SafeNet Authentication Client Integration Guide

Using SAC CBA with Juniper Junos Pulse



THE DATA PROTECTION COMPANY

Document Information

Document Part Number	007-012717-001, Rev. A
Release Date	October 2014

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Third-Party Software Acknowledgement	3
Description	3
Applicability	4
Environment	4
Audience	4
CBA Flow using SAC	5
CBA Prerequisites	6
Configuring Juniper for Certificate-based Authentication	7
Authenticator Assignment in SAC-CBA	11
Running the Solution	12
CBA Using Junos Pulse Software	12
Support Contacts	13

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Third-Party Product.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Juniper SA using any of SafeNet's certificate-based tokens.

SafeNet's certificate-based tokens provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). SafeNet Authentication Client manages SafeNet's extensive portfolio of certificate-based tokens, ensuring full support for all currently deployed eToken and iKey devices.

Junos Pulse software enables dynamic SSL VPN connectivity, network access control (NAC), mobile security, and collaboration, through a simple end-user interface. It simplifies and optimizes connectivity to end users at the same time it check their device type and security state, location, identity, and adherence to corporate access control policies.

Applicability

The information in this document applies to:

• Safenet Authentication Client (SAC)

SafeNet Authentication Client is the desktop software that manages SafeNet's eToken and iKey certificate based authenticators

• Juniper SA MAG2600

Environment

The integration environment that was used in this document is based on the following software versions:

- SAC 8.3
- Juniper SA MAG2600 GW
- Juniper Junos Pulse 3.0

Audience

This document is targeted to system administrators who are familiar with Juniper Junos Pulse and are interested in adding certificate based authentication capabilities using SafeNet Authentication Client.

CBA Flow using SAC

The image below shows the environment required to implement a Juniper solution using SafeNet's certificatebased authentication, and illustrates the dataflow of the authentication request.



- 1. A user is required to authenticate to Juniper MAG2600 via the Junos Pulse application using a SafeNet certificate-based token. The SafeNet token is deployed with a user-unique client certificate for authentication. When the user is authenticated, they must provide a PIN to access the token. The credentials are passed to the Juniper gateway, which will accept or reject the authentication request.
- 2. After successful authentication, the user receives VPN/SSL access to the network.

CBA Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificatebased authentication for Juniper SA using Junos Pulse.

- Microsoft CA to use CBA, the Microsoft Certificate Authority must be installed and configured. In this integration guide, a standalone Microsoft CA is installed on the domain controller machine.
- SAC 8.3 includes all the files and drivers needed to support SafeNet smart card integration. Safenet Authentication Client must be installed on each computer where the smart card is going to be used.
- Junos Pulse Software



NOTE: This document assumes that Juniper Junos Pulse is installed, and that the solution is using static passwords or any other user-authentication method. For additional information on how to install Junos Pulse, refer to:

http://www.juniper.net/techpubs/en_US/mag/topics/task/configuration/mag-modules-init-configuring.html

Configuring Juniper for Certificate-based Authentication

The configuration of Juniper with certificate-based authentication (CBA) requires the following:

- Certificate configuration
- Adding an authentication server
- Attaching an authentication server to user realms

Certificate Configuration

1. Open the Juniper SA web console

JUNIPEr.								
Junas Pulse Secure A	cess Service		Help Guidance Sign Out					
Status Configuration	System Status	System Status						
Clustering IF-MAP Federation	Overview Active Users M	Netroj Schodalo Vitual Desktop Sessions						
IP-MAP Preferences Legistion/ways Authorizesture Authorizesture Authorizesture Advenseturesture Advenseturesture Advenseturesture Advenseturesture Advenseturesture Authorizesture Authorizestur	Contract Location Contract Loca	Topology Topology						
			(Prew desite					

(The screen image above is from Juniper Networks Junos Pulse software. Trademarks are the property of their respective owners.)

