

# Table of Contents

<b>1 AuthControl Desktop.....</b>	<b>1</b>
<b>2 Introduction.....</b>	<b>2</b>
<b>3 Deploy ACD using MS group policies.....</b>	<b>3</b>
<b>4 Introduction.....</b>	<b>4</b>
<b>5 Steps.....</b>	<b>5</b>
<b>6 Notes.....</b>	<b>6</b>
<b>7 Changing Settings.....</b>	<b>7</b>
<b>8 Microsoft Windows Credential Provider Integration (Legacy OS).....</b>	<b>8</b>
<b>9 Introduction.....</b>	<b>9</b>
9.1 Swivel Credential Provider FAQ.....	9
<b>10 Prerequisites.....</b>	<b>10</b>
<b>11 Baseline.....</b>	<b>11</b>
<b>12 Architecture.....</b>	<b>12</b>
12.1 Offline Authentication.....	12
<b>13 Swivel Integration Configuration.....</b>	<b>13</b>
13.1 Configure a Swivel Agent.....	13
13.2 Configure Single Channel Access.....	13
13.3 Create a Third Party Authentication.....	14
<b>14 Microsoft Windows Swivel Credential Provider Installation.....</b>	<b>16</b>
14.1 Windows Swivel Credential Provider configuration.....	17
14.2 Additional Installation Options.....	19
14.3 Test Mode.....	20
14.4 Importing Configurations.....	21
<b>15 Verifying the Installation.....</b>	<b>22</b>
<b>16 ChangePIN.....</b>	<b>25</b>
<b>17 Uninstalling the Swivel Integration.....</b>	<b>27</b>
<b>18 Troubleshooting.....</b>	<b>28</b>
18.1 Disabling the Swivel Login.....	28
18.2 Error Messages.....	28
<b>19 Release Notes.....</b>	<b>32</b>
19.1 Release of Version 4.6.....	32
19.2 Release of Version 4.5.....	32
19.3 Release of Version 4.4.....	32
<b>20 Known Issues and Limitations.....</b>	<b>33</b>
<b>21 Microsoft Windows GINA login.....</b>	<b>34</b>
<b>22 Introduction.....</b>	<b>35</b>
<b>23 Prerequisites.....</b>	<b>36</b>
<b>24 Baseline.....</b>	<b>37</b>
<b>25 Architecture.....</b>	<b>38</b>
<b>26 Swivel Configuration.....</b>	<b>39</b>
26.1 Configure a Swivel Agent.....	39
26.2 Create a Third Party Authentication.....	40
<b>27 Terminal Services GINA Integration.....</b>	<b>42</b>
27.1 Terminal Services GINA Installation.....	42
27.2 Terminal Services GINA Configuration.....	45
<b>28 ChangePIN.....</b>	<b>49</b>
28.1 User Requested ChangePIN using Change Password.....	49
28.2 ChangePIN redirect at login.....	52
<b>29 Additional Installation Options.....</b>	<b>55</b>
<b>30 Verifying the Installation.....</b>	<b>56</b>
<b>31 Uninstalling the PINsafe Integration.....</b>	<b>58</b>
<b>32 Troubleshooting.....</b>	<b>59</b>
32.1 Error Messages.....	59

# Table of Contents

<b>33 Known Issues and Limitations.....</b>	<b>61</b>
<b>34 Additional Information.....</b>	<b>62</b>
<b>35 Swivel Windows Credential Provider.....</b>	<b>63</b>
<b>36 Introduction.....</b>	<b>64</b>
36.1 Downloads.....	64
36.2 Swivel Credential Provider FAQ.....	64
<b>37 Prerequisites.....</b>	<b>65</b>
<b>38 Baseline.....</b>	<b>66</b>
<b>39 Installation.....</b>	<b>67</b>
39.1 Basic Installation.....	67
39.2 Multiple Installation.....	67
<b>40 Architecture.....</b>	<b>68</b>
40.1 Offline Authentication.....	68
<b>41 Swivel Integration Configuration.....</b>	<b>69</b>
41.1 Configure a Swivel Agent.....	69
41.2 Configure Single Channel Access.....	69
41.3 Create a Third Party Authentication.....	70
<b>42 Microsoft Windows Swivel Credential Provider Installation.....</b>	<b>72</b>
42.1 Windows Swivel Credential Provider configuration.....	73
42.2 Test Mode.....	77
42.3 Importing Configurations.....	78
<b>43 Verifying the Installation.....</b>	<b>79</b>
<b>44 ChangePIN.....</b>	<b>81</b>
<b>45 Uninstalling the Swivel Integration.....</b>	<b>83</b>
45.1 Disabling the Credential Provider.....	83
<b>46 Known Issues and Limitations.....</b>	<b>84</b>
<b>47 Windows Credential Provider.....</b>	<b>85</b>
<b>48 Introduction.....</b>	<b>86</b>
48.1 Downloads.....	86
48.2 Swivel Credential Provider FAQ.....	86
<b>49 Prerequisites.....</b>	<b>87</b>
<b>50 Baseline.....</b>	<b>88</b>
<b>51 Installation.....</b>	<b>89</b>
51.1 Basic Installation.....	89
51.2 Multiple Installation.....	89
<b>52 Release Notes.....</b>	<b>90</b>
52.1 AuthControl Desktop 5.7.....	90
<b>53 Architecture.....</b>	<b>91</b>
53.1 Offline Authentication.....	91
<b>54 Swivel Integration Configuration.....</b>	<b>92</b>
54.1 Configure a Swivel Agent.....	92
54.2 Create a Third Party Authentication.....	92
<b>55 Microsoft Windows AuthControl Credential Provider Installation.....</b>	<b>94</b>
55.1 AuthControl Credential Provider configuration.....	95
55.2 Test Mode.....	100
55.3 Importing Configurations.....	101
<b>56 Verifying the Installation.....</b>	<b>102</b>
<b>57 ChangePIN.....</b>	<b>104</b>
<b>58 Uninstalling the Swivel Integration.....</b>	<b>106</b>
58.1 Disabling the Credential Provider.....	106
58.2 Temporarily Disabling the Credential Provider Remotely.....	106
<b>59 Known Issues and Limitations.....</b>	<b>108</b>
<b>60 Windows Credential Provider with RBA.....</b>	<b>109</b>
<b>61 Introduction.....</b>	<b>110</b>

## Table of Contents

62 Prerequisites.....	111
63 Limitations.....	112
64 RBA Configuration.....	113
65 WCP Configuration.....	115
66 Authenticating.....	116
67 RBA with fingerprint.....	117

# 1 AuthControl Desktop

## 2 Introduction

AuthControl Desktop is the brand name for Swivel Secure's custom Windows Credential Provider.

The detailed article can be found under [Windows Credential Provider](#).

### **3 Deploy ACD using MS group policies**

## 4 Introduction

These are the instructions to use the windows group policies to "deploy" the AuthControl Desktop (Credential Provider).

## 5 Steps

1 - Install the Credential Provider on a single machine. Configure it as required, then use File, Export Settings from the configuration program to create a settings file named acd.xml. Alternatively, if you have a pre-configured build, there is no need for this step.

2 - Create a network share that can be accessed by all computers. Copy both the credential provider MSI and acd.xml (if required) to that folder.

3 - From the domain controller, in Server Manager, select the Tools menu, then "Group Policy Management".

4 - Select the domain node on the left-hand window. Right-click and choose "Create a GPO in this domain and link it here".

5 - Give the GPO a name, such as "AuthControl Credential Provider", and click OK.

6 - Under Group Policy Objects, find the GPO you just created, right-click on it and click Edit.

7 - Choose Computer Configuration, Policies, Software Settings, Software installation. Right-click and select New -> Package.

8 - From the file browser, enter the location of the MSI. It must be entered as a network share, i.e. \\Computer\Share\AuthControlCredentialProvider.msi. Leave deployment method as "Assigned".

9 - Choose User Configuration, Policies, Software Settings, Software installation and repeat the last 2 steps, except this time, the deployment method should be "Published".

10 - Close the editor and left-click on the GPO. Under Scope you should see the domain name in the Links section. Right-click on it and check "Enforced". Note that this will install the CP on every computer in the domain. It should be possible to restrict the policy to a single Organisational Unit, by applying the GPO link to that OU. You can only apply policies to domains or OUs, not ordinary containers. You can also restrict the policy by creating a group of computers and adding that group to Security Filtering.

9a) Choose User Configuration, Policies, Software Settings, Software installation. Right-click and select New -> Package.

9b) From the file browser, enter the location of the MSI. It must be entered as a network share, i.e. \\Computer\Share\AuthControlCredentialProvider.msi. Set deployment method to "Published".

## 6 Notes

Our understanding is that steps 7 and 8 make the software available for network installation. This step installs the software automatically if it is not yet installed, the next time each user connects to the domain.

The notes on the final step suggest how you can restrict which computers have the WCP installed.

Check the link below for more details:

<https://support.microsoft.com/en-gb/help/816102/how-to-use-group-policy-to-remotely-install-software-in-windows-server>

## 7 Changing Settings

If you want to change the settings for computers that already have AuthControl Desktop installed, for example, to enable or disable test mode, currently the only way to do this is to change the registry settings directly.

All the settings are in the following registry key:

`\\HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\AuthControl Desktop`

You will need to know the names of the settings in the registry: please contact Swivel Secure support for specific requests. We will give an example below of enabling or disabling Test Mode, for which the setting name is "TestMode".

1. Open "Group Policy Management" from a Domain Controller.
2. Right-click on the domain, or an OU if you only want to apply the policy to a subset
3. Select "Create a GPO in this domain and link it here". Give the GPO a name.
4. Right-click on the GPO and select "Edit"
5. Expand the tree for "Computer Configuration" -> "Preferences" -> "Windows Settings" -> "Registry"
6. Right-click on "Registry" and select New -> Registry Item
7. Make sure that action is "Update" and Hive is "HKEY\_LOCAL\_MACHINE"
8. Enter Key Path as "SOFTWARE\Swivel Secure\AuthControl Desktop". Make sure you type this correctly, including the correct spacing
9. Enter the Value name as "TestMode". To change a different value, enter the name as given by Swivel Secure
10. Set the value type to REG\_DWORD (this is for numeric or on/off settings - for text settings use REG\_SZ)
11. Set the value data to 1 to enable TestMode, or 0 to disable it.
12. Click OK

Note two points:

- The settings are only applied when a computer is restarted
- The settings are not applied immediately, so it is possible that the first login after restart will still use the old settings.

## **8 Microsoft Windows Credential Provider Integration (Legacy OS)**

## 9 Introduction

Microsoft Windows Credential Provider is used in the desktop operating systems Windows Vista, 7, 8 and 8.1, and in the server operating systems Windows Server 2008 and 2012, including Remote Desktop Gateway. For newer operating systems (Windows Vista and Server 2012 R2 onwards), see [Windows Credential Provider](#). For integration with the older Windows GINA used in Windows 2000, 2003 and XP see [Microsoft Windows GINA login](#).

Users can authenticate using the Swivel Credential Provider allowing 2FA (Two Factor Authentication), or strong authentication at the Windows Logon. Offline authentication is also supported for single Channel authentication, following at least one successful authentication against the Swivel server with Third Party Authentication configured.

For new features in recent releases of the Credential Provider, see [below](#).

### 9.1 Swivel Credential Provider FAQ

Q). Does the Credential provider support offline authentication? A). Offline authentication is permissible for Swivel users who have previously authenticated to the device. Offline local authentication is always single channel, even if single channel is normally disabled.

Q). Do all users have to authenticate using Swivel? A). Swivel does have the option to *Allow Unknown Users*, users known to Swivel will be prompted for authentication in this instance.

Q). Is it possible to define users who do not have Swivel authentication? A). Only by using the *Allow Unknown Users* for non Swivel user authentication.

Q). Is it possible to login without AD password, A). No the AD password is required.

## 10 Prerequisites

Swivel 3.x Server

Connectivity to Swivel server during installation (with Third Party Authentication for GINA enabled)

Microsoft Windows Vista, 7 or 8 (including 8.1); Microsoft Windows 2008 or 2012 Server (including R2).

Microsoft .Net Framework version 4.

Swivel Windows Credential Provider 64 bit (version 4.6) or

Swivel Windows Credential Provider 32 bit (version 4.6) or

Both of the above files in a single zip

Documentation only

A separate Swivel Credential Provider license is not required, but the users authenticating to Swivel must be licensed.

User with AD account and valid password.

## 11 Baseline

Swivel 3.7

Windows 7, Windows 2008 Server R2

## 12 Architecture

Swivel is installed as a Windows Credential Provider, and when a Windows login is made, AD username and password is checked against AD and the username and Swivel OTC is sent to the Swivel server using XML authentication, or locally if offline authentication is enabled.

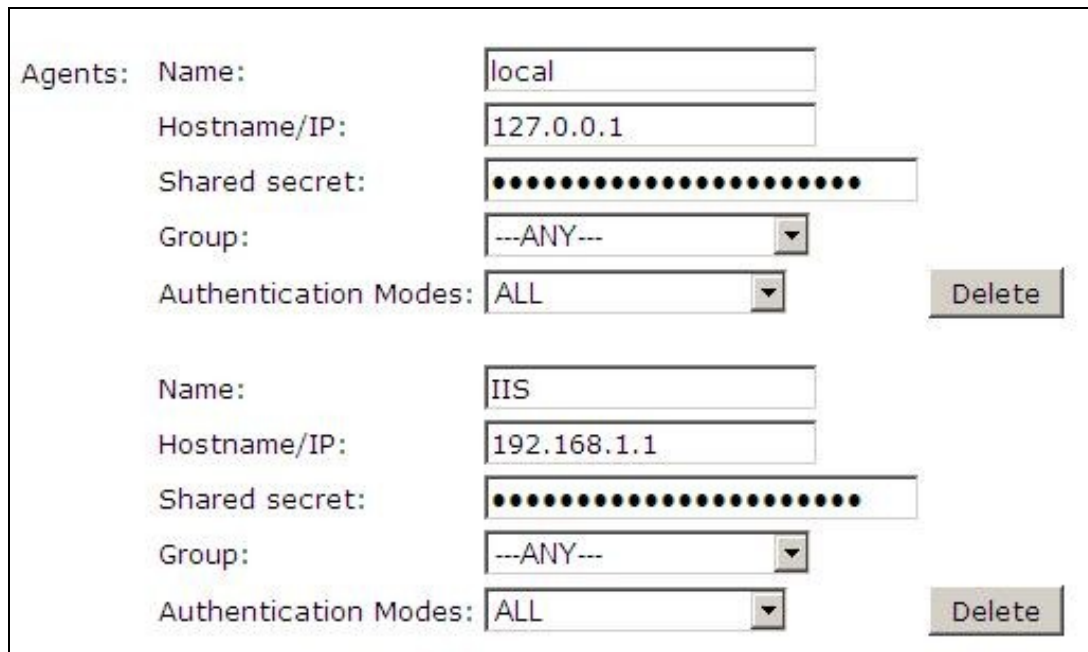
### 12.1 Offline Authentication

Swivel allows offline authentication using single channel but not dual channel authentication. For offline authentication the user attempting to authenticate must have made at least one successful authentication against the Swivel server while Offline Authentication has been enabled. Swivel caches a limited number of strings for authentication, and cycles through these so there is no limit on the number of authentications which can be made. Swivel Account lockout is disabled for Swivel offline authentication. ChangePIN will not function when the Swivel server is not contactable. Local authentication is always single channel, even if single channel is normally disabled.

## 13 Swivel Integration Configuration

### 13.1 Configure a Swivel Agent

1. On the Swivel Management Console select Server/Agent
2. Enter a name for the Agent
3. Enter the Credential Provider IP address. You can limit the Agent IP to an IP address range like: 192.168.0.0/255.255.0.0 where the mask of 255 requires an exact match and 0 allows any value, so the previous example would allow any Agent in the range 192.168, or you can use an individual IP address for the Credential Provider.
4. Enter the shared secret used above on the Credential Provider
5. Enter a group, (Note in this instance ANY is not a valid group and will cause authentication to fail)
6. Click on Apply to save changes



The screenshot displays the Swivel Management Console interface for configuring agents. It shows two entries, each with a 'Delete' button to its right. The first entry is for an agent named 'local' with a hostname/IP of '127.0.0.1'. The second entry is for an agent named 'IIS' with a hostname/IP of '192.168.1.1'. Both entries have a shared secret field filled with dots, a group dropdown set to '---ANY---', and an authentication modes dropdown set to 'ALL'.

Agents:	Name:	Hostname/IP:	Shared secret:	Group:	Authentication Modes:	Action
	local	127.0.0.1	.....	---ANY---	ALL	Delete
	IIS	192.168.1.1	.....	---ANY---	ALL	Delete

Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

### 13.2 Configure Single Channel Access

1. On the Swivel Management Console select Server/Single Channel
2. Ensure ?Allow session request by username? is set to YES

## Server>Single Channel

Please specify how single channel security strings are delivered.

Image file:	<input type="text" value="turing.xml"/>
Rotate letters:	<input type="text" value="No"/>
Allow session request by username:	<input type="text" value="Yes"/>
Only use one font per image:	<input type="text" value="Yes"/>
Jiggle characters within slot:	<input type="text" value="No"/>
Add blank trailer frame to animated images:	<input type="text" value="Yes"/>
Text Alpha Value:	<input type="text" value="80"/>
Number of complete display cycles per image:	<input type="text" value="10"/>
Inter-frame delay (1/100s):	<input type="text" value="40"/>
Image Rendering:	<input type="text" value="Static"/>
Multiple Authentications per String:	<input type="text" value="No"/>
Generate animated images:	<input type="text" value="No"/>
Random glyph order when animating:	<input type="text" value="No"/>
No. Characters Visible:	<input type="text" value="1"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

### 13.3 Create a Third Party Authentication

If offline authentication is to be allowed, a third party authentication must be created with an Identifier of WindowsGINA. (Even though the GINA is not part of Credential Provider the third party authentication module is still used and must be configured)

1. On the Swivel Management Console select Server/Third Party Authentication
2. For the Identifier Name enter: WindowsGINA (Even though the GINA is not used, this must be entered as WindowsGINA)
3. For the Class enter: com.swiveltechnologies.Swivel.server.thirdparty.WindowsGINA
4. For the License Key, leave this empty as it is not required
5. For the Group select a group of users (Note: the option Any cannot be selected)
6. Click Apply to save the settings

To allow offline authentication to be made a successful authentication must be made with the third party authentication in place.

Identifier:	<input type="text" value="WindowsGINA"/>
Class:	<input type="text" value="com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA"/>
License key:	<input type="text"/>
Group:	<input type="text" value="PINsafeUsers"/> 

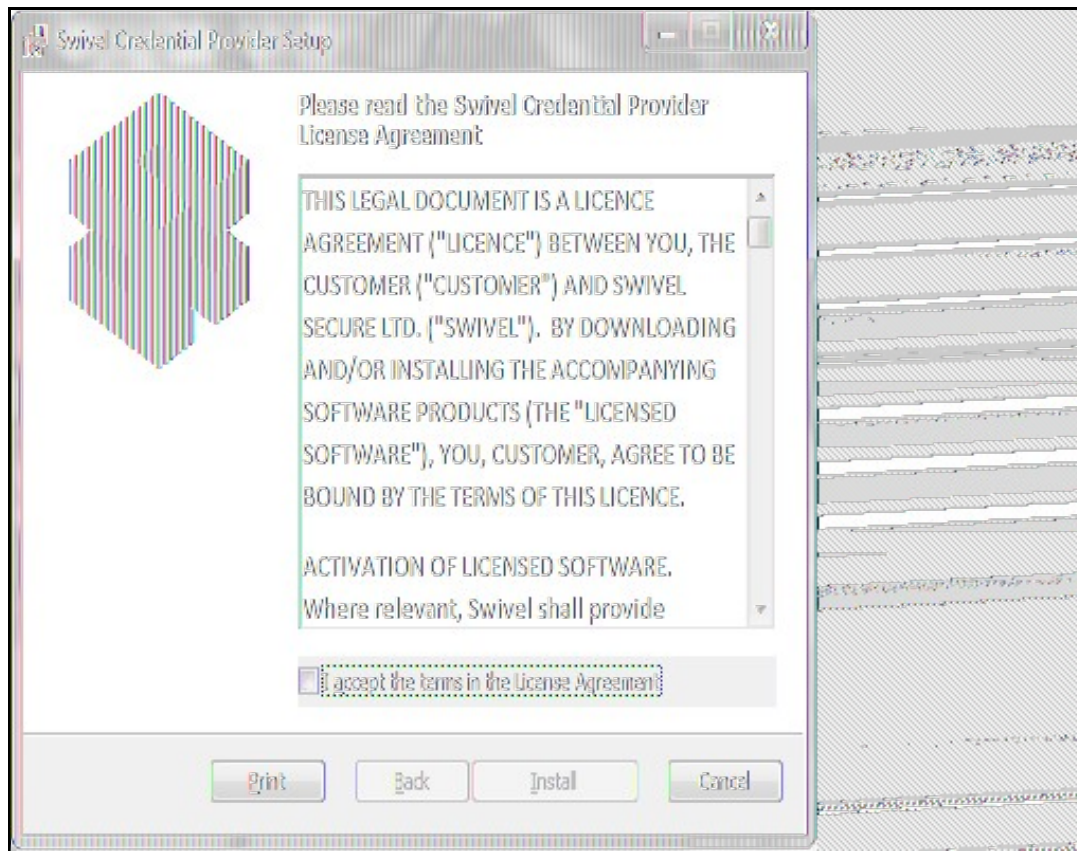
## 14 Microsoft Windows Swivel Credential Provider Installation

The Credential Provider is provided as a Microsoft Installer .msi file. You must run this as an administrator.

Ensure that the correct Swivel Windows Credential Provider is used: SwivelCredentialProvider\_x86.msi for 32-bit or SwivelCredentialProvider\_x64.msi for 64-bit.

Double-click the .msi file to run it. Alternatively, you can install from the command line, using the msixec command.

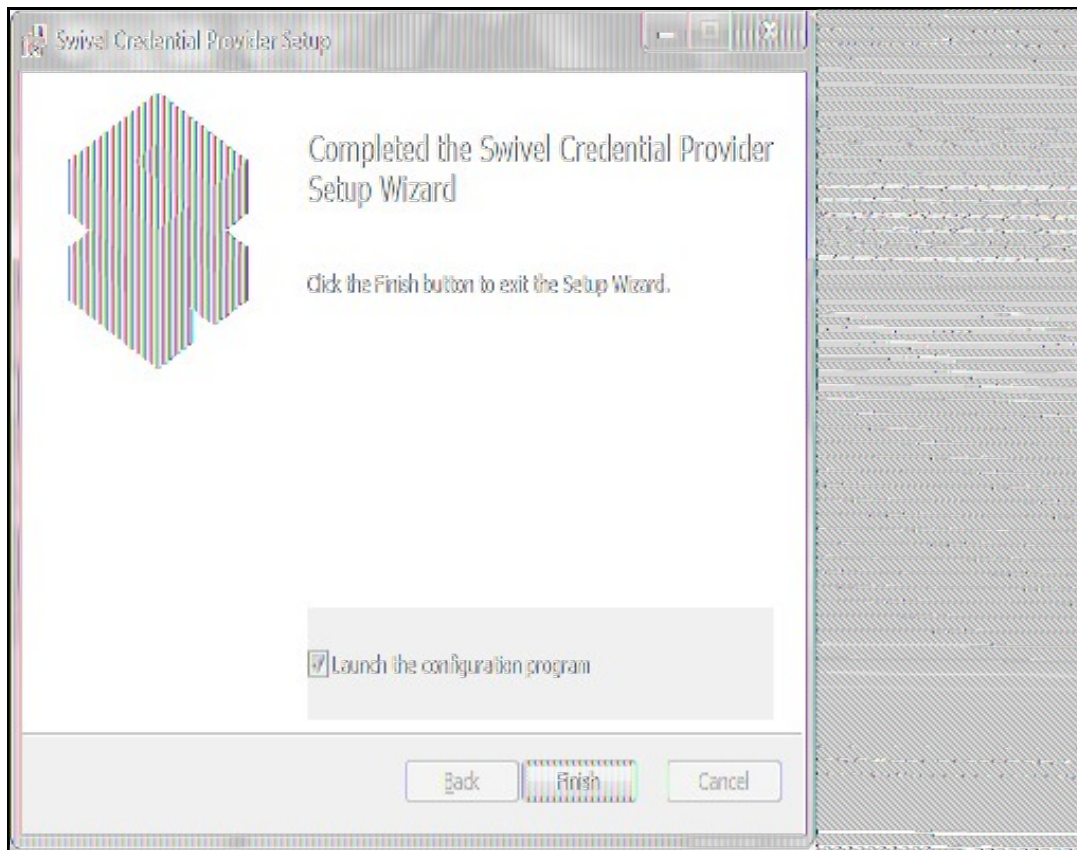
The first page is the licence agreement:



Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

The application will be installed to C:\Program Files\Swivel Secure\Swivel Credential Provider. If you have reconfigured the program files directory elsewhere, it will be installed there, but otherwise you cannot control where the application is installed.

When the install has completed, the following dialog is shown:



Ensure that the tick box is checked for *Launch the configuration program* to configure the Swivel instance then click on Finish.

## 14.1 Windows Swivel Credential Provider configuration

The following options are available:

**Server:** The Swivel virtual or hardware appliance or server IP or hostname. To add resilience for use the VIP on a swivel virtual or hardware appliance, see [VIP on PINsafe Appliances](#)

**NOTE:** it has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name in this section.

**Port:** The Swivel virtual or hardware appliance or server port

**Context:** The Swivel virtual or hardware appliance or server installation instance

**Secret:** and **Confirm Secret:** A shared secret which must be entered onto the Swivel virtual or hardware appliance or server

**Use SSL** The Swivel server or virtual or hardware appliance uses SSL communications

**Accept self signed SSL certificates** Check this box if Use SSL is enabled, and you do not have a commercial certificate on your Swivel server (or a certificate signed by an authority that the client machine trusts).

**Authentication Mode, Always** Swivel authentication is required for remote and local logins

**Authentication Mode, Remote Only** Swivel authentication is required for remote logins only

**Authentication Mode, Never** Swivel authentication is not used

**Show TURING images** Show [TURING](#) images if requested

**Show Request String** Show the Request string image to allow the user to obtain a new security string by dual channel

**Test Mode** With test mode the user can switch user to a standard authentication, see below

**Ignore Domain** Swivel will remove any domain prefix (domain\username) or suffix (username@domain) before matching username. This does not affect Windows authentication usernames.

