

SafeNet Authentication Service Agent for Cisco AnyConnect Client

Installation and Configuration Guide

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.

© 2018 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/ or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Release: 2.2.0

Document Part Number: 007-012458-003, Rev. B

Release Date: March 2018

Table of Contents

Preface	4
Customer Release Notes	4
Audience.....	4
Support Contacts.....	5
Customer Support Portal	5
Telephone Support	5
1 Introduction	7
Platform Compatibility	7
Applicability.....	7
Prerequisites	9
Cisco AnyConnect Client.....	9
2 Installation and Upgrade	11
Installing SafeNet Authentication Service Agent for Cisco AnyConnect Client.....	12
Uninstalling SafeNet Authentication Service Agent for Cisco AnyConnect Client.....	15
Upgrading SafeNet Authentication Service Agent for Cisco AnyConnect Client	15
Establishing VPN Connection	18
3 Configuration	21
Configuring Registry Keys.....	21
APPENDIX A Troubleshooting	8
RADIUS Authentication Issues	8

Preface

This document describes how to install, configure, and use the SafeNet Authentication Service (SAS) Agent for 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 SAS 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 Gemalto 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, refer to 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.

Customer Support Portal

The Customer Support Portal, at <https://supportportal.gemalto.com>, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.



NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the REGISTER link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

Region	Telephone number (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Global	+1-410-931-7520
Australia	1800.020.183
China	North: 10800-713-1971 South: 10800-1301-932
France	0800-912-857
Germany	0800-181-6374
India	000.800.100.4290
Israel	180-931-5798
Italy	800-786-421
Japan	0066 3382 1699

Korea	+82 2 3429 1055
Netherlands	0800.022.2996
New Zealand	0800.440.359
Portugal	800.863.499
Singapore	800.1302.029
Spain	900.938.717
Sweden	020.791.028
Switzerland	0800.564.849
United Kingdom	0800.056.3158
United States	(800) 545-6608

1

Introduction

By default, Cisco Adaptive Security Appliance (ASA) authentication requires that a user provide a correct user name and password to login successfully. This document describes the steps necessary to augment this login mechanism with strong authentication by adding a requirement to provide a One-Time Password (OTP) generated by a SAS token.

Platform Compatibility

The information in this document applies to:

- **SafeNet Authentication Service - Cloud (SAS Cloud)** — The SafeNet's cloud-based authentication service.
- **SafeNet Authentication Service - Service Provider Edition (SAS SPE)** — The on-premises, server version targeted at service providers interested in hosting SAS in their data center(s).
- **SafeNet Authentication Service - Private Cloud Edition (SAS PCE)** — The on-premises, server version targeted at organizations interested in hosting SAS in their private cloud environment.

Applicability

The information in this document applies to the following:

Security Partner	Cisco
Product Name	Cisco ASA 5500 series
ASA Version	9.2(4)
ASDM Version	7.6(1)
SAS SPE / PCE Version	3.4 and later
MobilePASS	v8.4 and later

The SAS Agent for Cisco AnyConnect Client is tested with the following versions of Cisco AnyConnect Client:

- 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
- 4.3.00748
- 4.4.03034
- 4.5.02036

**NOTES:**

- The SAS Agent for 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.
- If the Cisco AnyConnect Client version is upgraded to a later version after installation of the SAS agent, the user needs to uninstall and then reinstall the agent.
- Cisco AnyConnect Client version later than **4.5** is not supported. If used, the user will encounter an unsupported version error during agent's installation.

The following table 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 7 (32-bit and 64-bit)	3.1, 4.0, 4.1, 4.3, 4.4 and 4.5
Windows 8.1 (64-bit)	3.1, 4.0, 4.1, 4.3, 4.4 and 4.5
Windows 10 (32-bit and 64-bit)	4.3, 4.4 and 4.5

**NOTES:**

- The SafeNet Authentication Service Agent for Cisco AnyConnect v2.2.0 will work with Windows 7 Service Pack 1 (SP1).
- Use Microsoft's recommended **Windows 10** version(s). Users may face some

issues in upgrading the agent if they are using Windows 10 RTM version(s).

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 the Cisco ASA.
- Test user accounts with an active token.
- Ensure that Cisco AnyConnect Client is installed prior to installing the SAS Agent for Cisco AnyConnect Client.

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 **Preferences**.

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

1. Login with Username and Password.



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

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.)

