

ActivIdentity[®] ActivID[™] Card Management System and Juniper[®] Secure Access

Integration Handbook

Document Version 2.0 | Released | May 2, 2012



Table of Contents

1.0	Inti	roduction	3
	1.1	Scope of Document	3
	1.2	Prerequisites	3
2.0	Ju	niper Secure Access Configuration	4
	2.1	Procedure 1: Create New Certificate Server Instance	4
	2.2	Procedure 2: Define Juniper User Role(s)	5
	2.3	Procedure 3: Define Juniper Authentication Realm	6
	2.4	Procedure 4: Configure New Juniper Sign-In Page	9
	2.5	Procedure 5: Juniper Sign-In Policies	
	2.6	Procedure 6: Import the CMS Appliance Root CA	12
3.0	Au	thentication with a Smart Card and Client Certificate in the Sign-In Page	14



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 ActivIdentity solutions that work with Juniper Networks incorporate SSL VPN solutions with versatile, strong authentication that is flexible, scalable, and simple to manage.

1.1 Scope of Document

This document explains how to configure the ActivIdentity® ActivID[™] Card Management System Appliance and Juniper Networks Secure Access (SA) Series of appliances to enable client authentication via certificate and smart cards.

1.2 Prerequisites

- ActivIdentity ActivID CMS Appliance installed and Root CA certificate created.
- Juniper SA version 7.1.x installed and configured.
- Users have smart cards issued by the CMSA Appliance.



2.0 Juniper Secure Access Configuration

This chapter describes how to configure Juniper Secure Access for use with ActivIdentity CMS. 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 a new authentication server (a certificate server).

2.1 Procedure 1: Create New Certificate Server Instance

To define a certificate server instance, perform the following steps (this will create a new certificate 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:	Certificate Server	•	New Server

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

The following dialog is displayed.



		-		
Name:	Cert_Appliance			Label to reference this server.
User Name Template:	<certdn.cn></certdn.cn>			Template for constructing user names from
	The template can contai mapping custom expres	n textu sions a	al characters as nd policy conditi	well as variables for substitution. Variables s ons. All of the certificate variables are availables
	Examples: <certdn.cn> <certattr.serialnumber> <certattr.altname.cocc></certattr.altname.cocc></certattr.serialnumber></certdn.cn>	First Cl Certific Where	I from the subje ate serial numb xxx can be:	ect DN er
		Email UPN	The Email alte The Principal N	rnate name Iame alternate name
	<certdntext></certdntext>	The co	mplete subject l	DN
	cert- <certdn.cn></certdn.cn>	The te	xt "cert-" followe	ed by the first CN from the subject DN
User Record Synchroniza	tion			
Enable User	Record Synchronizati	on		
Logical Auth	Server Name:			
Save Changes?				

- **Name**—Specify a name to identify the server instance.
- User Name Template—Specify the appropriate template for constructing user names.
- 3. Click Save Changes.

2.2 Procedure 2: 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	Þ	User Roles
Resource Profiles	>	New User Role
		1 Star

- 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.



Roles > Users				
General Web Files SAM Telne	t/SSH Terminal Service	s Virtual Desktops	Meetings	Network Connect
Overview Restrictions VLAN/Source IP	Session Options UI Op	tions		
Source IP Browser Certificate Host	Checker			
 Only allow users with a client-side certificate restrictions or condition <u>Users Authentication</u> page. You can optionally require specific 	certificate signed by Centrificate signed	first choose to remen first choose to remen	o sign in. To nber certifica	change the certification a ate information or enable o
Certificate field (example "cn")	Expected value			
		Add		
Save Changes				
ton all and a proceeding	man drawned	Anna and	-	man and

- 3. Use the "certificate" as a restriction. On the General tab, click Restrictions -> Certificate.
- 4. Select the option to only allow users with a client-side certificate signed by the CA to sign in.
- 5. Click Save Changes.

2.3 Procedure 3: 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.

- Users		
User Realms	Þ	User Realms
User Roles	Þ	New User Realm
		2

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



User Authentication Realms > CMSA-Realm	
General Authentication Policy	Role Mapping
Name: Description:	CMSA-Realm
	When editing, start on the Role Mapping page
Servers	
Specify the servers to use for authentica	tion and authorization. To create or manage servers, see the <u>Servers</u> page
Authentication:	Cert_Appliance -
Directory/Attribute:	None -
Accounting:	None -
Additional authentication se	erver
Dynamic policy evaluation	
Other Settings	
Authentication Policy:	Certificate restrictions Password restrictions
Role Mapping:	1 Rule
Save changes?	
Save Changes	

- 2. On the **General** tab:
 - **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 Cert_Appliance server).
 - Accept the default for **Directory/Attribute**, None.
 - Accounting—Accept the default, None.
- 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.

