SafeNet Authentication Client

Integration Guide

Using SAC CBA with Juniper Junos Pulse

SafeNet
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

Document PN: 007-012717-001, Rev. A, Copyright © 2015 SafeNet, Inc., All rights reserved.

Contents

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.

Document PN: 007-012717-001, Rev. A, Copyright © 2015 SafeNet, Inc., All rights reserved.

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

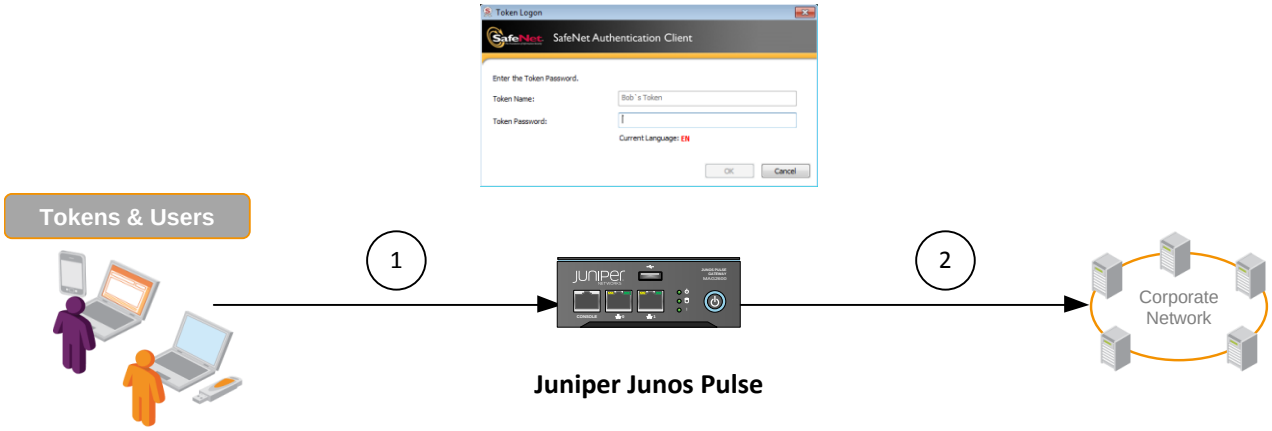
Audience

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.

Document PN: 007-012717-001, Rev. A, Copyright © 2015 SafeNet, Inc., All rights reserved.

CBA Flow using SAC

The image below shows the environment required to implement a Juniper solution using SafeNet's certificate-based 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.

Document PN: 007-012717-001, Rev. A, Copyright © 2015 SafeNet, Inc., All rights reserved.

CBA Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based 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

Document PN: 007-012717-001, Rev. A, Copyright © 2015 SafeNet, Inc., All rights reserved.

Configuring Juniper for Certificate-based Authentication

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

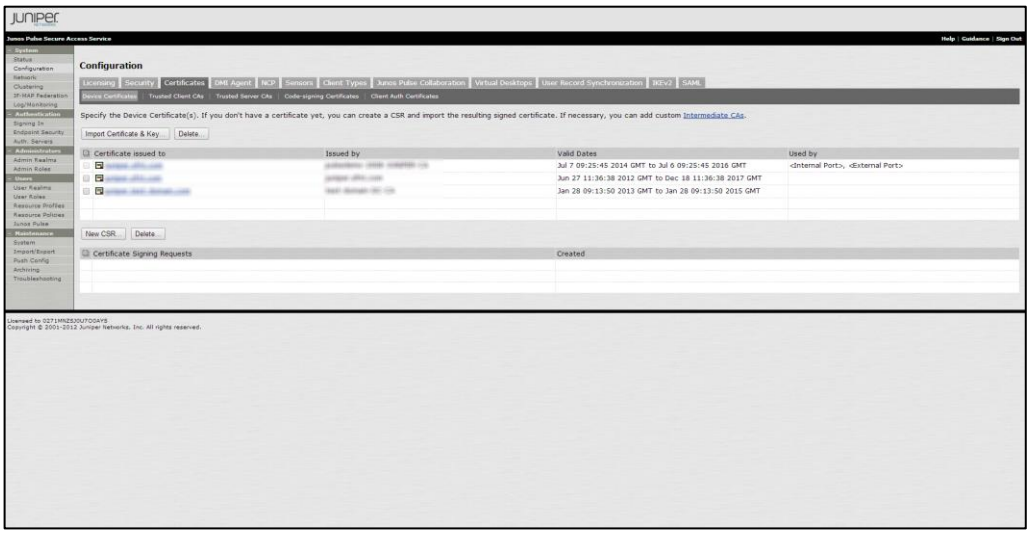
- Certificate configuration
- Adding an authentication server
- Attaching an authentication server to user realms

Certificate Configuration

1. Open the **Juniper SA** web console

(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.

