SafeNet Cisco AnyConnect Client

Configuration Guide

gemalto
security to be free

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Document Part Number: 007-012458-002, Rev. D

Release Date: November 2015

Contents

Preface

This document describes how to install, configure, and use the SafeNet Cisco AnyConnect Client.

Customer Release Notes

The Customer Release Notes (CRN) document provides important information about this release that is not included in other customer documentation. It is strongly recommended that you read the CRN to fully understand the capabilities, limitations, and known issues for this release.

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 Gemalto Customer Support. Gemalto 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 Gemalto 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	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	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 Gemalto Knowledge Base.	

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, 9.0
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.

SafeNet Cisco AnyConnect Client is tested with the following versions of Cisco AnyConnect Client:

- 2.4
- 2.5
- 3.0
- 3.1
- 3.1.04063
- 3.1.08009

- 3.1.10010
- 3.1.05187
- 3.1.04072
- 3.1.08
- 4.0.00048
- 4.0.00051
- 4.1.02011
- 4.1.00028

NOTE: The SafeNet Cisco AnyConnect Client is assumed to work with all minor versions of Cisco AnyConnect Client. However, full compatibility for minor versions of Cisco AnyConnect Client cannot be verified.

The table below lists the versions of the Windows operating system and the supported major versions of the Cisco AnyConnect Client:

Operating System	Cisco AnyConnect Client Supported (Version)
Windows Server 2008 R2 (64-bit)	2.5, 3.1, 4.0, and 4.1
Windows 7 (32-bit and 64-bit)	2.4, 2.5, 3.0, 3.1, 4.0, and 4.1
Windows 8 (32-bit and 64-bit)	3.1, 4.0, and 4.1
Windows 8.1 (64-bit)	3.1, 4.0, and 4.1

Prerequisites

- Ensure end users can authenticate through Cisco ASA with a static password before configuring 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 Cisco ASA.
- Test user accounts with an active token.
- MobilePASS application version 8.4 or higher is only supported.
- Ensure that Cisco AnyConnect Client is installed prior to installing SafeNet Cisco AnyConnect Client.

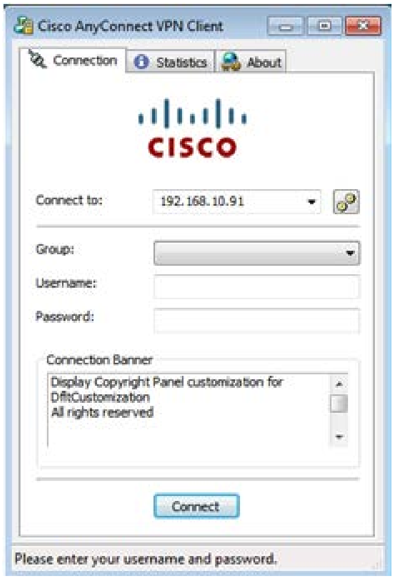
2

Cisco AnyConnect Client

The Cisco AnyConnect Client can dynamically display login fields based on the settings defined in the Cisco ASA device for 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.

Below are several examples of how Cisco AnyConnect Client is displayed, depending on the group selected in the Cisco ASA device.



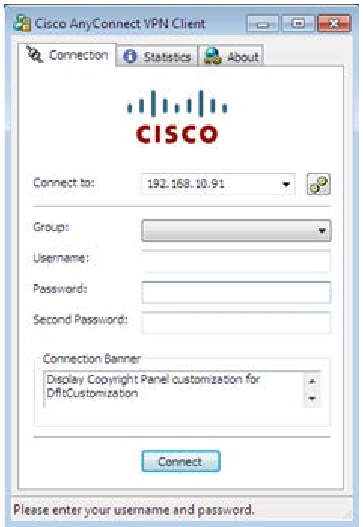
Connect to: 192.168.10.91

Display Copyright Panel customization for DfltCustomization
All rights reserved

Please enter your username and password.

Figure 1: Login with Username and Password (as in version 2.4 & 2.5)

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



Connect to: 192.168.10.91

Display Copyright Panel customization for DfltCustomization

Please enter your username and password.

