

# Swivel Windows Credential Provider

## Contents

- 1 Introduction
  - ◆ 1.1 Downloads
  - ◆ 1.2 Swivel Credential Provider FAQ
- 2 Prerequisites
- 3 Baseline
- 4 Installation
  - ◆ 4.1 Basic Installation
  - ◆ 4.2 Multiple Installation
- 5 Architecture
  - ◆ 5.1 Offline Authentication
- 6 Swivel Integration Configuration
  - ◆ 6.1 Configure a Swivel Agent
  - ◆ 6.2 Configure Single Channel Access
  - ◆ 6.3 Create a Third Party Authentication
- 7 Microsoft Windows Swivel Credential Provider Installation
  - ◆ 7.1 Windows Swivel Credential Provider configuration
    - ◇ 7.1.1 Server
    - ◇ 7.1.2 Authentication
    - ◇ 7.1.3 File menu
    - ◇ 7.1.4 Advanced Options
      - 7.1.4.1 Scale TURING Image
      - 7.1.4.2 Trusted Users
      - 7.1.4.3 Logging
  - ◆ 7.2 Test Mode
  - ◆ 7.3 Importing Configurations
- 8 Verifying the Installation
- 9 ChangePIN
- 10 Uninstalling the Swivel Integration
  - ◆ 10.1 Disabling the Credential Provider
- 11 Known Issues and Limitations

## 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 This documentation is out of date, and is not being maintained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.

## Downloads

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

## 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.

## 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.

## Baseline

Swivel 3.10.4

Windows 8, 10, Server 2012 R2.

## Installation

### 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.

### 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.

## 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.

### 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.

## Swivel Integration Configuration

### 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.

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"/>

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

## 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"/>	

## 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.

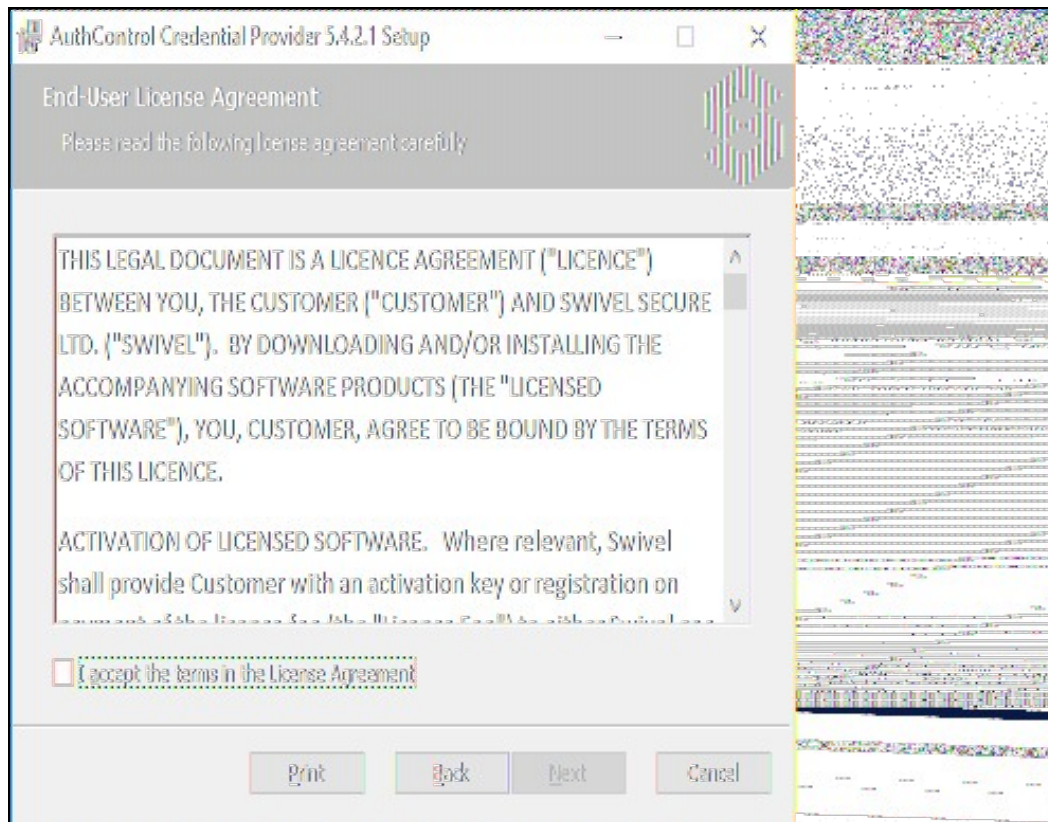
Identifier:	WindowsGINA
Class:	com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA
License key:	
Group:	PINsafeUsers ▼