**Allow Unknown Users Online** If the username is not recognized by Swivel, the user can authenticate using Windows credentials only. Any Swivel OTC entered will be ignored. If the user is known then they must authenticate using Swivel authentication.

**Allow Unknown Users Offline** If offline authentication is used, users that do not have credentials cached locally can authenticate using Windows credentials only. Any OTC entered will be ignored. If the user has previously authenticated in online mode, then they must enter the correct one-time code.

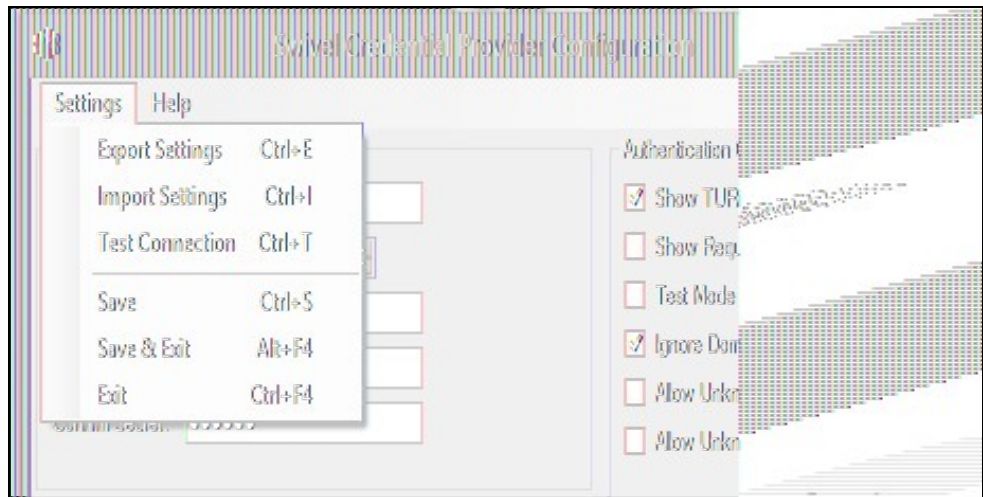
**If Swivel unavailable, Fail authentication** If the Swivel server cannot be contacted then authentication will fail

**If Swivel unavailable, Use standard authentication** If the Swivel server is unavailable use standard authentication, the OTC field is displayed but ignored.

**If Swivel unavailable, Use offline authentication** If the Swivel server cannot be contacted a locally generated Turing image can be used for authentication. If this option is enabled, users will be able to force offline mode using a checkbox on the login dialog.

**Always use local auth** A local Turing image is always used and the Swivel server is not contacted. All users must previously have authenticated using online authentication (unless the option "Allow unknown users offline" is enabled).

The remaining options are available from the Settings menu:



**Export Settings** Export settings as an XML file. These can be used to import settings elsewhere.

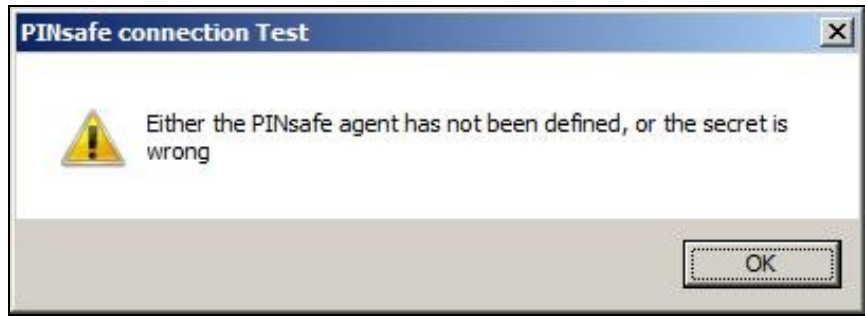
**Import Settings** Import settings from an XML file exported elsewhere.

**Test Connection** Tests link to Swivel server:

A correct configuration should produce a dialogue box with **Swivel Connection settings are correct**.



Incorrect settings will produce a dialogue box with **Either the Swivel agent has not been defined, or the secret is wrong**



**Save** Save the current settings.

**Save and Exit** Save the current settings and close the program.

**Exit** Close the program without saving the settings. You will be prompted to confirm if any settings have been changed.

## 14.2 Additional Installation Options

### 14.2.1 Manually configuring the Swivel Login

**NOTE:** It is recommended to use the Swivel Login Configuration Tool where possible.

If it is not possible to use the configuration utility the Swivel Login settings may be edited manually in the registry. The following values found within the "HKEY\_LOCAL\_MACHINE\SOFTWARE\Swivel Secure\Swivel Credential Provider" key are used by the Login:

**PINsafeServer** - The name or IP of the Swivel server

**PINsafePort** - The Swivel server port

**PINsafeContext** - The Swivel server context

**PINsafeSecret** - The Swivel agent secret

**PINsafeProtocol** - 1 for https, 0 for http

**PINsafeAllowSelfCert** - 1 to allow SSL requests to a Swivel server with certificate errors, 0 not to

**PINsafeLoginSelect** - determines when Swivel authentication is required: always, remote or disabled.

**PINsafeShowTURING** - 1 to show the TURING request link, 0 not to

**PINsafeRequestString** - 1 to show the request string link, 0 not to

**PINsafeAllowDefaultLogin** - 1 to allow default login if Swivel unavailable, 0 not to

**PINsafeUseLocalAuth** - When to use local TURING authentication: always, fallback or never.

**PINsafeDisableFilter** - 1 to enable test mode, 0 to hide the standard authentication option

**PINsafeAllowUnknownUsers** - 1 to allow unknown users in online mode

**PINsafeAllowUnknownOffline** - 1 to allow unknown users in offline mode

**PINsafeIgnoreDomain** - 1 to ignore the domain prefix when checking Swivel users

The following values may be seen in this registry key also, but should not be changed:

**PINsafeBackgroundsFolder**

**PINsafeFontsFolder**

**PINsafeResourceDLL**

**PINsafeHelpUrl**

**Directory**

**Uninstaller**

**Version**

## 14.3 Test Mode

In Test Mode the Windows Credential Provider has an additional login that can be used as a standard user login. In test mode the last successful login will be selected for login.



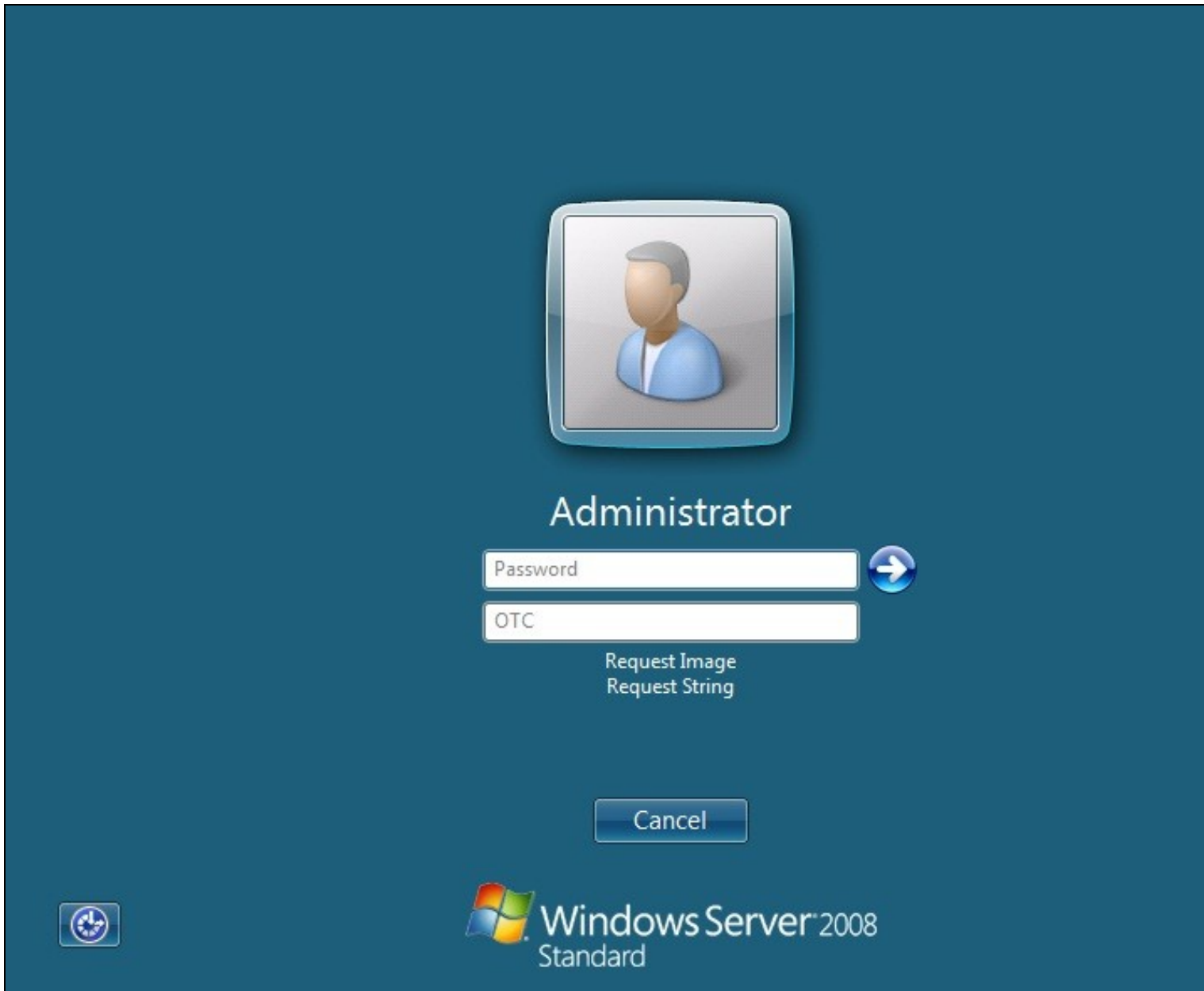
The Swivel credentials will always be on the left, the standard credentials on the right.

## 14.4 Importing Configurations

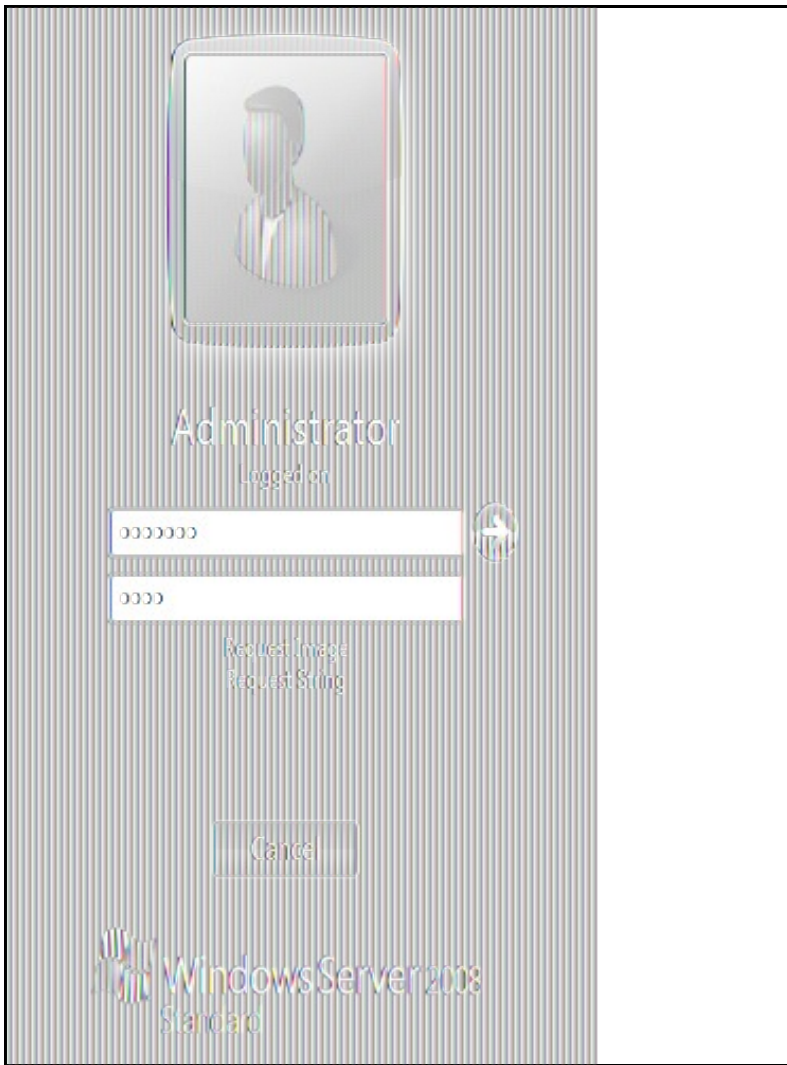
You can import credentials exported from other installations using the Import Settings menu item. Alternatively, if you need to install the Credential Provider on a large number of machines, you can modify the .msi file and replace the blank LoginSettings.xml file included with your own custom version. If you do not have the ability to modify MSI files, you can email your settings to [support@swivelsecure.com](mailto:support@swivelsecure.com) and request a custom build.

## 15 Verifying the Installation

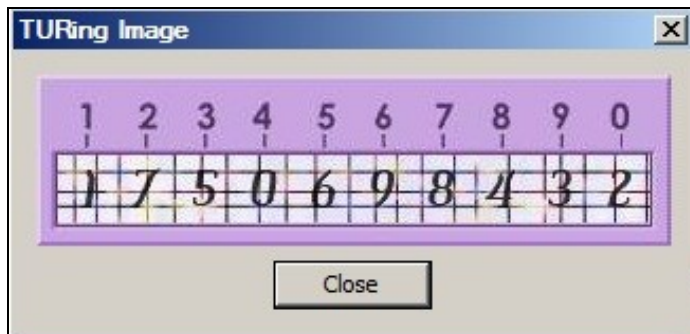
At the windows login a password and OTC login field should be available with Request Image and Request String options available.



If a Dual Channel login is made then the user should be able to enter their OTC. Note the Get Image should not be pressed, otherwise the log will be expecting a Single Channel login for the length of the session timeout (default 2 minutes).



Selecting the Request Image button should generate a Single channel Image for authentication. The Swivel log should show a session request message: *Session started for user: username.*



Administrator



Request Image  
Request String

Cancel



Windows Server<sup>®</sup> 2008  
Standard

A successful login should appear in the Swivel log: *Login successful for user: username*

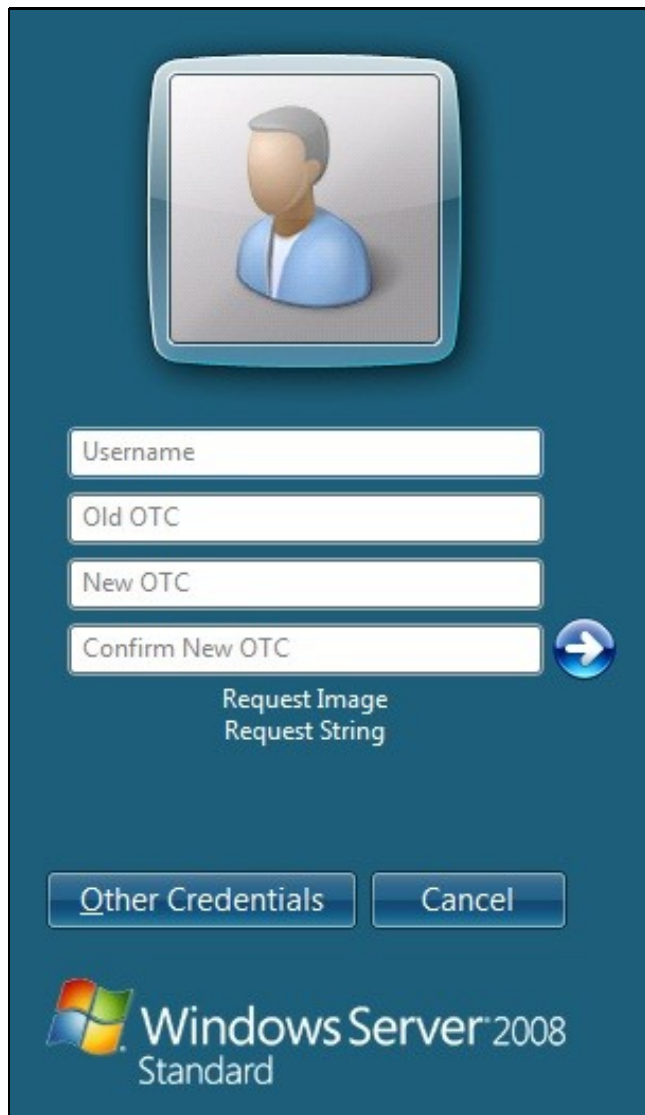
A failed login should not allow a login, and the following message should be displayed in the Swivel log: *Login failed for user: username*

## 16 ChangePIN

A user is usually able to change the password by using the Ctrl-Alt-Del keys (CTL-Alt-End for remote sessions). With the Windows Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the Other Credentials. This will not function for Offline authentication.

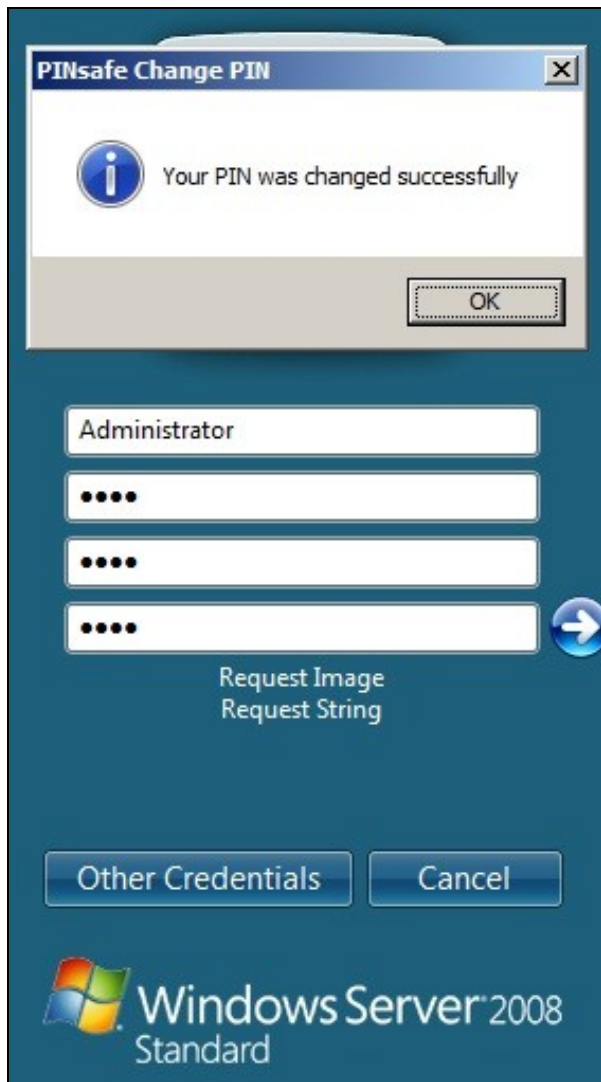
With Swivel authentication a user never changes enters PIN and this is true for ChangePIN. A user enters their current OTC, and then enters an OTC for what they wish their new PIN to be. PIN enforcement may be in place to the Swivel server to prevent the choosing of poor PIN numbers.

A user may use a single channel image or a dual channel security string to change their PIN.



The screenshot shows the 'ChangePIN' dialog box in Windows Server 2008 Standard. At the top is a user profile icon. Below it are four text input fields: 'Username', 'Old OTC', 'New OTC', and 'Confirm New OTC'. To the right of the 'Confirm New OTC' field is a blue circular button with a white right-pointing arrow. Below the input fields are two links: 'Request Image' and 'Request String'. At the bottom are two buttons: 'Other Credentials' and 'Cancel'. The Windows Server 2008 Standard logo is in the bottom left corner.

A successful Change PIN will show the message **Your PIN was changed successfully**



The Swivel server will also display in the logs a changePIN message **Change PIN successful for user: username**

## 17 Uninstalling the Swivel Integration

Use the Uninstall option from the Program menu, right click on the Windows Credentials provider and click on Uninstall. Note that uninstalling and reinstalling the Credential Provider will remove the settings, so if you need to reinstall at any point, make sure you have an exported settings file saved.

## 18 Troubleshooting

Test Mode enables you to login using the Standard Windows authentication and not Swivel authentication. If you disable Test Mode the additional logon users disappear and the machine will then be purely using Swivel.

If there is a problem then use Windows Safe Mode to login and enable Test Mode again. Safe Mode uses Standard Windows authentication.

### Pressing Ctrl+Alt+Del reverts user back to login screen

A normal login may be attempted after a short period. This can occur as the Windows login screen may appear before a network connection has been made during boot. To prevent the login screen from not being accessible, enable the option in group policy to Wait until network is ready before user logon.

### User must select the back button and select Other User to logon

This occurs when the system is running in Test mode. Disable the Test mode to allow normal login.

### Change Pin is displayed instead of the logon screen

This has been seen on Dell laptops that have the *Dell Control Point Security Manager* installed. Remove this prior to the Windows Swivel Credential Provider installation.

### FLUSHING\_IMAGE\_CACHE, ClientAbortException: java.net.SocketException: Connection reset

This error message can be seen in the Swivel log when a Windows login is attempting to use an animated gif. Turn off animated gifs and switch to 'Static', on Swivel - This is set under Server > Single Channel > Image Rendering.

### Double User Entry at login, enforced test mode when test mode is disabled

Some fingerprint scanning software may cause this issue, this has been seen on an IBM Thinkpad. Check in the registry under the following

\\HKEY\_LOCAL\_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Authentication\\Credential Provider Filters

look for keys which have values of: Fingerprint Logon Credential Provider Filter

and

\\HKEY\_LOCAL\_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Authentication\\Credential Providers

look for keys which have values of: Fingerprint Logon Credential Provider

To test if these are the cause, on a test system, either remove the fingerprint software (disabling may still leave the registry keys) or backup the keys by exporting them, then remove them.

## 18.1 Disabling the Swivel Login

If the Swivel Login fails to load correctly it can be disabled using the following process:

Using the F8 boot menu start Windows in safe mode

Either run the Swivel Login Configuration and edit the settings or

Using regedit.exe remove the "HKEY\_LOCAL\_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\WinLogon\\ginadll" registry value

Reboot Windows

Following this process the standard Windows Login should be restored allowing access.

## 18.2 Error Messages

### Unable to contact PINsafe server

Version 4.x only supports TLSv1 which means if you are running a version 3 Appliance, you must enable TLSv1 under Tomcat > SSL Protocols > Enable TLS1.0.



**Wrong Parameter or Parameter is incorrect**

This message is displayed at the Windows login and can have several causes, check the Swivel logs for errors:

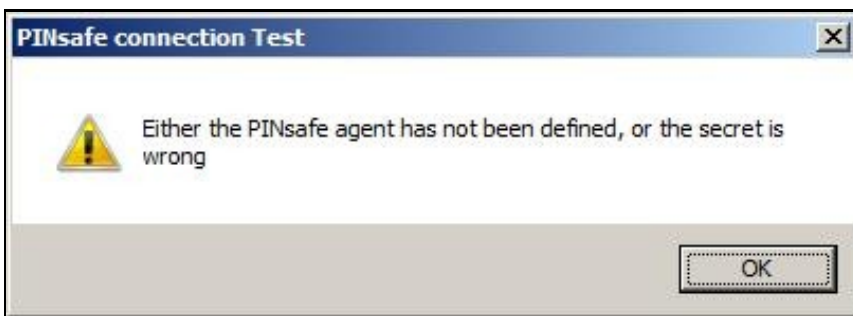
- The user must exist in AD and Swivel
- When an incorrect OTC is entered, when using local authentication. Unfortunately, local authentication will not work with the "Connect To" dialog. However, you should still get the remote desktop login displayed, and will be able to authenticate to this.
- The user account is locked in Swivel
- The Swivel Sever Agent has not been configured correctly

**Please enter a one-time code first**



A One Time Code was not entered in the OTC field during login.

**Either the Swivel agent has not been defined, or the shared secret is wrong**



**AgentXML request failed, error: The agent is not authorised to access the server.**

The credential Provider is not permitted to connect to the Swivel server. Add an Agent for communication.

**The user name or password is incorrect.**



**Check Password with Repository:** If this setting is enabled against the Agent, then you should disable it to prevent it attempting to check for a password against the repository. This is a potential cause when receiving "The user name or password is incorrect".

**AgentXML request failed, error: No suitable authentication method for the user "Administrator" was found. The user may be missing from the user repository or a synchronisation has not yet occurred.**

The user Administrator is not defined as a Swivel user

**Session start failed for user: x, error: No Data for user was found. or error: No data for the user was found**

The requested user does not exist in the database. If the user does exist in the repository (e.g. Active Directory) then Swivel needs to sync with that repository.

**Dual channel message request failed, error: On-demand dual channel delivery is disabled.**

A dual channel message request was made but the On-demand delivery is not enabled. If it should be enabled, on the Swivel Administration console select Server/Dual Channel, then set On-demand delivery to Yes.

**AgentXML request contained third party data for a third party class that does not exist. Third Party Class ID: WindowsGINA.**

and

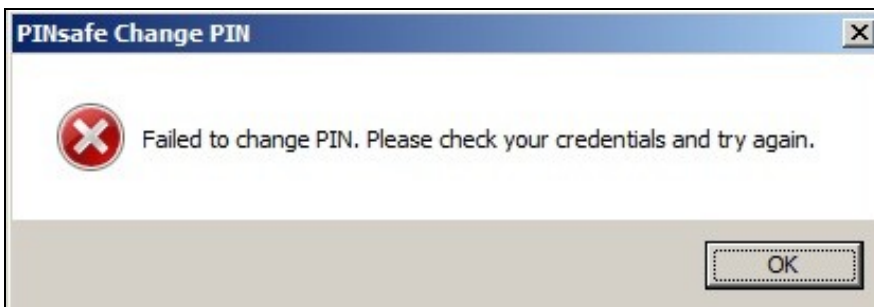
**error: The third party class could not be found.**

The Third Party Authentication class does not exist or has been created incorrectly. Create the class, see [Create a Third Party Authentication](#)

**The third party class could not be found**

This error can also be created when the Swivel Administration console Server/Agents, Group is set to Any. A group should be specified.

**Failed to change PIN. Please check your credentials and try again.**



The user has failed to change the PIN number. This could occur if the Swivel server cannot be contacted.

**Unhandled exception has occurred in your application. If you click Continue the application will ignore this error and attempt to continue. If you click Quit, the application will close immediately.**

**The remote Server returned an error: (502) Bad Gateway.**



This error has been seen when a Test Connection is made from the Credential Provider and can be caused by being unable to connect to the Swivel server. Check for network settings such as proxy settings on the local server, and if an SSL connection is required.