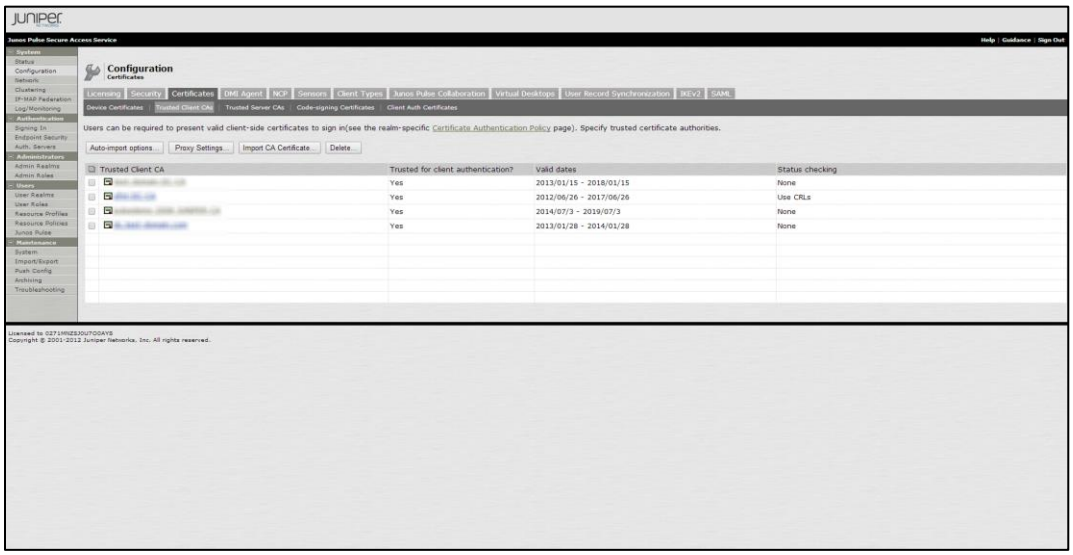


(The screen image above is from Juniper Networks Junos Pulse software. Trademarks are the property of their respective owners.)

4. Select the T**rusted Client CAs** tab.

Document PN: 007-012717-001, Rev. A, Copyright © 2015 SafeNet, Inc., All rights reserved.

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



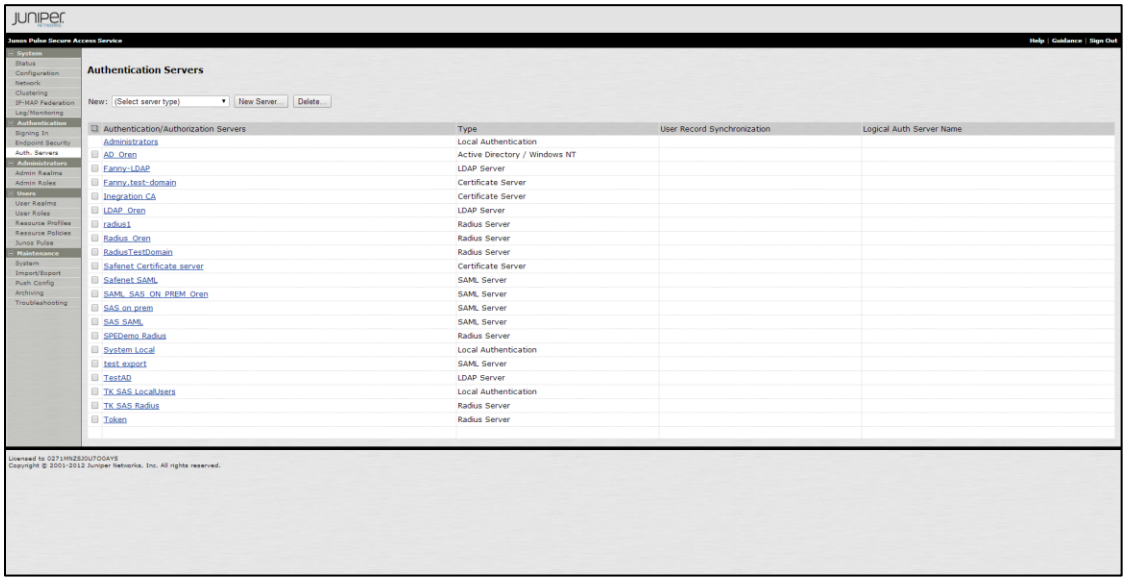
(The screen image above is from Juniper Networks Junos Pulse software. Trademarks are the property of their respective owners.)

