of the device as known to Radius server
Primary Server			
Radius Server:	10.16.	72.140	Name or IP address
Authentication Port:	1812		
Shared Secret:	••••		
Accounting Port:	1813		Port used for Radius accounting, if applicable
NAS-IP-Address:			IP address
Timesut	20	escondo	
rimeout:	30	seconds	
Ketnes:	0		
Users authentica Note: If you select t and this credential v	te usir this, the will not i	ng tokens or or a device will send be used in autom	ne-time passwords the user's authentication method as "token" if you use SAML, ratic SSO to backend applications.
Backup Server (required	l only if	Backup server e	xists)
Radius Server:	-		Name or IP address
Authentication Port:			
Shared Secret:	_		
Accounting Port:	-		Port used for Radius accounting, if applicable
Accounting Port:	and a	and the state of the	Port used for Radius accounting, if applicable

- 3. On the **Settings** tab, enter the following attributes.
 - Name—Specify a name to identify the server instance.
 - Radius Server—Specify the name or IP address.
 - Authentication Port—Enter the authentication port value for the RADIUS server. Typically, this port is 1812.
 - Shared Secret—Enter a string. You will also enter this string when configuring the RADIUS server to recognize the SA Series SSL VPN appliance as a client.
 - Accounting Port—Accept the default,1813.
 - **Timeout**—Accept the default, 30 seconds.
 - Retries—Accept the default, 0 seconds.

Custom R	adius Rules			
Delete		New Radius Rule		
	Name	Response Packet Type	Attribute criteria	Action



4. In the **Custom Radius Rules** section, click **New Radius Rule**. When a person enters a username and password, the initial authorization request is sent to the server. The server may respond with either a Challenge or Reject packet.

5. In the Add (or Edit) Custom RADIUS Challenge Rule window, select the packet type (Challenge or Reject), and then specify what action to take (used for OOB authentication and emergency access—4TRESS sends an SMS if a correct SMS PIN is entered = access-challenge).

6. To create a custom challenge rule, select the **Response Packet Type**:

- Access Challenge—sent by the RADIUS server requesting more information in order to allow access.
- Access Reject—sent by the RADIUS server rejecting access.

The following image illustrates two sample options.

Auth Servera > 4TRESS AAA > Edit Custom Radius Rule	Option (1)			Auth Servers > 4TRESS AAA > Edit Custom Radius Rule	Opt	ion 2	
Name: SMS PIN OK				Name: SMS PIN NOK			
If received Radius Response Packet				If received Radius Response Packet			
Response Packet Type: Access Ch	allenge 👻 🔶			Response Packet Type: Access Re	ject 🗸 🔶		
Attribute criteria:				Attribute criteria:			
Radius Attribute	Operand	Value		Radius Attribute	Operand	Value	
Reply-Message (18) -	matches the expression -		Add	Reply-Message (18) -	matches the expression	£ [Add
Reply-Message	matches the expression	(.*)	×	Reply-Message	matches the expression	(.*)	×
Then take action				Then take action			
Show New Pin page				Show New Pin page			
Show Next Token page				Show Next Token page			
show Generic Login page	-			Show Generic Login page			
Show user login page with erro	or message			show user login page with erro	or message ←		
Show Reply-Message attr	ibute from the Radius server to th	ne user		show Reply-Message attri	bute from the Radius server to	the user 🔶	
Send Access Request with add	litional attributes			Send Access Request with add	itional attributes		
Radius Attribute	Value			Radius Attribute	Value		
User-Name (1)	•	Add		User-Name (1)	•	Add	

7. Click Save.

Once you have saved your custom rule, it appears in the Custom RADIUS Authentication Rule section (illustrated next).

Custom R Delete	adius Rules	New Radius Rule		
	Name	Response Packet Type	Attribute criteria	Action
	SMS PIN OK	Access Challenge	(Reply-Message matches the expression " $(.*)$ ")	Show Defender page
	SMS PIN NOK	Access Reject	(Reply-Message matches the expression "(.*)")	Show user login page with error message show Reply-Message attribute from the Radius server to the user

Note: To delete a rule, select the checkbox next to the rule, and then click Delete.



2.3 Procedure 3: Define Juniper User Role(s)

A user role is an entity that defines user session parameters, personalization settings, and enabled access features.