## 19 Release Notes

### 19.1 Release of Version 4.6

4.6.2.1, released 27th June 2016.

The main change in version 4.6 is that there is better support for offline authentication: it has been observed in previous versions that the strings ran out after a number of offline authentications. This has now been resolved.

There is a known issue with version 4.6, in that it requires [Microsoft Update KB2999226](#) to have been applied. This should be applied automatically by Windows Update, but if you have a problem installing or running the program, check that this update has been applied.

### 19.2 Release of Version 4.5

4.5.4.1, released 4th February 2015.

Version 4.5 includes the following fixes and enhancements over previous versions:

- Swivel authentication is optionally applied to the Unlock screen as well as the login screen
- Swivel authentication may be disabled (and by default is disabled) when connecting to remote computers
- The image window resizes dynamically depending on the type of image. The scale option is on the Settings drop-down menu.

### 19.3 Release of Version 4.4

Version 4.4 includes the following fixes and enhancements over the previous releases:

- It is fully-compatible with Windows 8 and Windows 2012 Server.
- It switches to single-channel mode if local authentication is enabled and the Swivel server is not available.
- Unlike the previous beta, version 4.3, this version is compatible with ALL Windows Operating Systems from Windows Vista onwards.
- If the user's password has expired, they are correctly redirected to the change password page.
- A problem which occasionally caused crashes when entering the username has now been resolved.
- You can now import settings exported from other installations.
- The installer is now a standard Windows MSI file. This makes it possible to customise the installation to contain your company's settings file, if you have the tools to modify MSI files. Alternatively, you can send your exported settings to [support@swivelsecure.com](mailto:support@swivelsecure.com), who can create a custom installer for your organisation.

## 20 Known Issues and Limitations

This version of the Swivel Credential Provider is not compatible with the Swivel version 3 appliance. An update will be available shortly.

The Swivel Windows Credential Provider does not support the use of

- Pinpad
- Animated gifs

for Single Channel authentication.

It has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name for the Swivel server.

Local authentication only works in single channel mode: the dual channel strings are not available offline. To use offline authentication, TURING image display must be enabled, even if normal authentication is dual channel.

If a Swivel server has been configured with a Single Channel login configuration that is not viewable, the following options are available to recover access:

- Login using dual channel
- Login using an image generated elsewhere such as on the Swivel Administration console or Taskbar on another server
- Alter the settings on the Swivel server to serve a permitted image
- Login offline if permitted
- Login to safe mode as described elsewhere

In Windows 8 and Windows Server 2012, the Credential Provider appears as a single key icon, which you must select before logging on. In some cases, where Windows should show the last used credential, you will need to click the back arrow and then select the Credential Provider. A similar problem occurs with the Unlock screen. An updated version, specific to Windows 8 and Windows Server 2012, will be released in due course.

By default, the credential provider assumes that administrator is the local administrator, rather than the domain administrator, so you have to explicitly state the domain name to logon as domain administrator. This is a feature of the default credential provider as well.

In the Swivel administration console, the Windows GINA menu item is present, but there are no configurable options, so is not selectable.

## 21 Microsoft Windows GINA login

## 22 Introduction

Windows GINA (graphical identification and authentication) is the login for Windows 2000 Server, 2003 Server and XP. Also available is the [Windows GINA login User Guide](#).

The Winlogon GINA has been replaced in Vista, 2008 Server, Windows 7 and Windows 8, by the Windows Credential Provider, See [Microsoft Windows Credential Provider Integration](#)

The PINsafe GINA supports the use of Dual Channel (in advance, not on-demand) and Single Channel authentication for Terminal Services using Windows 2000 and 2003 server. It does not support an offline authentication mode, whereas the Windows Credential provider does, thus the PINsafe GINA should only be used for networked machines or for Terminal Services.

This version of the PINsafe GINA supersedes an earlier version which would overwrite the AD password. The current version of the PINsafe GINA does not overwrite the AD password.

## 23 Prerequisites

PINsafe 3.x

Recommended platform is Windows 2003 with Microsoft.Net Framework 2 and Terminal Services

A separate PINsafe GINA license is not required, but the users authenticating to PINsafe must be licensed.

Microsoft Visual C++ 2010 SP1 redistributable. For the 32-bit version of the GINA, [the x86 redistributable](#) is required. For the 64-bit version, **both** the x86 redistributable **and** [the x64 redistributable](#) are required. These must be installed before the GINA, as they are required by the installer.

[PINsafe GINA 32 bit software](#)

[PINsafe GINA 64 bit software](#)

NOTE: the latest version is version 3.6.1. This adds support for dual-channel message on-demand and allowing unknown users to authenticate without Swivel credentials.

## 24 Baseline

## 25 Architecture

The 64-bit GINA is the same as the (32-bit) Terminal Services GINA, except built for 64-bit operating systems.

## 26 Swivel Configuration

### 26.1 Configure a Swivel Agent

1. On the Swivel Management Console select Server/Agent
2. Enter a name for the Agent
3. Enter the GINA IP address. You can limit the Agent IP to an IP address range like: 192.168.0.0/255.255.0.0 where the mask of 255 requires an exact match and 0 allows any value, so the previous example would allow any Agent in the range 192.168, or you can use an individual IP address for the Credential Provider.
4. Enter the shared secret used above on the GINA
5. Enter a group, (Note in this instance ANY is not a valid group and will cause authentication to fail)
6. Click on Apply to save changes

Agents:

Name:	<input type="text" value="local"/>
Hostname/IP:	<input type="text" value="127.0.0.1"/>
Shared secret:	<input type="password" value="....."/>
Group:	<input type="text" value="---ANY---"/>
Authentication Modes:	<input type="text" value="ALL"/>
	<input type="button" value="Delete"/>

Name:	<input type="text" value="IIS"/>
Hostname/IP:	<input type="text" value="192.168.1.1"/>
Shared secret:	<input type="password" value="....."/>
Group:	<input type="text" value="---ANY---"/>
Authentication Modes:	<input type="text" value="ALL"/>
	<input type="button" value="Delete"/>

#### Configure Single Channel Access

1. On the PINsafe Management Console select Server/Single Channel
2. Ensure ?Allow session request by username? is set to YES

## Server>Single Channel

Please specify how single channel security strings are delivered.

Image file:	<input type="text" value="turing.xml"/>
Rotate letters:	<input type="text" value="No"/>
Allow session request by username:	<input type="text" value="Yes"/>
Only use one font per image:	<input type="text" value="Yes"/>
Jiggle characters within slot:	<input type="text" value="No"/>
Add blank trailer frame to animated images:	<input type="text" value="Yes"/>
Text Alpha Value:	<input type="text" value="80"/>
Number of complete display cycles per image:	<input type="text" value="10"/>
Inter-frame delay (1/100s):	<input type="text" value="40"/>
Image Rendering:	<input type="text" value="Static"/>
Multiple Authentications per String:	<input type="text" value="No"/>
Generate animated images:	<input type="text" value="No"/>
Random glyph order when animating:	<input type="text" value="No"/>
No. Characters Visible:	<input type="text" value="1"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

## 26.2 Create a Third Party Authentication

A third party authentication must be created with an Identifier of WindowsGINA.

1. On the PINsafe Management Console select Server/Third Party Authentication
2. For the Identifier Name enter: WindowsGINA
3. For the Class enter: com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA
4. For the License Key, leave this empty as it is not required
5. For the Group select a group of users
6. Click Apply to save the settings

Identifier:	<input type="text" value="WindowsGINA"/>
Class:	<input type="text" value="com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA"/>
License key:	<input type="text"/>
Group:	<input type="text" value="PINsafeUsers"/> ▼

Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

## 27 Terminal Services GINA Integration

The PINsafe GINA Configuration utility provides a convenient means of configuring the installed PINsafe GINA.

Microsoft.Net 2 is only required for the configuration application. The GINA will work without .Net 2, but you will have to configure it manually. If your system does not meet the requirements, when you click "Next", you will see a dialog showing what components are missing. You can still install, but with the provisos mentioned above.

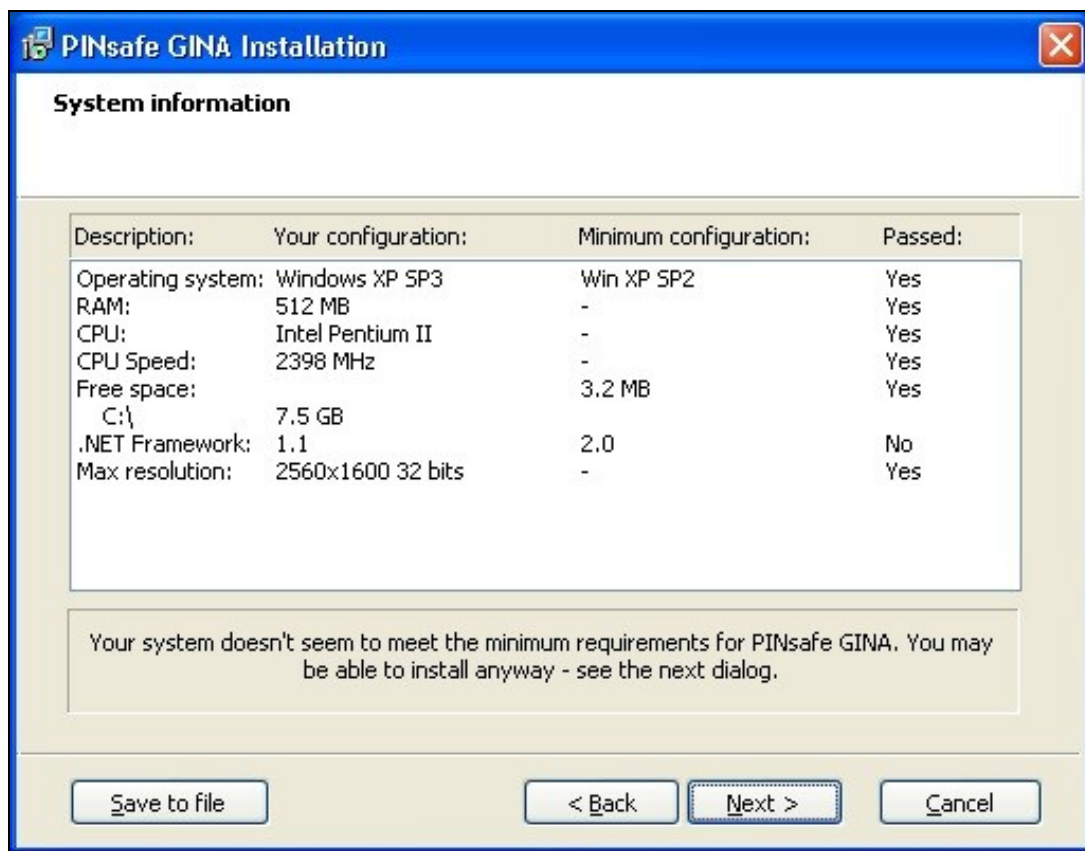
Install the GINA software on the Windows Terminal Server.

### 27.1 Terminal Services GINA Installation

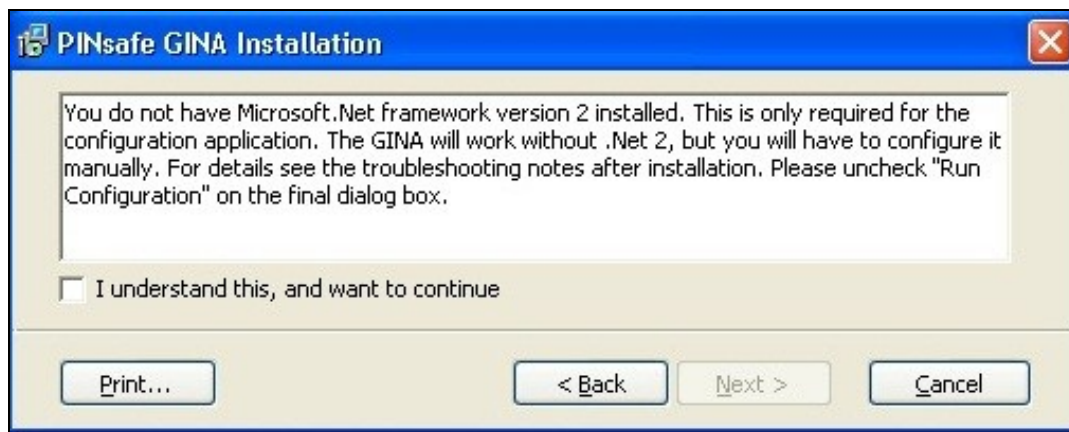
Start the PINsafe installation Wizard



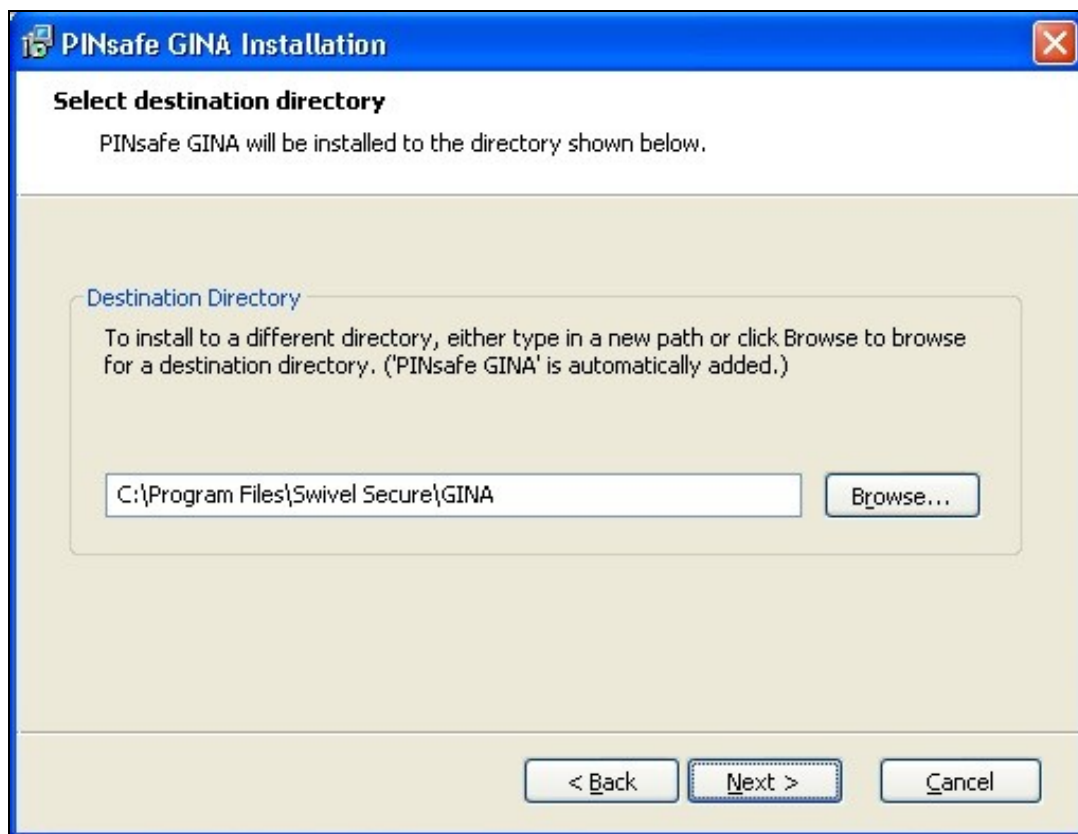
The system summary will report on any requirements which are not met, in this example .Net



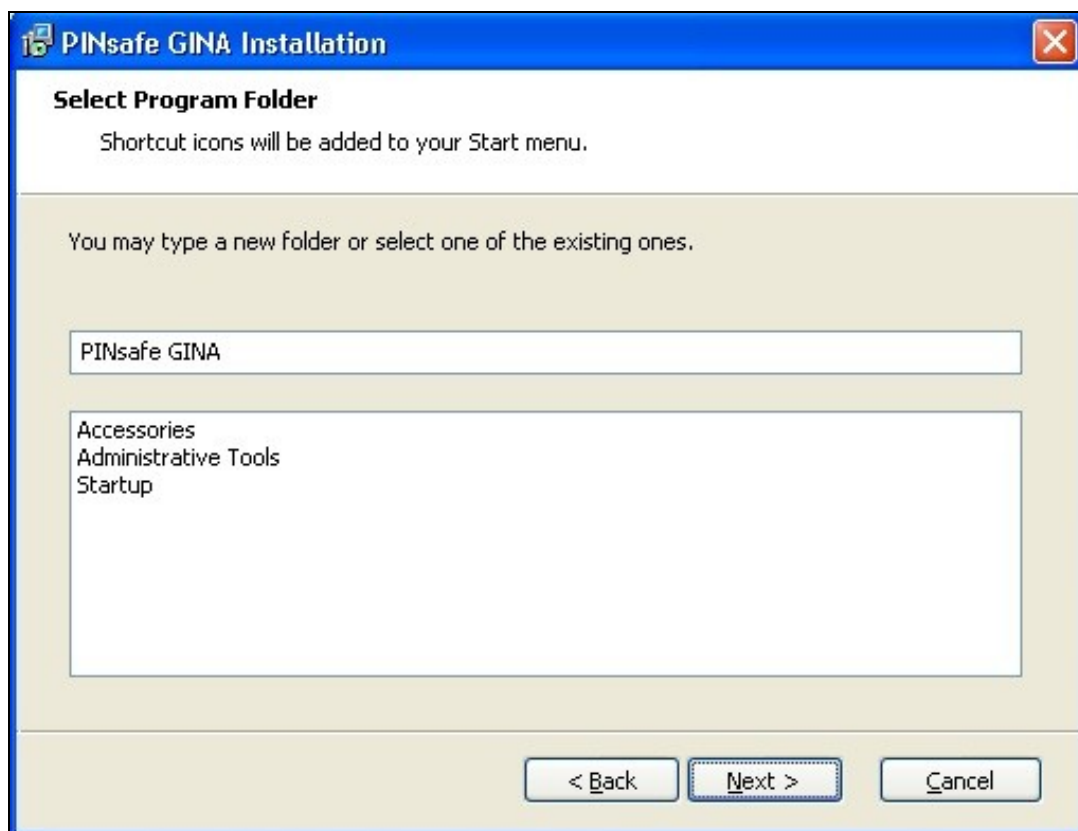
The PINsafe GINA may optionally be installed without .Net, the PINsafe GINA configuration utility requires .Net to install, but may be configured manually



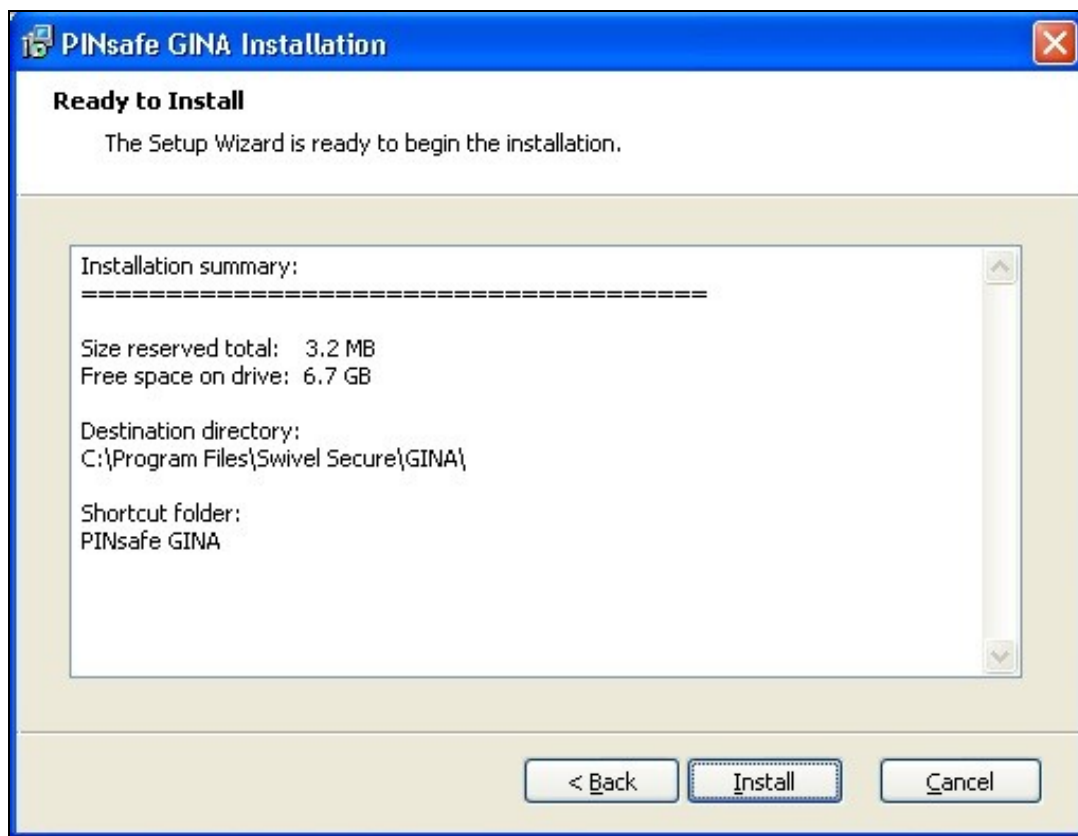
Select the install directory



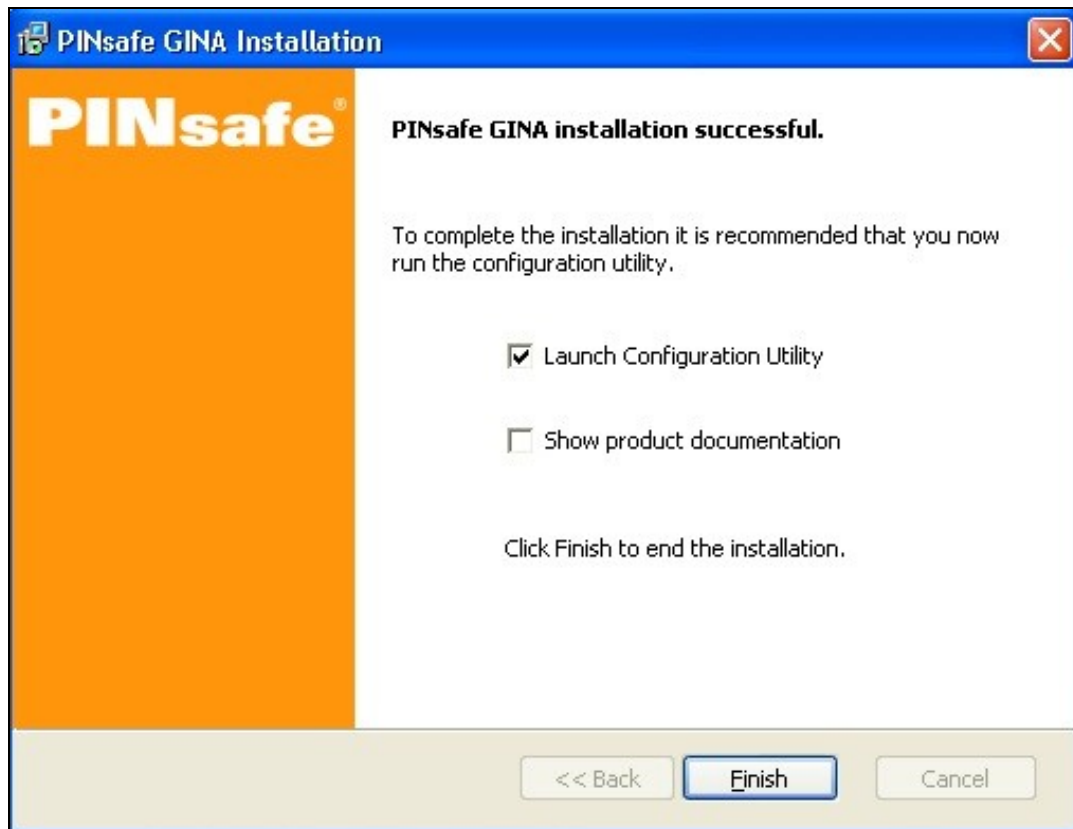
Select the Start Program files group



Check the installation details

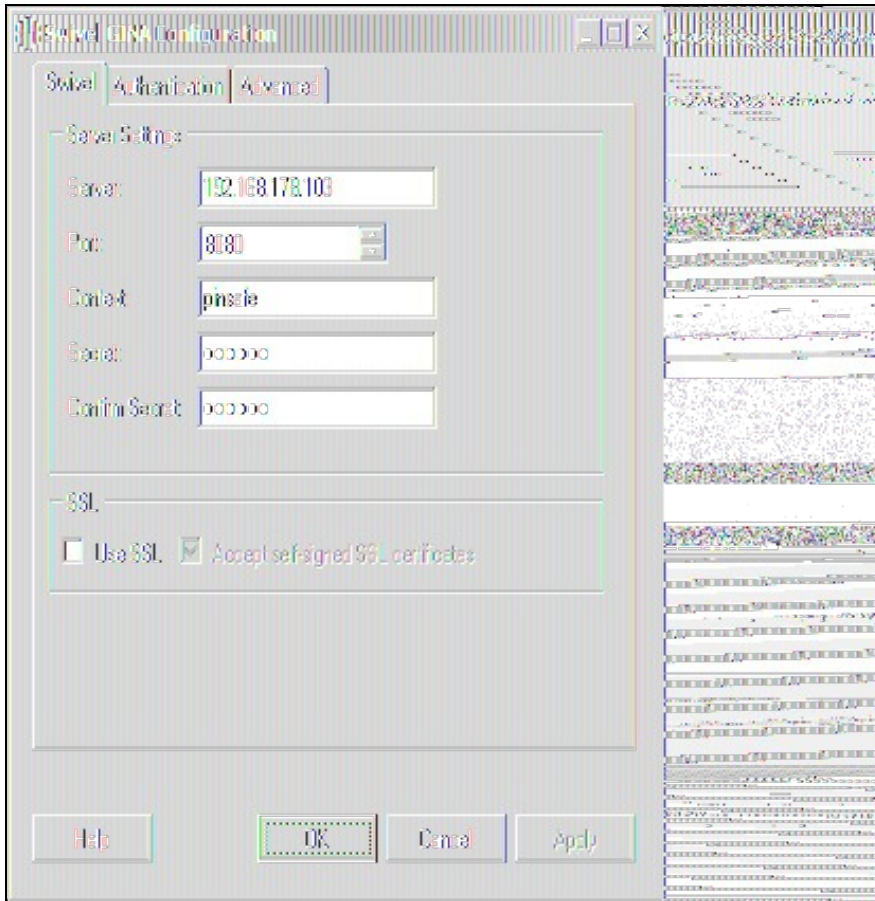


The PINsafe GINA installation reports when it is complete and allows the configuration utility to be run



## 27.2 Terminal Services GINA Configuration

## 27.2.1 Server Settings



**Server** The IP address or hostname of the PINsafe server to use for authentication.

**Port** The TCP/IP port used by the PINsafe server. Commonly "8080" or "8443" if SSL is enabled.

**Context** The web application context used by the PINsafe server. Commonly "pinsafe" for standard installations.

**Secret** The shared secret configured for the GINA agent.

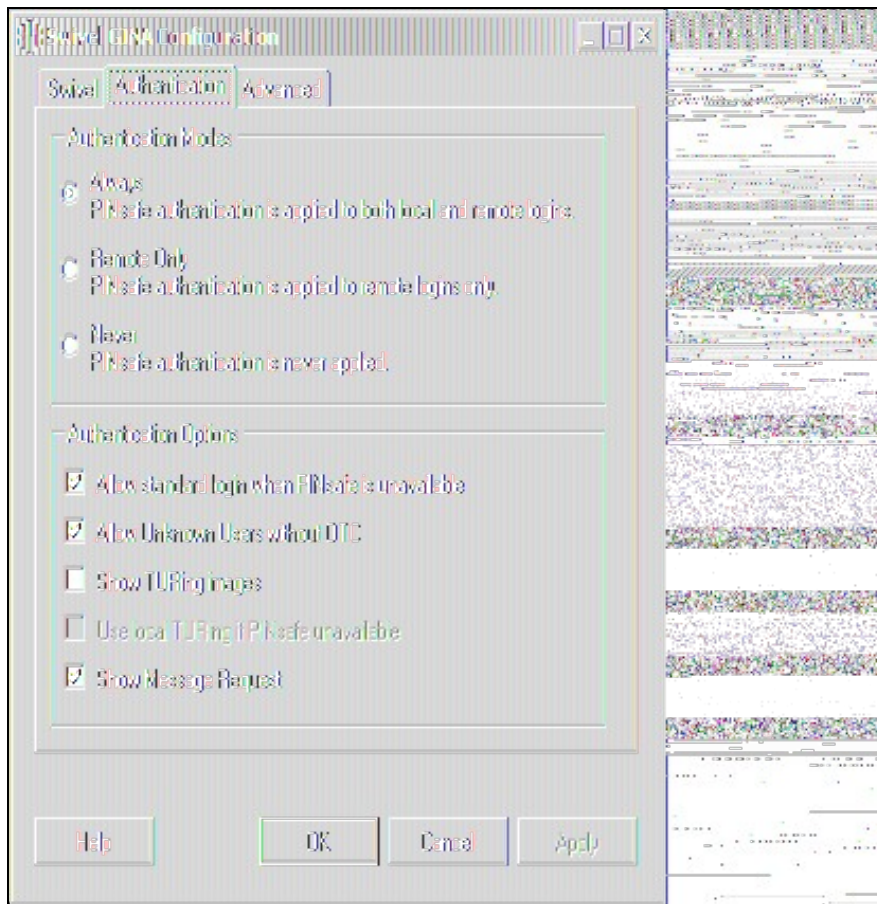
**Confirm Secret** Repeat the shared secret to ensure it has been entered correctly.