2

Installation and Upgrade

The SAS Agent for Cisco AnyConnect Client enable 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 OTPs from one application to another.

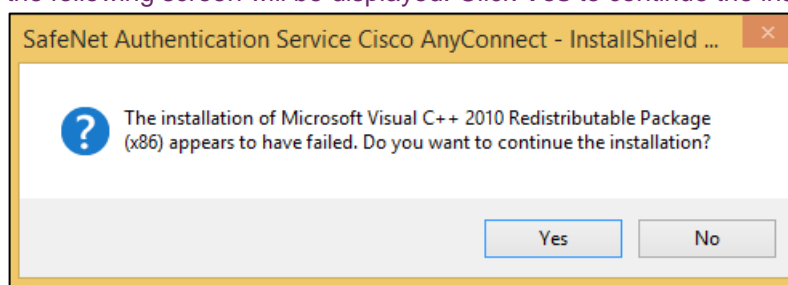


NOTE: The SAS Agent for Cisco AnyConnect Client v2.2.0 requires VC++ Redistribute Packages:

Package Name	Version
Microsoft Visual C++ 2005 SP1 Redistributable MFC Security update KB2538242(x86)	8.0.61001
Microsoft Visual C++ 2010 Redistributable (x86)	10.0.30319
Microsoft Visual C++ 2015 Redistributable (x86)	14.0.23026.0

The agent's installer will prompt to install the applicable Redistribute Packages if the system does not contain (or contains lower version of) the applicable packages.

In case, the system already contains higher version of the Redistribute Packages, the following screen will be displayed. Click **Yes** to continue the installation.



Installing SafeNet Authentication Service Agent for Cisco AnyConnect Client



NOTE: If you have logged into the system as an administrator or if you are a member of the Domain Admin group, the installation process will run successfully. Otherwise, a window will appear requiring you to provide administrator credentials.

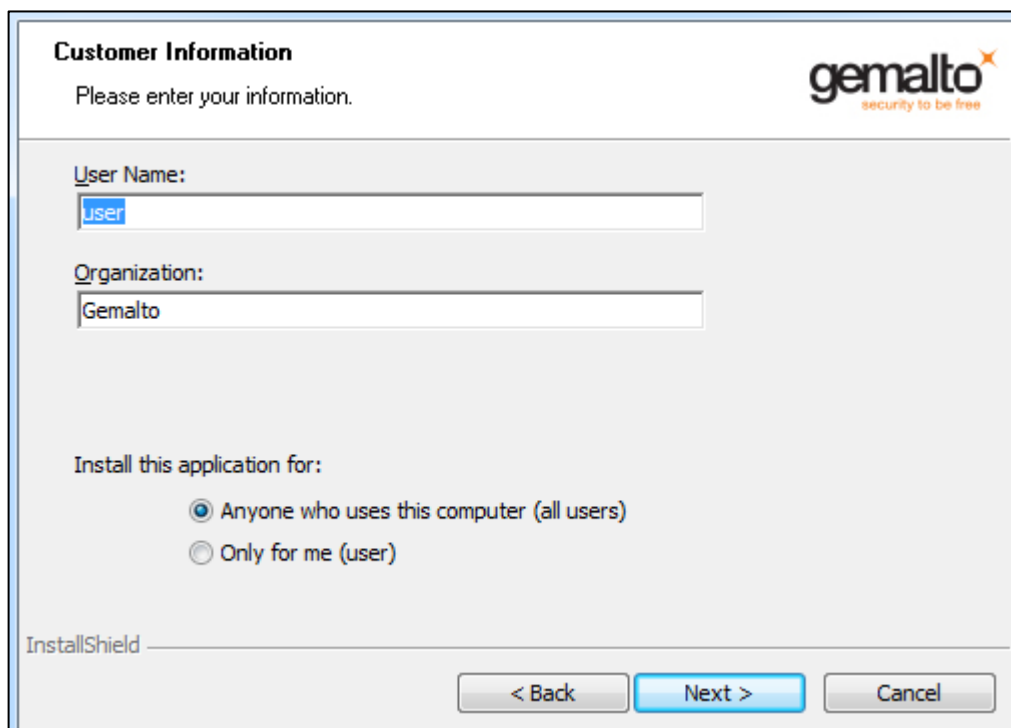
1. Execute the required installation file:
 - 32-bit: SafeNet Authentication Service Agent for Cisco AnyConnect x86.exe*
 - 64-bit: SafeNet Authentication Service Agent for Cisco AnyConnect x64.exe*
2. On the **Welcome to the InstallShield Wizard...** window, click **Next**.