Users	
User Realms	Users
User Roles	User Roles
Resource Profiles	New User Role

- 1. From the Admin console, expand the **Users** menu, point to **User Roles**, and then click **New User Role**.
- 2. Configure the new user role according to your requirements.

2.4 **Procedure 4: Define Juniper Authentication Realm**

An authentication realm specifies the conditions that users must meet in order to sign in to the SA Series appliance. A realm consists of a grouping of authentication resources.

and it wanting	User kealms
Iser Roles	New User Realm

1. From the Admin console, expand the Users menu, point to User Realms, and then click New User Realm.



User Authentication Realms > 4TRESS AS REalm	
General Authentication Policy	Role Mapping
Name:	4TRESS AS Realm
Description:	
	When editing, start on the Role Mapping page
Servers	
Charify the servers to use for suthentics	Non and authorization. To create or manage servers, see the Servers page
openy the servers to use for addictions	uon and authorization. To create of manage servers, see the <u>Dervers</u> page.
Authentication:	Client04 -
Directory/Attribute:	Same as above 👻
Accounting:	None -
Additional authentication se	erver
You can specify an additional authentica	tion server for single sign-on (SSO) purposes. The additional credentials can be speci ch case the user will not be prompted for the credential.
or they can be pre-defined below, in which	
or they can be pre-defined below, in whit Authentication #2:	4TRESS AS 👻
Authentication #2: Username is:	4TRESS AS
or they can be pre-defined below, in whit Authentication #2: Username is:	4TRESS AS → ② specified by user on sign-in page ④ predefined as: <username></username>
or they can be pre-defined below, in whi Authentication #2: Username is: Password is:	4TRESS AS → Specified by user on sign-in page predefined as: <usemame> specified by user on sign-in page</usemame>
or they can be pre-defined below, in whit Authentication #2: Username is: Password is:	4TRESS AS

- 2. On the General tab, enter the following attributes and select the following options.
 - Name—Enter a name to label this realm.
 - **Description**—Enter a meaningful description.
 - In the **Servers** section:
 - Select an option from the **Authentication** drop-down list to specify an authentication server to use for authenticating users who sign in to this realm (for example, the LDAP server).
 - Accept the default for **Directory/Attribute** (Same as above).
 - **Accounting**—Accept the default, None.



- To submit secondary user credentials to enable two-factor authentication to access the Secure Access device, select the option, **Additional authentication server**.
 - Authentication #2—Select 4TRESS AS from the drop-down list (the name of the authentication server might be different).
 - By default, Secure Access submits the <username> session variable that holds the same username used to sign in to the primary authentication server. To automatically submit a username to the secondary server, select the option, **predefined as**.
 - If you want to prompt the user to manually submit a password to the secondary server during the Secure Access sign-in process, then select the option, **Password is specified by user on sign-in page**.
 - Select the option, End session if authentication against this server fails.
- 3. At the bottom of the page, click **Save Changes**.
- 4. To configure one or more role mapping rules (based on the role defined previously), select the **Role Mapping** tab.

Seneral Authentication Policy Role Mapping		
pecify how to assign roles to users when they sign in. Users that are New Rule Duplicate Delete •	not assigned a role will not be able to	sign in.
	assign these r	oles Rule Name Stop
When users meet these conditions	assign areac in	



2.5 Procedure 5: Configure New Juniper Sign-In Page



1. From the Admin console, expand the **Authentication** menu, point to **Signing In**, and then click **Sign-in Pages**.

Custom text			
Welcome message:	Welcome to the		
Portal name:	Secure Access SSL	VPN	
Submit button:	Sign In		
Instructions:	Please sign in to session. <t Javascript is disa</t 	begin y noscrip abled or	your secure >>Note: h your browser.
	This text appears on the r	ight-hand	side of the sign-in page. You can use , , , , <no< td=""></no<>
Username:	Username		
Password:	LDAP Password		
Realm:	Realm OTP	This pro-	mpt appears when the sign in page supports more than one re
Secondary username: :	<username></username>		
Secondary password: :	One Time Password		
Prompt the secon	day credentials on the	second	page
	These labels appear when	a realm u	sing this sign-in page specifies a secondary authentication ser
Sign Out message:	Your session has e	ended	Text appears in message box when user signs out
Sign In link text:	Click here to sign	nin	Text appears as link to sign in page when user signs out

- 2. On the **Custom text** page, enter the following attributes.
 - Welcome message—Enter an appropriate salutation, such as Welcome to the.
 - Portal name—Enter a meaningful name. This will be what comes after Welcome to the.
 - Submit button—Customize as desired.
 - Instructions—Enter the text you want the user to see on the sign-in page.
 - **Username**—This is used by the realm to mask the secondary username on the sign-in page.
- 3. Accept the defaults for all other attributes.