## 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 msiexec command.

The first page is the licence agreement:

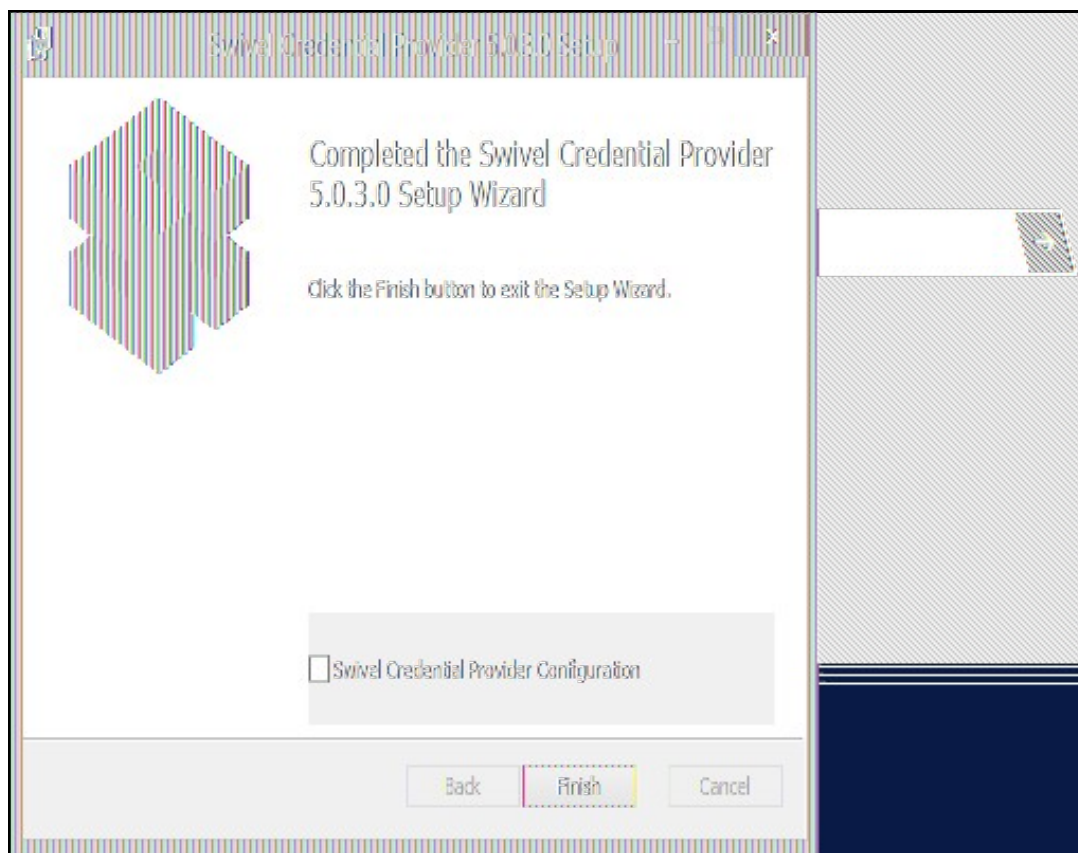


Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

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.