User Authentication Realms >			
General Authentication Policy Role Mapping			
Specify how to assign roles to users when they sign in. Users that are	not assigned a role wil	not be able to sign in.	
New Rule Duplicate Delete 🔹 🖡			Save Changes
When users meet these conditions		assign these roles	Rule Name Stop
1. username is ***	\rightarrow	Users	IIA
When more than one role is assigned to a user:			
Merge settings for all assigned roles			
 User must select from among assigned roles 			
Output the sets of merged roles assigned by each rule			

5. Use the certificate as a restriction. Select the **Authentication Policy** tab, and then click **Certificate**.

er Authentication Realms > MSA-Realm						
eneral Authentication Policy Role Mapping						
urce IP Browser Certificate Password Host Checker 1						
Allow all users (no client-side certificate required) Allow all users and remember certificate information wh Only allow users with a client-side certificate signed by You can ontionally require specific values in the client of	ile user is signed in. · Trusted Client CAs to sign in. To change the certification autho · certificate ·	prity, see the <u>Trusted Client CA</u> page.				
Certificate field (example "cn")	Expected value					
		Add				
ave Changes						
we changes						

- 6. Select the option to only allow users with a client-side certificate signed by a Trusted Client CA to sign in.
- 7. Click Save Changes.



2.4 Procedure 4: Configure New Juniper Sign-In Page

- Authentication		
Signing In	Þ	Sign-in Policies
Endpoint Security		Shar-in Pages
		12

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

fault Sign-In Page				
Name:	Default Sign-In Page	Label to	reference the sign-in page.	
Page Type:	Users/Administrat	tors		
stom text				
Welcome message:	Welcome to the			
Portal name:	Secure Access SSL VF	PN		
Submit button:	Sign In			
Instructions:	Please sign in to begin your secure session. >roscript>Note: Javascript is disabled on your browser. 			
	This text appears on the	right-hand	side of the sign-in page. You can use , <	
Username:	Username			
Password:	One Time Password			
Realm:	Realm	This pror	mpt appears when the sign in page supports r	
Secondary username:	LDAP User			
Secondary password:	LDAP Password			
Prompt the second	dary credentials on th These labels appear whe	e second n a realm u	page sing this sign-in page specifies a secondary a	
Sign Out message:	Your session has ende	d.	Text appears in message box when user si	

- 2. Accept the default Name and Page Type. Accept the defaults in the Custom text section of the page.
 - Welcome message—The page salutation.



- **Portal name**—Optionally, change this. This will be what comes after *Welcome to the*.
- Submit button—The button name.
- **Instructions**—Optionally, change 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.

2.5 Procedure 5: Juniper Sign-In Policies

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

- Authentication		
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**.



igning In		
Sign-in Policies Sign-in Pag	ges Sign-in Notifications	
Restrict access to admini Only administrator URLs will b disabled.	istrators only be accessible. Note that Administrators	can attempt to sign in even if a
Enable multiple user sess	ions	
Select this check box and enter Authentication Policy > Limits you limit the user to one sess	er the maximum number of sessions page. By default, this is 1, or one ses sion for all realms of this user.	per user per realm in Users > U ssion per user per realm. If you
Display open user session Check this option to notify use follow the instructions on the y	n[s] warning notification ers if they have other active session[s warning notification page to proceed o] in progress when they attemp rr cancel the login.
	otification page to users	
Select when to display a no Always If the maximum session lim	it per user for the realm has been rea	iched
Select when to display a no Always If the maximum session limination of the maximum session limination of the maximum session limination of the second sec	it per user for the realm has been rea	iched
Select when to display a no Always If the maximum session limit New URL Delete Administrator URLs	it per user for the realm has been rea inable Disable • •	Authentication
Select when to display a no Always If the maximum session lim New URL Delete Administrator URLs _/admin/	inable Disable 🔹 🗣	Authentication Admin Users
Select when to display a no Always If the maximum session lim New URL Delete Administrator URLs /admin/ User URLs	it per user for the realm has been real inable Disable • • Sign-In Page <u>Default Sign-In Page</u> Sign-In Page	Authentication Admin Users Authentication
Select when to display a no Always If the maximum session limit New URL Administrator URLs //admin/ User URLs //	it per user for the realm has been real inable Disable • • Sign-In Page Default Sign-In Page Sign-In Page Default Sign-In Page	Authentication Admin Users Authentication Users
Select when to display a no Always If the maximum session limit New URL Administrator URLs Administrator URLs Juser URLs Loser URLs // // //	it per user for the realm has been real inable Disable • • Sign-In Page Default Sign-In Page Default Sign-In Page Default Sign-In Page OOB	Authentication Admin Users Authentication Users Users
Select when to display a no Always If the maximum session lim New URL Delete E Administrator URLs // admin/ User URLs // //OOB/ //WST/	it per user for the realm has been realmable Disable Sign-In Page Default Sign-In Page Default Sign-In Page OOB VisibleWST	Authentication Admin Users Authentication Users Users Users Users
Select when to display a no Always If the maximum session lim New URL Delete E Administrator URLs */admin/ User URLs */(*/OOB/ */VWST/ */HWST/	it per user for the realm has been real inable Disable • • Sign-In Page Default Sign-In Page Default Sign-In Page OOB VisibleWST HiddenWST	Authentication Admin Users Authentication Users Users Users Users Users
Select when to display a no Always If the maximum session limit New URL Delete El Administrator URLs #/admin/ User URLs #/ /OOB/ #/VWST/ //OOB-AAA/	it per user for the realm has been real inable Disable • • Sign-In Page Default Sign-In Page Default Sign-In Page OOB VisibleWST HiddenWST OOB	Authentication Admin Users Authentication Users Users Users Users Users
Select when to display a no Always If the maximum session lim New URL Delete E Administrator URLs */admin/ User URLs */ /OOB/ */VWST/ */OOB-AAA/ */VWST-AAA/	it per user for the realm has been real inable Disable • • Sign-In Page Default Sign-In Page Default Sign-In Page OOB VisibleWST HiddenWST OOB VWST-AAA	Authentication Admin Users Authentication Users Users Users Users Users Users Users Users Authentication

