Cisco AnyConnect

Contents

Introduction

The Cisco AnyConnect client allows authentication using the following methods from Swivel:

- SMS Text
- Mobile Phone Client
- Token
- Taskbar Utility

This document describes a custom AnyConnect Windows client with built-in support for single channel Swivel authentication, both TURing and Pinpad. For the IPSEC client see Cisco IPSEC Client Integration.

Our custom Cisco AnyConnect clients are available for versions 2.4, 3.1, 4.4 and 4.7 of AnyConnect. Note that the 4.4 client has been successfully tested with version 4.5 as well.

Cisco AnyConnect Integration

Product Integration

Product	SMS Text	SMS On Demand	Mobile Phone Client	Token	Taskbar Utility	TURing Image	Pinpad	Index number display
Standard Cisco AnyConnect 2.4	Yes	No	Yes	Yes	Yes	No	No	No
Swivel modified AnyConnect 2.4	Yes	No	Yes	Yes	Yes	Yes	No	No
Standard Cisco AnyConnect 3.1	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Standard Cisco AnyConnect 4.4/5	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Standard Cisco AnyConnect 4.7	Yes	No	Yes	Yes	Yes	Yes	Yes	No

The Cisco AnyConnect client should be downloaded from the Cisco website. The Swivel AnyConnect modifications, where available, can be downloaded below.