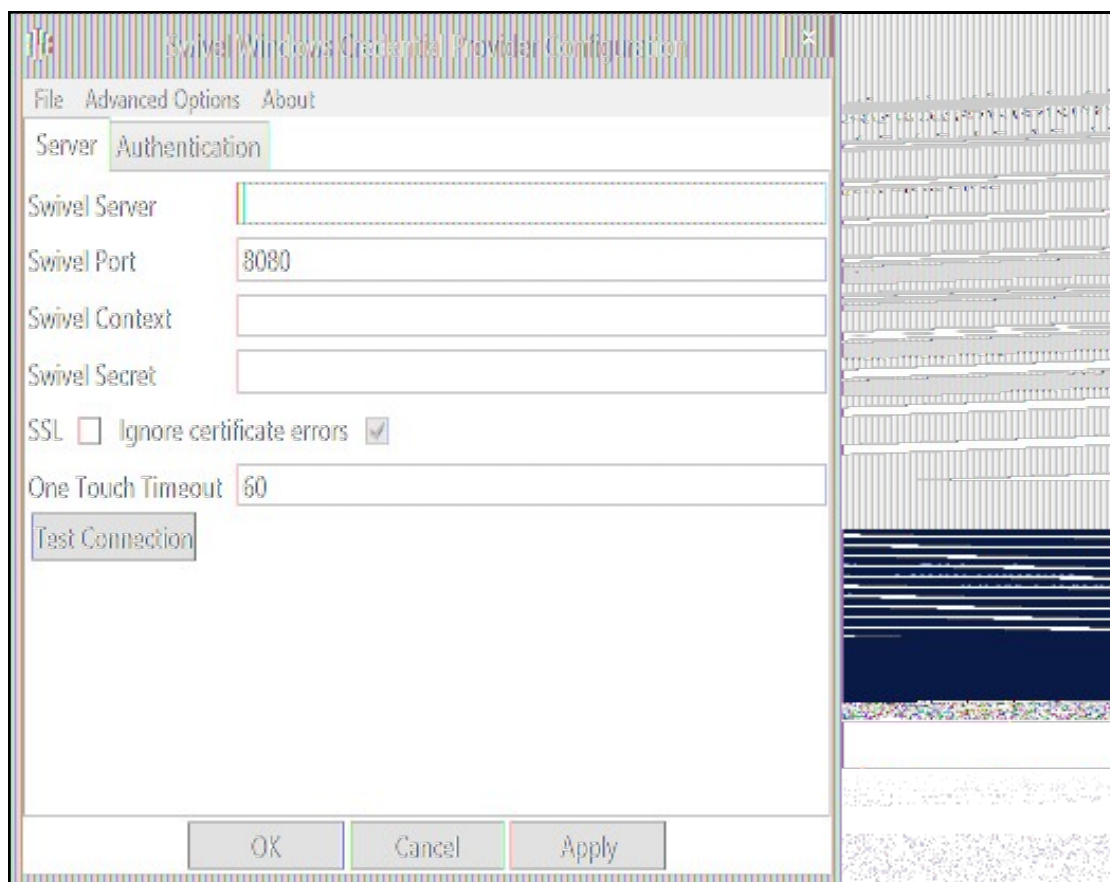
When the install has completed, the following dialog is shown:





## Windows Swivel Credential Provider configuration

### 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.

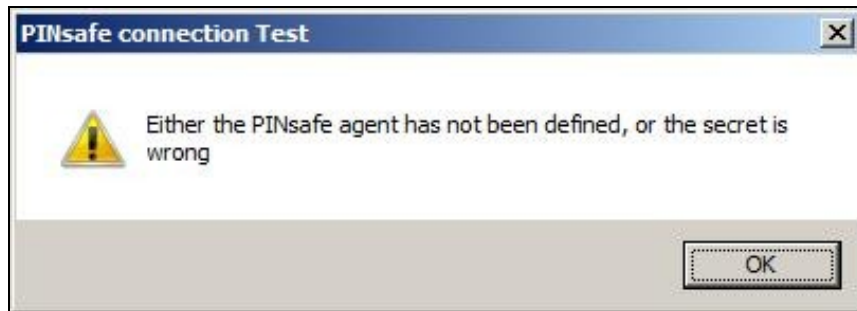
**Use SSL** The Swivel server or virtual or hardware appliance uses SSL communications.