4. **Optional**: You can modify Juniper custom sign-in pages to hide the SMS PIN (the activation code). If you do this, then all the users will use the same activation code. For details, call your HID Global Identity Assurance technical contact to obtain a sample page. After you obtain a custom file, you can upload it directly using the **Sign-in Pages** tab (illustrated next).

JUNIPEr.				
Junos Pulse Secur	e Ace	cess Service		
- System				_
Status	*			
Configuration		Signing In		1
Network		No. of Concession, Name of		-
Clustering		Sign-in Policies	Sign-in Pages	Sign-
IF-MAP Federatio	on +			
Log/Monitoring	*	New Page	Unload Custom Pa	ides
- Authentication		Litter i age	opioud odoloini e	geom
Sincing In	and	m.o.	and the second	

5. On the Signing In page, select the Sign-in Pages tab, and then click Upload Custom Pages.

Signing In > Custom Sign-In	Pages		11
Custom sign-in page pages that may app for information abou	es allow you to ear during the it creating vali	o provide customized templates f e sign-in process. Refer to the do id templates.	or
Sign-In Pages			
Name:	00B Label to referen	ice the custom sign-in pages.	
Page Type:	Access		
Templates File:		Browse	
	Zip file containir Current Templat sample oob 2012	ng the custom templates and assets, te File: o.zip Size 96114 bytes Uploaded on Tue I	eb 2
Save Changes?			
Skip validation cl	hecks during u	upload	
Save Change	s		

6. Enter an appropriate Name, select the Access option for Page Type, and then click the Browse button.



2.5.1 Examples of Custom Sign-In Pages

FIGURE 1: Sample Juniper Sign-In Page Before Customization

JUNIPEC.	
Welcome to the Secure Access SSL VI	PN
LDAP Password	emeau4
SMS PIN or One Time Password	••••
	Sign In

FIGURE 2: Sample Juniper Sign-In Page After Customization

JUNIPEr.		
Welcome Instant	^{to the} t Virtual Extranet	
username password		Please sign in to begin your secure session.
	Sign In	



2.6 Procedure 6: Juniper Sign-in Policies

User sign-in policies also determine the realm(s) that users can access.

- Authentication		Liten i uge
Signing In	Þ	Sign-in Policies 💥
Endpoint Security	*	Sign-in Pages
Auth. Servers		Sign-in Notifications

1. To create or configure user sign-in policies, in the Admin console, expand the **Authentication** menu, point to **Signing In**, and then click **Sign-in Policies**.

Sign-in Policies Sign-in Pages Sign Restrict access to administrators Only administrator URLs will be accessibilitiabled. Sign-in Policy Enable multiple user sessions Select this check box and enter the max Authentication Policy > Limits page. By you limit the user to one session for all Image: Display open user session[s] warm	only ole. Note that Administrators can a ximum number of sessions per us default, this is 1, or one session p realms of this user.	ittempt to sign in even if a er per realm in Users > Us
 Restrict access to administrators Only administrator URLs will be accessib disabled. Enable multiple user sessions Select this check box and enter the max Authentication Policy > Limits page. By a you limit the user to one session for all Display open user session[s] warr 	only ile. Note that Administrators can a ximum number of sessions per us default, this is 1, or one session p realms of this user.	ittempt to sign in even if a er per realm in Users > U:
 Only administrator URLs will be accessib disabled. Enable multiple user sessions Select this check box and enter the map Authentication Policy > Limits page. By you limit the user to one session for all Display open user session[s] warr 	wimum number of sessions per us default, this is 1, or one session p realms of this user.	ittempt to sign in even if a er per realm in Users > U
Enable multiple user sessions Select this check box and enter the max Authentication Policy > Limits page. By you limit the user to one session for all Oisplay open user session[s] warr	ximum number of sessions per us default, this is 1, or one session p realms of this user.	er per realm in Users > U
Select this check box and enter the ma: Authentication Policy > Limits page. By you limit the user to one session for all Display open user session[s] warr	ximum number of sessions per us default, this is 1, or one session p realms of this user.	er per realm in Users > U
Display open user session[s] warr		er user per realm. If you
	ning notification	
Check this option to notify users if they	have other active session[s] in p	rogress when they attempt
follow the instructions on the warning no	obtication page to proceed or canc	el the login.
Select when to display a potification	n name to users	
Select when to display a nouncado	in page to users	
Always If the maximum session limit per user	for the realm has been reached	
0		
New ORL Delete Enable		
Administrator URLs	Sign-In Page	Authentication
	Default Sign-In Page	Admin Users
User URLs	Sign-In Page	Authentication
	Default Sign-In Page	Users
<u>-/008/</u>	OOB	Users
<u>_/vws1/</u>	VisibleWST	Upera
HWST/	HiddenWST	Users
//oob-AAA/	OOB	Users-AAA
	VWST-AAA	Users-AAA
=/VWST-AAA/		

