SafeNet Authentication Service

Cisco AnyConnect Agent Configuration Guide

Document Information

Document Part Number	007-012458-001, Rev C
Release Date	September 2014

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.

Trademarks

Contents

Preface

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet Authentication Service users and security officers, key manager administrators, and network administrators. It is assumed that the users of this document are proficient with security concepts.

All products manufactured and distributed by SafeNet, Inc. are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

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.	

CHAPTER 1
Overview

By default, Cisco ASA (Adaptive Security Appliance) user authentication requires that a user provide a correct user name and password to log on successfully. This document describes the steps necessary to augment this logon mechanism with strong authentication by adding a requirement to provide a one-time password (OTP) generated by a SafeNet Authentication Service token.

Applicability

This guide is applicable to the following:

Security Partner	Cisco
Product Name	Cisco ASA 5500 series
ASA Version	8.3
ADSM Version	6.3(1)

Platform Compatibility

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—A cloud service of SafeNet, Inc.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—The software used to build a SafeNet authentication service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A term used to describe the implementation of SAS-SPE on-premises.

NOTE: References to BlackShield and CRYPTOCard reflect CRYPTOCard branding prior to acquisition by SafeNet. Over time, these references will change to reflect SafeNet branding, including program installation locations.

Prerequisites

- Ensure end users can authenticate through the Cisco ASA with a static password before configuring the Cisco Secure ASA to use RADIUS authentication.
- Configure a RADIUS Client in SafeNet Authentication Server with a shared secret and port number identical to that being programmed in the Cisco ASA.
- Test user accounts with an active token.

CHAPTER 2
Cisco ASA AnyConnect Client

The Cisco ASA device can dynamically display login fields based on the settings defined in each Group Profile.

The Cisco ASA device may also restrict users from selecting the Group Profile, and it can implement additional customizable options using the **Preferences** button.

Here are several examples of how Cisco AnyConnect is displayed, depending on the group selected:

Figure 1: Login with Username and Password

(The screen image above is from Cisco® software. Trademarks are the property of their respective owners.)

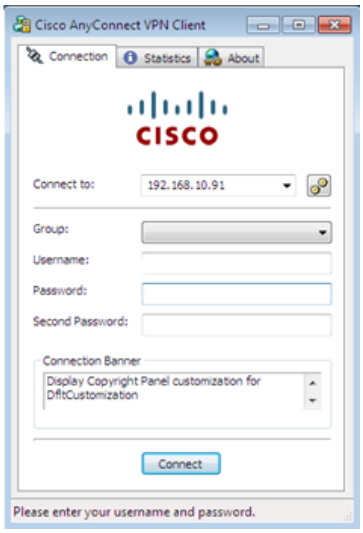


Figure 2: Login with Username, Password, and Second Password (OTP)

(The screen image above is from Cisco® software. Trademarks are the property of their respective owners.)

SAS Cisco AnyConnect Client

Organizations may wish to integrate software-based two-factor authentication tokens with the Cisco AnyConnect Client to simplify the login process for users, thus eliminating the need to copy and paste a one-time password from one application to another.

With the SAS Cisco AnyConnect Agent, the ability to integrate software-based two-factor authentication tokens with Cisco AnyConnect becomes a reality.

SafeNet Authentication Service is compatible with the following versions of Cisco AnyConnect Client:

- 2.4
- 2.5
- 3.0
- 3.1
- 3.1.04063
- 3.1.04072

Here are several examples of how the **SAS Cisco AnyConnect** agent is displayed, depending on which group is selected and which field in the agent has been configured to display the software token detection.

Figure 3: MobilePASS Token detection on the Primary Password field

Figure 4: MobilePASS Token detection on the Secondary Password field

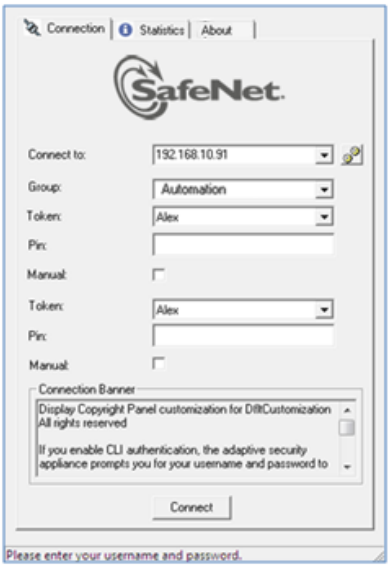


Figure 5: MobilePASS Token detection in both the Primary and Secondary Password fields

Cisco AnyConnect Client and MobilePASS Token Detection

CAUTION: The Cisco AnyConnect Client must be installed prior to the installation of the SafeNet Authentication Service Cisco AnyConnect package.

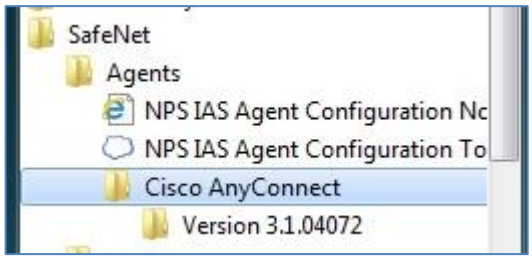
SafeNet provides a Cisco AnyConnect Client capable of detecting the presence of SafeNet software tokens.