Figure 2: Login with Username, Password, and Second Password (OTP) (as in version 2.4 & 2.5)

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

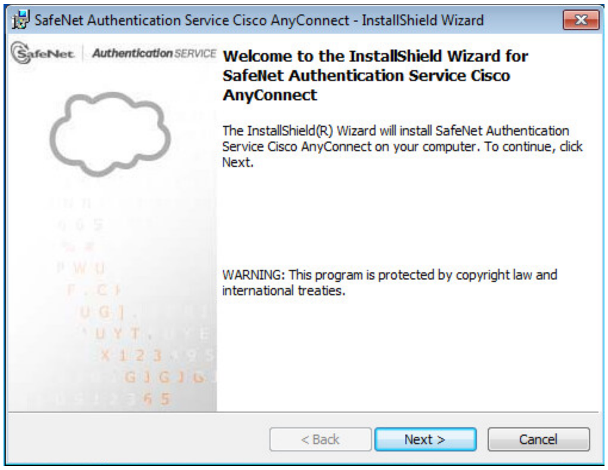
3
SafeNet Cisco AnyConnect Client

SafeNet Cisco AnyConnect Client enables organizations to integrate software-based two-factor authentication tokens with their Cisco AnyConnect Client in a seamless way, thus simplifying the login process for users, eliminating the need to copy and paste a one-time password from one application to another.

Installing SafeNet Cisco AnyConnect Client

NOTE: If you are on a 64-bit operating system, install the SafeNet Cisco AnyConnect Client 64-bit version. The installer can be found in the **html/agents/x64** directory within the SAS download package.

1. Start the SafeNet Cisco AnyConnect Client setup application. Click **Next**.

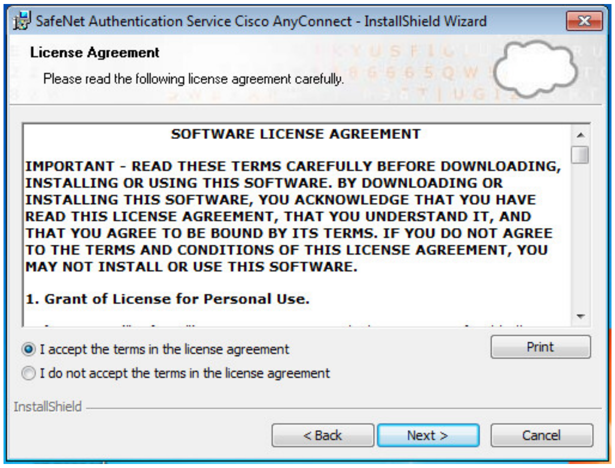

SafeNet Authentication Service Cisco AnyConnect - InstallShield Wizard
SafeNet | Authentication SERVICE

Welcome to the InstallShield Wizard for SafeNet Authentication Service Cisco AnyConnect

The InstallShield(R) Wizard will install SafeNet Authentication Service Cisco AnyConnect on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

2. On the **License Agreement** window, select **I accept the terms in the license agreement**, and then click **Next**.



SafeNet Authentication Service Cisco AnyConnect - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

SOFTWARE LICENSE AGREEMENT

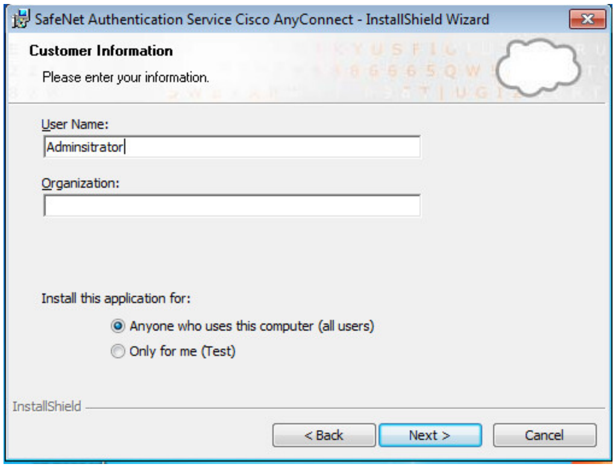
IMPORTANT - READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THIS SOFTWARE. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, YOU MAY NOT INSTALL OR USE THIS SOFTWARE.