**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.

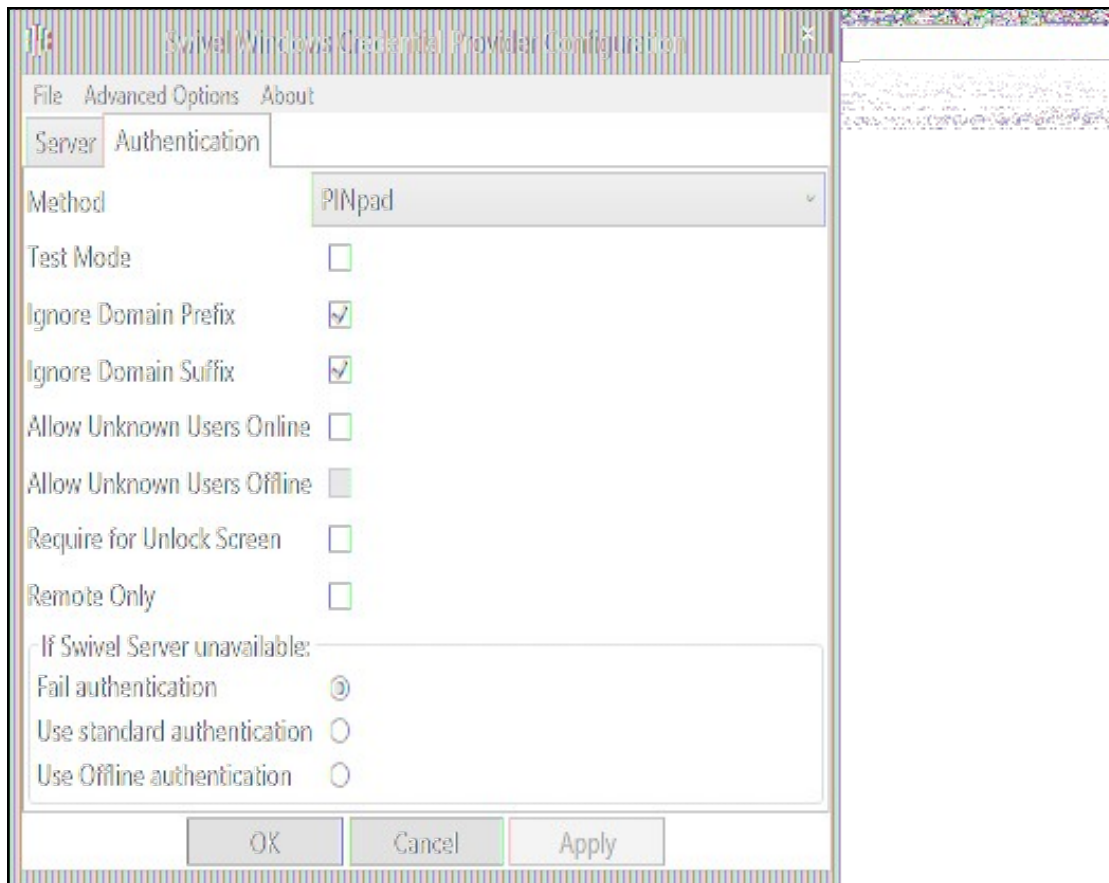
**Test Connection** Tests link to Swivel server. A correct configuration should produce a dialogue box with **Swivel Connection settings are correct.**



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.



## 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.

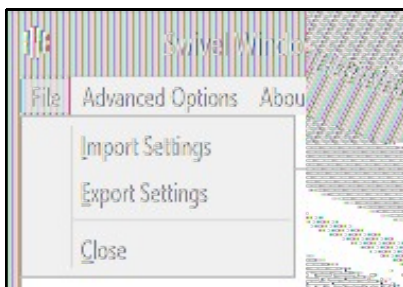
**Remote Only** The selected authentication method will only be shown for users logging into the machine remotely.