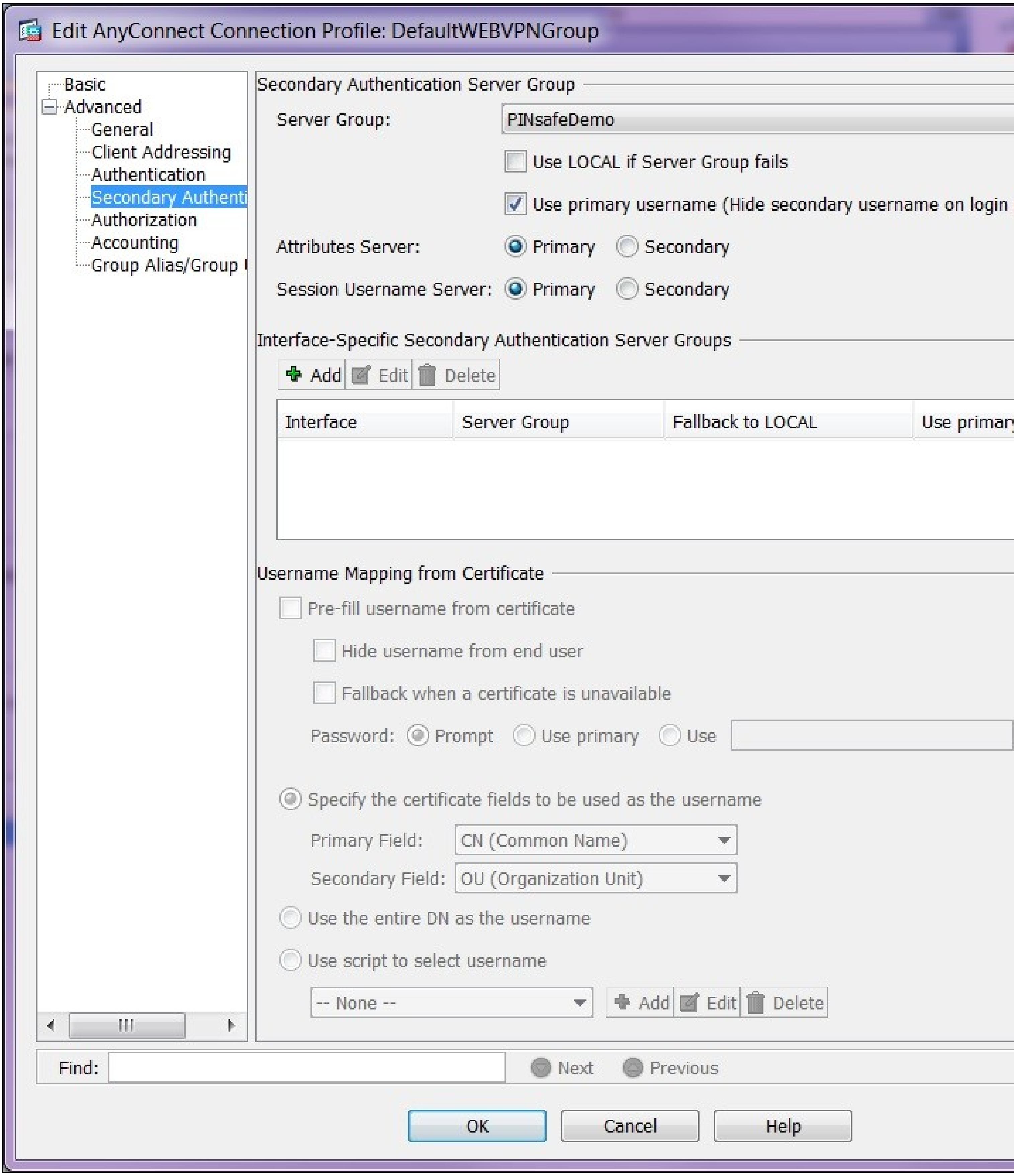
Cisco AnyConnect Client Integration

Configure the Cisco ASA

In order to use Swivel authentication, you need to follow the instructions in Cisco ASA Integration, creating a RADIUS server for Swivel authentication within the Cisco AnyConnect configuration. However, ignore the section on Login Page Customisation, as it is not relevant for the AnyConnect client.

The basic steps for AD Primary and Swivel RADIUS secondary are:

- Configure the ASA for Primary authentication server access, such as AD, and test that it works.
- From Remote Access VPN > AAA/Local Users > AAA Server Groups, create a Swivel group, and add the Swivel RADIUS servers.
- From Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles open the required Connection Profile, and under Advanced Secondary Authentication, set the Secondary Authentication Server Group to the Swivel group.



Edit AnyConnect Connection Profile: DefaultWEBVPNGroup

Secondary Authentication Server Group

Server Group: PINsafeDemo

□ Use LOCAL if Server Group fails

☑ Use primary username (Hide secondary username on login

Attributes Server: ● Primary ○ Secondary

Session Username Server: ● Primary ○ Secondary

Interface-Specific Secondary Authentication Server Groups

Interface	Server Group	Fallback to LOCAL	Use primar

Username Mapping from Certificate

□ Pre-fill username from certificate

□ Hide username from end user

□ Fallback when a certificate is unavailable

Password: ● Prompt ○ Use primary ○ Use

● Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

○ Use the entire DN as the username

○ Use script to select username

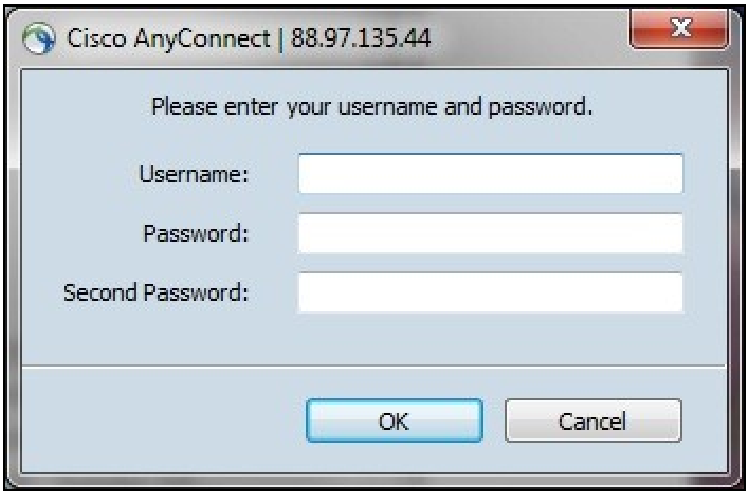
-- None --

When using a Primary authentication service such as Active Directory and a secondary authentication service such as Swivel, the AnyConnect client will display an extra password field, allowing entry of username, password and One Time Code.

