Click Studios

Passwordstate

SafeNet Two-Factor Configuration

Table of Contents

1 Introduction

This document will describe the process for initially configuring Passwordstate to use two-factor authentication with SafeNet's Authentication Service (SAS), either Cloud-Based, or On-Premise.

System Requirements

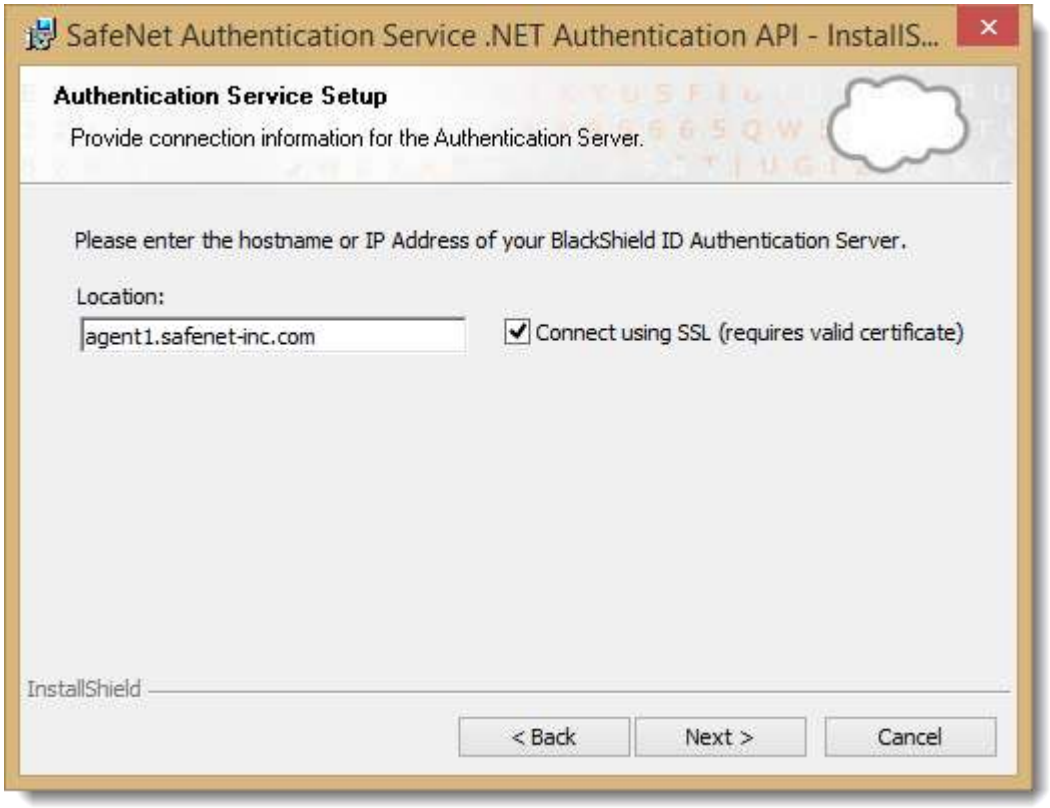
You Passwordstate web server also requires for following components to be installed:

- .NET Framework 2 (.NET 3.5 also includes the install of version 2)
- Microsoft Visual C++ 2008 Redistributable Package

2 Installing BlackShield ID .NET Authentication API Files

In order for Passwordstate to communicate with SafeNet's authentication services, we must first install the appropriate 'Blackshield ID .NET Authentication API' files, perform various configurations, and then copy a few files into the Passwordstate folder.

- Download the appropriate BlackShield API installer file, depending on your server processor architecture:
  - http://www.clickstudios.com.au/downloads/BlackShieldAPI.zip (32-bit)
  - http://www.clickstudios.com.au/downloads/BlackShieldAPIx64.zip (64-bit)
- Unzip the file and copy across the executable to your Passwordstate web server
- Run the BlackShield executable as an Administrator, and when you get to the screen below, enter the Hostname or IP Address of the appropriate BlackShield ID Authentication Server for your environment – this can be an internal server, or SafeNet's external cloud based authentication server



- Once installed, copy the files below across into the ***c:\inetpub\passwordstate\bin*** folder (these paths may be different for you). If you wish to use this authentication option with the Passwordstate Mobile client, you will also need to copy these files into the ***c:\inetpub\passwordstate\mobile\bin*** folder.
  - C:\Program Files\CRYPTOCard\BlackShield ID\API\BSIDAPI.dll
  - C:\Program Files\CRYPTOCard\BlackShield ID\API\BSIDAPI.XmlSerializers.dll
  - C:\Program Files\CRYPTOCard\BlackShield ID\API\CryptoCOM.dll

NOTE: Copying files into the Passwordstate bin folder causes any user sessions in Passwordstate to end – please only do this when you know users aren't currently using Passwordstate.

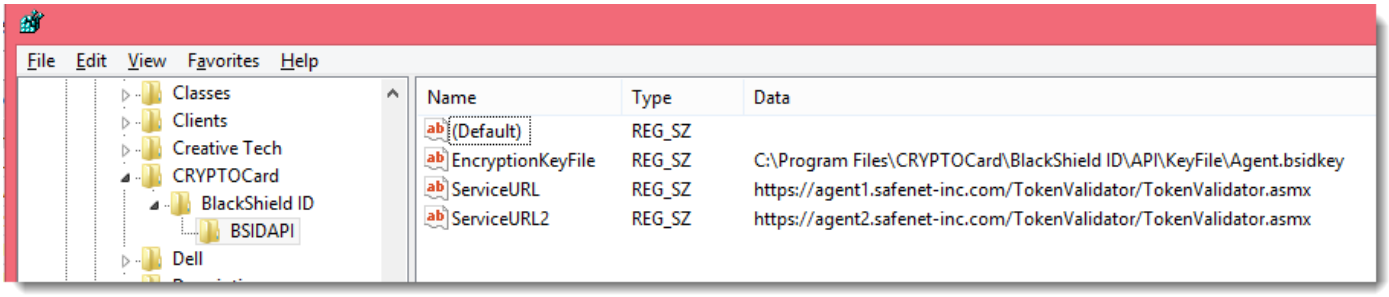
3 Configuring a Fail-Over Authentication Server

We need to add another registry key on your Passwordstate web server, so that in the event your BlackShield Primary Authentication Server is unavailable, we can authenticate against a secondary fail-over server.