**SSL**

**Use SSL** Enable the use of SSL when communication with the PINsafe server. In order to use this option SSL must have been configured on the PINsafe server with an appropriate certificate.

**Allow self-signed SSL certificates** Accept an SSL certificate from the PINsafe server that has not been signed by a recognised certificate authority.

## 27.2.2 Authentication Settings



**Always** Selecting this mode enables PINsafe authentication for local and remote logins.

**Remote Only** Selecting this mode enables PINsafe authentication for remote logins only. Local logins continue to only require a standard Windows username and password combination.

**Never** Selecting this mode disables the use of PINsafe authentication by the GINA.

#### Authentication Options

**Allow standard login when PINsafe is unavailable** When enabled this option temporarily disables PINsafe authentication if the GINA determines that the PINsafe server is not available for authentication.

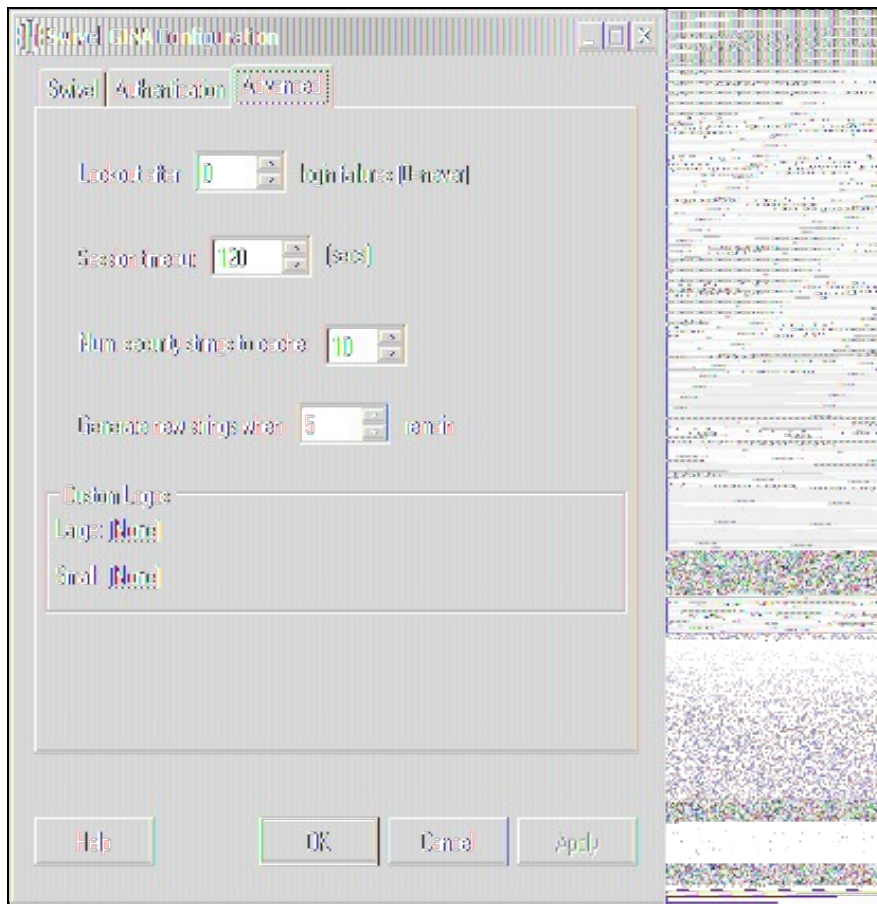
**Allow unknown users without OTC** When enabled, if a user is not known to PINsafe, they are not required to enter a one-time code to authenticate. There is no visible indication that the user is not known to PINsafe.

**Show TURING images** Enable the ability for users to request a single-channel TURING image from the PINsafe server.

**Use local TURING if PINsafe unavailable** When enabled, if the GINA is unable to connect to PINsafe, it will display a locally-generated TURING image to users who have previously authenticated to this computer. Users who have not previously authenticated on-line will not be able to authenticate.

**Show Message Request** When enabled, a button is shown to request a new security string to be sent to the user's designated transport (email or SMS). This cannot be selected together with TURING: disable TURING to use this option.

### 27.2.3 Advanced Settings



**Lockout after # failures** The number of authentication failures before a user is locked out. This only applies to local authentication: Swivel authentication is managed by policies on the Swivel Server.

**Session timeout** The length of time to wait before closing the login dialog.

**Num. security strings to cache** The number of security strings to request from the Swivel server for local authentication.

**Generate new strings when # remain** Controls the minimum number of cached local security strings.

**Custom logos** This allows you to re-brand the GINA with your own logos. The large logo is displayed when the GINA is first displayed, and must be 413 by 88 pixels. The small logo is displayed at the top of the login screen, and must be 413 by 72 pixels.

## 28 ChangePIN

Users may change their PIN using the Change Password option, or if automatically directed at login time.

Remember that to use ChangePIN, a user does not enter their PIN, but uses an OTC and generates a OTC for which they want the new PIN to be. Dual channel and mobile Phone Clients may be used with the ChangePIN as well as the TURING image.

### 28.1 User Requested ChangePIN using Change Password

From the Windows menu select Ctrl-Alt-Delete



The user may change their PIN and or password. To ChangePIN, password details can be left blank.

Change Password

# PINsafe®

User name:

Log on to:  ▼

Old Password:

New Password:

Confirm New Password:

Old OTC:

New OTC:

Confirm New OTC:

ChangePIN using dual channel or mobile phone client

Change Password

# PINsafe®

User name:

Log on to:  ▼

Old Password:

New Password:

Confirm New Password:

Old OTC:

New OTC:

Confirm New OTC:

ChangePIN using TURING

**Change Password**

# PINsafe®

User name:

Log on to:  ▼

Old Password:

New Password:

Confirm New Password:

Old OTC:

New OTC:

Confirm New OTC:

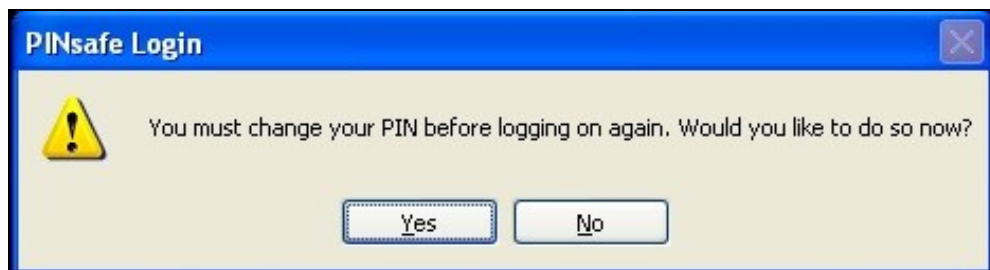
1	2	3	4	5	6	7	8	9	0
3	2	7	9	4	6	5	1	0	8

ChangePIN successful



## 28.2 ChangePIN redirect at login

Where the user is required to ChangePIN the user is redirected at login.





The dialog box is titled "PINsafe Change PIN" with a blue header bar and a red close button in the top right corner. It contains four text input fields: "User name:" with the text "graham", "Old OTC:", "New OTC:", and "Confirm New OTC:". Below these fields is a "Get Image" button. At the bottom are "OK" and "Cancel" buttons. A large empty rectangular area is located below the "Get Image" button.

**PINsafe Change PIN**

User name:

Old OTC:

New OTC:

Confirm New OTC:

ChangePIN using dual channel or mobile phone client



This dialog box is identical in layout to the one above, but the "Old OTC:", "New OTC:", and "Confirm New OTC:" fields are masked with four black dots (••••) instead of being empty.

**PINsafe Change PIN**

User name:

Old OTC:

New OTC:

Confirm New OTC:

ChangePIN using TURING


**PINsafe Change PIN** [X]

User name:

Old OTC:

New OTC:

Confirm New OTC:



ChangePIN successful

**PINsafe Change PIN** [X]

 Your PIN was changed successfully

## 29 Additional Installation Options

## 30 Verifying the Installation

When a user logs out they should be prompted for PINsafe authentication



**PINsafe Login**

# PINsafe®

 This computer is in use and has been locked.  
Only QWERTY-D2ACFFB8\graham (graham) or an administrator can unlock this computer.

User name:

Password:

OTC:

A user may use dual channel authentication to login by entering AD password and One Time Code.



**PINsafe Login**

# PINsafe®

User name:


Password:

OTC:

A user can also authenticate using single channel by generating a TURING image.

**PINsafe Login**

# PINsafe®

 This computer is in use and has been locked.  
Only QWERTY-D2ACFFB8\graham (graham) or an administrator can unlock this computer.

User name:

Password:

OTC:

1	2	3	4	5	6	7	8	9	0
7	3	2	1	0	6	5	9	4	8

Standard authentication when the PINsafe server cannot be contacted.

**Log On to Windows**

# PINsafe®

User name:

Password:

## 31 Uninstalling the PINsafe Integration

To uninstall the PINsafe GINA select Start, Programs, PINsafe GINA, PINsafe GINA Uninstaller or Start, Control panel, Add or Remove Programs, select PINsafe GINA then remove.

Follow the instructions to remove the PINsafe installation.

## 32 Troubleshooting

### PINsafe login options not displayed

If the "Allow standard login when PINsafe is unavailable" is enabled then the GINA will only display PINsafe login options if it is able to contact the PINsafe server. If PINsafe options are not displayed check the server settings and connectivity to the PINsafe server.

### Manually configuring the PINsafe GINA

If it is not possible to use the configuration utility the PINsafe GINA settings may be edited manually in the registry. The following values found within the "HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\WinLogon" key are used by the GINA:

PINsafeServer

PINsafePort

PINsafeContext

PINsafeSecret

PINsafeProtocol

PINsafeLoginSelect

PINsafeShowTURING

PINsafeAllowDefaultLogin

PINsafeAllowSelfCert

### Disabling the PINsafe GINA

If the PINsafe GINA fails to load correctly it can be disabled using the following process:

Using the F8 boot menu start Windows in safe mode

Using regedit.exe remove the "HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\WinLogon\ginadll" registry value

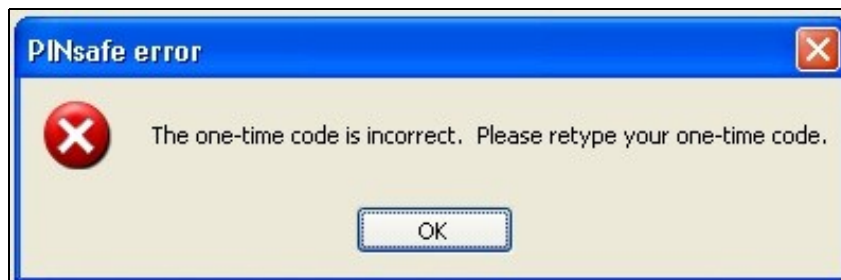
Reboot Windows

Following this process the standard Windows GINA should be restored allowing access.

## 32.1 Error Messages

### The one-time code is incorrect. Please retype your one-time code

The One Time Code is incorrect



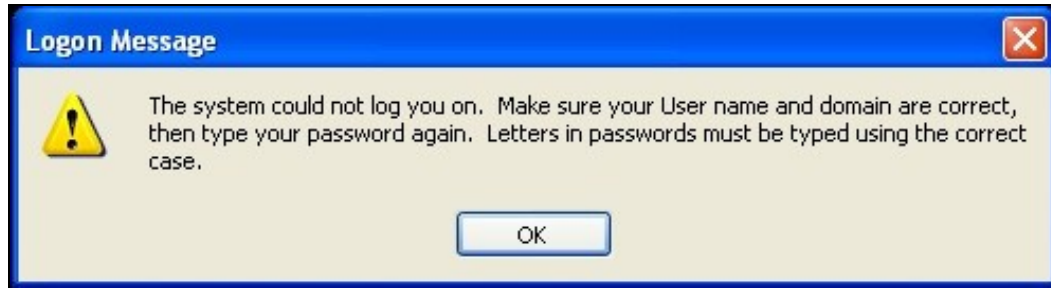
### The password is incorrect. Please retype your password. Letters in passwords must be typed using the correct case.

The Active Directory Password is incorrect



The system could not log you on. Make sure your username and domain are correct, then type your password again. Letters in passwords must be typed using the correct case.

The PINsafe account may be locked contact the PINsafe system Administrator



To recover a locked system protected by PINsafe see [PINsafe GINA](#)

#### Installing without Microsoft.Net Framework 2.0

The GINA itself does not require the .Net Framework - only the configuration utility. Therefore, if you are unwilling to install Microsoft.Net 2.0, you can ignore the warning about this being missing and install GINA anyway. However, you will have to configure the application manually, as described below.

#### Unable to find a runtime of the runtime to run this application

The PINsafe configuration utility is being un without the .Net version 2.0



#### FLUSHING\_IMAGE\_CACHE, ClientAbortException: java.net.SocketException: Connection reset

This error message can be seen in the PINsafe log when a Windows login is attempting to use an animated gif. Turn off animated gifs and switch to 'Static', on Swivel - This is set under Server > Single Channel > Image Rendering.

#### The third party class could not be found

This error can also be created when the Swivel Administration console Server/Agents, Group is set to Any. A group should be specified.

## 33 Known Issues and Limitations

Installation on a Windows 2003 server without Terminal Services, will only provide administrator logon, and only 3 simultaneous logins (including the console session).

Installation on Windows XP will work, but only one user can log on at a time, and then only if no-one is logged on directly to the machine.

There is a usability issue with Windows 2000: it takes about 20 seconds to display a TURING image. For this reason, we are not supporting Windows 2000 in this release, and recommend that if you absolutely have to use it, you should use Dual Channel only.

The following are not supported for Single Channel Authentication when using the Windows GINA:

- BUTton
- PATtern
- Animated Gifs

Dual channel on-demand is not supported.

The Windows GINA menu item is present, but there are no configurable options, so is not selectable.

## 34 Additional Information

## 35 Swivel Windows Credential Provider

## 36 Introduction

Version 5 of the Credential Provider is now released. Documentation on it can be found at [Windows Credential Provider](#). This documentation is out of date, and is not being maintained

This version has been tested on Windows 8, Windows 10 and Windows Server 2012 R2

The current version only works for 64 bit operating systems.

Swivel Windows Credential Provider is used in the desktop operating systems Windows 8 and 10 and the server operating system Windows Server 2012. For integration with Windows Vista and 7 and Server 2008, see [Microsoft Windows Credential Provider Integration](#).

Users can authenticate using the Swivel Credential Provider allowing 2FA (Two Factor Authentication), or strong authentication at the Windows Logon. Offline authentication is also supported for single Channel authentication, following at least one successful authentication against the Swivel server with Third Party Authentication configured.

Supported methods are:

- **TURing** Lets the user sign into windows by using [TURing](#).
- **PINpad** Lets the user sign into windows by using [PINpad](#).
- **On Demand** Lets the user sign into windows by requesting a security string to their preferred method (SMS or email). [More information](#).
- **Other Two Factor** Lets the user sign into windows by entering a one-time code based on a security string received previously or [OATH token](#).

NOTE: [One Touch](#) is not currently supported.

### 36.1 Downloads

[Swivel Windows Credential Provider 64 bit \(version 5.1.0\)](#)

### 36.2 Swivel Credential Provider FAQ

Q). Does the Credential provider support offline authentication? A). Offline authentication is permissible for Swivel users who have previously authenticated to the device. Offline local authentication is always single channel, even if single channel is normally disabled.

Q). Do all users have to authenticate using Swivel? A). Swivel has the option to *Allow Unknown Users*, users known to Swivel will be prompted for authentication in this instance. There is also a "Trusted Users" list where specific users can be added.

Q). Is it possible to define users who do not have Swivel authentication? A). Yes either by the *Allow Unknown Users* for non Swivel user authentication or by adding the user to the "Trusted Users" list

Q). Is it possible to login without AD password, A). No the AD password is required.

## 37 Prerequisites

Swivel version 3.11.3 or later.

Connectivity to Swivel server during installation (with Third Party Authentication for GINA enabled).

Microsoft Windows 8 (including 8.1) and 10 or Windows Server 2012.

Microsoft .Net Framework version 4.

Swivel Windows Credential Provider 64 bit (version 5.1.0)

A separate Swivel Credential Provider license is not required, but the users authenticating to Swivel must be licensed.

User with AD account and valid password.

## 38 Baseline

Swivel 3.10.4

Windows 8, 10, Server 2012 R2.

## 39 Installation

### 39.1 Basic Installation

To install the Swivel Windows Credential Provider run the installer and follow the on-screen instructions. At the end of the on-screen instructions you will be given the option to launch the configuration program to customise the Credential Provider. This can normally be found in the start menu under "Swivel Secure" and in "C:\Program Files\Swivel Secure\Swivel Credential Provider".

After installation and configuration:

- On Windows 8, 8.1 and 10 the computer must be restarted.
- On Windows Server 2012 R2 the Administration account can be signed out rather than doing a full restart.

### 39.2 Multiple Installation

If a configured Swivel Windows Credential Provider has been set up then the settings can be imported automatically on new installations.

1. Extract the settings using the existing Credential Provider from the "File > Export Settings" option, keeping the default name.
2. Copy this file and the installation file onto the new computer, they must be in the same location (example both files on the desktop).
3. Run the installation as described above and the settings will be automatically loaded during installation.

## 40 Architecture

Swivel is installed as a Windows Credential Provider, and when a Windows login is made, AD username and password is checked against AD and the username and Swivel OTC is sent to the Swivel server using XML authentication, or locally if offline authentication is enabled.

### 40.1 Offline Authentication

Swivel allows offline authentication using single channel but not dual channel authentication. For offline authentication the user attempting to authenticate must have made at least one successful authentication against the Swivel server while Offline Authentication has been enabled. Swivel caches a limited number of strings for authentication, when one is shown then it's classed as used and will not be re-shown, if the user makes a successful offline authentication then the number of strings will be replenished however if the user runs out of strings then they will need to authenticate online to get some more. Swivel Account lockout is disabled for Swivel offline authentication. ChangePIN will not function when the Swivel server is not contactable. Local authentication is always single channel, even if single channel is normally disabled.

Update: from version 5.4 onwards, offline is also supported for OATH tokens and for mobile app in OATH mode. This requires Sentry version 4.0.5 or later.

## 41 Swivel Integration Configuration

### 41.1 Configure a Swivel Agent

1. On the Swivel Management Console select Server/Agent.
2. Enter a name for the Agent.
3. Enter the Credential Provider IP address. You can limit the Agent IP to an IP address range like: 192.168.0.0/255.255.0.0 where the mask of 255 requires an exact match and 0 allows any value, so the previous example would allow any Agent in the range 192.168, or you can use an individual IP address for the Credential Provider.
4. Enter the shared secret used above on the Credential Provider.
5. Enter a group, (Note in this instance ANY is not a valid group and will cause authentication to fail).
6. Click on Apply to save changes.

The screenshot displays the Swivel Management Console interface for configuring agents. It features two distinct configuration sections, each with a 'Delete' button to its right. Each section contains the following fields: 'Name' (text input), 'Hostname/IP' (text input), 'Shared secret' (password field with dots), 'Group' (dropdown menu showing '---ANY---'), and 'Authentication Modes' (dropdown menu showing 'ALL').

Field	Value
Agents: Name:	local
Hostname/IP:	127.0.0.1
Shared secret:	.....
Group:	---ANY---
Authentication Modes:	ALL
Name:	IIS
Hostname/IP:	192.168.1.1
Shared secret:	.....
Group:	---ANY---
Authentication Modes:	ALL

Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

### 41.2 Configure Single Channel Access

1. On the Swivel Management Console select Server/Single Channel.
2. Ensure ?Allow session request by username? is set to YES.

## Server>Single Channel

Please specify how single channel security strings are delivered.

Image file:	<input type="text" value="turing.xml"/>
Rotate letters:	<input type="text" value="No"/>
Allow session request by username:	<input type="text" value="Yes"/>
Only use one font per image:	<input type="text" value="Yes"/>
Jiggle characters within slot:	<input type="text" value="No"/>
Add blank trailer frame to animated images:	<input type="text" value="Yes"/>
Text Alpha Value:	<input type="text" value="80"/>
Number of complete display cycles per image:	<input type="text" value="10"/>
Inter-frame delay (1/100s):	<input type="text" value="40"/>
Image Rendering:	<input type="text" value="Static"/>
Multiple Authentications per String:	<input type="text" value="No"/>
Generate animated images:	<input type="text" value="No"/>
Random glyph order when animating:	<input type="text" value="No"/>
No. Characters Visible:	<input type="text" value="1"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

### 41.3 Create a Third Party Authentication

If offline authentication is to be allowed, a third party authentication must be created with an Identifier of WindowsGINA. (Even though the GINA is not part of Credential Provider the third party authentication module is still used and must be configured).

1. On the Swivel Management Console select Server/Third Party Authentication.
2. For the Identifier Name enter: WindowsGINA (Even though the GINA is not used, this must be entered as WindowsGINA).
3. For the Class enter: com.swiveltechnologies.Swivel.server.thirdparty.WindowsGINA.
4. For the License Key, leave this empty as it is not required.
5. For the Group select a group of users (Note: the option Any cannot be selected).
6. Click Apply to save the settings.

To allow offline authentication to be made a successful authentication must be made with the third party authentication in place.

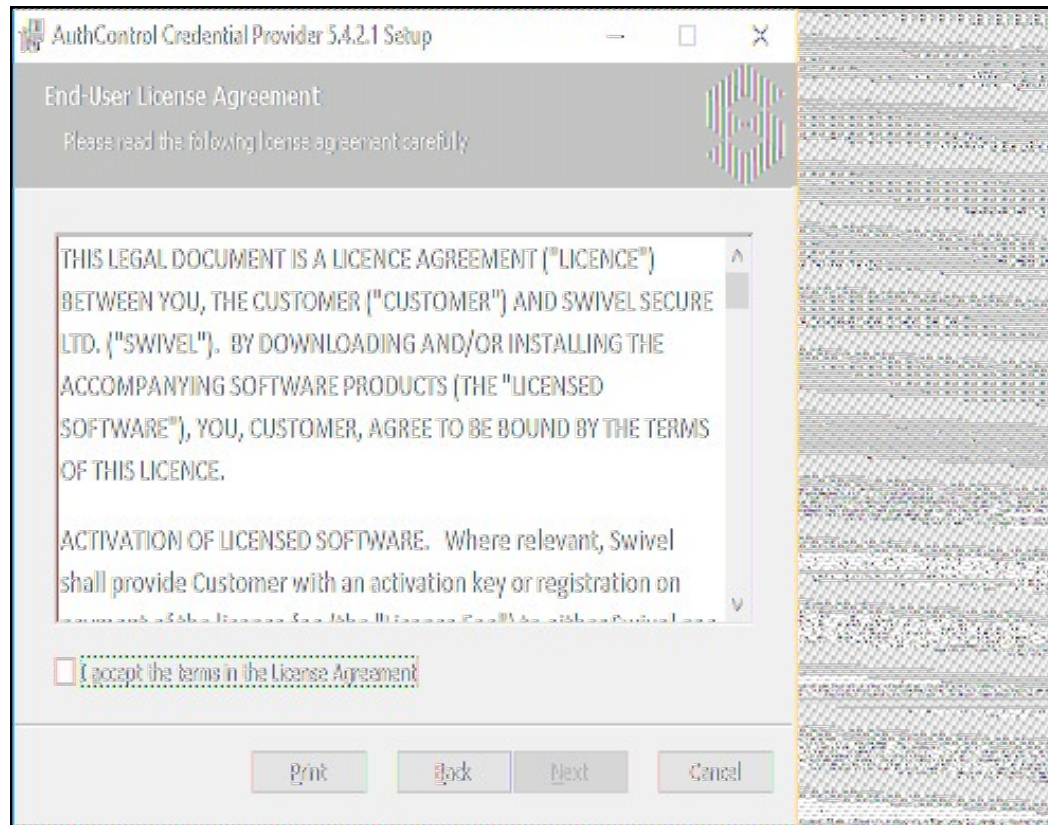
Identifier:	<input type="text" value="WindowsGINA"/>
Class:	<input type="text" value="com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA"/>
License key:	<input type="text"/>
Group:	<input type="text" value="PINsafeUsers"/> ▼

## 42 Microsoft Windows Swivel Credential Provider Installation

The Credential Provider is provided as a Microsoft Installer .msi file. You must run this as an administrator.