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



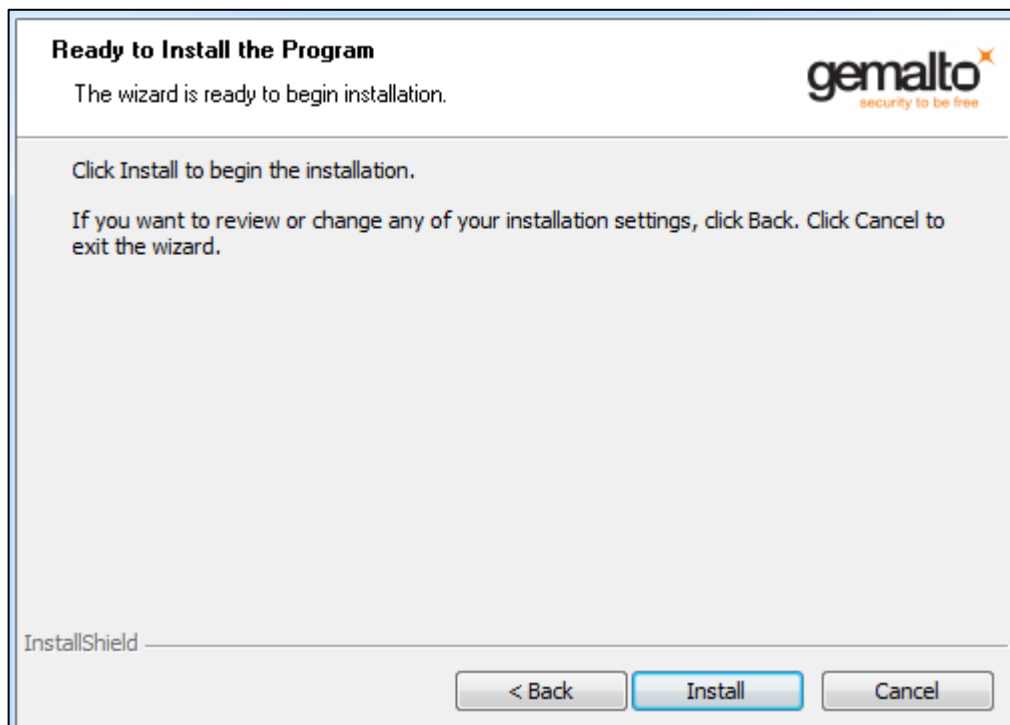
4. On the **Customer Information** window, enter the User Name, and Organization (any names can be used) and click **Next**.



5. On the **Destination Folder** window, perform one of the following steps:
- To change the installation folder, click **Change** and navigate to the required folder, and then click **Next**.
 - To accept the default installation folder as displayed, click **Next**.



6. On the **Ready to Install the Program** window, click **Install**.



7. Once the installation is completed, the **InstallShield Wizard Completed** window is displayed. Click **Finish** to exit the installation wizard.



Uninstalling SafeNet Authentication Service Agent for Cisco AnyConnect Client

To uninstall the SAS Agent for Cisco AnyConnect Client, perform the steps:

1. Navigate to **Start > Control Panel > Programs and Features**.
2. Select the SAS Agent for Cisco AnyConnect Client program.
3. Click **Uninstall**.



NOTES:

- The SAS Agent for Cisco AnyConnect Client can also be uninstalled using the InstallShield Wizard.
- After uninstall, ensure that all directories are removed. If not, remove the remaining directories manually before proceeding to reinstall the agent.

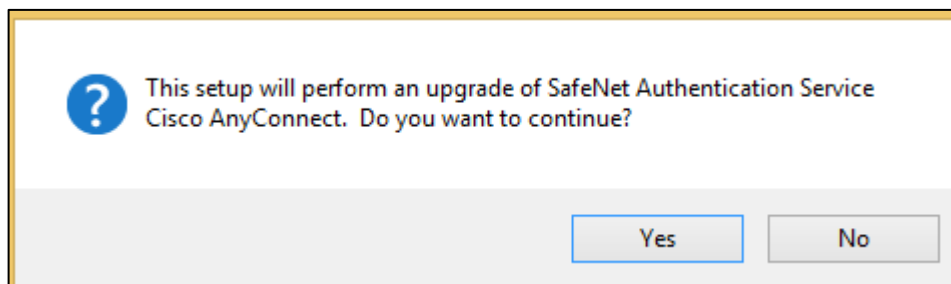
Upgrading SafeNet Authentication Service Agent for Cisco AnyConnect Client

You can upgrade to the SAS Agent for Cisco AnyConnect Client v2.2.0, if any prior version is installed.