- 2. To create a new sign-in policy, click New URL.
- 3. In the **Sign-in URL** field displayed, enter the URL that you want to associate with the policy. Use the format <host>/<path>, where <host> is the host name of the Secure Access device and <path> is any string you want users to enter.



- 4. For **Sign-in Page**, select the sign-in page that you want to associate with the policy.
- 5. For **Authentication realm**, specify which realm(s) map to the policy, and how users should pick from amongst realms.
- 6. Click Save Changes.

3.0 4TRESS AS Configuration

This chapter describes the procedures required to configure 4TRESS Authentication Appliance support for a RADIUS Front End (RFE) component installed on an Appliance.

You will perform these steps using the 4TRESS Management Console. Be sure you have the *ActivIdentity* 4TRESS Authentication Appliance Administration Guide: Management Console technical publication on hand. This chapter does not provide all the details.

3.1 Configure RADIUS Channel

A RADIUS channel for the RFE deployment defines a group of access controllers and specifies how to handle authentication requests.

Using a policy configured for the channel, you will filter the requests according to the IP address or hostname of the access controllers.

1. Launch the 4TRESS Management Console.

ftadmin
•••••

2. When prompted, enter your User name and Password, and then click Submit.





3. Select the **Configuration** tab, and then in the pane to the left under **Policies**, click **Channels**.



Important: To configure the RADIUS channel policy, you can either create a new channel using the **Add** or **Copy** options, or edit an existing channel by clicking the channel name in the list displayed to the right of the page. HID Global Identity Assurance recommends that you use the Remote Access channel—this is the pre-defined RADIUS channel.

4. In the list displayed to the right when you click **Channels**, click the **VPN Remote Access** channel.

lame*	VPN Remote Access	Code*	CH_VPN
escription	Default RADIUS channel		
ype*	Radius		

5. In the VPN Remote Access Details section displayed, accept the default for Description, or change it. Make sure the Name, Type, and Code are correct.



6. Click **Channel Policy** to expand the section and display the configuration options.

Channel Policy			
Shared secret*			
Confirm Shared sec	et*	•••••	
User Identification*		User Centric	
Add Delete			
Autno	ized IP addre	esses or host names	
10.16	72.130		

7. Enter and confirm the Shared secret.

The **Shared secret** encrypts the information exchanges between the appliance(s) and the access controllers.

The secret must be the same for each controller configured in the channel policy. The secret must not exceed 40 characters. By default, the secret for a pre-defined gate is ActivIdentity.

8. Click Add.

The **Add Authorized IP addresses or host names** list is displayed. Use these settings to configure the access controllers that are authorized to use the gate for authentication.



Important: You can select either a host name—and then enter the name of the machine hosting the access controller—or you can enter an IP address, and then enter an address and range of the access controller. HID Global Identity Assurance recommends that you use an IP address rather than a host name. If the DNS cannot translate the host name, then the RFE will not restart.

- 9. For an IP address, enter the valid network range (for example, 192.168.0.0/24).
- 10. Click Save.

The access controller is displayed in the **Channel** page. Now, it is authorized to use the gate for authentication requests.