Double-click the .msi file to run it. Alternatively, you can install from the command line, using the msixec command.

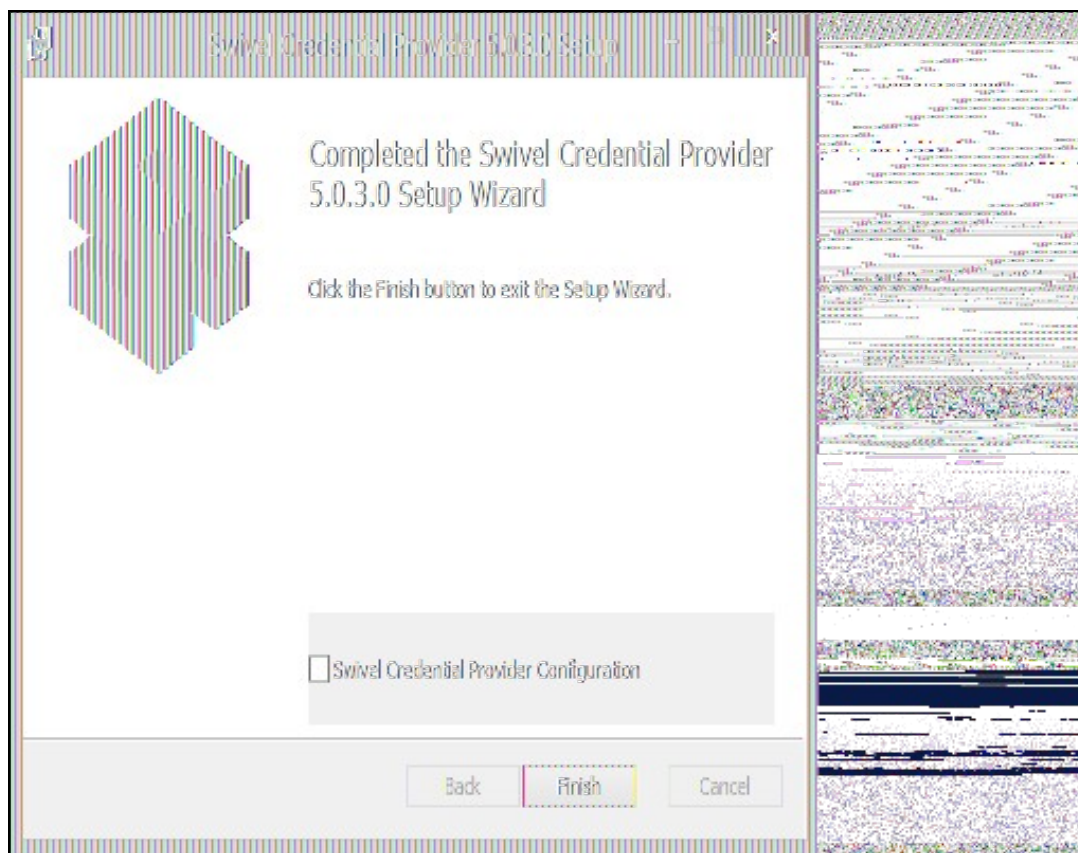
The first page is the licence agreement:



Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

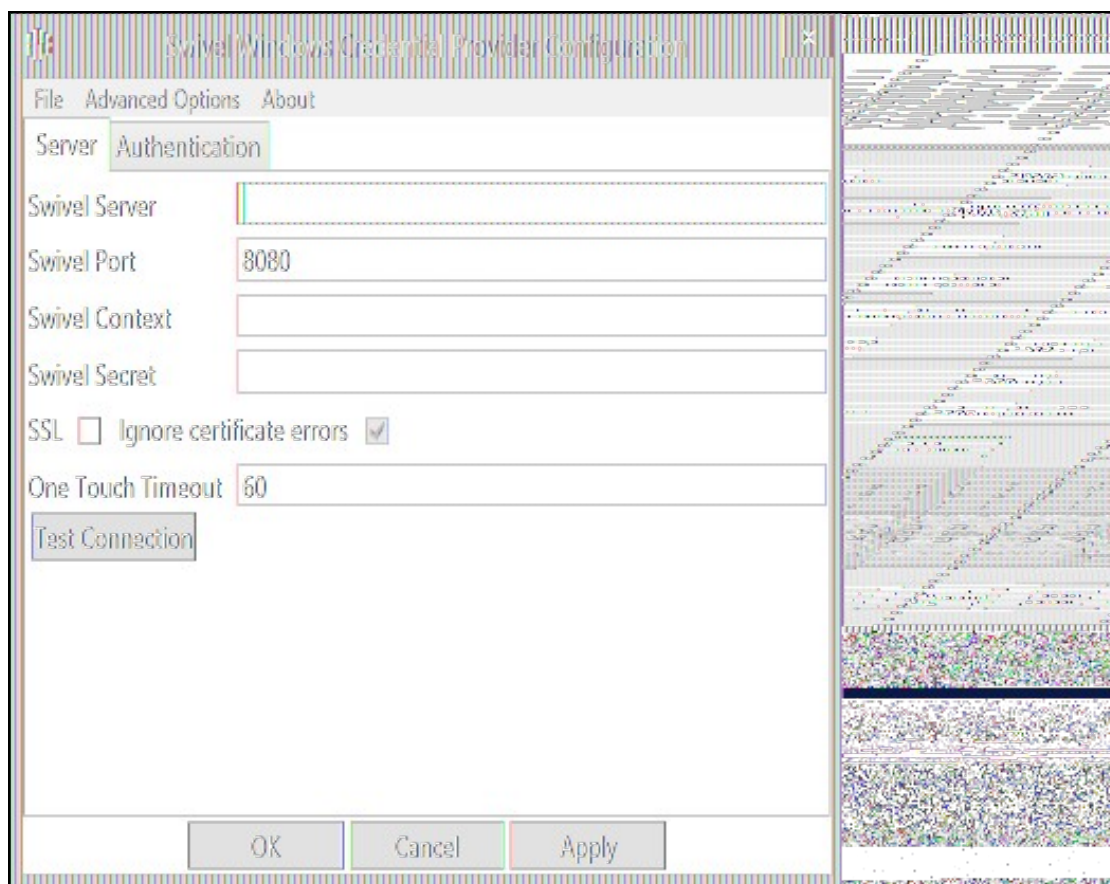
The application will be installed to C:\Program Files\Swivel Secure\Swivel Credential Provider. If you have reconfigured the program files directory elsewhere, it will be installed there, but otherwise you cannot control where the application is installed.

When the install has completed, the following dialog is shown:



## 42.1 Windows Swivel Credential Provider configuration

### 42.1.1 Server



**Server:** The Swivel virtual or hardware appliance or server IP or hostname. To add resilience, use the VIP on a swivel virtual or hardware appliance. See [VIP on PINsafe Appliances](#).

NOTE: it has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name in this section.

**Port:** The Swivel virtual or hardware appliance or server port.

**Context:** The Swivel virtual or hardware appliance or server installation instance.

**Secret:** and **Confirm Secret:** A shared secret which must be entered onto the Swivel virtual or hardware appliance or server.

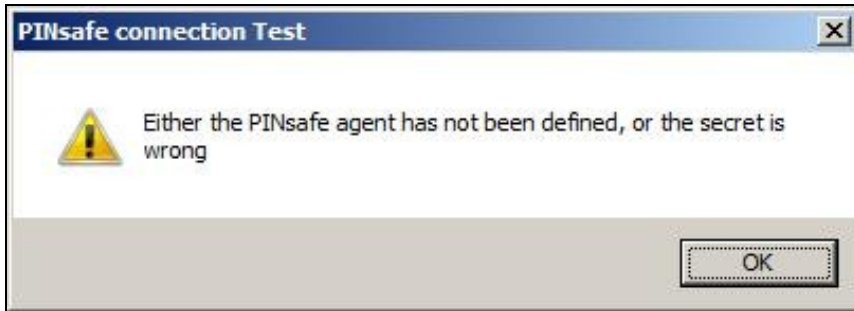
**Use SSL** The Swivel server or virtual or hardware appliance uses SSL communications.

**Accept self signed SSL certificates** Check this box if Use SSL is enabled, and you do not have a commercial certificate on your Swivel server (or a certificate signed by an authority that the client machine trusts). You should also check this box if you are using IP address rather than host name, as recommended above.

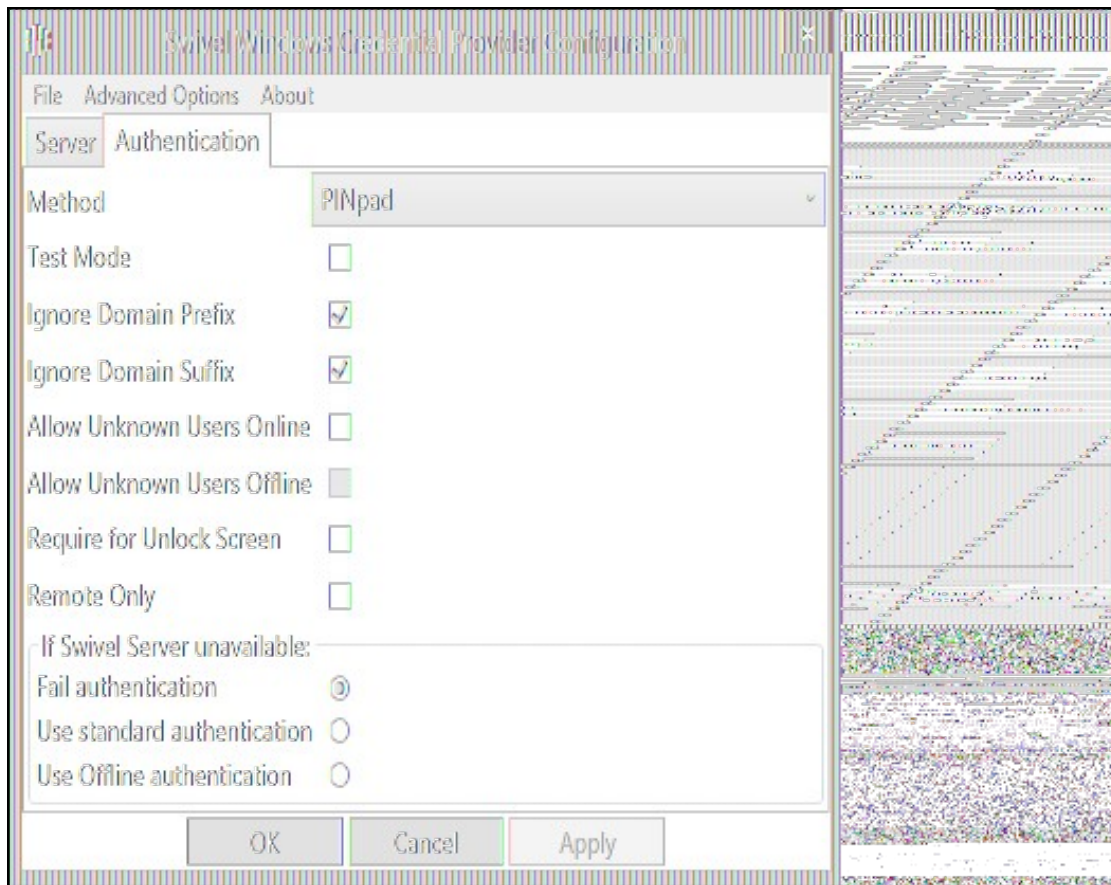
**Test Connection** Tests link to Swivel server. A correct configuration should produce a dialogue box with **Swivel Connection settings are correct.**



Incorrect settings will produce a dialogue box with **Either the Swivel agent has not been defined, or the secret is wrong**, Please check that the machine can contact Swivel and that the entered settings are correct.



## 42.1.2 Authentication



**Method** Select the method of authenticating with Swivel, see [above](#).

**Test Mode** With test mode the user can switch to a standard authentication, see [below](#).

**Ignore Domain Prefix** Swivel will Remove any domain prefix (domain\username) before matching username. This does not affect Windows authentication usernames.

**Ignore Domain Suffix** Swivel will Remove any domain suffix (username@domain) before matching username. This does not affect Windows authentication usernames.

**Allow Unknown Users Online** If the username is not recognized by Swivel, the user can authenticate using Windows credentials only. Any Swivel OTC entered will be ignored. If the user is known then they must authenticate using Swivel authentication.

**Allow Unknown Users Offline** If Swivel is not found and the user has not authenticated with Swivel before then the user can authenticate using Windows credentials only.

**Require for Unlock Screen** Shows the selected authentication method on the unlock screen.

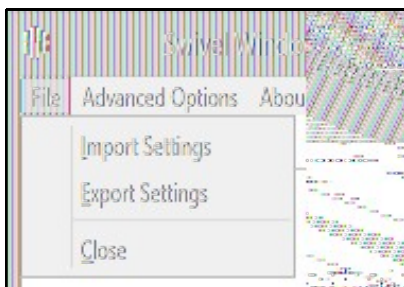
**Remote Only** The selected authentication method will only be shown for users logging into the machine remotely.

**If Swivel unavailable, Fail authentication** If the Swivel server cannot be contacted then authentication will fail.

**If Swivel unavailable, Use standard authentication** If the Swivel server is unavailable use standard authentication, the OTC field is displayed but ignored.

**If Swivel unavailable, Use offline authentication** If the Swivel server cannot be contacted a locally generated Turing image can be used for authentication. If this option is enabled, users will be able to force offline mode using a checkbox on the login dialog. (Only works for single channel authentication methods)

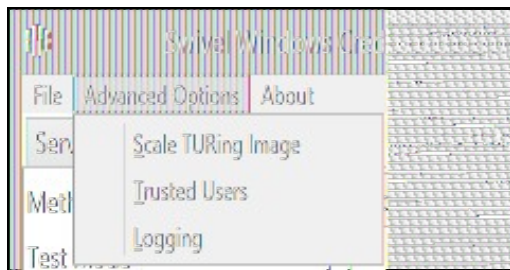
### 42.1.3 File menu



**Export Settings** Export settings as an XML file. These can be used to import settings elsewhere.

**Import Settings** Import settings from an XML file exported elsewhere.

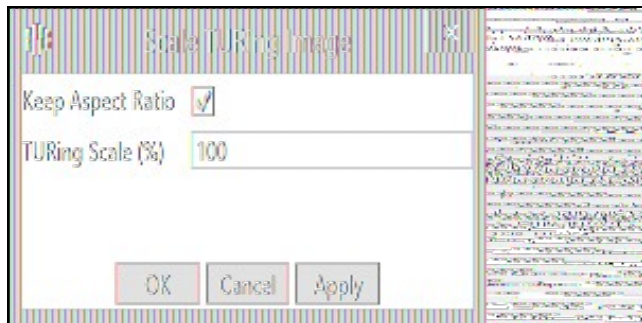
#### 42.1.4 Advanced Options



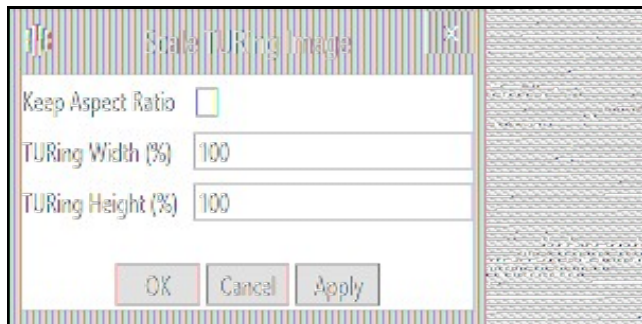
##### 42.1.4.1 Scale TURING Image

**Scale TURING Image...** Opens a dialog to let you scale the size of the TURING shown.

If **Keep Aspect Ratio** is selected then select the scale (%) of the TURING.

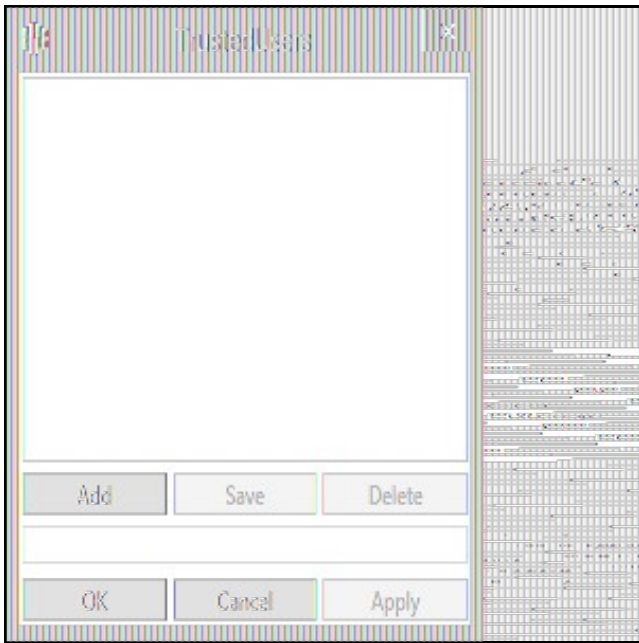


If its not selected then you can select the width and hight independently.



##### 42.1.4.2 Trusted Users

""Trusted Users"" Lets listed users Authenticate without Swivel.



To add a trusted user you must first click ""Add"" then enter the username in the text-box and click ""Save"", repeat these sets to add more users.

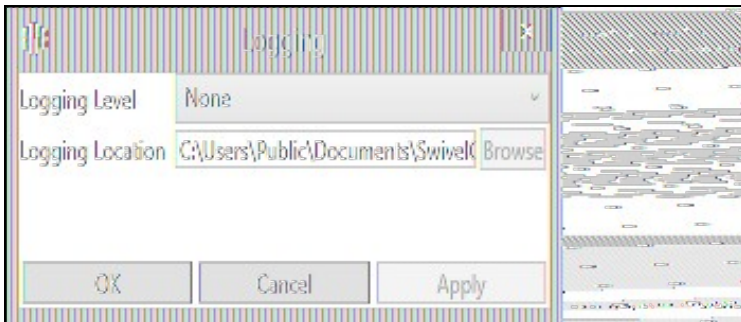
To edit a username select the username from the list, change the name in the text-box and click ""Save"".

To delete a username select the username from the list and press delete.

Make sure that the ""Apply"" or ""OK"" button to save these settings.

#### 42.1.4.3 Logging

""Logging"" change settings relating to logging, recommended to be turned off unless problem are found.

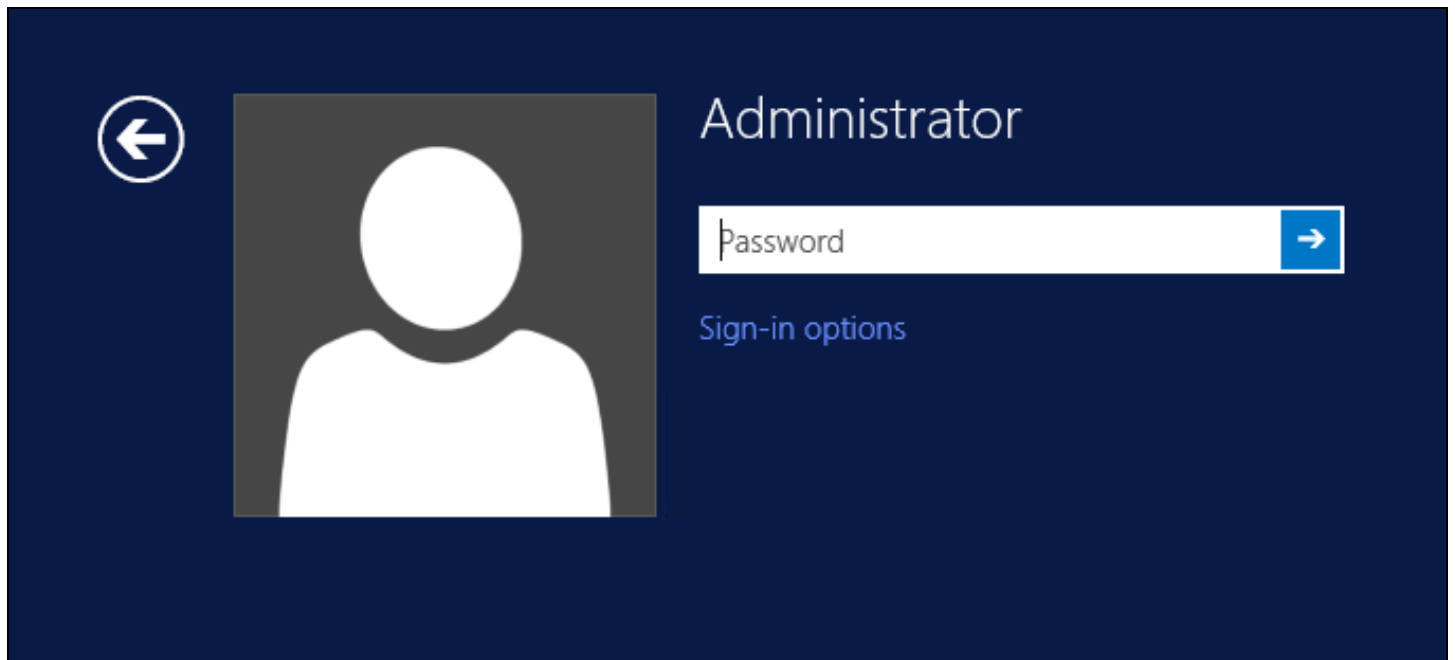


""Logging Level"" The account of message that will be logged.

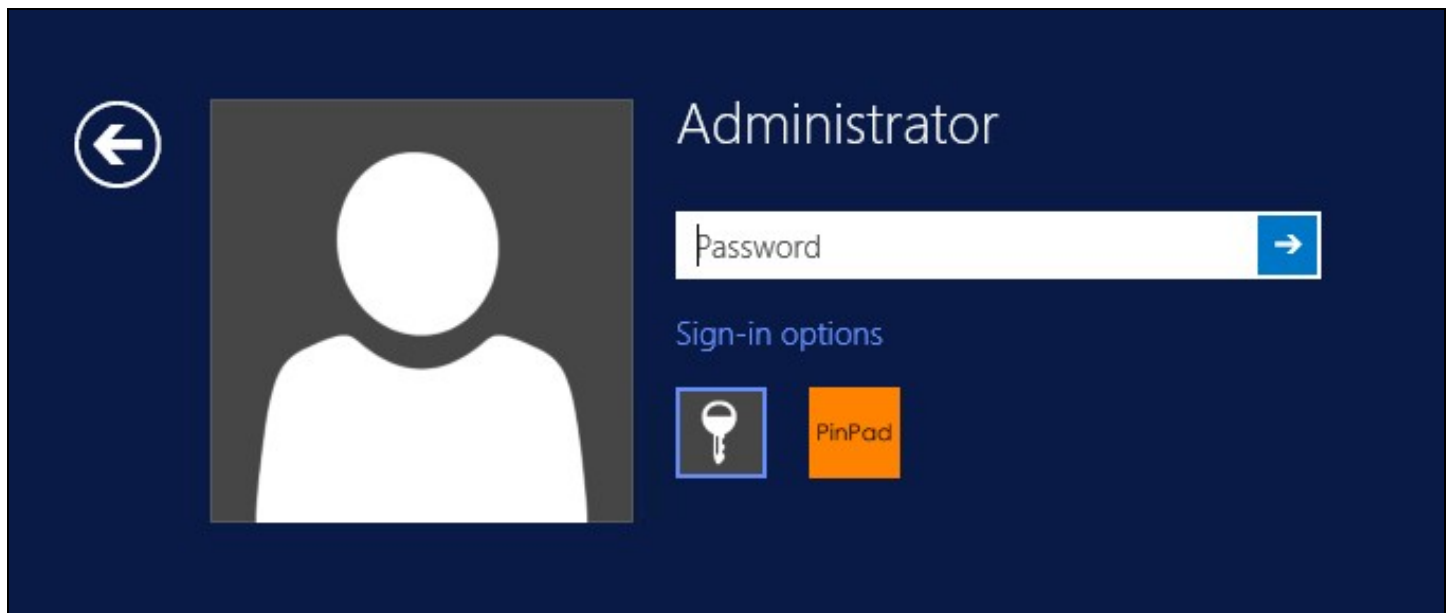
""Logging Location"" The location the logs will be created, this must be somewhere any account has access to.

## 42.2 Test Mode

With Test Mode enabled the user will be able to select how they will authenticate



The **Sign-in options** button is shown to let users select from the list which method they would like to use.



The last successful authentication method will be selected by default when the credential is loaded.

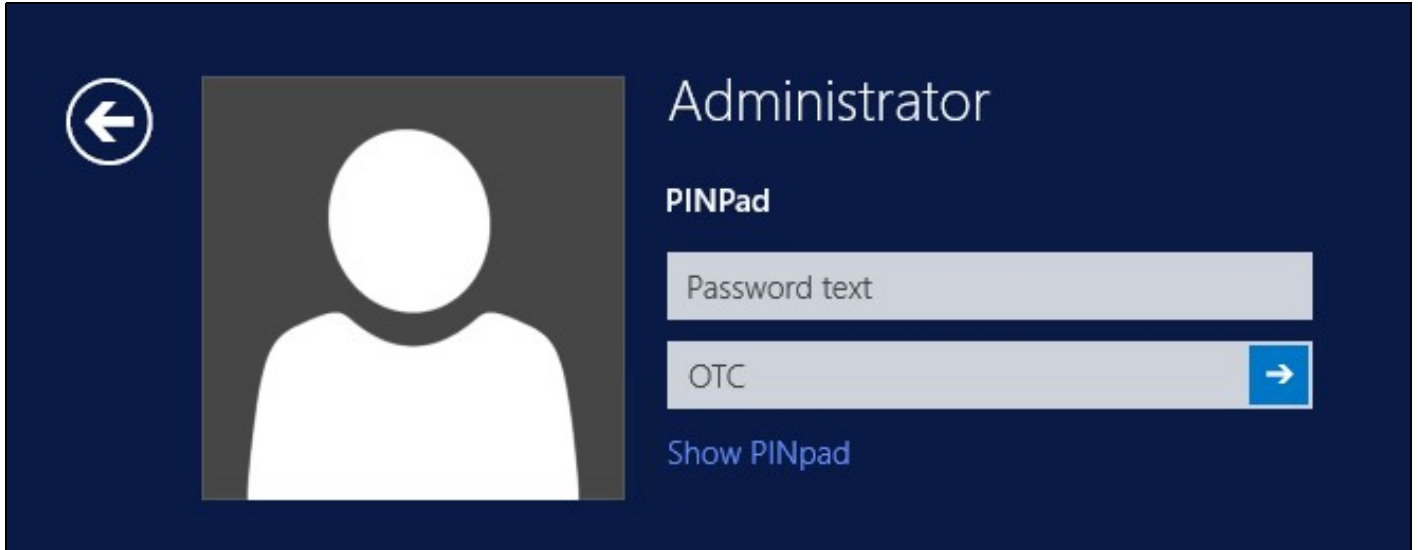
## 42.3 Importing Configurations

You can import credentials exported from other installations using the Import Settings menu item.