**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)

## File menu

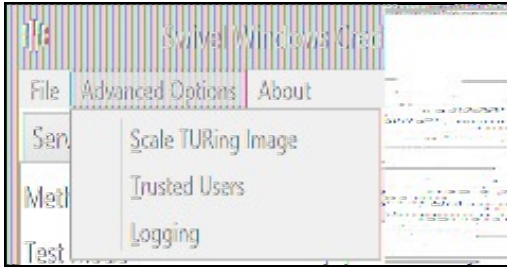


**Export Settings** Export settings as an XML file. These can be used to import settings elsewhere.

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



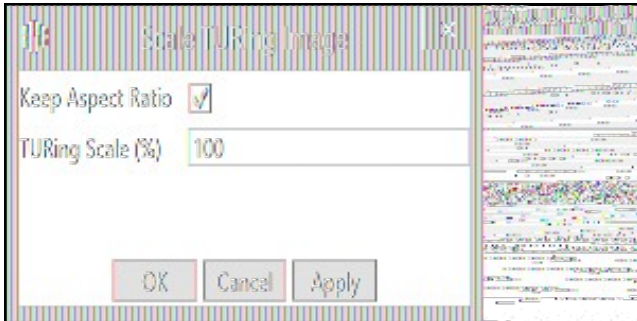
## Advanced Options



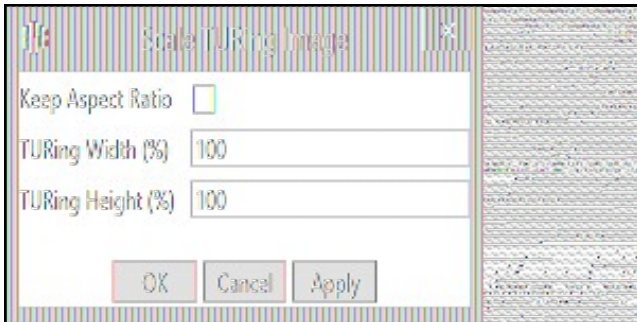
### Scale TURING Image

**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.

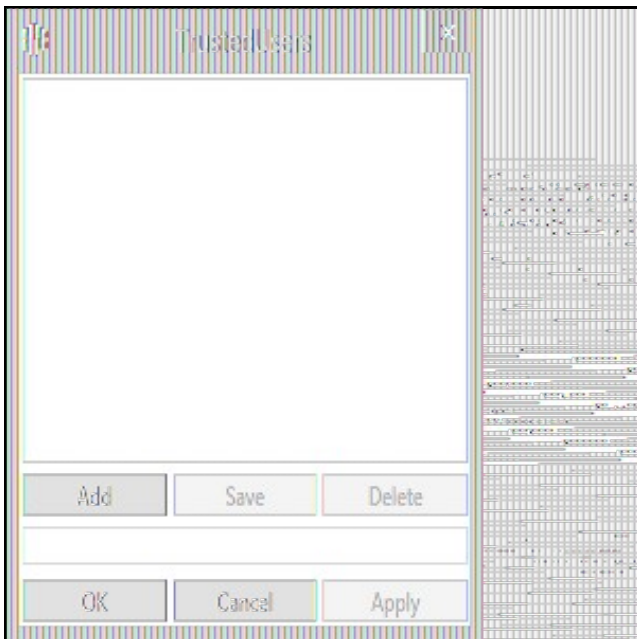


If its not selected then you can select the width and hight independently.



### 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.

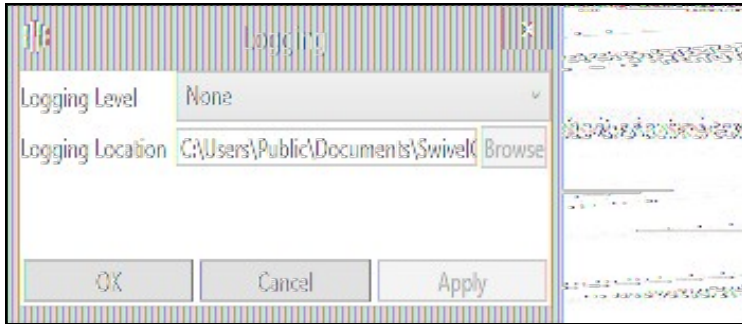
To edit a username select the username from the list, change the name in the text-box and click ""Save"".

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.