**NOTES:**

- Previous versions of SAS Agent for Cisco AnyConnect Client directly support only MP-1 tokens. After upgrading to SAS Agent for Cisco AnyConnect Client 2.0 (or later), only MobilePASS tokens will be detected.
- Use Microsoft's recommended **Windows 10** version(s). Users may face some issues in upgrading the agent if they are using Windows 10 RTM version(s).

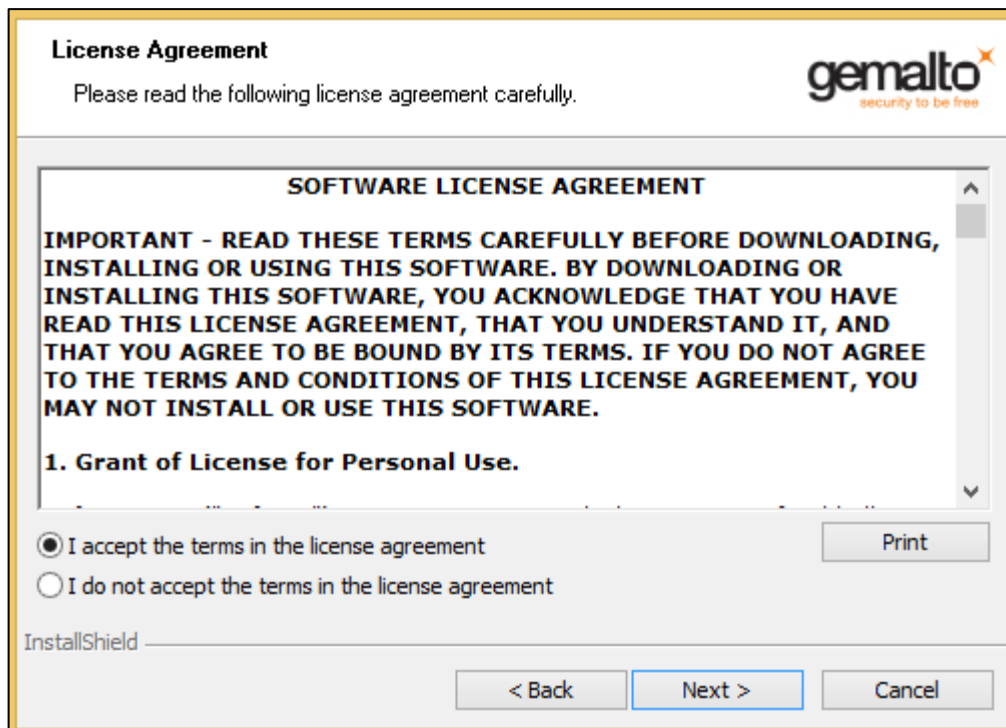
1. Run the SAS Agent for Cisco AnyConnect Client setup application. Click **Yes** when prompted.



2. On the **Welcome to the InstallShield Wizard...** window, click **Next**.



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



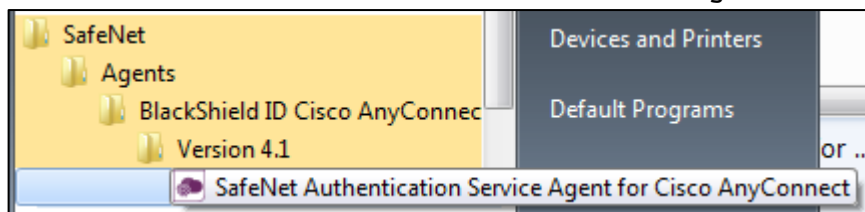
- Once the upgrade is completed, the **InstallShield Wizard Completed** window is displayed. Click **Finish** to exit the installation wizard.