- 2. In the left pane, select System > Configuration.
- 3. In the right pane, select the **Certificates** tab.

	ccess Service			Help Caida
1				
relian	Configuration			
	Interesting According Institutional Institutional	HTP Sansors Chart Turnes Junes Pulse Collaboration Write	al Desistone Line: Record Superformation 105-2 SAM	
Federation .	Device Certification Trusted Client CAs Trusted Server	CAs Code-signing Certificates Chert Auth Certificates	and a second and a second and a second and a second a second a second a second as	
privating				
g in	Specify the Device Certificate(s). If you don't have	e a certificate yet, you can create a CSR and import the resulting	signed certificate. If necessary, you can add custom Intermediate CAs.	
vint Security	Import Certificate & Key			
Servers initiations	D. Certificate issued to	Insued by	Valid Dates	Dated by
Realma		and the second s	3ul 7 09:25:45 2014 GMT to 3ul 6 09:25:45 2016 GMT	diternal Porto, dexternal Porto
Roles		and the own	Jun 27 11:36:38 2012 GMT to Dec 18 11:36:38 2017 GMT	
Realms		ingli damati ili cia	Jan 28 09:13:50 2013 GMT to Jan 28 09:13:50 2015 GMT	
Abies				
ource Policies				
on Pulse	New CSR Delate			
iem.	[manual]			
ort/Expert	Certificate Signing Requests		Created	
reing				
iteing ableshooting				
itring ableshapting				
iking Ibleshooting				
ving Slexhaoting				
ving bleshaoting ed to 02711MR2 JM © 2001-20	SSUJTOGAYS 2. Junger Retworks, Tec. All rights reserved.			
ring Neshaoting d to 02711MR2 IM © 2001-20	sourosavs 12 Junger Networks, Inc. All rights reserved.			
ing leshading d to 0271MM2 M © 2001-20	SSUTODAYS 2 Junger Networks, Toc. All rights reserved.			
ving bleshading ed to 0271M(2) pM © 2001-20	250/7004/YS 13 Junger Retentes, Inc. All rights reserved.			
rring bleshooting ed to 0271MN2: jM & 2001-20	2020/02449 13 Jonger Velevine, Inc. MI rights meanwerk.			
ving bleshooting ed to 0271MN21 JM & 2003-20	opurpoint 12 Jongie federalis, Inc. III righte maanwel.			
ring Mexhaoting id to 0271M121 Idt © 2001-20	D20/722478 12: Xorgen Hellewing, Teo, All rights reasoned.			
reing bleahaoting ad to 0271MA2: ght © 2003-20:	20.070975 23.25097 Menolog, Tot, Mil Aphteresenvel.			
reing disentating ad to 0271MK22 ght © 2003-20	SUCCOM 1) Surger Research, Inc. & open research.			
ning Dischasting id to 0271MA2 2001-20	zourooms 12 Jonge Newena, Inc. M right reaerved.			
rring Bleehaating ed to 0271M02 phr © 2001-20	Durbourg Durbourg I Angele Manuel, Inc. di njete reseven			
ving Deshaating id to 0271MM2 MI © 2001-20	2020/2020 23 Songer Helmonte, Erc, dir Ingele reserved.			
ering bleeheating ed to 0271Mk2 gin © 2001-20	200700015 13 Jonger Hennes, Inc. All oper Hennes.			
Norms ubleshauting	2000001 13 Jonge Helmont, Ior, di njën nesever.			
htting Liberhauting	sourcours 2. Jonger Manaka, Inc. All oper Haaved.			
Norms ubleshapting	SUCCOST 13 Junge Henriet, Inc. 61 oper resourc			

(The screen image above is from Juniper Networks Junos Pulse software. Trademarks are the property of their respective owners.)

4. Select the Trusted Client CAs tab.

5. In the **Trusted Client CAs** list, import the root CA certificate by clicking on **Import CA Certificate**.

JUNIPEr.							
Junos Pulse Secure Act	cess Service			Help Guidance Sig	Out		
Sectors Status Configuration Detection Chartering IP-MAP Rederation Log/Monitoring Anti-Interfeature Signing In Endpoint Security Auth, Servers	Configuration Science (Configuration) Science (Configu						
- Administrators							
Admin Roles	Trusted Client CA	Trusted for client authentication?	Valid dates	Status checking			
- Users		Yes	2013/01/15 - 2018/01/15	None			
User Roles		Yes	2012/06/26 - 2017/06/26	Use CRLs	_		
Resource Profiles		Yes	2014/07/3 - 2019/07/3	None			
Junos Pulse		Yes	2013/01/28 - 2014/01/28	None	_		
- Mantenance							
Import/Export							
Push Config					_		
Traubleshooting							
					_		
Lisensed to 0274M022 Copyright © 2001-2011	90199919 Junger hannen, in, Al right nuernel.						

(The screen image above is from Juniper Networks Junos Pulse software. Trademarks are the property of their respective owners.)