1. Grant of License for Personal Use.

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

3. On the **Customer Information** window, specify the user name, organization name, and who can access the application. Then, click **Next**.



SafeNet Authentication Service Cisco AnyConnect - InstallShield Wizard

Customer Information

Please enter your information.

User Name: Adminsitrator

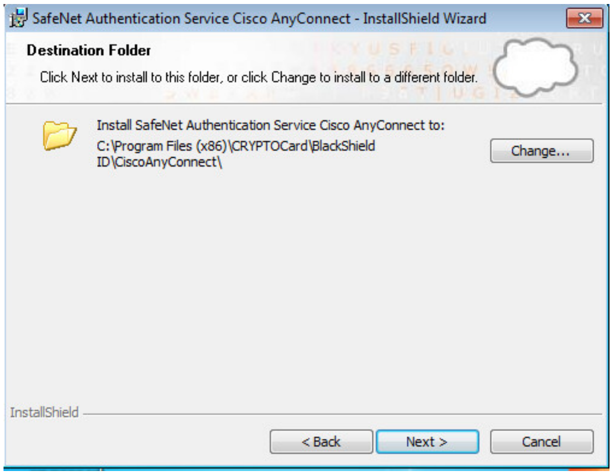
Organization:

Install this application for:

● Anyone who uses this computer (all users)

○ Only for me (Test)

4. On the **Destination Folder** window, select the folder where installation has to be done. Then, click **Next**.



SafeNet Authentication Service Cisco AnyConnect - InstallShield Wizard

Destination Folder

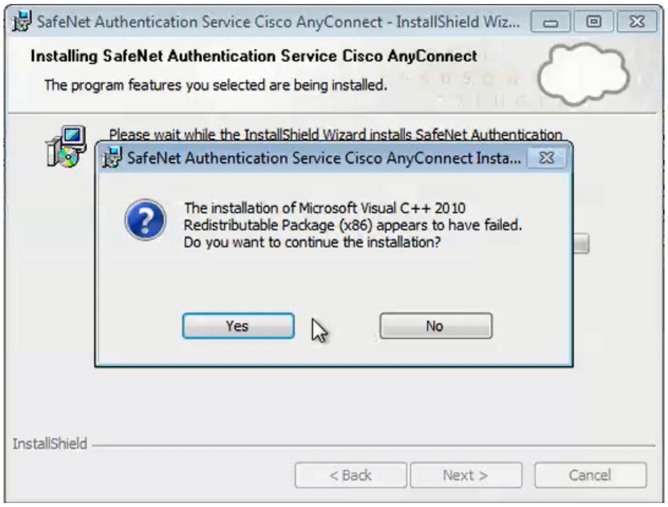
Click Next to install to this folder, or click Change to install to a different folder.

Install SafeNet Authentication Service Cisco AnyConnect to:
C:\Program Files (x86)\CRYPTOCard\BlackShield ID\CiscoAnyConnect\

The setup application will install the program features you selected.

NOTE: The SafeNet Cisco AnyConnect Client 2.0 requires VC++ 2010 redistribute package. The installer already contains the redistribute package version 10.0.30319.

In case the system already contains the higher version of redistribute package, the screen shown below will appear. Click **Yes** to continue.



SafeNet Authentication Service Cisco AnyConnect - InstallShield Wiz...

Installing SafeNet Authentication Service Cisco AnyConnect

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs SafeNet Authentication

SafeNet Authentication Service Cisco AnyConnect Insta...

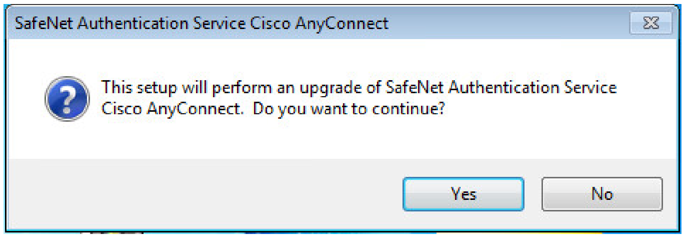
The installation of Microsoft Visual C++ 2010 Redistributable Package (x86) appears to have failed. Do you want to continue the installation?