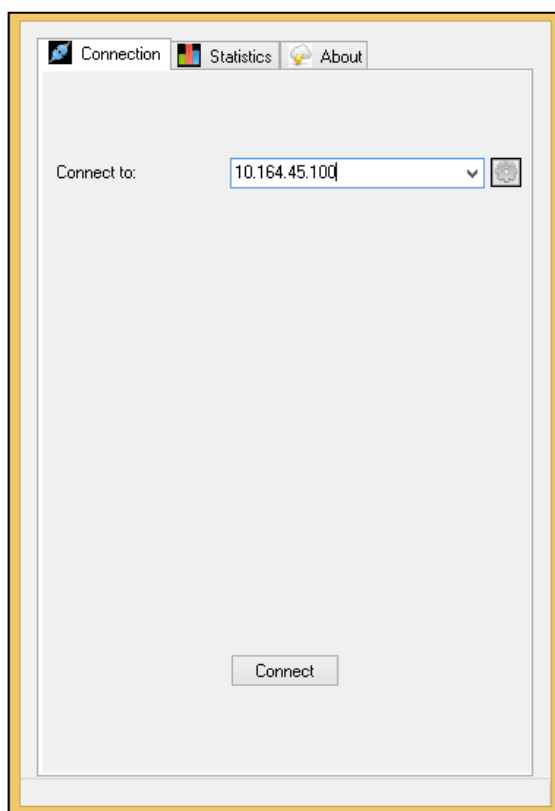
Establishing VPN Connection

1. Navigate to the following path:

Start > All Programs > SafeNet > Agents > BlackShield ID Cisco AnyConnect > <Version> > SafeNet Authentication Service Agent for Cisco AnyConnect

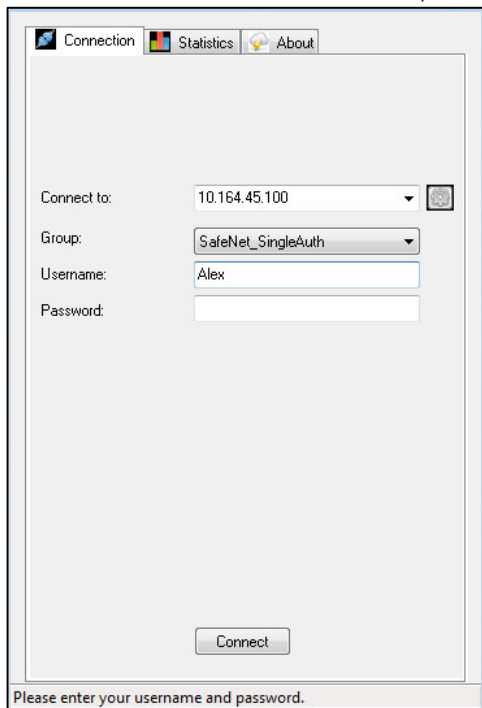


2. In **Connect to** field, enter the VPN server host name or the IP address, and click **Connect**.



3. The next window is displayed depending on one of the following scenarios:
 - a. **Scenario 1:** If no MobilePASS token is detected on the client machine, the Username and Password fields are displayed.

Enter the Username and Password, and click **Connect**.



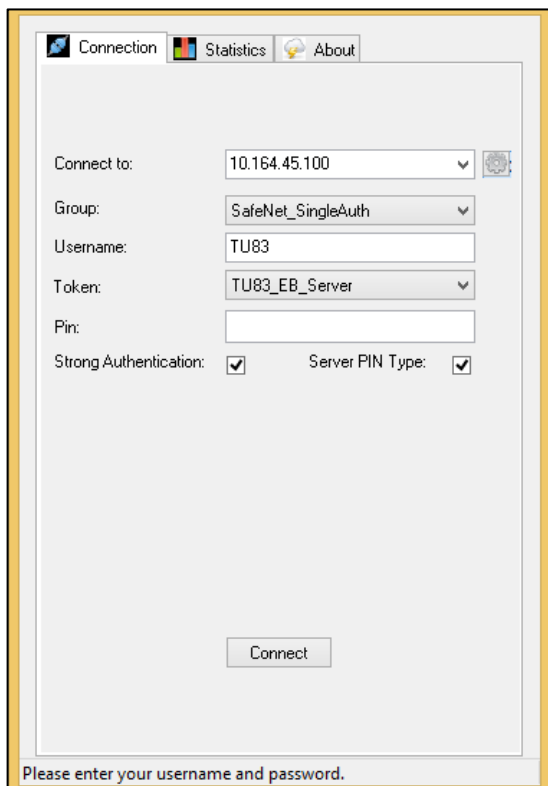
The screenshot shows a dialog box titled "Connection" with three tabs: "Connection", "Statistics", and "About". The "Connection" tab is active. It contains the following fields and controls:

- Connect to:** A dropdown menu with "10.164.45.100" selected and a small icon to its right.
- Group:** A dropdown menu with "SafeNet_SingleAuth" selected.
- Username:** A text input field containing "Alex".
- Password:** An empty text input field.
- Connect:** A button at the bottom center.