Important: Make sure that each access controller is configured with the shared secret you specified above. If necessary, repeat the steps to authorize access for additional controllers.



3.2 Create User Repository

The "User Repositories" function of the 4TRESS Management Console defines parameters for using LDAP servers as the source of user data for the appliance system. By configuring the appliance to communicate with your LDAP directory server, you enable access to user data for authentication purposes.

Home	Configuration
4	
Environment	
User Repositori	es
OOB Delivery Ga	ateway
Radius	
Fraud Detection	
and a second second	

- 1. Logged into the 4TRESS Management Console, select the Configuration tab.
- 2. In the pane to the left, under Environment, click User Repositories.

Home	Configuration	Access Administration	Reporting	Help Desk
Environment		User Repositories		
User Repositor	ies ateway	User Repositories define	e parameters for L	DAP servers. The
Radius Eraud Detection	alonay	Add Copy Delete Name 👻	*	
Dolicies		User Repositori	ies	
Policies		🔲 Local Dat	abase	

3. In the page displayed to the right, click Add.



	40	0.44	0.0.1101	
Name *	AD	Code-	DS_1101	_
Adapter*	The datasource adapter for N	ficrosoft Active Directory.		
Connection Settings				
Enter IP/hostname and port				
Host*	10.16.72.131	Port*	389	
Backup Host		Backup Port		
Base Node*	DC=commander04,DC=com			
Enable I DAPs				
LINDONG LOPPIO				
	12112			
Configure user attributes and	groups attributes mapping.	1.010.0000 01000		
Configure user attributes and User Class*	groups attributes mapping. Person	LDAP Group Class	group	
Configure user attributes and User Class* User ID Attribute*	groups attributes mapping. Person sAMAccountName	LDAP Group Class Group Member Attribute	group memberOf	
Configure user attributes and User Class* User ID Attribute* Account Status Attribute	groups attributes mapping. Person sAMAccountName UserAccountControl	LDAP Group Class Group Member Attribute GUID Attribute Name*	group memberOf objectguid	
Configure user attributes and User Class* User ID Attribute* Account Status Attribute Configure connection login cre	groups attributes mapping. Person sAMAccountName UserAccountControl	LDAP Group Class Group Member Attribute GUID Attribute Name*	group memberOf objectguid	
Configure user attributes and o User Class* User ID Attribute* Account Status Attribute Configure connection login cre User DN*	groups attributes mapping. Person sAMAccountName UserAccountControl edentials cn=administrator.cn=users.dc	LDAP Group Class Group Member Attribute GUID Attribute Name*	group memberOf objectguid	
Configure user attributes and e User Class* User ID Attribute* Account Status Attribute Configure connection login cre User DN* Password*	groups attributes mapping. Person sAMAccountName UserAccountControl edentials cn=administrator,cn=users.dc	LDAP Group Class Group Member Attribute GUID Attribute Name*	group memberOf objectguid	

- 4. **Name**—Enter a meaningful name.
- 5. Adapter—Select the adapter from the drop-down list that corresponds to your directory type (either Novell® eDirectory or Microsoft® Active Directory).
- 6. Host—Enter the IP address or hostname of the server where your LDAP directory resides.
- 7. Port—Enter the Port (the LDAP directory server's listening port).
- 8. In the **Configure connection login credentials** section of the page, enter the user credentials that the appliance will use to access the LDAP database. Then, enter and confirm the user's **Password**. You MUST indicate the full **User DN**.
- 9. Expand the Attributes section, and then expand the Available section.



ributes		
ap the User repository (LDAP) attributes corresp	onding to the 4TRESS attributes listed.	
FTRESS Name	LDAP Name	Enabled
Enabled Attributes		
Mobile Phone Number	mobile	V
E-Mail Address	mail	1

- 10. In the **Attributes** section, select the **Enabled** options next to the appliance attributes to be mapped to the LDAP attributes.
- 11. Click Save. A success message appears.
- 3.3 Configure Administration Groups, User Types, User Repositories, and Authentication Policies



Have the ActivIdentity 4TRESS Authentication Appliance Administration Guide: Management Console technical documentation on hand. This section summarizes the remaining procedures to perform before Web Soft Tokens can be activated. It does not provide the step-by-step instructions that are explained already in the core documentation.