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:

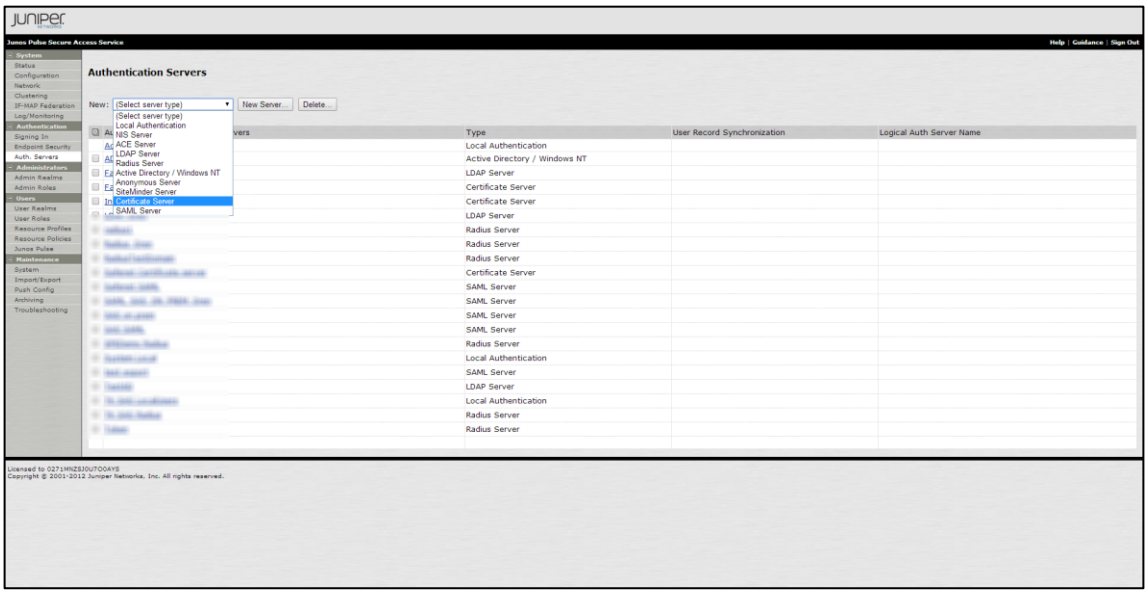
1. In the left pane, click **Authentication > Auth. Servers**.



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

Document PN: 007-012717-001, Rev. A, Copyright © 2015 SafeNet, Inc., All rights reserved.

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



(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.

(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**.

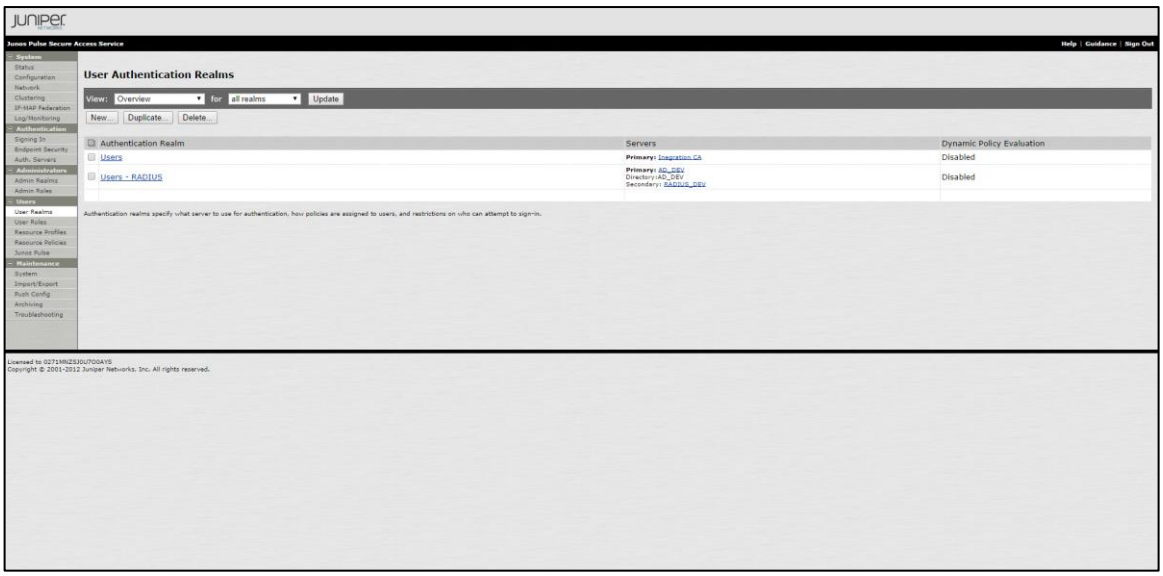
Document PN: 007-012717-001, Rev. A, Copyright © 2015 SafeNet, Inc., All rights reserved.