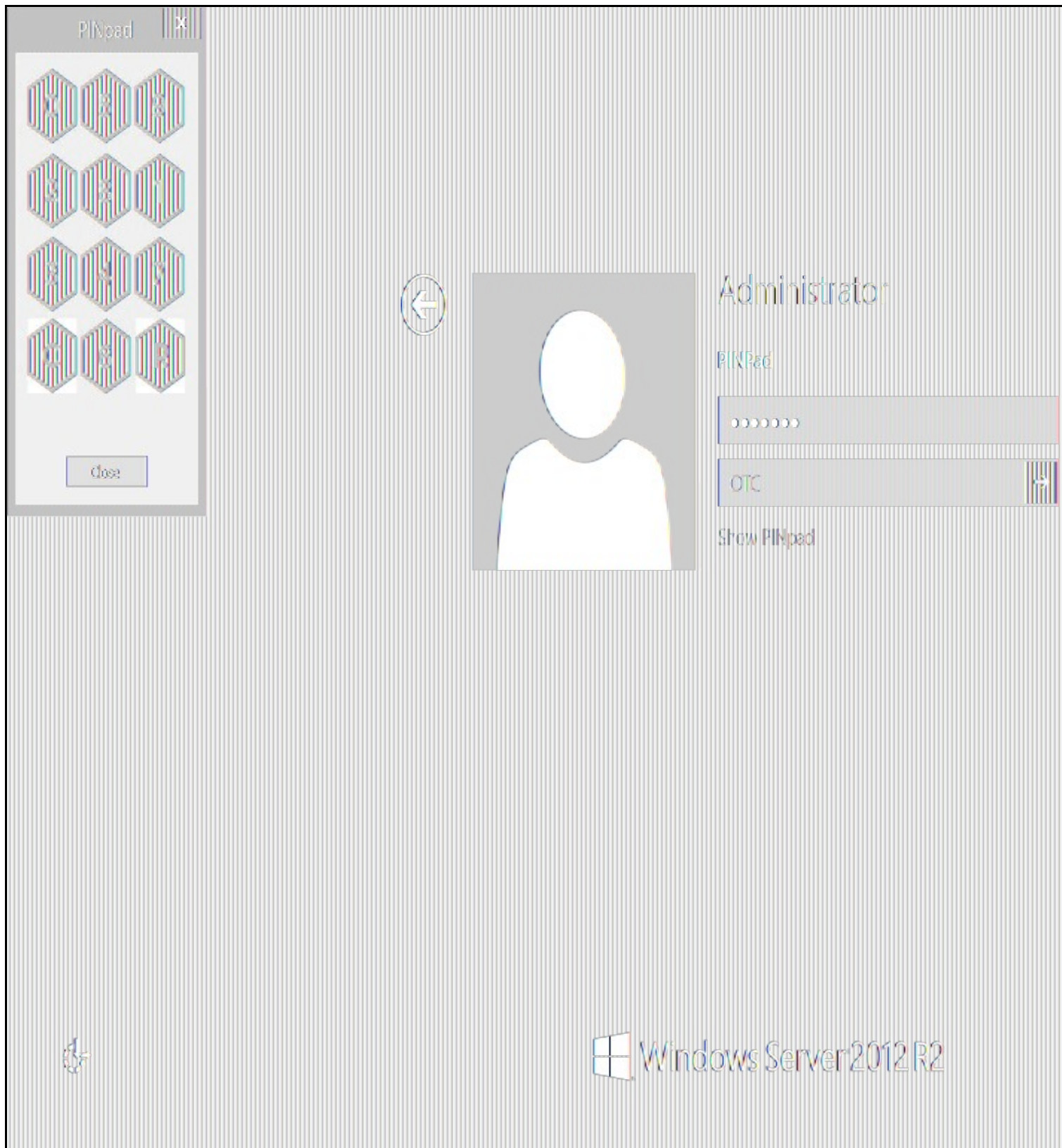
## 43 Verifying the Installation

This will be an example of one of the credentials.

At the windows login screen a password and OTC login field should be available with a "Show PINpad" Button.



Pressing the "Show PINpad" button will generate a PINpad image for authentication. The Swivel log should show a session request message: *Session started for user: username*.



A successful login should appear in the Swivel log: *Login successful for user: username.*

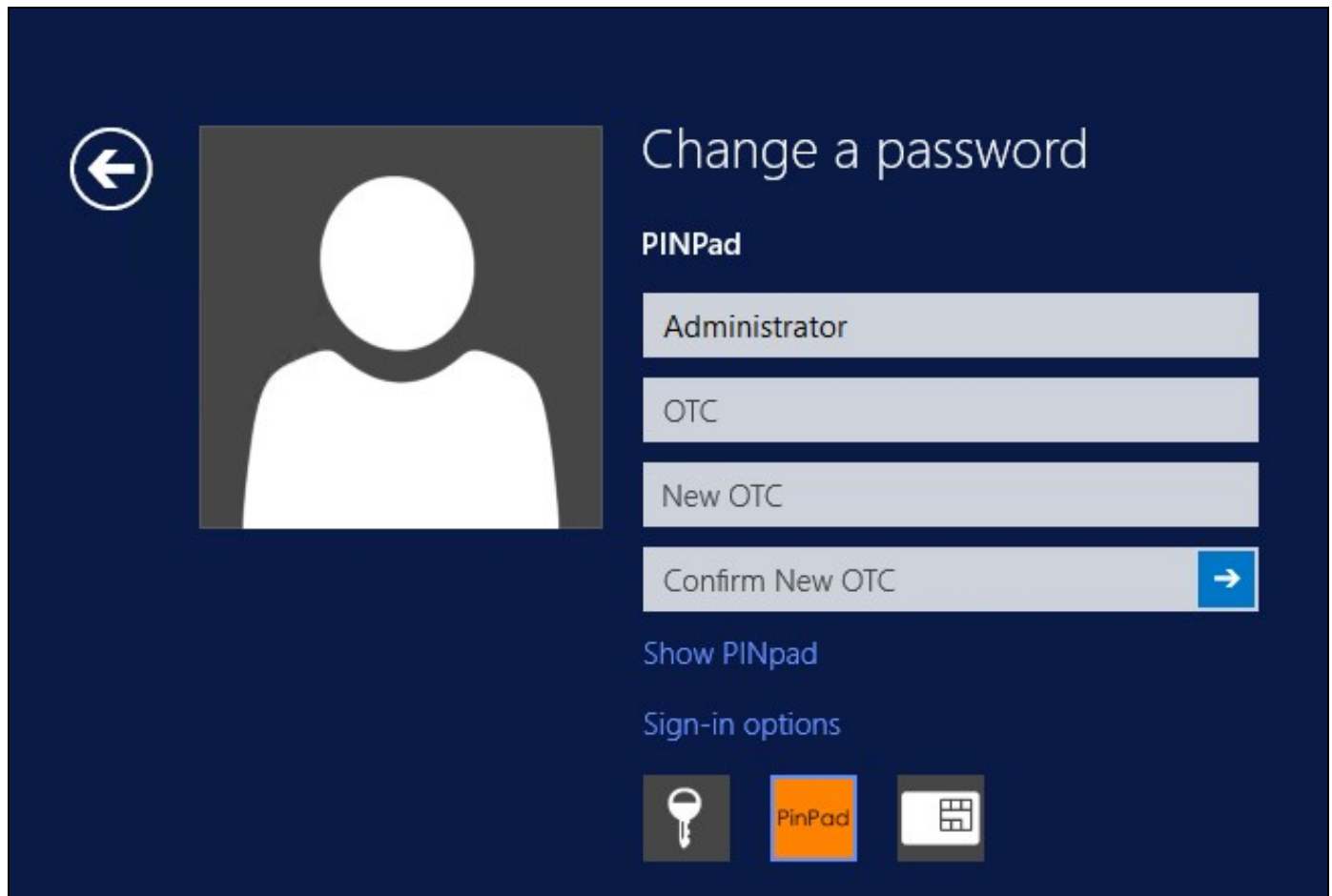
A failed login should not allow a login, and the following message should be displayed in the Swivel log: *Login failed for user: username.*

## 44 ChangePIN

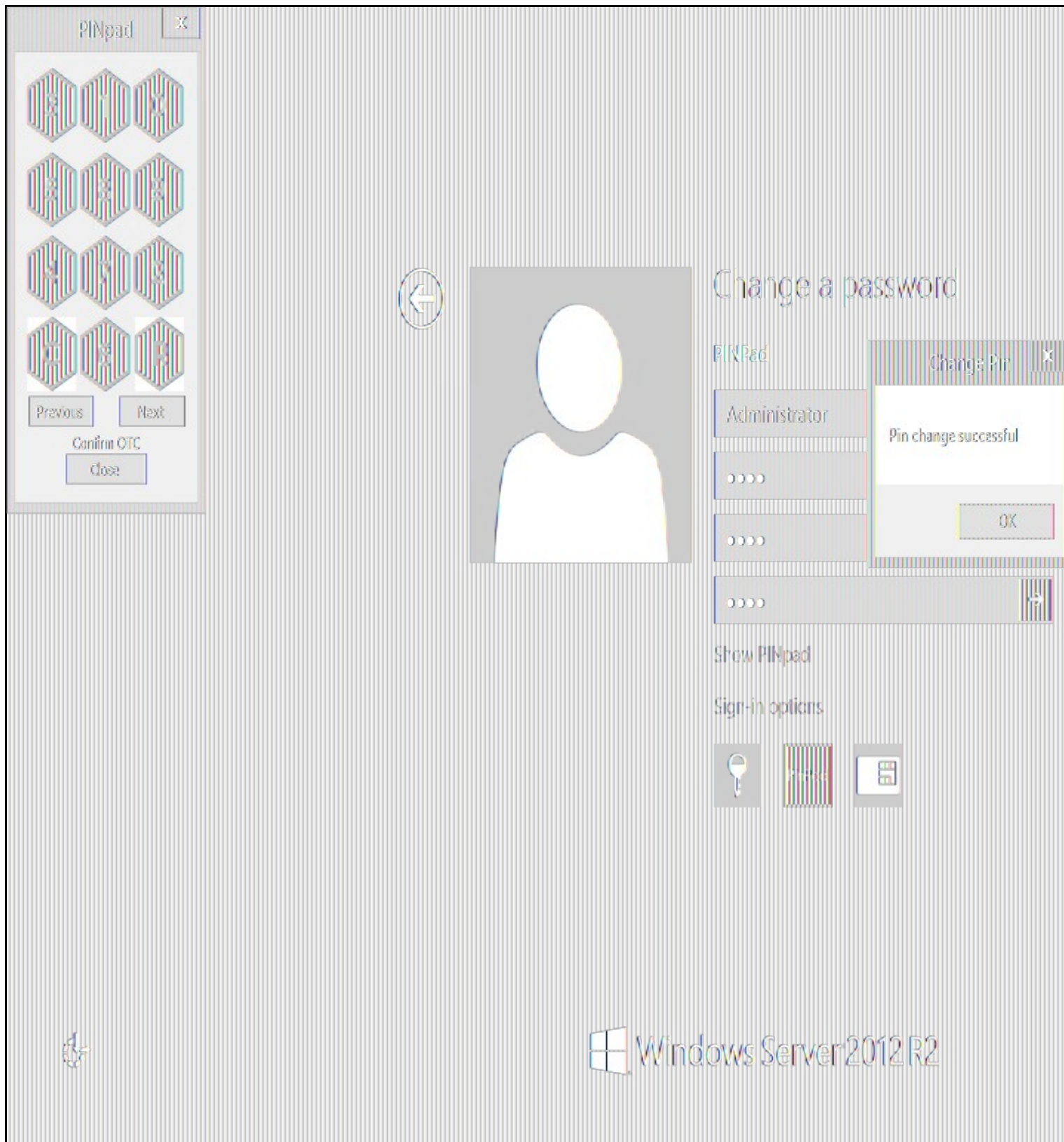
A user is usually able to change the password by using the Ctrl-Alt-Del keys (Ctrl-Alt-End for remote sessions). With the Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the "Sign-in options" button and selecting the Swivel credential. This will not function for Offline authentication.

With Swivel authentication a user never changes enters PIN and this is true for ChangePIN. A user enters their current OTC, and then enters an OTC for what they wish their new PIN to be. PIN enforcement may be in place to the Swivel server to prevent the choosing of poor PIN numbers.

A user may use a single channel image or a dual channel security string to change their PIN.



A successful Change PIN will show the message **Your PIN was changed successfully**, the Swivel server will also display in the logs a changePIN message **Change PIN successful for user: username**.



Other Changes to PINpad are that the PINpad dialog has buttons to select which text-box the numbers will be entered and text to show which text-box is currently selected.

## 45 Uninstalling the Swivel Integration

Use the Uninstall option from the Program menu, right click on the Windows Credentials provider and click on Uninstall. Note that uninstalling and reinstalling the Credential Provider will remove the settings, so if you need to reinstall at any point, make sure you have an exported settings file saved.

### 45.1 Disabling the Credential Provider

If the Credential Provider needs to be disabled temporarily, use the following procedure:

If the credential provider is preventing the machine starting normally, boot the machine into safe mode and log in as an administrator.

Try each of the following in turn. Only one of the following is required, so use the first one that works.

- Run the Swivel Login Configuration and edit the settings to disable the provider.
- Using regedit.exe, edit the following registry keys. Add a DWORD value named "disabled" to each one, set to 1. To re-enable it, you can set disabled to 0, rather than deleting the value.
  - ◆ "HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
  - ◆ "HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
- Uninstall the Credential Provider.
- Using regedit.exe, remove the following registry keys:
  - ◆ "HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
  - ◆ "HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
  - ◆ "HKEY\_CLASSES\_ROOT\CLSID\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"

## 46 Known Issues and Limitations

- The Swivel Windows Credential Provider does not support the use of Animated gifs for Single Channel authentication.
- It has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name for the Swivel server.
- Local authentication only works in single channel and OATH modes: the dual channel strings are not available offline.
- If the user gets an online TURING with a different scale then gets an offline TURING, the TURING is broken, the fix is to close the dialog and request an new TURING.
- If **Allow Unknown Users Offline** is enabled then users that have not previously authenticated to Swivel online can bypass Swivel by checking the offline box and authenticating with AD only.
- On Windows server 2012 R2 there is an update from Microsoft to fix an issue where dialogues will not be displayed, please ensure that windows update 2919355 is installed.
- Local authentication does not know if a users PIN has expired or even if the account is locked or deleted. Once a user has successfully authenticated they are allowed offline until their offline strings are deleted or the offline option is deselected.

## 47 Windows Credential Provider

## 48 Introduction

Swivel Secure AuthControl Desktop (formerly Windows Credential Provider) is used in the desktop operating systems Windows 8, 10 and 11 and the server operating system Windows Server 2012 and 2019. For integration with Windows Vista and 7 and Server 2008, use version 5.3 or later, or see [Microsoft Windows Credential Provider Integration \(Legacy OS\)](#).

Users can authenticate using the Swivel Credential Provider allowing 2FA (Two Factor Authentication), or strong authentication at the Windows Logon. Offline authentication is also supported for single Channel authentication, following at least one successful authentication against the Swivel server with Third Party Authentication configured.

Supported methods are:

- **TURING** Lets the user sign into windows by using [TURING](#).
- **PINpad** Lets the user sign into windows by using [PINpad](#).
- **On Demand** Lets the user sign into windows by requesting a security string to their preferred method (SMS or email). [More information](#).
- **Other Two Factor** Lets the user sign into windows by entering a one-time code based on a security string received previously or [OATH token](#).
- **Push** for Windows 8 and Server 2012 R2 onwards.
- **Fingerprint** (From v5.4.2 onwards and requires AuthControl Sentry v4.0.5) Lets the user sign into windows using Biometric Fingerprint.

### 48.1 Downloads

Latest Release Version:

[Swivel AuthControl Desktop 64-bit version MSI 5.7.31.1](#)

[Swivel AuthControl Desktop 64-bit version executable 5.7.31.1](#)

[Swivel AuthControl Desktop 32-bit version MSI 5.7.31.1](#)

If you have difficulties downloading these files, please contact [teamsupport@swivelsecure.com](mailto:teamsupport@swivelsecure.com) for an alternative method.

The two versions install identical products. The difference is that the executable will copy the current settings from version 5.x and reapply them after installation. The MSI will always overwrite the settings with either blank settings or the contents of acd.xml or scps.xml if provided (see later). As of 5.7, old settings are no longer removed on upgrade, but that only applies to the version that is uninstalled, so upgrading to 5.7 from an earlier version will still remove the old settings.

Settings from versions earlier than 5 cannot be imported automatically on upgrade: you will need to export the settings, uninstall the version 4 credential provider and then install the new version and import the settings.

Important: the Credential Provider requires Microsoft Visual Studio C++ redistributable to work. Recent operating systems already include this, but it will need to be installed on older operating systems if it has not already been installed. You can retrieve it from [here](#). If you have already installed the credential provider, it is not necessary to uninstall it before installing the redistributable.

Note that this article has not yet been fully updated to reflect the changes in version 5.6 or 5.7. See below for release notes.

Older Versions:

[Swivel AuthControl Desktop 64-bit version executable 5.6.10.1](#)

NOTE: we discovered a bug in version 5.6.3.1 whereby the stored secret fails to be decrypted at unpredictable times. We therefore recommend using the following version, 5.6.10.1, which stores the secret unencrypted. This version also fixes a problem with Push authentication, which did not work in 5.6.3.1 or 5.6.9.1.

[Swivel AuthControl Desktop 64-bit version MSI 5.6.10.1](#)

[Swivel AuthControl Desktop 64-bit version executable 5.5.11.1](#)

[Swivel AuthControl Desktop 64-bit version MSI 5.5.11.1](#)

[Swivel AuthControl Credential Provider 64 bit version 5.4.4.2](#)

[Swivel AuthControl Credential Provider 64 bit version 5.4.3.2](#)

[Swivel AuthControl Credential Provider 64 bit version 5.4.2.1](#)

[Swivel AuthControl Credential Provider 64 bit version 5.3.1.5](#)

[Swivel Windows Credential Provider 64 bit version 5.1.1](#)

[Swivel Windows Credential Provider 64 bits version 5.3.0.1](#)

### 48.2 Swivel Credential Provider FAQ

Q). Does the Credential provider support offline authentication?

A). Offline authentication is permissible for Swivel users who have previously authenticated to the device. Offline local authentication is a

Q). Do all users have to authenticate using Swivel?

A). Swivel has the option to *Allow Unknown Users*. Users known to Swivel will be prompted for authentication in this instance. There is also a

Q). Is it possible to define users who do not have Swivel authentication?

A). Yes either by the *Allow Unknown Users* for non Swivel user authentication or by adding the user to the "Trusted Users" list

Q). Is it possible to login without AD password?

A). Yes, there is an option to log in without the AD password, but you must previously have logged in with the AD password.

## 49 Prerequisites

Swivel version 3.11.3 or later. For password caching, version 4.0.4 or later is required.

Connectivity to Swivel server during installation (with Third Party Authentication for GINA enabled).

Microsoft Windows 8 (including 8.1), 10 and 11 or Windows Server 2012 (including R2) and Windows Server 2019. Version 5.3 and later have backward support for Windows Vista or later, and Windows Server 2008 or later.

Microsoft.Net Framework version 4.5.

AuthControl Windows Credential Provider 64-bit - see above for links.

A separate Swivel Credential Provider license is not required, but the users authenticating to Swivel must be licensed.

User with AD account and valid password.

## 50 Baseline

Swivel 3.11.3

Windows 8, 10, 11 Server 2012 R2, Server 2019.

# 51 Installation

## 51.1 Basic Installation

To install the Swivel Windows Credential Provider run the installer and follow the on-screen instructions. At the end of the on-screen instructions you will be given the option to launch the configuration program to customise the Credential Provider. This can normally be found in the start menu under "Swivel Secure" and in "C:\Program Files\Swivel Secure\Swivel Credential Provider".

After installation and configuration:

- On Desktop Windows versions the computer must be restarted.
- On Windows Server versions the Administration account can be signed out rather than doing a full restart.

## 51.2 Multiple Installation

If a configured Swivel Windows Credential Provider has been set up then the settings can be imported automatically on new installations.

1. Extract the settings using the existing Credential Provider from the "File > Export Settings" option, naming the output file either "acd.xml" or "scps.xml". Alternatively, you can export the settings as encrypted and name the file "acd.enc". Note that for the file to be imported automatically you must not specify a password (the default password will be used).
2. Copy this file and the installation file onto the new computer. They must be in the same location (for example both files on the desktop).
3. Run the installation as described above and the settings will be automatically loaded during installation.

NOTE: in version 5.6.9.1 and later builds, the configuration file can be named "acd.xml" instead of "scps.xml". The latter will be used by preference if both files exist.

Alternatively, you can build an pre-configured installer executable. Please contact Swivel Secure support to get the necessary build script.

1. Extract the files from the zip link above into a folder
2. Extract the settings using the existing Credential Provider from the "File > Export Settings" option, naming the output file "acd\_in.xml".
3. Replace acd\_in.xml in the extracted folder with your customised one
4. Compile the executable using ACDInstall.nsi with Nullsoft installation system. If you don't have a copy of Nullsoft, it can be downloaded from [here](#).

# 52 Release Notes

## 52.1 AuthControl Desktop 5.7

### 52.1.1 New Features

#### 52.1.1.1 Generate offline strings outside ACD

The credential manager application allows you to authenticate to Sentry and to download offline security strings. These strings can then be exported to another machine and used there to authenticate users offline

#### 52.1.1.2 All displayed text is customisable

The configuration program allows you to customise the text displayed in the Windows credential. Additionally, you can copy the customised text to the same folder as the ACD installer and it will be imported to the target machine on installation. Currently, only one set of strings is possible per installation, but it is hoped in the future to support multiple languages.

#### 52.1.1.3 Proxy for Sentry connections

You can optionally specify an HTTP proxy for connecting to the Sentry server.

#### 52.1.1.4 Enhancements to Import and Export Settings

Version 5.6 introduced encrypted settings files using a password. Version 5.7 expands on this by allowing for a fixed password, used automatically if encryption is selected but no password is given. Automatic import of settings on installation works with encrypted settings, provided the fixed password is used for encryption. Automatic import of settings will look for the following file names, in this order:

- scps.xml (previously the only name that worked)
- acd.xml
- scps.enc ? assumes the settings are encrypted using the default password
- acd.enc ? as above

Note that the MSI installation no longer deletes the old settings on uninstallation. However, this only applies to upgrading FROM 5.7 or reinstalling. Since the settings are deleted by uninstalling the old version, upgrading from a version older than 5.7 will still remove the old settings.

#### 52.1.1.5 Change PIN for locked users

Previously, if a user attempted to log in and the account was locked due to PIN expiry, authentication would fail. Now, the PIN change screen is shown. It should be noted that in order to change a PIN when the account is locked, you need Sentry version 4.1.4 or later.

#### 52.1.1.6 Optionally, OTC field is not shown initially for Other User

It is possible to specify that the OTC field is not initially shown for the 'Other User' credential. This is the credential that is shown with an empty username field. In the case where users unknown to Sentry are permitted to log on without MFA, it might be preferable not to show the OTC field, in case it is not required. If a user logs in with username and password, and it is subsequently discovered that an OTC is required, the login form is redisplayed with the OTC field.

#### 52.1.1.7 Offline OATH works with On Demand credential

Previously, offline OATH only worked if the authentication method was set to 'Other Two-Factor' (and that not reliably ? see bug fixes). Now it also works with 'On Demand'.

## 52.1.2 Bug Fixes / Improvements

#### 52.1.2.1 Error messages displayed for PIN change errors

Previously, if an error occurred in the PIN change screen, no message was displayed. The screen was simply redisplayed with no additional information. Now, an error is displayed on the screen indicating why the PIN change failed.

#### 52.1.2.2 Improved configuration for Single Sign-On

In 5.6 and earlier, the use of Single Sign-On (SSO) to check if MFA is required was indicated simply by providing a port and context for SSO. This could result in the settings being entered when they were not really needed, just because the fields are there. Version 5.7 shows a check-box to indicate that SSO is active. Activating SSO will display a pop-up dialog requesting the SSO settings, which includes a host name as well as port and context, so the SSO server does not have to be the same as the Sentry Core.

#### 52.1.2.3 Push authentication not working

Version 5.6 (prior to 5.6.10.1) did not support Push authentication due to incompatible changes in the code. Version 5.7 now supports Push correctly.

#### 52.1.2.4 Offline OATH not working

Version 5.6 did not always work for OATH if the token details were stored locally. This was due to an error in the encryption code that affected several features. This has now been corrected.

#### 52.1.2.5 Fixed problems with Secret not encrypting/decrypting on occasions

This problem was caused by the same encryption issue as the previous one. As a workaround, versions 5.6.9.1 and 5.6.10.1 were released with the secret being stored unencrypted, as it was in version 5.5 and earlier. Now that the encryption issue has been resolved, the secret is once again stored in encrypted format, although the encryption is not backward-compatible with 5.6, so copying the secret registry entry from 5.6 to 5.7 will not work. Exporting and importing will work, provided the secret is not encrypted in the export file.

#### 52.1.2.6 Allow unknown users online

It was discovered that version 5.6 did not correctly handle the situation where users were not known to Sentry but could authenticate with password only. This has now been fixed.

## 53 Architecture

Swivel is installed as a Windows Credential Provider. When a Windows login is made, AD username and password is checked against AD and the username and Swivel OTC is sent to the Swivel server using XML authentication, or locally if offline authentication is enabled.