To do this, open Regedt32 as admin, and add the following registry key:

- Location = HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\BlackShield ID\BSDIDAPI
- String = ServiceURL2
- Value = https://agent2.safenet-inc.com/TokenValidator/TokenValidator.asmx

The value will also be different if using internally hosted BlackShield servers. Below is a screenshot of what this would look like.

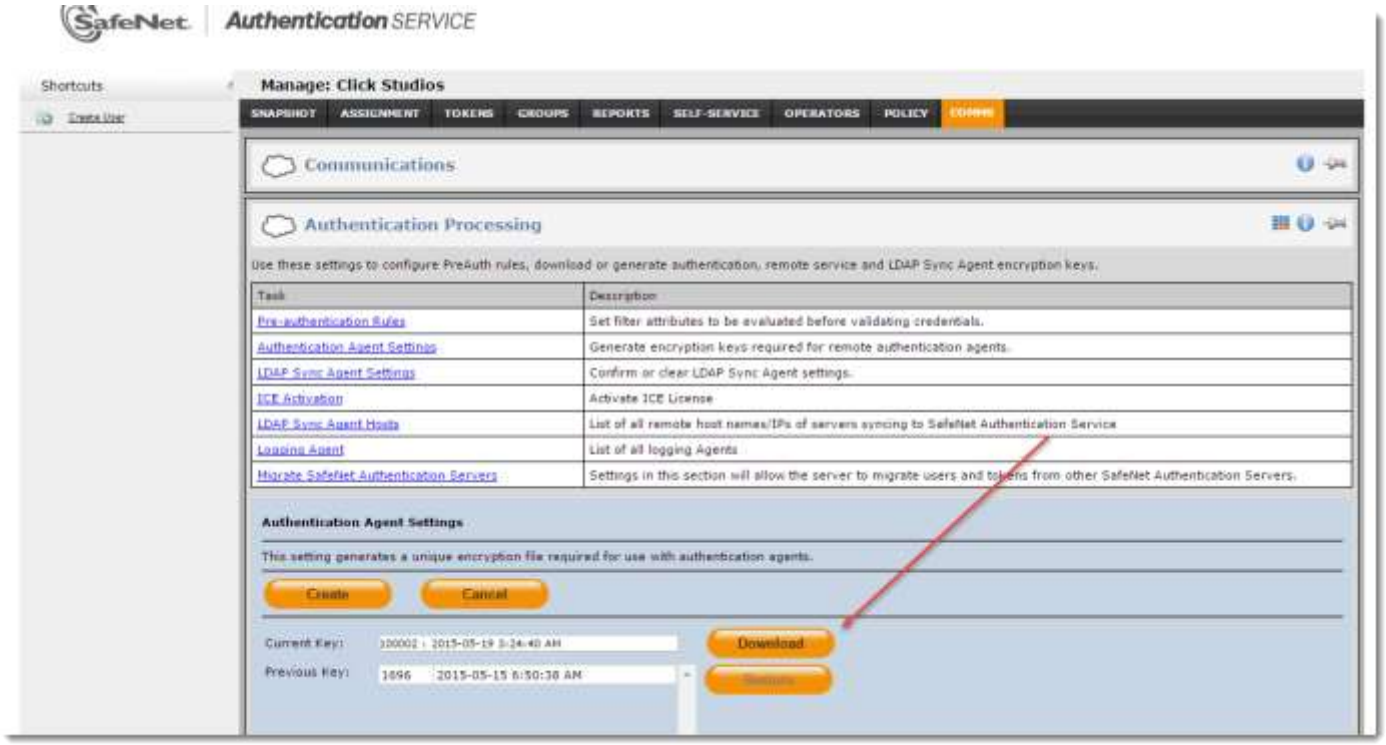


4 SafeNet Authentication Service Portal Configurations

There are two more steps required to finalize the configuration. To do these, you must log into the SafeNet Authentication Service Portal, either Cloud-Based or On-Premise, and follow the instructions below.

Download Encryption Key

- Navigate to the Comms tab, click on Authentication Processing -> Authenticate Agent Settings
- Click the Download button, as per the screenshot below, and save the file into the 'C:\Program Files\CRYPTOCard\BlackShield ID\API\KeyFile' folder on your web server – overwrite the existing file here



Create Authentication Node

This step may not be required if you are already using SafeNet Authentication Services with other "applications" in your environment – check with the System Administrator who is responsible.

- Navigate to the Comms tab, click on Auth Nodes, and then click on the Add button
- You will then see a screen similar to the one below which allows you to create an Authenticate Node appropriate for your environment. Ask your System Administrator what the appropriate settings are here, and if using SafeNet's cloud based authentication services, you will need to ensure you specify the IP Address from where the BlackShield API Calls are being made from – so generally the Public IP Address or your firewall. If you continue to get 'Failed Authentication' attempts in Passwordstate, then the Authentication Node settings could be incorrect.