Upgrading SafeNet Cisco AnyConnect Client

This section refers to upgrading the SafeNet Cisco AnyConnect Client to version 2.0, if any prior version is installed.

NOTE: The previous versions of SafeNet Cisco AnyConnect Client directly support only MP-1 tokens. After upgrading to SafeNet Cisco AnyConnect Client 2.0, only MobilePASS tokens will be detected.

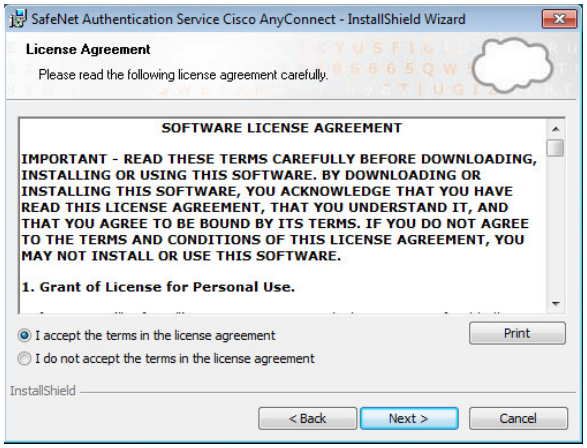
1. Start the SafeNet Cisco AnyConnect Client setup application. Click **Yes**.



SafeNet Authentication Service Cisco AnyConnect

This setup will perform an upgrade of SafeNet Authentication Service Cisco AnyConnect. Do you want to continue?

2. On the **License Agreement** window, select **I accept the terms in the license agreement**, and then click **Next**.



SafeNet Authentication Service Cisco AnyConnect - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

SOFTWARE LICENSE AGREEMENT

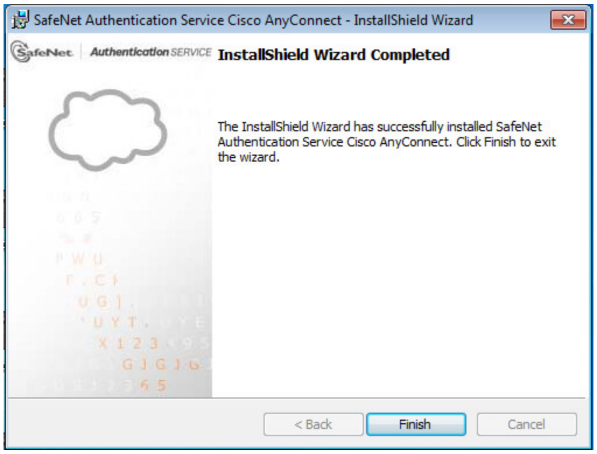
IMPORTANT - READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THIS SOFTWARE. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, YOU MAY NOT INSTALL OR USE THIS SOFTWARE.

1. Grant of License for Personal Use.

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

3. Click **Finish**. The setup application has completed the upgrade process.



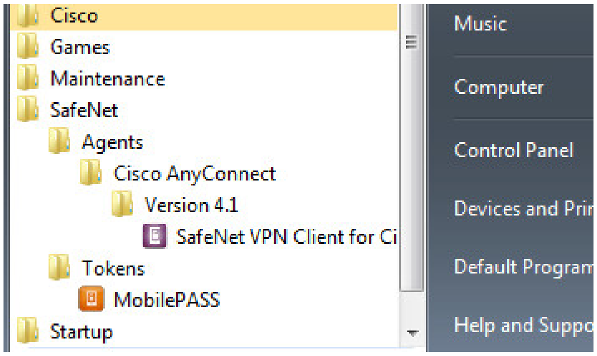
SafeNet Authentication Service Cisco AnyConnect - InstallShield Wizard