### 53.1 Offline Authentication

Swivel allows offline authentication using single channel or OATH, but not dual channel authentication. For offline authentication the user attempting to authenticate must have made at least one successful authentication against the Swivel server while Offline Authentication has been enabled. Swivel caches a limited number of strings for authentication: when one is shown then it's classed as used and will not be re-shown. If the user makes a successful offline authentication then the number of strings will be replenished: however if the user runs out of strings then they will need to authenticate online to get some more. Swivel Account lockout is disabled for Swivel offline authentication. ChangePIN will not function when the Swivel server is not contactable. Local authentication is always single channel, even if single channel is normally disabled. The exception is that OATH authentication is also supported offline, provided the user has previously authenticated online using the same token.

## 54 Swivel Integration Configuration

### 54.1 Configure a Swivel Agent

1. On the Swivel Management Console select Server/Agent.
2. Enter a name for the Agent.
3. Enter the Credential Provider IP address. You can use an individual IP address for the Credential Provider, such as 192.168.0.99, or you can specify an IP address range like 192.168.0.0/24, which means the first 24 bits, or 3 numbers, are significant or you (i.e. 192.168.0.x).
4. Enter the shared secret used above on the Credential Provider.
5. Select a group, or leave it as "Any" to allow all users to authenticate.
6. Click on Apply to save changes.

**Server>Agents** 

Please enter the details for any Swivel agents below. Agents are permitted to access the authentication server.

Agents:

⊕ [local](#)

⊖

Name:

Network

Hostname/IP:

172.22.5.0/24

Shared secret:

.....

Group:

---ANY--- ▾

Authentication Modes:

ALL ▾

Check password with Repository:

Yes ▾

Check password for non-user:

Yes ▾

Username attribute for repository:

userPrincipalName

Allow alternative usernames:

Yes ▾

Alternative username attributes:

altusername

Can act as Repository:

No ▾

URL Check password:

Encryption/Decryption key:

⊕ [New Entry](#)

Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

### 54.2 Create a Third Party Authentication

If offline authentication is to be allowed, a third party authentication must be created with an Identifier of WindowsGINA. The name must be exactly as shown. This entry should already exist, but check that the settings are as shown.

1. On the Swivel Management Console select Server/Third Party Authentication.
2. For the Identifier Name: WindowsGINA.
3. For the Class: com.swiveltechnologies.Swivel.server.thirdparty.WindowsGINA.
4. Ensure that Enabled is set to Yes.
5. For the Group select a group of users, or Any to allow any users to authenticate using this third party.
6. For the License Key, leave this empty as it is not required.
7. Click Apply to save the settings.

## Server>Third Party Authentication

Please enter the details of any third party authentication methods to be used. Third party authentication allows checking of additional credentials to take place on top of the standard Swivel traffic.


Third parties:


 [PositiveID](#)



Identifier:

Class:

Enabled:  

Group:  

License key:

 [New Entry](#)

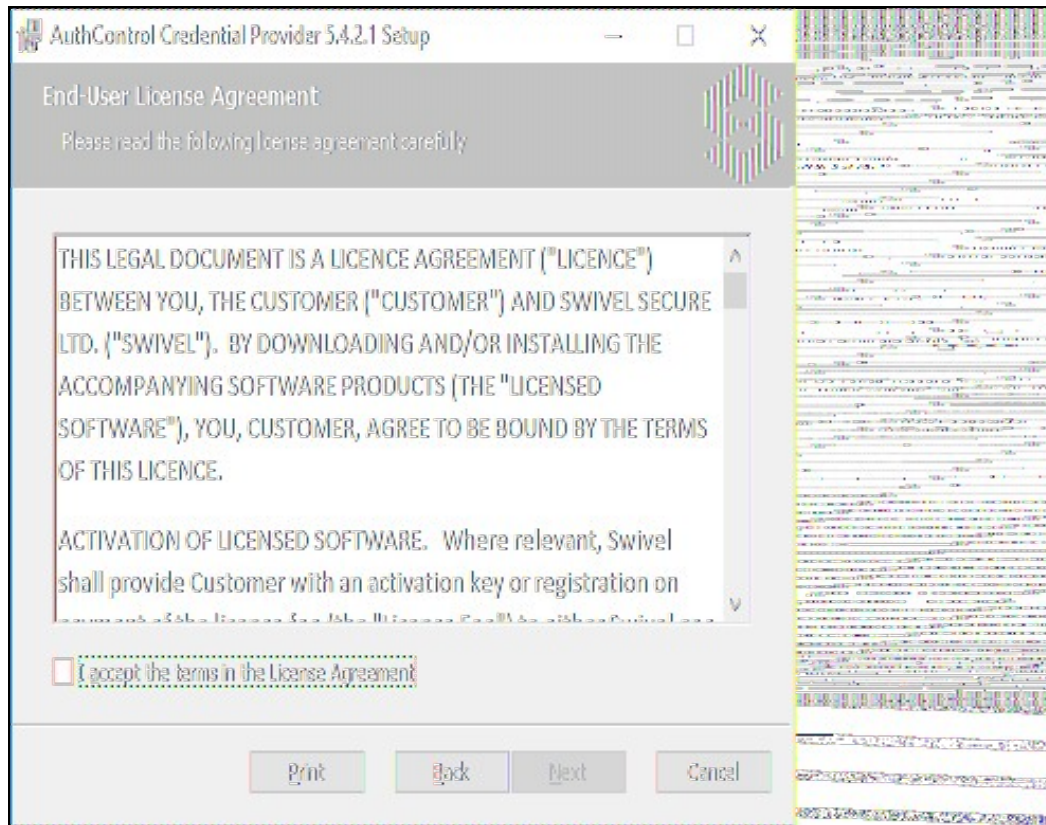
 Appl

## 55 Microsoft Windows AuthControl Credential Provider Installation

The Credential Provider is provided as a Microsoft Installer .msi file. You must run this as an administrator.

Double-click the .msi file to run it. Alternatively, you can install from the command line, using the msixec command.

The first page is the licence agreement:

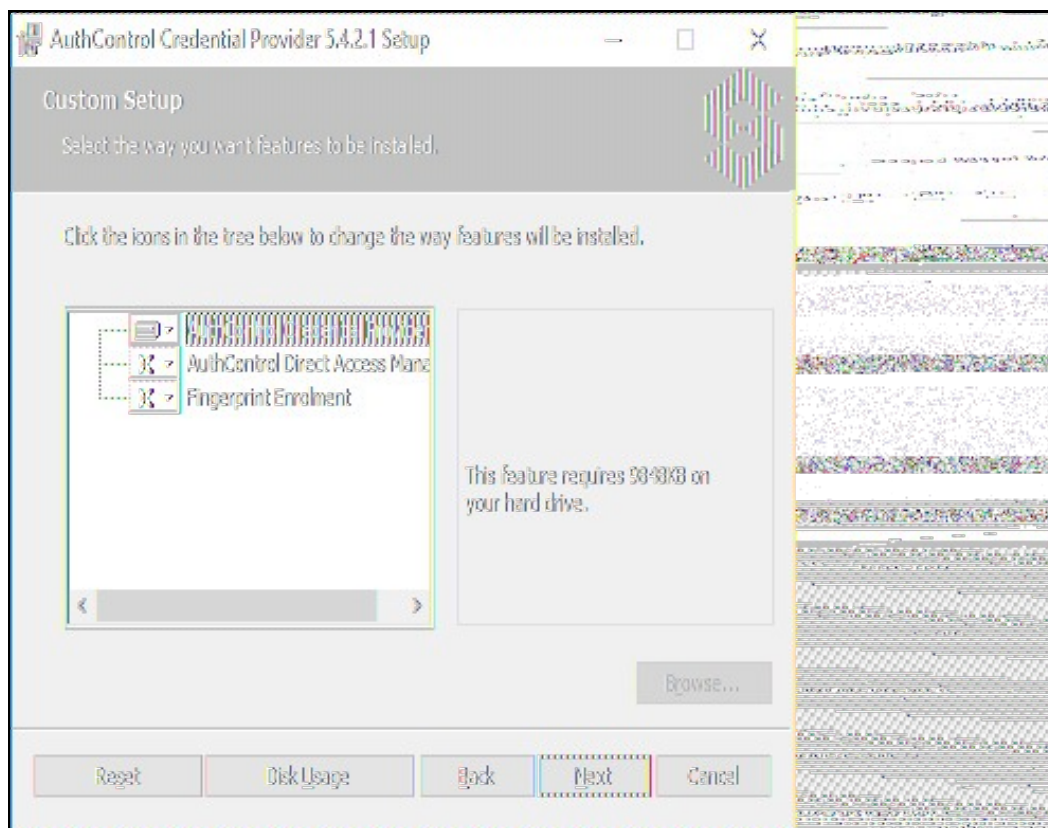


Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

Select the necessary addons:

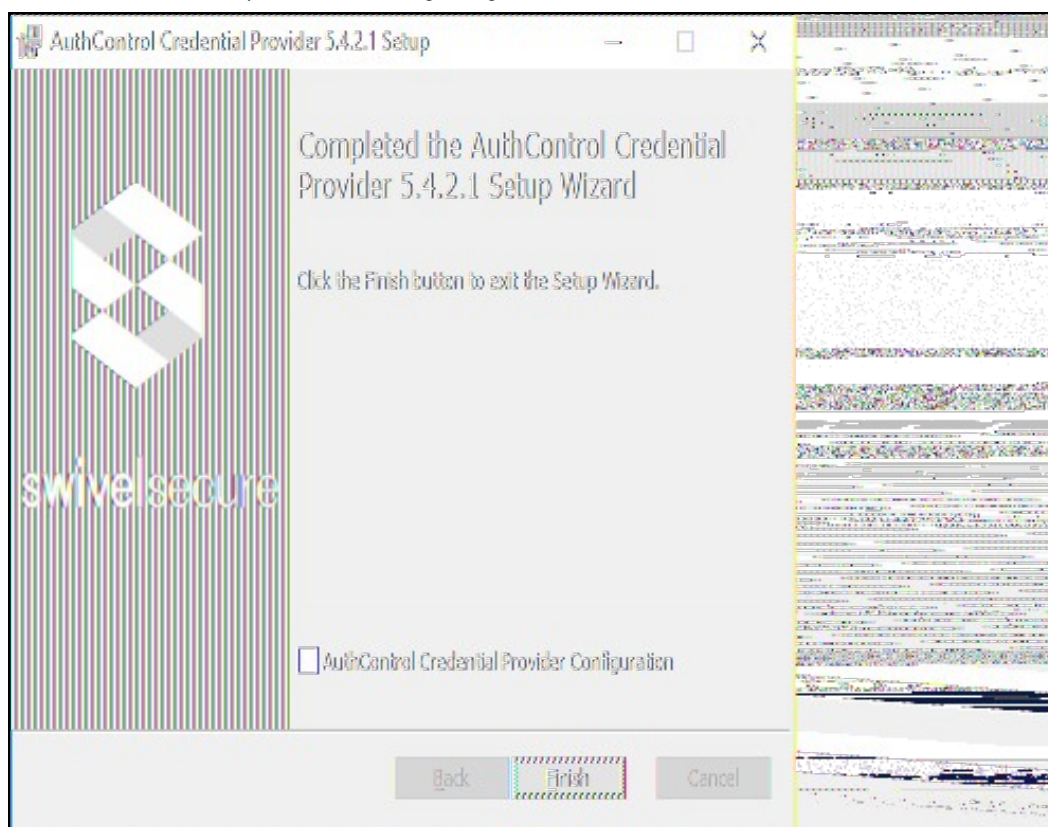
**AuthControl Direct Access Manager** - for integration with Direct Access

**Fingerprint Enrolment** - for Biometric Fingerprint enrolment and use Biometric authentication



The application will be installed to C:\Program Files\Swivel Secure\Swivel Credential Provider. If you have reconfigured the program files directory elsewhere, it will be installed there, but otherwise you cannot control where the application is installed.

When the install has completed, the following dialog is shown:



## 55.1 AuthControl Credential Provider configuration

### 55.1.1 Server

The screenshot shows the 'AuthControl Credential Provider Configuration' dialog box with the 'Server' tab selected. The 'Authentication' sub-tab is also visible. The 'Swivel Server' field is empty. The 'Swivel Port' field contains '8080'. The 'Swivel Context' field contains 'pinsafe'. The 'Swivel Secret' field is empty. The 'Swivel SSO Port' field is empty. The 'Swivel SSO Context' field is empty. The 'SSL' section has a checkbox for 'Ignore certificate errors' which is checked. The 'Security Protocol' section lists 'TLS1.2', 'TLS1.1', 'TLS1.0', and 'SSL3', each with an unchecked checkbox. The 'One Touch Timeout' field contains '60'. There is a 'Test Connection' button. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

**Server:** The Swivel virtual or hardware appliance or server IP or hostname. To add resilience, use the VIP on a swivel virtual or hardware appliance. See [VIP on PINsafe Appliances](#).

**NOTE:** it has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name in this section.

**Port:** The Swivel virtual or hardware appliance or server port.

**Context:** The Swivel virtual or hardware appliance or server installation instance.

**Secret:** and **Confirm Secret:** A shared secret which must be entered onto the Swivel virtual or hardware appliance or server.

**SSO Port:** (Sentry v4.0.5 required) The AuthControl Sentry SSO port to allow [RBA](#) usage. (ex: 8443)

**SSO Context:** (Sentry v4.0.5 required) The AuthControl Sentry SSO context to allow [RBA](#) usage. (ex: sentry)

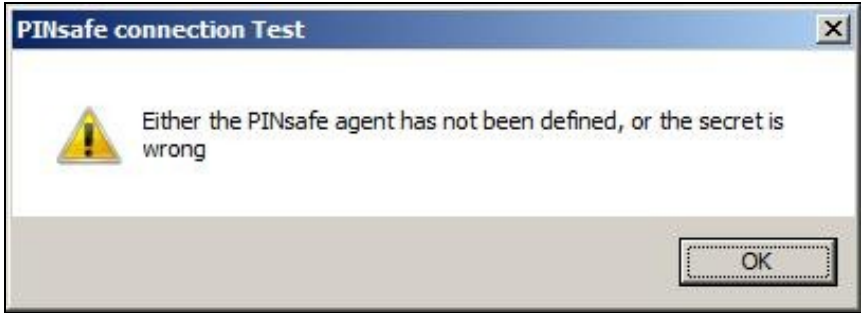
**Use SSL** The Swivel server or virtual or hardware appliance uses SSL communications.

**Accept self signed SSL certificates** Check this box if Use SSL is enabled, and you do not have a commercial certificate on your Swivel server (or a certificate signed by an authority that the client machine trusts). You should also check this box if you are using IP address rather than host name, as recommended above.

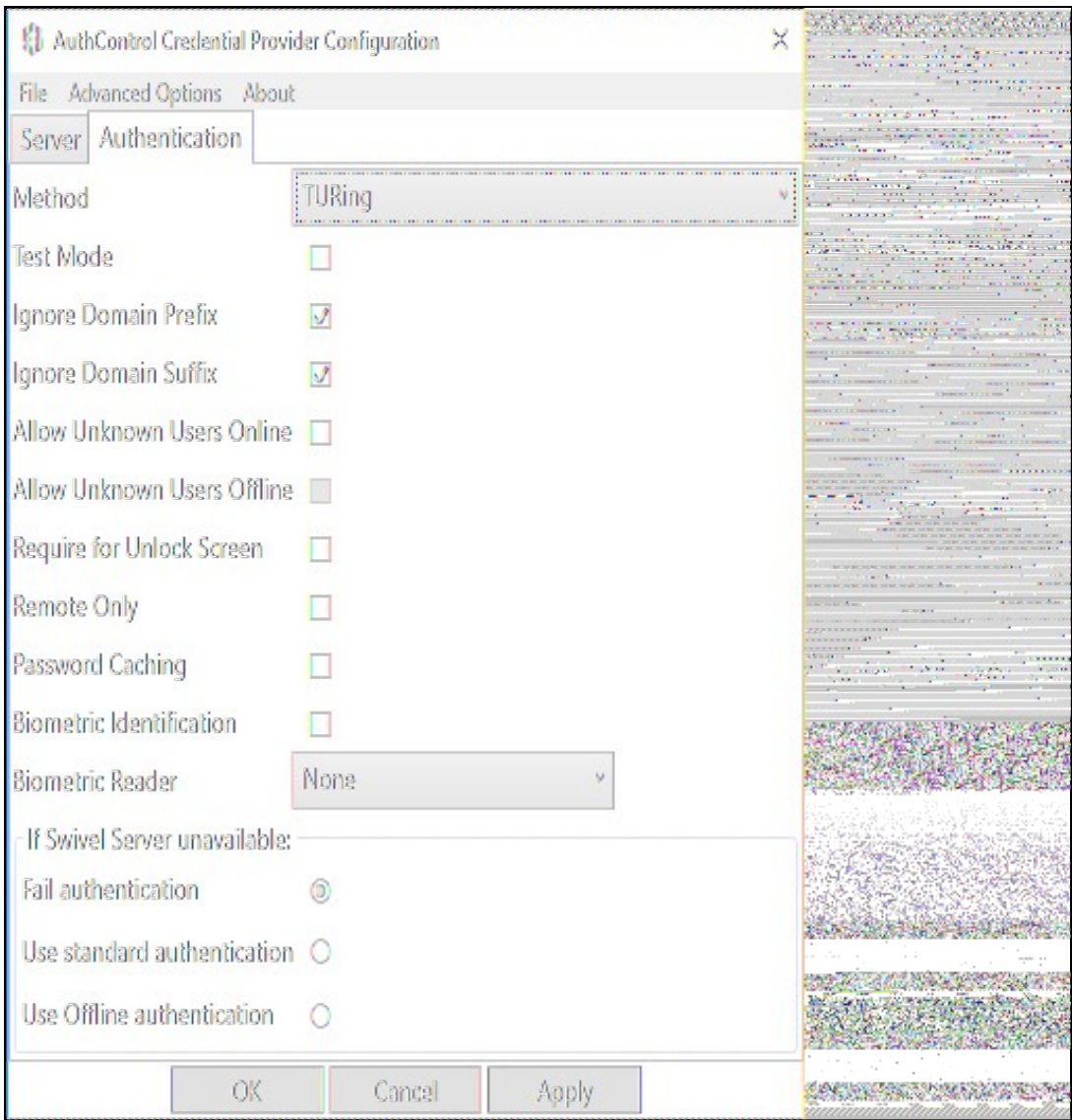
**Test Connection** Tests link to Swivel server. A correct configuration should produce a dialogue box with **Swivel Connection settings are correct**.



Incorrect settings will produce a dialogue box with **Either the Swivel agent has not been defined, or the secret is wrong**. Please check that the machine can contact Swivel and that the entered settings are correct.



55.1.2 Authentication



**Method** Select the method of authenticating with Swivel, see [above](#).

**Test Mode** With test mode the user can switch to a standard authentication, see [below](#).

**Ignore Domain Prefix** Swivel will Remove any domain prefix (domain\username) before matching username. This does not affect Windows authentication usernames.

**Ignore Domain Suffix** Swivel will Remove any domain suffix (username@domain) before matching username. This does not affect Windows authentication usernames.

**Allow Unknown Users Online** If the username is not recognized by Swivel, the user can authenticate using Windows credentials only. Any Swivel OTC entered will be ignored. If the user is known then they must authenticate using Swivel authentication.

**Allow Unknown Users Offline** If Swivel is not found and the user has not authenticated with Swivel before then the user can authenticate using Windows credentials only.

**Require for Unlock Screen** Shows the selected authentication method on the unlock screen.

**Remote Only** The selected authentication method will only be shown for users logging into the machine remotely.

**Password Caching** Allows to cache the password and login using only 2fa. This option only works online.

**Biometric Identification** Allows to use the Biometric Reader to obtain the username.

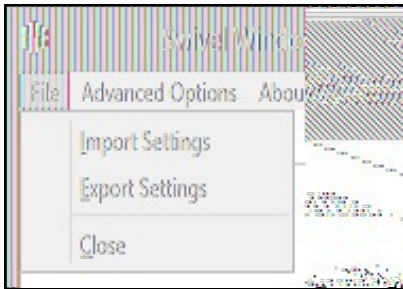
**Biometric Reader** The type of Biometric Reader: Nitgen or Native Laptop.

**If Swivel unavailable, Fail authentication** If the Swivel server cannot be contacted then authentication will fail.

**If Swivel unavailable, Use standard authentication** If the Swivel server is unavailable use standard authentication, the OTC field is displayed but ignored.

**If Swivel unavailable, Use offline authentication** If the Swivel server cannot be contacted a locally generated Turing image can be used for authentication. If this option is enabled, users will be able to force offline mode using a checkbox on the login dialog. (Only works for single channel authentication methods)

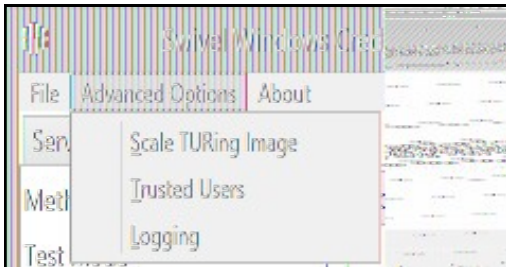
### 55.1.3 File menu



**Export Settings** Export settings as an XML file. These can be used to import settings elsewhere.

**Import Settings** Import settings from an XML file exported elsewhere.

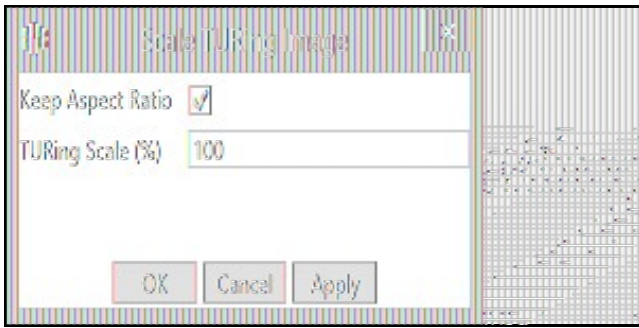
### 55.1.4 Advanced Options



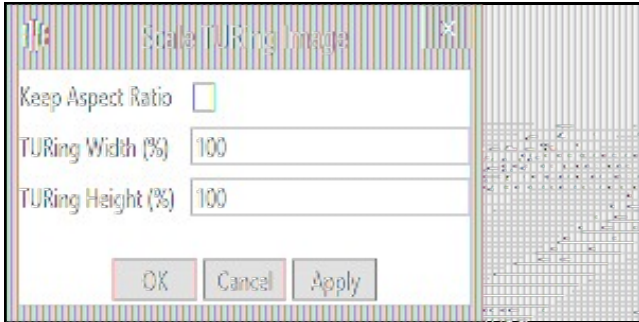
#### 55.1.4.1 Scale TURING Image

**Scale TURING Image...** Opens a dialog to let you scale the size of the TURING shown.

If **Keep Aspect Ratio** is selected then select the scale (%) of the TURING.

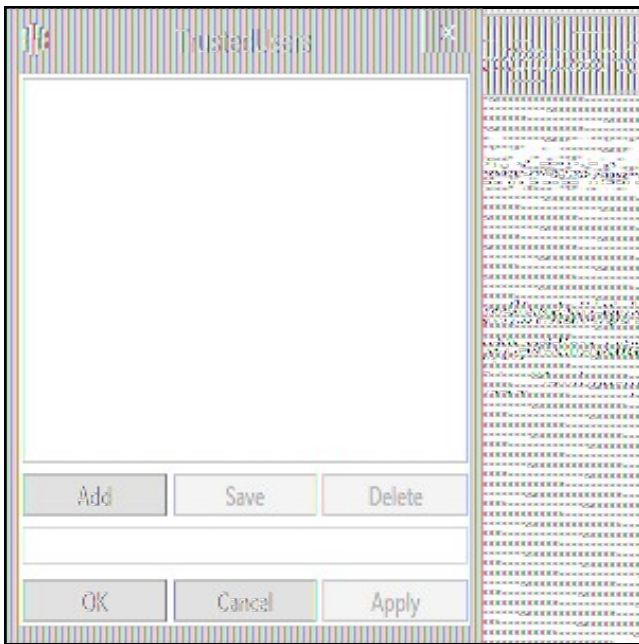


If its not selected then you can select the width and hight independently.



#### 55.1.4.2 Trusted Users

""Trusted Users"" Lets listed users Authenticate without Swivel.



To add a trusted user you must first click ""Add"" then enter the username in the text-box and click ""Save"", repeat these sets to add more users.

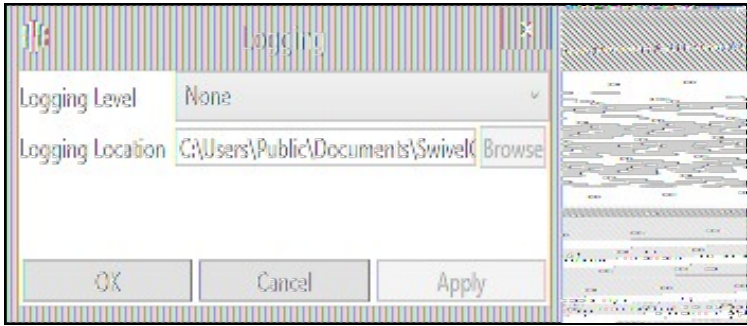
To edit a username select the username from the list, change the name in the text-box and click ""Save"".

To delete a username select the username from the list and press delete.

Make sure that the ""Apply"" or ""OK"" button to save these settings.