Adding an Authentication Server

This section describes the creation of an authentication server. The authentication server will be configured with CBA support. Later, the authentication server will be set as the main authentication server of Juniper SA. This enables Juniper SA to be accessed with a certificate that is on a SafeNet token.

To configure the Authentication Server:

1. In the left pane, click **Authentication > Auth. Servers**.

 Attentication Servers Attenticatintentication Servers Attentication Servers	e Secure Ac	ccess Service			Stelp C
Ner: Ner: Ner: Ner: Ner: Deta: Ner: Addression/Autorization Servers Local Autorization Local Autorization Local Autorization Addressization Addressization Local Autorization Local Autorization Local Autorization Addressization Addressization Local Autorization Local Autorization Local Autorization Addressization Addressization Local Autorization Local Autorization Local Autorization Addressization Control Local Autorization Local Autorization Local Autorization Addressization Control Lobe Server Local Autorization Local Autorization Addressization Control Educitic structure Local Autorization Local Autorization Addressization Control Educitic structure Local Autorization Local Autorization Addressization Control Educit structure Local Autorization Local Autorization Addressization School Pittol School Pittol School Pittol Local Autorization Addressiz	ration	Authentication Servers			
Image: Province and inductation Servers Type User Record Synchronization Logical Auth Server Name A D. Drom ADD Structure ADD Structure ADD Structure ADD Structure A D. Drom ADD Structure ADD Structure ADD Structure ADD Structure B ADD Structure Centificate Server Centificate Server ADD Structure ADD Structure B ADD Structure Centificate Server Centificate Server Centificate Server B ADD Structure Lobd Server Centificate Server Centificate Server B ADD Structure Lobd Server Centificate Server Centificate Server B ADD Structure Lobd Server Centificate Server Centificate Server B ADD Structure Lobd Server Centificate Server Centificate Server B ADD Structure Saddus Server Centificate Server Centificate Server B ADD Server Saddus Server Centificate Server Centificate Server B ADD Server Saddus Server Centificate Server Centificate Server B ADD Server Saddus Server Centificate Server Centificate Server B ADD Server Saddus Server Centificate Server Centificate Server B ADD Server Saddus Server Centificate Server <th>ng Federation nitoring</th> <th>New: (Select server type) New Server Delete</th> <th></th> <th></th> <th></th>	ng Federation nitoring	New: (Select server type) New Server Delete			
i Admitistation Local Admitistation i Admitistation Local Variadoris Var	tication In	Authentication/Authorization Servers	Туре	User Record Synchronization	Logical Auth Server Name
• AD.000 Active Orecomy / Windows MT • AD.000 Active Orecomy / Windows MT • AD.000 Centry Label • Parry Label Centry Label • Parry Label Centry Label • D.000 Sabel • D.000 Sabel </td <td>ecurity</td> <td>Administrators</td> <td>Local Authentication</td> <td></td> <td></td>	ecurity	Administrators	Local Authentication		
i i gray_LDB ² i gray_LDB ² i gray_LDB ² cefficite Sever i lengration CA cefficite Sever i Cablat cablat Sever i Cablat, Croto neurono cablat Sever i Cablat, Croto neurono cablat Sever i Cablat, Croto neurono cablat Sever i Sabat, Scoto NEUX Croto cablat Sever i Sabat, Scoto Neurono cablat Sever	ars	AD_Oren	Active Directory / Windows NT		
• • <td>ima</td> <td>Eanny-LDAP</td> <td>LDAP Server</td> <td></td> <td></td>	ima	Eanny-LDAP	LDAP Server		
Bageation C.A Certificate Server Bageation C.A Certificate Server Bageation C.A DADE Server Bageation C.A Radous Server Bageation C.Extificate autory SAME Server Bageation SAME SAME Server Bageation Sameation SAME	15	Eanny.test-domain	Certificate Server		