InstallShield Wizard Completed

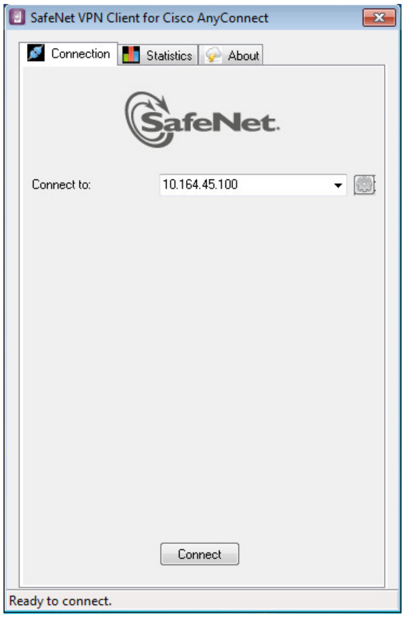
The InstallShield Wizard has successfully installed SafeNet Authentication Service Cisco AnyConnect. Click Finish to exit the wizard.

Establishing VPN Connection and Detecting MobilePASS Token

1. Click **Start** > **All Programs** > **SafeNet** > **Agents** > **Cisco AnyConnect** > **Version [2.4, 2.5, 3.1, 4.0, or 4.1]** > **SafeNet VPN Client for Cisco AnyConnect**.



2. In the **Connect to** field, enter the VPN server host name or IP address, and then click **Connect**.



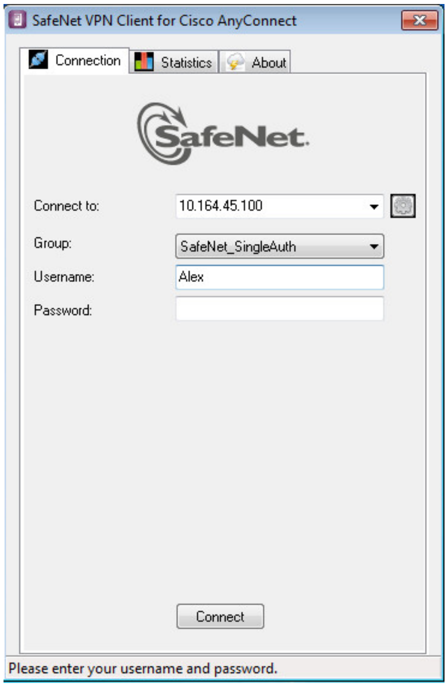
Connect to: 10.164.45.100

Ready to connect.

3. The next window is displayed depending on one of the scenarios as explained below.

   Scenario 1: If no MobilePASS token is detected on the client machine, the Username and Password fields are displayed.

   Enter the user name and password, and then click **Connect**.



Connect to: 10.164.45.100

Group: SafeNet_SingleAuth

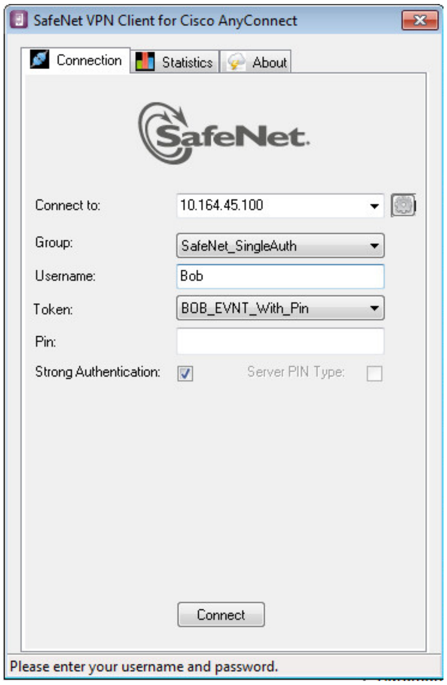
Username: Alex

Password:

Please enter your username and password.

   Scenario 2: If the MobilePASS token is detected on the client machine, the fields are displayed for strong authentication. All the MobilePASS tokens detected are listed in the **Token** filed.