1. Use the 4TRESS Management Console to create and update administration groups within user types. Then, you can add users to the administration groups.

User types define categories of users. A hierarchy of administration groups exists for each user type.

For each user type, you can define:

- User repositories relating to the user type,
- Authentication policies accessible to users of this type, and
- User attributes for users of this type.

There are default user types. Installing the 4TRESS Appliance Server automatically sets up a number of user types. For each user type, there are pre-defined system users. Collectively, these sample users have all the required privileges to administer the system. You can use the base data set as provided, or modify it to meet your specific requirements.

- 2. Map the user repository to a user type.
- 3. Assign an authentication policy to a user type.
- 4. Map the user repository to an administration group.



Administration groups provide a way to organize (partition) users for administrative purposes, as well as a way to assign permissions to users through membership of administration groups.

3.4 Create OOB Delivery Gateway

4TRESS supports two OOB authentication types: SMS (Phone) and Email. The actual SMS/Email OTP is a random number generated by the appliance and sent to the end user by SMS or Email through a delivery gateway.

1. Logged into the 4TRESS Management Console, select the **Configuration** tab.

Home	Configuration
Environment	
🛛 User Repositori	es
DOB Delivery Ga	ateway
Radius	
Fraud Detection	

2. In the pane to the left under **Environment**, click OOB Delivery Gateway.



blama t	D	0 dt 11074
Name -	Proxy SMPP Local	Code 11074
Description		
Delivery Provider*	SMS SMPP Delivery Provider -	
SMPP hostname*	10.16.72.130	
SMPP port*	9001	
SMSC system ID*	ai	
Password for SMSC server*	••	
Source TON	0	
Source NPI	0	
ESME address range		
User Attribute that stores the phone number*	ATR_MOBILE	
Name of template for Credential messages*	credential-sms	
Name of template for Challenge messages*	challenge-sms	
templates' directory		

- 3. Enter a Name and Description.
- 4. Select SMS SMPP Delivery Provider from the Delivery Provider drop-down list.
- 5. Click **Next** to display the set of the fields on the page.
 - SMPP hostname—Hostname or IP address of the SMPP provider.
 - **SMPP port**—Port number of the SMPP provider.
 - SMSC system ID—ID of the SMS Center.
 - Password for SMSC server—Password of the SMS Center.
 - **Source TON**—Obtain this value from your SMPP provider.
 - **Source NPI** Obtain this value from your SMPP provider.
 - **ESME address range** Obtain this value from your SMPP provider.
 - User Attribute that stores the phone number—User attribute for the phone number of the user registered.
 - Name of template for Credential messages—By default, it is pre-populated with credentialemail. Enter credential-sms.
 - Name of template for Challenge messages—Enter challenge-sms.
- 6. Click Save.



3.5 Assign An Out-of-Band Delivery Gateway

Have the main *ActivIdentity 4TRESS Authentication Appliance Administrator Guide: Configurer Portal* technical documentation handy for easy reference. This is a summary section only.

1. Launch the 4TRESS Configurer, log in, and then select the Authentication Policies tab.

stages:	olicies			
Code	Name	Class	Encryption Key	Notes
AT_CSTEMVT	Customer EMV transaction	DEVICE	des	Customer EMV transaction
T_CSTEPWD	Customer Emergency Password	LOGIN	des	Emergency password for customer authentication
T_CUSTEMV	Customer EMV authentication	DEVICE	des	Customer EMV authentication
T_CUSTMD	Customer Emergency Q&A	SQ	des	Emergency Q&A for customer authentication
T_CUSTMW	Customer memorable word	LOGIN	des	Memorable word for supplementary authentication
T_CUSTOOB	Customer OOB authentication	DEVICE	des	Out of the Band login for customer authentication
T_CUSTOTP	Customer One Time Password	DEVICE	des	One time password login for customer authentication
AT_CUSTPIN	Customer PIN	LOGIN	des	Numeric PIN for customer authentication

2. Edit the AT_CUSTOTP Customer One Time Password authentication policy.

Available Delivery Gateways		Selected Delivery	Gateways	8
*	**	Local_SMPP	*	*
	44			۳
*				

- 3. Add the new delivery gateway (for example, Local_SMPP) that you just created in the previous section of this document to the **Selected Delivery Gateways** box.
- 4. Update the authentication policy.