I DAP_Com LDAP_Som I DAP_Com DADAS I DAP DADAS I TADAS DAD	ns	Inegration CA	Certificate Server		
I Salad Control Radad Server I Salad, Control Radad Server Image: Control Radad Server I Salad, Control Radad Server Image: Control Radad Server I Salad, Control Radad Server Image: Control Radad Server I Salad, Son DreBin Control Radad Server Image: Control Radad Server I Salad, Son DreBin Control Radad Server Image: Control Radad		LDAP_Oren	LDAP Server		
Image: Marging Control Radous Server Image: Statistication Radous Server Image: Statistication Certificatis Server Image: Statistication Statistication Image: Statistication Radous Server Image: Traditication Statistication Image: Traditication Statistication Image: Traditication Statistication	Profiles	adus1	Radius Server		
Solution Radius Server Safara Cartinatas servar Safara Cartinatas servar Safara Cartinatas servar Safara Cartinatas servar Safara Cartinatas servar Safara Cartinatas servar Safara Cartinatas servar Safara Safara Safara Cartinatas servar Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara Safara	Policies 10	Radius Oren	Radius Server		
Safting Cartification surver Certification surver In Safting Safti	laintenance stern	RadiusTestDomain	Radius Server		
Schnott SAM, SAM. Strver SAS. SAG. UPERFA Oran SAM. Strver SAS. SAM. SAM. Strver SAS. SAM. SAM. Strver Stribut Load Load Authentication Stribut Load Lobe Strver TatASA Exclusion Lobe Strver T. XASA Exclusion Radus Strver T. XaSA Stadua Radus Strver		Safenet Certificate server	Certificate Server		
Image: State Out PINK Orage SAME Starver Image: State State Out PINK Orage SAME Starver Image: State Stat	9	Safenet SAML	SAML Server		
SAS: Sna prem SAN. Striver SS: SAMS SAN. Striver SS: SAMS SAN. Striver SS: Standard Radius Striver SS: Standard Cond Authentication Tatala LoAP Striver Tatala LoAP Striver Tatala Cond Authentication Tatala Cond Authentication Tatala Cond Authentication Tatala Radius Striver Tatala Radius Striver		SAML SAS ON PREM Oren	SAML Server		
Add Bada SAME Sarver Sectors Badar Sadas Server Spatem Local Local Authentication Instrument Bada Server TatAda Lobe Server TatAda Lobe Server TatAda Server TatAda Server TatAda Server TatAda Server TatAda Server	ooting	SAS on prem	SAML Server		
SPECame, Radua Radua Server System, Local Local Authentication Intel. saport SAME, Server TastAD LDAP Server TastAG Radua Server TastAG Radua Server		SAS SAM	SAML Server		
System Local Local Authentication Intel Local KAL Server TetAD LDAP Server TEXAD Local Authentication TX_SAS_Exclusters Robus Server TX_SAS_Exclusters Robus Server		SPEDemo Radius	Radius Server		
Istit sport SAN. Server Istit sport LDP Server ISt Sol Local Asterni Local Authentication ISt Sol Stadue Radus Server Istan Radus Server		System Local	Local Authentication		
I TathD LDA* Server IT X5AA Localutars Local Automitation IT X5AA Stabuture Kabus Server II TathD Rabus Server		E test export	SAML Server		
Tr SAS Acceluters Local Authentication Tr SAS Acceluters Radius Server Tr SAS Acceluters Radius Server		TestAD	LDAP Server		
TX: SAS: Radius Radius Server Izalem Radius Server		TK SAS LocalUsers	Local Authentication		
Token Radius Server		TK SAS Radius	Radius Server		
		I Token	Radius Server		
	_				
	271MNZS 2001-201	JOU7OOAYS 2 Juniper Networks, Inc. All rights reserved.			
The second s					
27 FINASSUUTOGAN 2001-2012 Jungke Indextrike, Inc. All righte reserved.					
071/mRX00/OdAY DD2 312 Angee Mataning, Inc. All rights reserved.					
U2TANKERSUUTODAYN 2001-2012 Jonger Tankofan, Tac, All nghla nearwel.					
227 UMERSIO/OdoXY DOC 2012 Angene Mattanina, Inc. All righte reserved.					
227 Jan Zalov (2004) 2001-2012 Jong de Tataloria, Inc. Al rights reserved.					