   Enter the user name, select the associated token, and enter the pin, and then click **Connect**. If the MobilePASS token has no pin policy, the Pin field will be disabled.



Connect to: 10.164.45.100

Group: SafeNet_SingleAuth

Username: Bob

Token: BOB_EVNT_With_Pin

Pin:

Strong Authentication: ☑ Server PIN Type: □

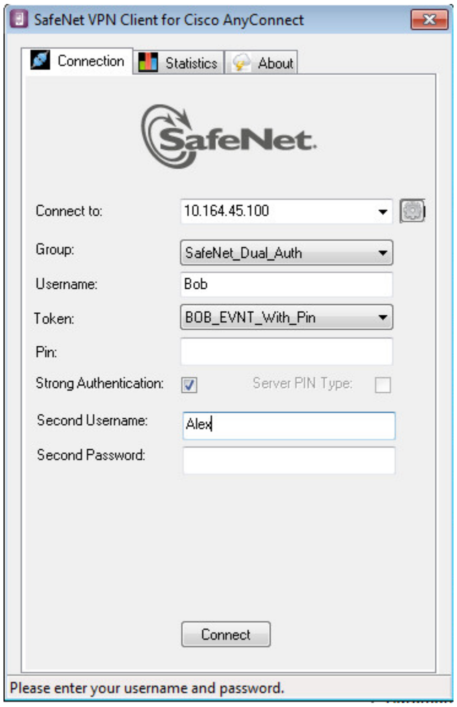
Please enter your username and password.

Scenario 3: If the Group selected is configured as Dual Authentication type, the primary and secondary user name and password fields are displayed, along with fields for strong authentication.

a. For first factor authentication, enter the **Username**, select the associated **Token**, and enter the **Pin**. If the MobilePASS token has no pin policy, the Pin field will be disabled.

b. For second factor authentication, enter the **Second Username** and **Second Password**.

c. Click **Connect**.



Connect to: 10.164.45.100

Group: SafeNet_Dual_Auth

Username: Bob

Token: BOB_EVNT_With_Pin

Pin:

Strong Authentication: ☑ Server PIN Type: □

Second Username: Alex

Second Password:

Please enter your username and password.

Configuring Registry Key

This section contains information on registry settings allowing administrators to change behavior of the application according to the environment and security infrastructure.

- 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 **UseServerSidePIN** registry key allows you to specify if the MobilePASS token should be allowed to be considered as the Server Side Pin Type. This policy depends on if SAS Administrator/Operator has provisioned users with Server Side Pin Type tokens.
- The **ServerSidePINPolicy** registry key is based on the Server Side Pin policy applied in SAS identity provider. Value must be either **Append** or **Prepend**.

SoftTokenInclusion Registry Key Example

Registry Value Options	Description	Note (If any)
ALL+ALL+1;	Display MobilePASS in the first Username field. For dual authentication, MobilePASS tokens are displayed in the first factor, and username and password fields are displayed for the second factor.	This is the default setting after installing SafeNet Cisco AnyConnect Client.
<VPN host name>+<Group name>+1;	This setting will work when connecting to the specific VPN host name (for example, ASA.gemalto.com). All the MobilePASS tokens detected will be listed only for the specified Group profile. The MobilePASS tokens detected will be shown in the first field.	
ALL+ALL+2;	Display username and password in the first factor, and MobilePASS in the second factor.	This option is used if dual authentication is required; for example, Microsoft Password [Top], and then SafeNet Identity Provider [Bottom].
ALL+ALL+3	Display tokens in both Primary and Secondary fields.	For dual authentication, if Identity Provider is SAS for both primary and secondary authentication.

Authentication Combination Example

The table below lists the types of authentication that can be configured against different soft token inclusion values:

Soft Token Inclusion Value	Single Authentication	Dual Authentication Options
ALL+ALL+1	Password or Token	(Token and Password) (Password and Password)
ALL+ALL+2	Password	(Password and Token) (Password and Password)
ALL+ALL+3	Password or Token	(Password and Password) (Token and Password) (Password and Token) (Token and Token)

APPENDIX A
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.