Install the Cisco AnyConnect Client

Download and install the normal Cisco AnyConnect client from your Cisco VPN.

The client should connect and allow authentication using SMS, Mobile Phone Client, Token, and the Taskbar Utility. For PINpad and TURing the below modification is available for testing.



Cisco AnyConnect | 88.97.135.44

Please enter your username and password.

Username:

Password:

Second Password:

Swivel modified AnyConnect Client for TURing and PINpad

Download the client modifications

You can download the 4.7 client from here.

You can download the 4.4 client from here.

You can download the 3.1 client from here.

You can download the 2.4 client from here.

Prerequisites for the modified client

The client machine must be running a recent Microsoft Windows operating system. This client will not work on non-Windows systems. It has been tested on Windows 7 and XP, but we would expect it to work on any Windows system supported by Cisco.

The client machine must have the Microsoft.Net Framework version 3.5 or later installed. Windows 7 and later will probably have this installed by default.

Your Cisco VPN must support version 2.4, 3.1 or 4.4 of the AnyConnect client.

You must have Swivel 3.4 or later. For Pinpad support, you must either have Swivel 3.9.2 or later, or an appliance with the latest release of the Proxy application.

The client makes a direct call to request the TURing or Pinpad images, so you must have direct access to the Swivel server, or else have a proxy set up to redirect requests. The current version always adds "SCImage" to the URL for TURing images and "SCPinPad" to the Pinpad URL, so you cannot at present use our ASP, ASP.Net or PHP proxy solutions. This will be rectified before the product is released.

Installation of the Cisco AnyConnect client modifications

Locate the installation directory: by default this is **C:\Program Files\Cisco\Cisco AnyConnect VPN Client**. If you have a 64-bit operating system, the folder will probably be **C:\Program Files (x86)...**.

Take a copy of the file vpnui.exe and rename it or store it in a safe place. You will need to restore this to use the default AnyConnect client again.

Copy the files vpnui.exe, Interop.vpnapi.dll and SwivelSettings.xml from the downloaded zip file into the AnyConnect folder. Alternatively, if you want to keep both clients alongside each other, you can rename the new vpnui.exe to something else.

Run the AnyConnect client. If you get an error at this point, check that you have the right Microsoft.Net Framework library installed.

Cisco Modified AnyConnect Configuration for PINpad and TURing

The first time you run the client, you will need to configure it. Click the arrow to the right of the **Options** button and select **Preferences** from the pop-up menu.

Fill in the correct settings in the dialog box. For a Swivel Appliance, the Swivel URL should be **https://*<Swivel Server>*:8443/proxy/**. For a software only install see Software Only Installation. If you are using a proxy, or a software-only installation, use the URL appropriate for your installation.

Note the option **PINsafe is primary authentication**. This should be checked if Swivel is the only form of authentication, or is the primary authentication. It should be unchecked if you are using PINsafe as secondary authentication. This option is only relevant for Pinpad, as it determines which password field is populated by the pad.

To add new Cisco VPNs, if yours is not shown, right-click on the box labelled **Use PINsafe for the following connections**, and select **Add Server...**. Note that you can specify that the Swivel security string is not shown for certain VPNs.

Now you have entered the preferences, you should be able to click **Connect** and see the login prompt. After you enter a username, or if you have checked the option to remember the last username, immediately, you should see either a TURing image, or a Pinpad. Use these to enter the Swivel one-time code.

Assuming you have entered the correct credentials, you will be connected to the Cisco VPN, and the client will minimize to the system tray. Click on the tray icon to restore the dialog.