(The screen image above is from Juniper Networks Junos Pulse software. Trademarks are the property of their respective owners.)

2. In the New field, select Certificate Server, and then click New Server.

JUNIPEr.					
Junos Pulse Secure Ace	cess Service				Help Guidance Sign Out
System Status Configuration Network Clustering JF-MAP Federation Leg/Monitoring	Authentication Servers New: (Select server type) (Select server type)	New Server			
Authentication	Local Authentication	vere	Tune	Liear Record Supphropization	Logical Auth Server Name
Signing In	ACE Server	vera.	Local Authentication	osa necora synchronzadon	Logical Addition ver Hame
Auth, Servers	AL LDAP Server		Active Directory / Windows NT		
- Administrators	Ea Active Directory / Windows NT		LDAP Server		
Admin Realms Admin Roles	E Fa Anonymous Server		Certificate Server		
- Users	In Certificate Server		Certificate Server		
User Realms User Roles	SAML Server]	LDAP Server		
Resource Profiles	- C rather		Radius Server		
Resource Policies	· Ralles. Stat		Radius Server		
Maintenance	······································		Radius Server		
System	· indication in the second		Certificate Server		
Push Config	· Inducation and the		SAML Server		
Archiving	· DAME AND OR PARK OVER		SAML Server		
Troubleshooting	·····		SAML Server		
	10 1040-104N		SAML Server		
	······································		Radius Server		
	······································		Local Authentication		
	· Ind. agent		SAML Server		
	· Institut		LDAP Server		
	······································		Local Authentication		
	· Th. Intil Balling		Radius Server		
	· Instance		Radius Server		
Licensed to 0271MNZSJ Copyright © 2001-2012	JOU7OOAYS 3 Juniper Networks, Inc. All rights reserved.				

(The screen image above is from Juniper Networks Junos Pulse software. Trademarks are the property of their respective owners.)

3. In the **Name** field, enter a rule name.

JUNIPER				
20nos Polse Secore Acc System Status Configuration	Auth Jacons > Inegration CA			Huly Galdanie Sign Out
Clustering IP-MAP Federation Log/Monitoring	Settings Users			
Signing In	* Name:	Inegration CA		Label to inference this server.
Endpoint Security Juhr, Server Adhrun, Radiner Adhrun, Radiner Adhrun, Radiner User, Radiner User, Radiner User, Radiner Besouche Boldes Junes Sulas Statem Später Hanthawas Später Adhrung Archung Archung Archung	User Name Template: User Record Synchronization Enable User Re- Logical Auth S Save Changes?	ccentDNLCN> The terminate care care workfolde. Beampiers coertMML.areinfilemoties coertMML.areinfilemoties coertMML.areinfilemoties coertMML.areinfilemoties caref.MML.areinfilemoties coert-foundDMLCN> a ccoert Synchronizatio erver Name:	ani fescular disarchiner an Frect Car Kinnon the subget Confinitate series' number 9 Whene was can be UNN Trag Honorapa In 40 at 10 at 10 at 10 at 10 at 10 at 10 at 10 at 10 at 10 The sensylate subject T The sensylate subject S The sensylate subject S	Template no constructing user search (on setting as should be endowed in page backets like the samplate, The samplate part is a series as the same as these seed in rule maging states expressions and palay samplates. All of the setting as a samplate for substitution, 'Variable' which is endowed in page backets like the samplate backets are as the same as these seed in rule maging states expressions and palay samplates. All of the setting as a samplate backet is rule maging states expressions and palay samplates. All of the setting as a samplate backet is rule maging states expressions and palay samplates. All of the setting as a samplate backet is not expression as a samplate backet is not expression and palay samplates. All of the setting as a samplate backet is not expression and palay samplates. All of the setting as a samplate backet
	Save Changes R	leset		
Licensed to 027140253 Cepyright © 2001-2013	007004YS Juniper Networks, Inc. All righ	ta reserved.		

(The screen image above is from Juniper Networks Junos Pulse software. Trademarks are the property of their respective owners.)

- 4. In the User Name Template field, leave the default value.
- 5. Click Save Changes.

Attaching Authentication Servers to User Realms

To use CBA, you must attach the authentication server's policy created in the previous section to a user realm.

To attach the authentication server to the user realm:

1. In the left pane, click **Users > User Realms**.

JUNIPEr.			
Junos Pulse Secure /	Access Service		Help Guidance Sign Out
Status Configuration	User Authentication Realms		
Clustering	View: Overview • for all realms • Update		
Log/Monitoring	New. Duplicate		
Signing In	Authentication Realm	Servers	Dynamic Policy Evaluation
Auth. Servers	Users	Primary: Inegration CA	Disabled
Admin Realms Admin Realms	Users - RADIUS	Primary: AD_DEV Directory:AD_DEV Secondary: BADIUS_DEV	Disabled
Administration Administratio Administration Administration Administration Adminis	Authentication names specify what server its use for antihentication, here policies are sampled to user), and notifications on who can attained to agr-m.		
Loopard to 027518025 Copyright © 2001-001	SURGANS		

(The screen image above is from Juniper Networks Junos Pulse software. Trademarks are the property of their respective owners.)