## Logging

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

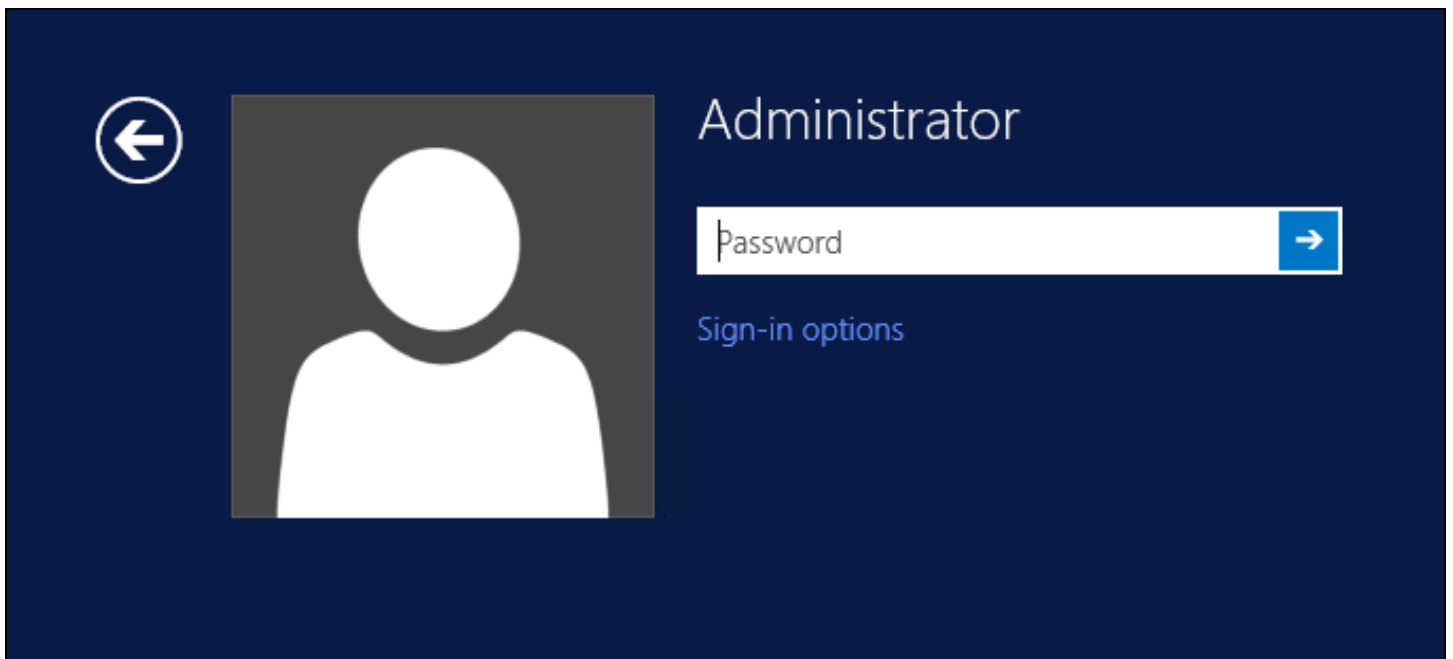


""Logging Level"" The account of message that will be logged.