At the bottom of the dialog, there is a message: "Please enter your username and password."

- b. **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** field.

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

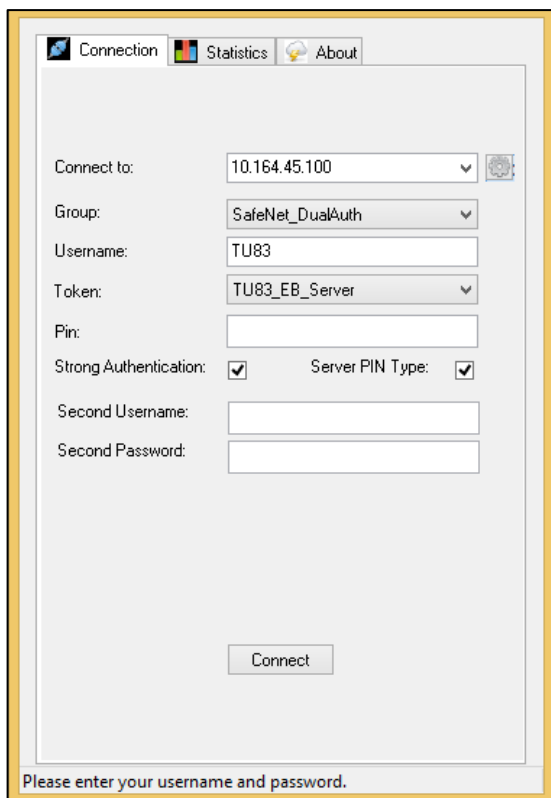


The screenshot shows the same "Connection" dialog box as above, but with additional fields and checked options:

- Connect to:** Same as above.
- Group:** Same as above.
- Username:** A text input field containing "TU83".
- Token:** A dropdown menu with "TU83_EB_Server" selected.
- Pin:** An empty text input field.
- Strong Authentication:** A checked checkbox.
- Server PIN Type:** A checked checkbox.
- Connect:** A button at the bottom center.

At the bottom of the dialog, there is a message: "Please enter your username and password."

- c. **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.
- 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.
 - For second factor authentication, enter the **Second Username** and **Second Password**.
 - Click **Connect**.



Connection Statistics About

Connect to: 10.164.45.100

Group: SafeNet_DualAuth

Username: TU83

Token: TU83_EB_Server

Pin:

Strong Authentication: Server PIN Type:

Second Username:

Second Password:

Connect

Please enter your username and password.

Configuration

Configuring Registry Keys

This section contains information on registry settings that allow administrators to modify application behaviour based on environment and security infrastructure.

- The **SoftTokenInclusion** registry key allows to specify where the MobilePASS token drop-down list will appear and which password field(s) will be used when the OTP is submitted to the server.
- On a Windows XP / Vista / 7 (32-bit) operating system, the registry key is located at the following path:
`\HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\CiscoAnyClientPlugin`
- On a Windows XP / Vista / 7 (64-bit) operating system, the registry key is located at the following path:
`\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CRYPTOCard\CiscoAnyClientPlugin`
- The **UseServerSidePIN** registry key allows 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 either be **Append** or **Prepend**.

Registry Key Example: **SoftTokenInclusion**

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 SAS Agent for 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	This option is used if dual

	factor, and MobilePASS in the second factor.	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 following table list 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 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 provide explanations of the logging messages that may appear in the Event Viewer for the IAS or 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: <ul style="list-style-type: none"> • The Username does not correspond to a user on the SAS 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: <ul style="list-style-type: none"> • The SAS Agent for IAS / NPS cannot contact the SAS server. • The Pre-Authentication Rules on the SAS server do not allow incoming requests from the SAS Agent for IAS / NPS. • The SAS Agent for IAS / NPS Keyfile does not match the Keyfile stored on the SAS server. • The Username does not correspond to a user on the SAS server.