3.6 Assign An Out-of-Band Delivery Credential to An Existing Authentication Policy

Have the main *ActivIdentity 4TRESS Authentication Appliance Administrator Guide: Configurer Portal* technical documentation handy for easy reference. This is a summary section only.

- 1. Launch the 4TRESS Configurer, log in, and then select the Authentication Policies tab.
- 2. Edit the AT_CUSTOTP Customer One Time Password authentication policy by assigning the following credential types.

CT_CRTCHK1		bb CT_AIIN1	
CT PKICR1		CT ACODE	100
		AA CT ALOT	
		CT ALAT	
	-	CT_ALAT	
	1.7.1	CT_AIAEOE	

- 3. Assign the CT_ACODE and CT_OOB credential types to the Selected Credential Types box.
- 4. Update the authentication policy.

4.0 Assign SMS Token(s)

- 4.1 Prerequisite: Assign An SMS Token
- 1. Logged into the 4TRESS Management Console, search for the user.
- 2. To create an OOB record, click the **Register Out of Band** link.

dest de de service de se	Deline	
elect Authentication	Policy	
uthentication Policy	Customer One Time Password	

3. Select Customer One Time Password from the Authentication Policy drop-down list.

legister OOB for emea04	
Configure activation code	
The activation code either generated or s trigger the Out of Band password deliver	set must be communicated to the user. It will be used to y.
C Generate Activation Code	
Set Activation Code	
Activation Code	••••
Activation Code	



- 4. Select the Set Activation Code option, and then enter and confirm an Activation Code.
- 5. Click Next.

tatus	Enabled	-				
alid From	2012/01/24 15:37		To 2022	/01/21 15:	37	
laximum numi	ber of successful authentica	tion:				
	No maximum numbe	rofsuccess	ful autheni	tication		
	C Maximum number of	authenticatio	on before e	opiry		

- 6. Check the Set Policy Settings dialog, and match it to the one illustrated.
- 7. Click Save. A success message is displayed (Out of Band created successfully).

5.0 Sample Authentication Using Out-of-Band Authentication

Welcome to the Secure Access SSL VP	PN .
Username	emea04
LDAP Password	•••••
SMS PIN or One Time Password	••••
	Sign In

1. The user authenticates to the Juniper Activation Realm with an OOB device (and optionally with an LDAP password). This depends on Juniper configuration.

If you modify this page (the Juniper Custom sign-in page) to hide the SMS PIN (activation code), then all users will use the same activation code. Contact your HID Global Identity Assurance technical contact to obtain a sample page. For example:



Welcome Instant	to the Contraction Contraction
username password	
	Sign In

After the user enters his/her credentials, s/he receives a one-time password via telephone or email message.

Welcome to the Secure Access SSL VPN				
Challenge	e / Response			
Challenge: Enter the password you just received on your phone				
Enter the challenge string above into your token, and then enter the one-time response in the field below.				
Response				
	Sign In Cancel			

2. The user enters the password in the Response box, and then clicks Sign In.



Copyright

© 2012-2013 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

Trademarks

HID, the HID logo, ActivID, 4TRESS and/or other HID Global products or marks referenced herein are registered trademarks or trademarks of HID Global Corporation in the United States and/or other countries.

The absence of a mark, product, service name or logo from this list does not constitute a waiver of the HID Global trademark or other intellectual property rights concerning that name or logo. The names of actual companies, trademarks, trade names, service marks, images and/or products mentioned herein are the trademarks of their respective owners. Any rights not expressly granted herein are reserved.

Revision History

Date	Author	Description	Document Version
May 2012	Eco-System Workgroup	Initial release	2.0
February 2013	Eco-System Workgroup	Rebranded for HID Global and changed copyright from ActivIdentity to HID Global	2.1
May 2013	Eco-System Workgroup	Updated copyright statement, rebranding to HID Global TP template	2.2



 Americas
 +1 510.574.0100

 US Federal
 +1 571.522.1000

 Europe
 +33 (0) 1.42.04.84.00

 Asia Pacific
 +61 (0) 3.9809.2892

 Web
 http://www.hidglobal.com/identity-assurance

Corporate Headquarters

15370 Barranca Parkway Irvine, CA 92618 <u>www.hidglobal.com</u> +1 949.732.2000