#### 55.1.4.3 Logging

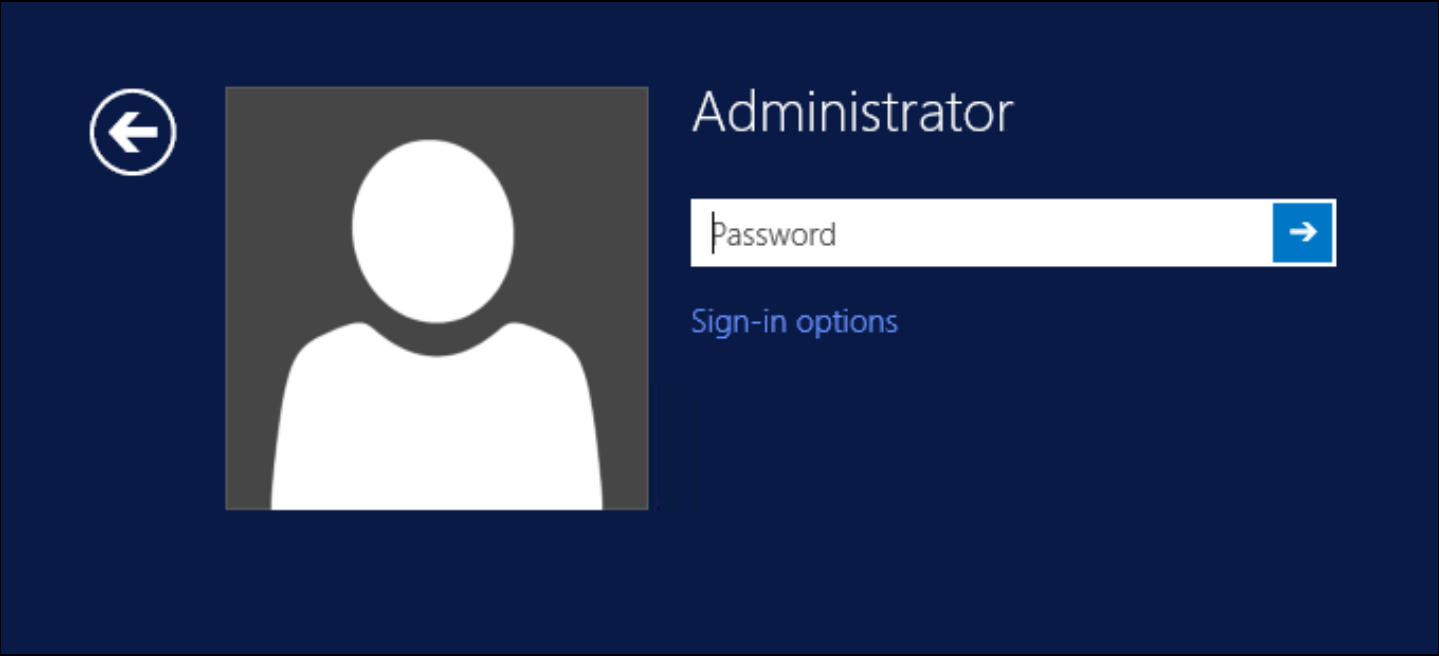
""Logging"" change settings relating to logging, recommended to be turned off unless problem are found.



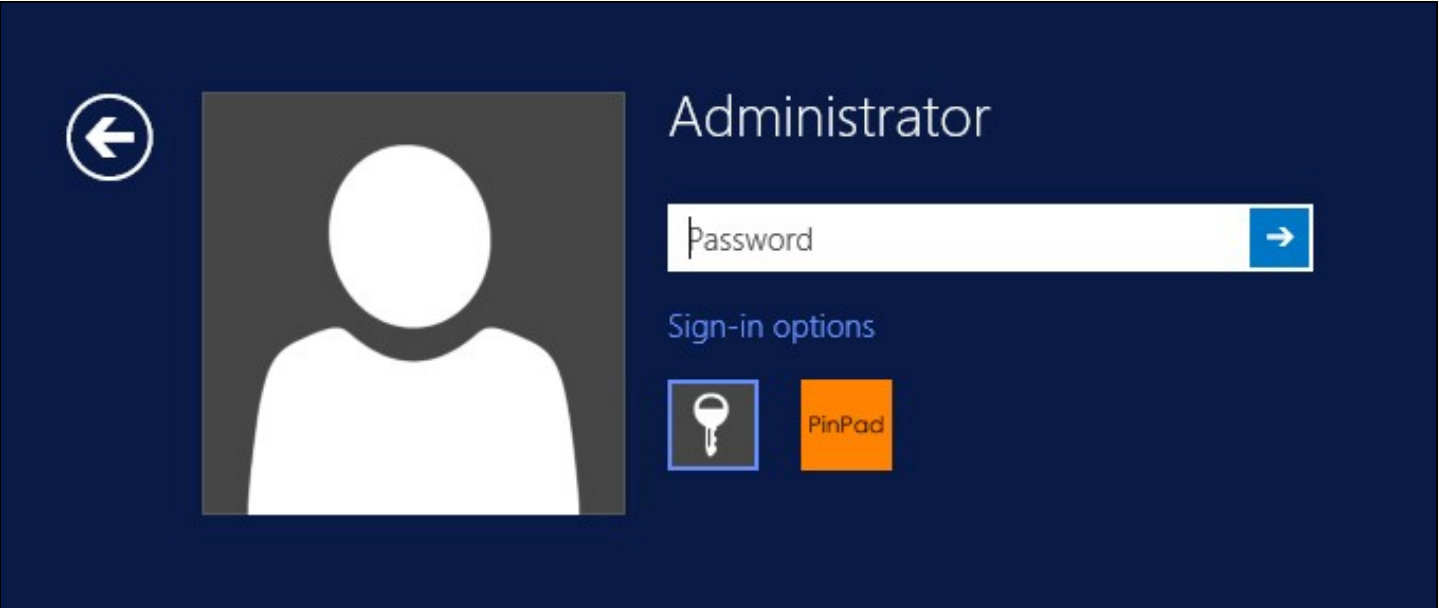
- ""Logging Level"" The account of message that will be logged.
- ""Logging Location"" The location the logs will be created, this must be somewhere any account has access to.

### 55.2 Test Mode

With Test Mode enabled the user will be able to select how they will authenticate



The **Sign-in options** button is shown to let users select from the list which method they would like to use.



The last successful authentication method will be selected by default when the credential is loaded.

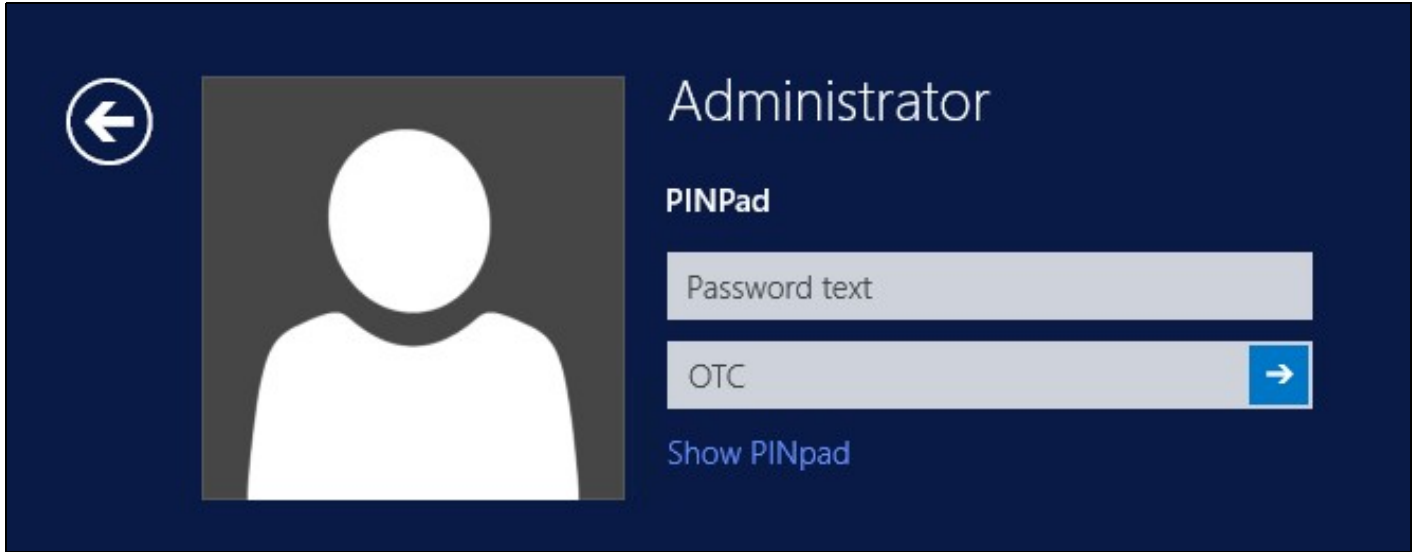
## 55.3 Importing Configurations

You can import credentials exported from other installations using the Import Settings menu item.

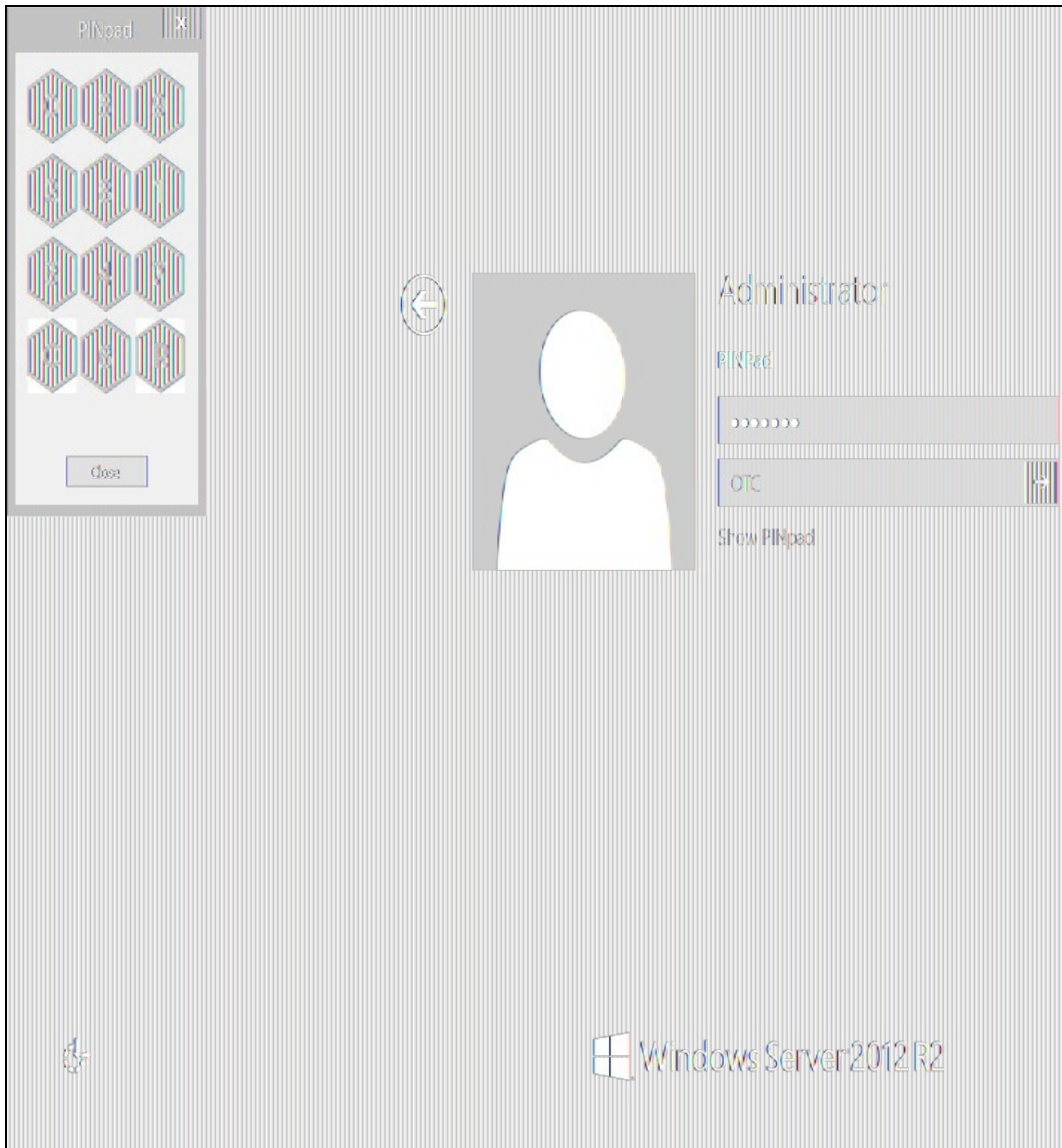
## 56 Verifying the Installation

This will be an example of one of the credentials.

At the windows login screen a password and OTC login field should be available with a "Show PINpad" Button.



Pressing the "Show PINpad" button will generate a PINpad image for authentication. The Swivel log should show a session request message: *Session started for user: username*.



A successful login should appear in the Swivel log: *Login successful for user: username.*

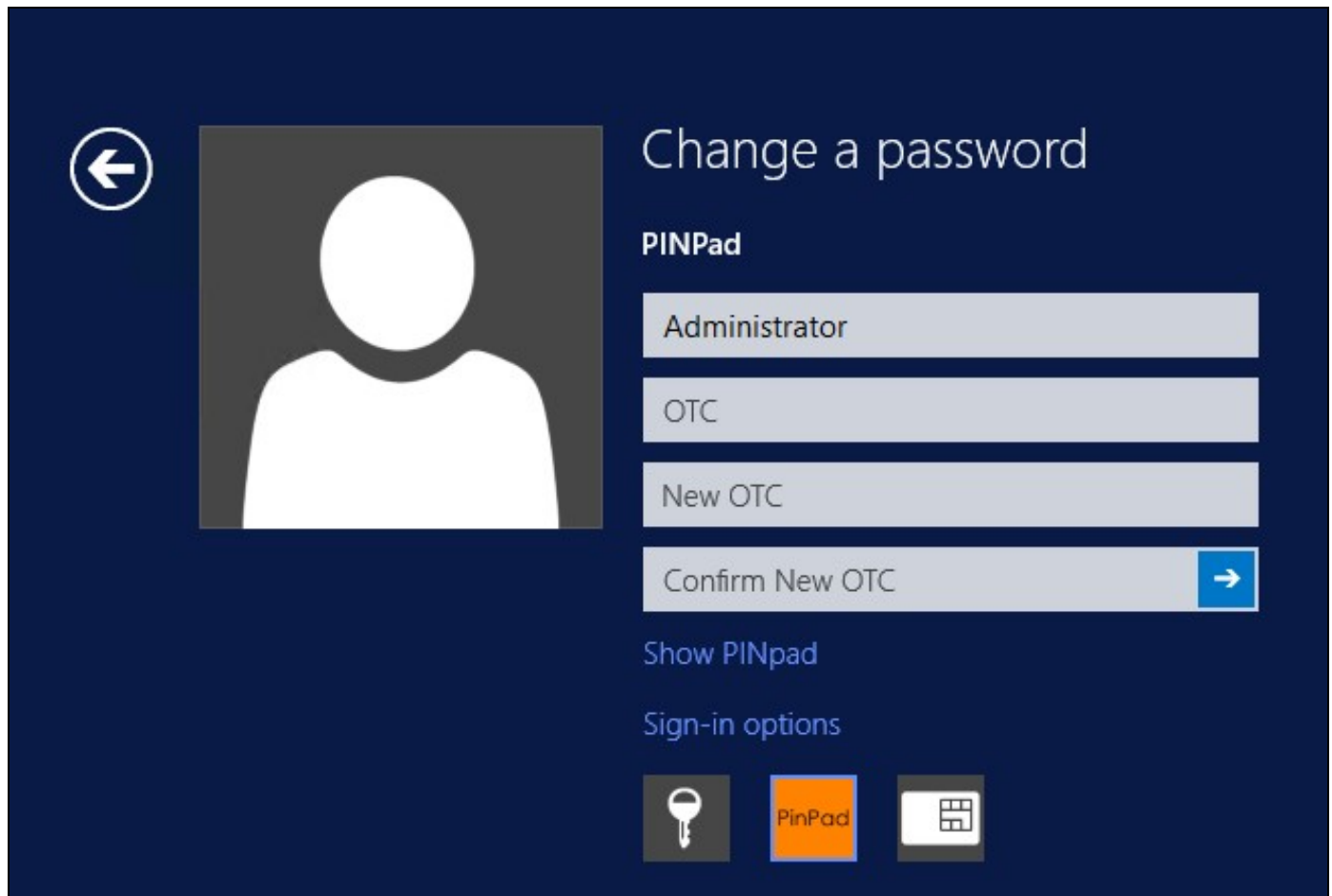
A failed login should not allow a login, and the following message should be displayed in the Swivel log: *Login failed for user: username.*

## 57 ChangePIN

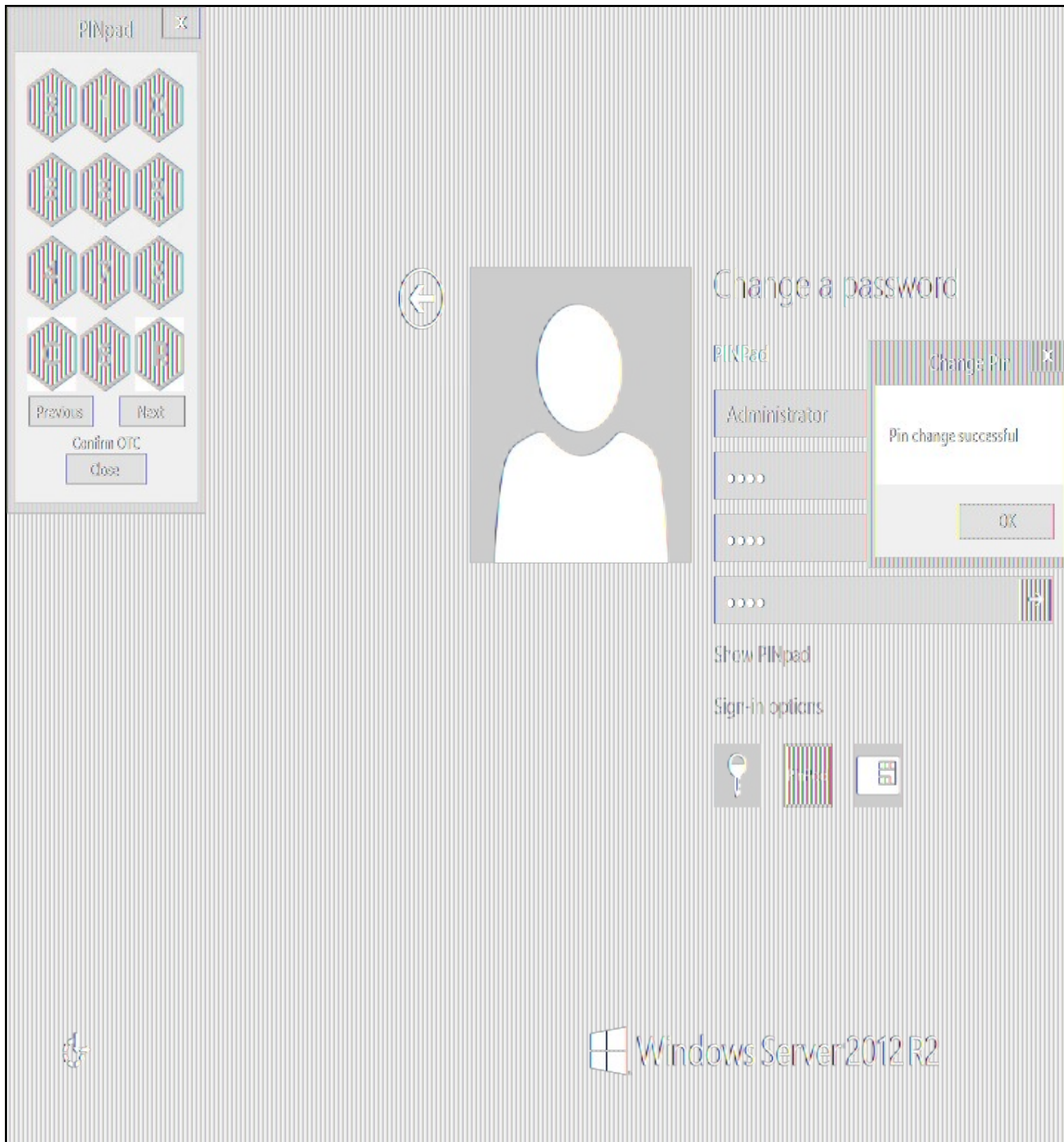
A user is usually able to change the password by using the Ctrl-Alt-Del keys (Ctrl-Alt-End for remote sessions). With the Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the "Sign-in options" button and selecting the Swivel credential. This will not function for Offline authentication.

With Swivel authentication a user never changes enters PIN and this is true for ChangePIN. A user enters their current OTC, and then enters an OTC for what they wish their new PIN to be. PIN enforcement may be in place to the Swivel server to prevent the choosing of poor PIN numbers.

A user may use a single channel image or a dual channel security string to change their PIN.



A successful Change PIN will show the message **Your PIN was changed successfully**, the Swivel server will also display in the logs a changePIN message **Change PIN successful for user: username**.



Other Changes to PINpad are that the PINpad dialog has buttons to select which text-box the numbers will be entered and text to show which text-box is currently selected.

## 58 Uninstalling the Swivel Integration

Use the Uninstall option from the Program menu, right click on the Windows Credentials provider and click on Uninstall. Note that uninstalling and reinstalling the Credential Provider will remove the settings, so if you need to reinstall at any point, make sure you have an exported settings file saved.

### 58.1 Disabling the Credential Provider

If the Credential Provider fails to load correctly it can be disabled using the following process:

Boot the machine into safe mode and log in as an administrator.

Try each of the following in turn. Only one of the following is required, so use the first one that works. Experience suggests that the first two options do not work in Windows 10.

- Run the Swivel Login Configuration and edit the settings to disable the provider.
- Uninstall the Credential Provider.
- Using regedit.exe add or alter the following registry values:
  - ◆ "HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}\Disabled=1"
  - ◆ "HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}\Disabled=1"
- Using regedit.exe remove the following registry keys:
  - ◆ "HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
  - ◆ "HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
  - ◆ "HKEY\_CLASSES\_ROOT\CLSID\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"

The third option disables the credential provider, whereas the others actually remove it.

### 58.2 Temporarily Disabling the Credential Provider Remotely

If there is a problem with the Swivel Secure appliance, and you need to disable the AuthControl Credential Provider on a number of machines temporarily, you can do this using a PowerShell script.

#### 58.2.1 Enabling Powershell Remoting

In order to be able to run PowerShell scripts on remote machines, you need to enable the WinRM service on both the target machines and the machine running the script. [This article](#) provides a step-by-step guide on setting up PowerShell remoting.

#### 58.2.2 Setting up a List of Computers

The first step is to get a list of computers that you want to disable. [This article](#) suggests three alternative methods: hard-code the list in your script, read it from a file, or query the Active Directory. The last is only useful if you want to run the script on every computer on your domain. We will use the second method in our example, so assume there is a list of computer names, one per line, in "CPComputers.txt". This also assumes that the list is in the directory from which you are running the script, so you might want to use a full path in your script.

#### 58.2.3 Setting up Credentials

For completeness, we will describe how to set up credentials to connect to the remote machines. If you are able simply to use the current logged-in user credentials on all remote PCs, then you can ignore this part.

To initialize a credential for use on the remote computers, use the following PowerShell command:

```
$cred = Get-Credential domain\adminuser
```

Replace "domain\adminuser" with the qualified name of the user whose credentials you will be using: note that you must include the domain. You will be prompted for the user's password.

If you are using the current user's credentials, leave off -Credential \$cred from the Enter-PSSession command below.

#### 58.2.4 The Script

Here is an example script for disabling the Credential Provider on a number of remote computers:

```
$cred = Get-Credential domain\adminuser
$computers = Get-Content -Path ".\CPComputers.txt"
foreach ($pc in $computers) {
    Enter-PSSession -ComputerName $pc -Credential $cred
    $filterPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
    if (Test-Path $filterPath) { Set-ItemProperty -Path $filterPath -Name Disabled -Value 1 }
    $credPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
    if (Test-Path $credPath) { Set-ItemProperty -Path $credPath -Name Disabled -Value 1 }
    Exit-PSSession
}
```

#### 58.2.5 Known Limitations

Be aware that running this script may not immediately disable the Credential Provider. You may need to wait a few minutes, or restart the computer, for the change to take effect.

#### 58.2.6 Re-enabling the Credential Provider

To re-enable the Credential Provider, use the same script, but change the Disabled Value to 0 in two lines. So the script between Enter-PSSession and Exit-PSSession becomes

```
$filterPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
```

```
if (Test-Path $filterPath) { Set-ItemProperty -Path $filterPath -Name Disabled -Value 0 }
$credPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
if (Test-Path $credPath) { Set-ItemProperty -Path $credPath -Name Disabled -Value 0 }
```

## 59 Known Issues and Limitations

- The Swivel Windows Credential Provider does not support the use of Animated gifs for Single Channel authentication.
- It has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name for the Swivel server.
- Local (offline) authentication only works in single channel and OATH modes: the dual channel strings are not available offline.
- If the user gets an online TURING with a different scale then gets an offline TURING, the TURING is broken, the fix is to close the dialog and request an new TURING.
- If **Allow Unknown Users Offline** is enabled then users that have not previously authenticated to Swivel online can bypass Swivel by checking the offline box and authenticating with AD only.
- On Windows server 2012 R2 there is an update from Microsoft to fix an issue where dialogues will not be displayed, please ensure that windows update 2919355 is installed.
- Local authentication does not know if a users PIN has expired or even if the account is locked or deleted. Once a user has successfully authenticated they are allowed offline until their offline strings are deleted or the offline option is deselected.

## 60 Windows Credential Provider with RBA

## 61 Introduction

From AuthControl Sentry v4.0.5, you can use your RBA rules with AuthControl Credential Provider to disable 2fa in case the user has enough points.

## 62 Prerequisites

AuthControl Credential Provider v5.4.2

AuthControl Sentry v4.0.5

## 63 Limitations

Certificate rule does not work with WCP

# 64 RBA Configuration

In AuthControl Sentry SSO administration page you have a new application type WCP. Add a new application.

Start Page

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

Application Types

RADIUS VPN - Cisco ASA

RADIUS VPN - Citrix Netscaler

RADIUS VPN - Juniper

RADIUS VPN - Other

SAML - ADFS

WCP

Select WCP.

Start Page

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

# Windows Credential Provider Ap

i

Note: The Endpoint URL is used only if it is n

Name

Windows Credential Provider

Image

Windows.png

Points

100

Entity ID

wcp

Enter a name, the required points for authentication without 2fa, **the entity ID must be wcp** and click Save.

If you haven't configure any rules, please look at [Authcontrol v4 Sentry SSO and Adaptive Authentication](#).

## 65 WCP Configuration

Open AuthControl Credential Provider Configuration

AuthControl Credential Provider Configuration

File Advanced Options About

Server Authentication

Swivel Server

Swivel Port 8080

Swivel Context pinsafe

Swivel Secret

Swivel SSO Port

Swivel SSO Context

SSL ☐ Ignore certificate errors ☒

Security Protocol:

TLS1.2 ☐

TLS1.1 ☐

TLS1.0 ☐

SSL3 ☐

One Touch Timeout 60

Test Connection

OK Cancel Apply

enter the Swivel SSO Port as 8443 and Swivel SSO Context as sentry. This will enable the check for RBA rules in WCP.

## 66 Authenticating

When you try to login now it will check for the rules. If the user has enough points, it will allow authentication without using 2fa.

## 67 RBA with fingerprint

If you have Biometric Identification active, you can use this to give more points to RBA and disable 2fa.