1. Install the SAS Software Tools package.

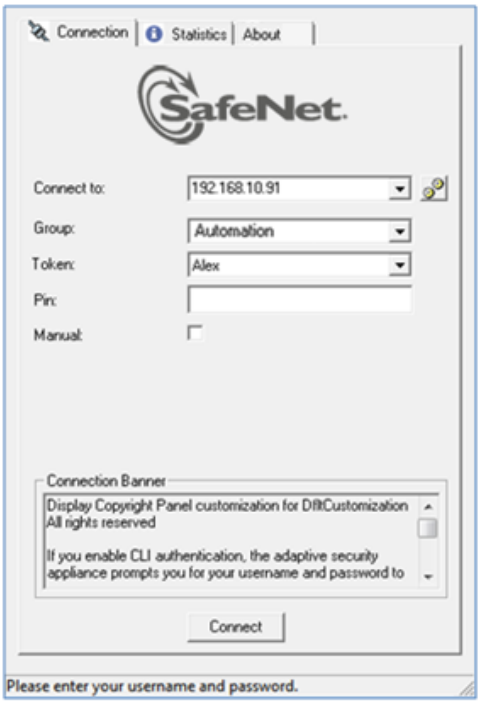
NOTE: If you are on a 64-bit operating system, install the SAS Software Tools 64-bit version. The installer can be found in the html, agents, x64 directory within the SAS download package.

2. Assign or provision the user with a MobilePASS token.
3. Install the **SafeNet Authentication Service Cisco AnyConnect** package.

4. Select **Start > All Programs > SafeNet > Agents > Cisco AnyConnect > Version [2.4, 2.5, or 3.1] > Cisco AnyConnect Client [2.4, 2.5 or 3.1]**.



Once connected to the Cisco ASA, the following window is displayed. The settings displayed on the **Connection** tab represent the default configuration for the SafeNet Authentication Service Cisco AnyConnect Agent.



If the default configuration is incorrect, and the MobilePASS token is being detected in the wrong fields, then follow the steps in the next section to change the MobilePASS token detection settings.

SAS Cisco AnyConnect Agent Registry Key

The **SoftTokenInclusion** Registry key allows you to specify where the MobilePASS token drop-down list will appear and which password field(s) will be used when the one-time password is submitted to the server.

- On a Windows XP/Vista/7 (32-bit) operating system, the Registry key is located in:

  \HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\CiscoAnyClientPlugin

- On a Windows XP/Vista/7 (64-bit) operating system, the Registry key is located in:

  \HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CRYPTOCard\CiscoAnyClientPlugin

The default value for the **SoftTokenInclusion** key is:

ALL+ALL+1;

The key value is defined as follows:

“Connect To”+”Group Profile”+”Field Position to display MobilePASS and submit one-time password”;

Multiple options can be appended to the key. For example:

ALL+Corporate+1;ALL+Automation+2;ALL+CRYPTOCard+3;

SoftTokenInclusion Registry Key Examples

Example 1

ASA.cryptocard.com+Automation+1;

- This setting will work when connecting to ASA.cryptocard.com.
- MobilePASS token detection will only show up using the **Automation** Group Profile.
- It will display MobilePASS token detection in the first field.

Example 2

The following is an example of changing MobilePASS token detection to a different field:

ALL+ALL+1;

- Display MobilePASS in the first **Username** field and submit a one-time password to the first **Password** field.
- This is the default setting after installing **SafeNet Authentication Service Cisco AnyConnect** and **SafeNet Authentication Service Software Tools**.
- This option is used if authentication is going against the SafeNet Authentication Service Professional Server.

Example 3

The following is an example of changing MobilePASS token detection to a different field:

ALL+ALL+2;

- Display MobilePASS in the second Username field and submit a one-time password to the second **Password** field.
- This option is used if dual authentication is required; for example, Microsoft Password [Top], and then SafeNet [Bottom].

Example 4

The following is an example of changing MobilePASS token detection to a different field:

ALL+ALL+3;

- Displays MobilePASS in the first and second **Username** field and submits a one-time password to the first and second **Password** fields.
- This setting is used if there needs to be authentication against the SAS server. Typically, this setting would rarely be used.

CHAPTER 3
Troubleshooting

RADIUS Authentication Issues

- When troubleshooting RADIUS authentication issues, refer to the logs on the Cisco ASA device.
- All logging information for Internet Authentication Service (IAS) or Network Policy Server (NPS) can be found in the Event Viewer.
- All logging information for the SAS IAS\NPS agent can be found in the following location:

  \ProgramFiles\CRYPTOCard\BlackShield ID \IAS Agent\log
- The following is an explanation of the logging messages that may appear in the Event Viewer for the Internet Authentication Service (IAS) or Network Policy Server (NPS) RADIUS Server:

Error Message	Solution
Packet DROPPED: A RADIUS message was received from an invalid RADIUS client.	Verify that a RADIUS client entry exists on the RADIUS server.
Authentication Rejected: Unspecified	This will occur when one or more of the following conditions exists: • The username does not correspond to a user on the SafeNet Authentication Server. • The SafeNet password does not match any tokens for that user. • The shared secret entered in Cisco Secure ACS does not match the shared secret on the RADIUS server.
Authentication Rejected: The request was rejected by a third-party extension DLL file.	This will occur when one or more of the following conditions exists: • The SafeNet Agent for IAS\NPS cannot contact the SafeNet Authentication Service server. • The Pre-Authentication Rules on the SafeNet Authentication Service server do not allow incoming requests from the SafeNet Agent for IAS\NPS. • The SafeNet Agent for IAS\NPS Keyfile does not match the Keyfile stored on the SafeNet Authentication Service server. • The username does not correspond to a user on the SafeNet Authentication Service server.