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**.



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

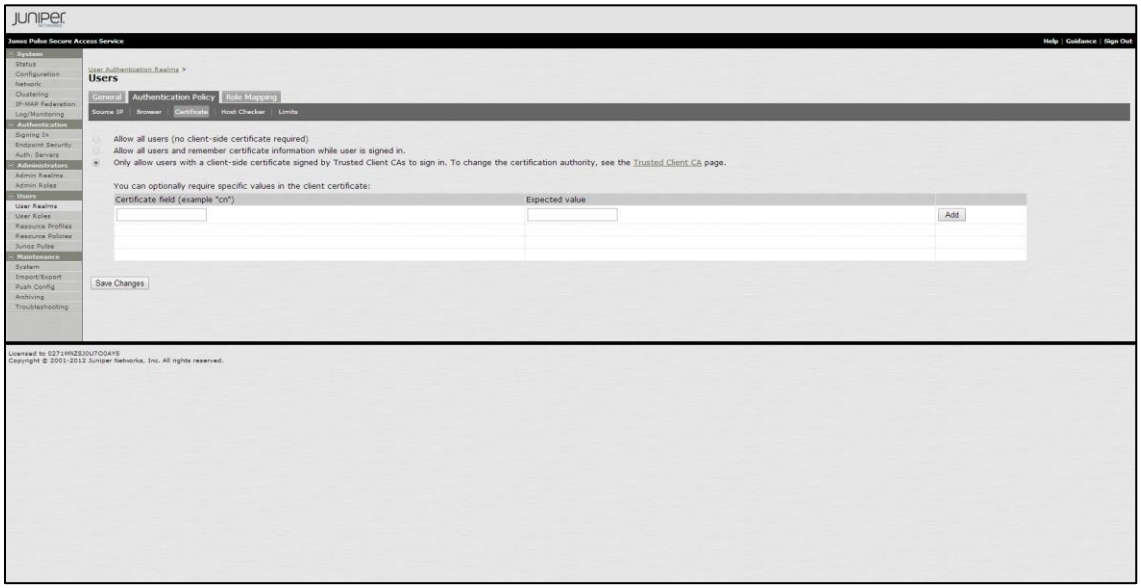
2. In the right pane, under **Authentication Realms**, click the required user realm to be edited.
3. On the **General** tab, under **Servers**, in the **Authentication** field, select the authentication server you created in the previous section.

(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.

Document PN: 007-012717-001, Rev. A, Copyright © 2015 SafeNet, Inc., All rights reserved.

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



(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

Document PN: 007-012717-001, Rev. A, Copyright © 2015 SafeNet, Inc., All rights reserved.

Running the Solution

This section describes CBA using the Junos Pulse software.

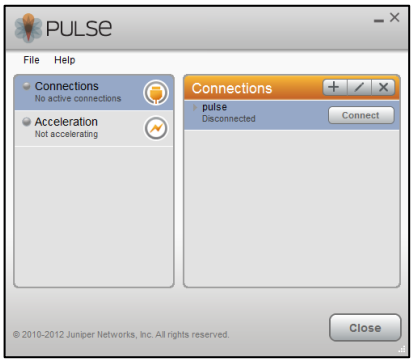
CBA Using Junos Pulse Software

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.**

The user is authenticated and a VPN connection is established.



Document PN: 007-012717-001, Rev. A, Copyright © 2015 SafeNet, Inc., All rights reserved.

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	1-800-545-6608
	International	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.	

Document PN: 007-012717-001, Rev. A, Copyright © 2015 SafeNet, Inc., All rights reserved.