- 2. To create a new sign-in policy, click **New URL**.
- 3. In the **Sign-in URL** field displayed (not illustrated), 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.



2.6 Procedure 6: Import the CMS Appliance Root CA

JUNIPEC.			
Central Manager			
- System			
Status >			
Configuration >	Security >		_
Network >	Certificates >	Device Certificates	insting
Clustering >	DMI Agent	Trusted Client CAs	Ications
IF-MAP Federation >	NCP	Trusted Server CAs	
Log/Monitoring >	Sensors >	Code-signing Certificates	5
- Authentication	Client Types	Client Auth Certificates	
Signing In 💦	Secure Meeting	will be accessible, note th	at Administrate
Endpoint Security >	Virtual Desktops		
Auth. Servers	User Record Synchronization >	sessions	
- Administrators	IKEv2	d enter the maximum nu	mber of session
Admin Realms		rect this check box, you lin	nit the user to o

1. Navigate to Signing In -> Certificates -> Trusted Client CAs.

Import from:	Browse
 Ch-++ C + 2	

2. In the **Certificate file** section, click the **Browse** button to locate the CMS Appliance Root CA certificate, and then click **Import Certificate**.

The certificate is located as illustrated next:





Configuration			
Security Certificates DMI Agent NCP Sensors C	ient Types Secure Meeti	ng Virtual Desktops User Record Synchroniz	ation IKEv2
Device Certificates Trusted Client CAs Trusted Server CAs C	Code-signing Certificates Clie	nt Auth Certificates	
Users can be required to present valid client-side certificat	es to sign in (see the realm	n-specific Certificate Authentication Policy page). Specify trusted certifica
Auto-import options Import CA Certificate Delete			
Trusted Client CA	Trusted for client authentication?	Valid dates	Status checking
ActivIDCMS1	Yes	2011/12/27 - 2041/12/27	None
and the second sec			



3.0 Authentication with a Smart Card and Client Certificate in the Sign-In Page.

1. The user launches the Juniper User Portal.

vorites 🛛 👍 🙋 Activide		
	intity Secure Acce 🙋 Liv	ve Meeting - Se connecter 🏾 🏉 Suggested Sites 👻 🙋 Get More Add-ons 💌
ertificate Error: Navigation B	Blocked]
There is a pro	oblem with this we	bsite's security certificate.
The security cert	ificate presented by this	website was not issued by a trusted certificate authority.
The security cert	ificate presented by this	Windows Security
Security certificat	te problems may indicat	Confirm Certificate
convor		Confirm this certificate by clicking OK. If this is not the correct certificate,
berver.		
We recommend	d that you close this w	click Cancel.
We recommend	d that you close this w	click Cancel.
We recommend	d that you close this w close this webpage.	click Cancel. re fred2's PIV Authentication Issuer: ActivIDCMS1
We recommend Click here to to Continue to to	d that you close this w close this webpage. his website (not recomm	click Cancel.

2. The user is prompted to confirm the certificate, and then clicks OK.



3. The user enters a **PIN**, and then clicks **OK**.



+1 510.574.0100 +1 571.522.1000 +33 (0) 1.42.04.84.00 Asia Pacific +61 (0) 2.6208.4888 info@actividentity.com www.actividentity.com

Legal Disclaimer

ActivIdentity, the ActivIdentity (logo), and/or other ActivIdentity products or marks referenced herein are either 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 trademark or other intellectual property rights concerning that name or logo. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The names of other thirdparty companies, trademarks, trade names, service marks, images and/or products that happen to be mentioned herein are trademarks of their respective owners. Any rights not expressly granted herein are reserved.