- 2. In the right pane, under Authentication Realms, click the required user realm to be edited.
- 3. On the **General** tab, under **Servers**, in the **Authentication** field, select the authentication server you created in the previous section.

JUNIPEr.							
Junos Pulse Secure Ac	ccess Service			Help Guidance Sign O			
Cleoyatem Status Configuration	User Authentication Realma > Users						
Clustering	General Authentication Policy Role Mapping						
2F-MAD Federation Leo/Monitoring	manufactured, constrained and a second						
- Authentication	* Name:	Users	Label to reference this realm				
Signing In Endpoint Security	Description:	Default authentication					
Auth, Servers		realm for users					
- Administrators							
Admin Roles		The second second second second second second second					
- Users		 when edicing, scart on the kole mapping page 					
User Roles	Servers						
Resource Profiles		and the second state of th					
Junos Pulse	Specify the servers to use for authentication and authorization. To	create or manage servers, see the <u>Servers</u> page.					
Maintenance	Authentication:	Inegration CA •	Specify the server to use for authenticating users.				
Import/Export	Directory/Attribute:	None •	Specify the server to use for authorization.				
Pueh Config	Accounting	None	Specify the server to use for Radius accounting.				
Troubleshooting							
	Additional authentication server						
	U Dynamic policy evaluation						
	Other Settings						
	Authentication Policy:	Certificate restrictions					
	Role Mapping:	1 Rule					
	Save changes?						
	Save Changes						
	 Indicates required field 						
Licensed to 0271MNZ9 Cepyright © 2001-201	5JOU7DOAYS 12 Juniper Networks, Inc. All rights reserved.						

(The screen image above is from Juniper Networks Junos Pulse software. Trademarks are the property of their respective owners.)

- 4. Click Save Changes.
- 5. In the right pane, select the **Authentication Policy** tab.

6. Click the **Certificate** tab and then select **Only allow users with a client-side certificate signed by trusted client CAs.**

JUNIPEr.				
Junos Pulse Secure Ac System Status Configuration Retwork Clustering	ccess Service Lines Authentication Fealms > USSCTS General Authentication Policy Role Mapping			Help Guidance Sign Out
D*MAP Pederation Log/Monitoring Automatication Signing In Endpoint Seturity Auto, Servers Endpoint Seturity	Source 17 Boower Certificate Host Checker Limits Allow all users (no client-side certificate required) Allow all users and remember certificate information while use The second	er is signed in. ted Client CAs to sign in. To change the certification	authority, see the <u>Trusted Client CA</u> page.	
Admin Realma Admin Roles	You can optionally require specific values in the client certific Certificate field (example "cn")	cate: Expecte	1 value	
User Roles Resource Profiles Resource Policies Junos Pulse				Add
System Import/Export Push Config Arshiving Troubleshooting	Save Changes			
Licensed to 0271MNZS Copyright © 2001-201	SJOUTOGANS 2 Juniper Iteliupike, Inc. All rights reserved.			

(The screen image above is from Juniper Networks Junos Pulse software. Trademarks are the property of their respective owners.)

7. Click Save Changes.

Authenticator Assignment in SAC-CBA

SAC 8.3 supports a number of authentication methods

The following authenticators are supported:

- Safenet eToken 5100
- Safenet eToken Pro 72K
- Safenet eToken 7300-Standard
- Safenet eToken 4100
- Safenet eToken PRO Smartcard (Mask *)

The software package + documentation is available for download from our support site: https://kb.safenet-inc.com/kb/link.jsp?id=DOW3194

Running the Solution

This section describes CBA using the Junos Pulse software.

CBA Using Junos Pulse Software

- 1. Open the Junos Pulse software.
- 2. In the left pane, click **Connections**.
- 3. In the right pane, select the required connection and then click **Connect**.



(The screen image above is from Juniper Networks Junos Pulse software. Trademarks are the property of their respective owners.)

4. In the SAC Token Logon window, enter the Token Name and Token Password.

SafeNet Sa	feNet Authentication Client
Enter the Token Password	
Token Name:	Bob's Token
Token Password:	L
	Current Language: EN

The user is authenticated and a VPN connection is established.

🍀 PULSE		_×
File Help		
Connections Notable connections Acceleration Not accelerating	Connections - puise Disconnected	Connect
© 2010-2012 Juniper Networks, Inc. All	ights reserved.	Close

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information		
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA		
Phone	United States International	1-800-545-6608 1-410-931-7520	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.		