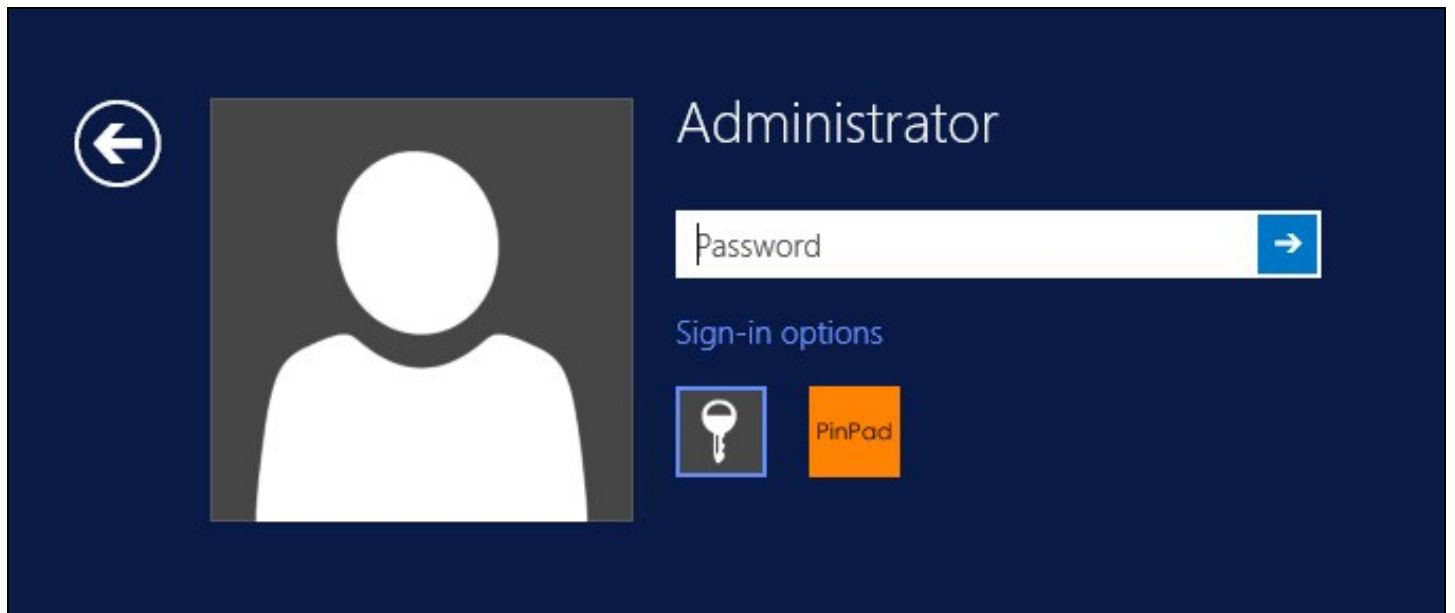
""Logging Location"" The location the logs will be created, this must be somewhere any account has access to.

## 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.

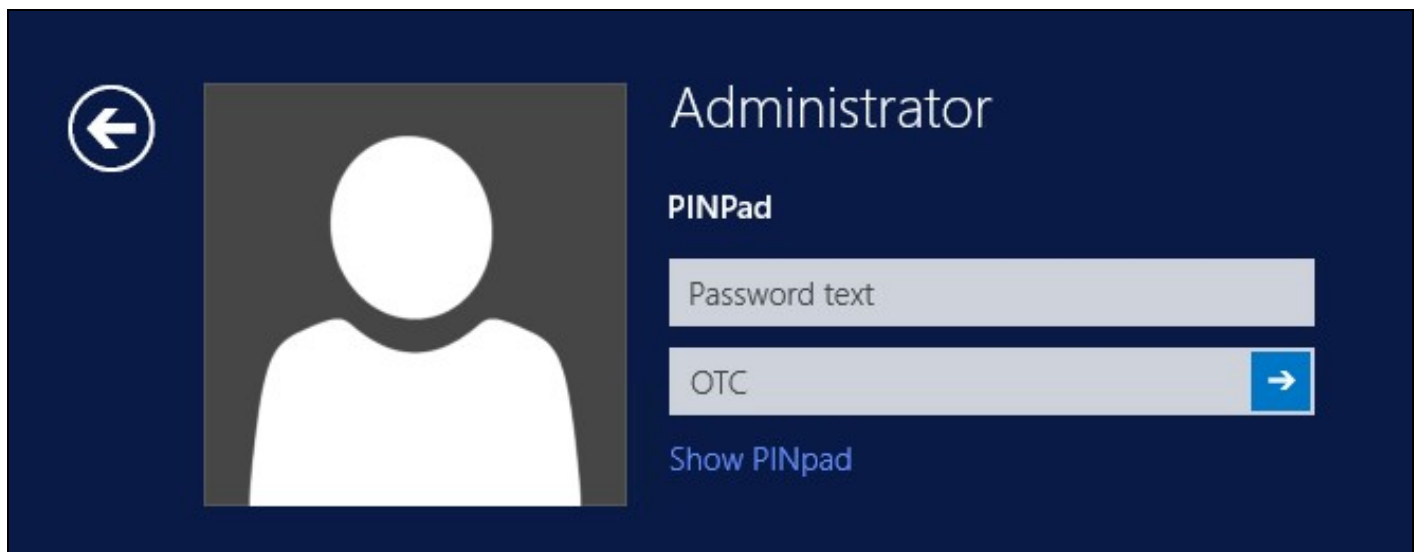
## Importing Configurations

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

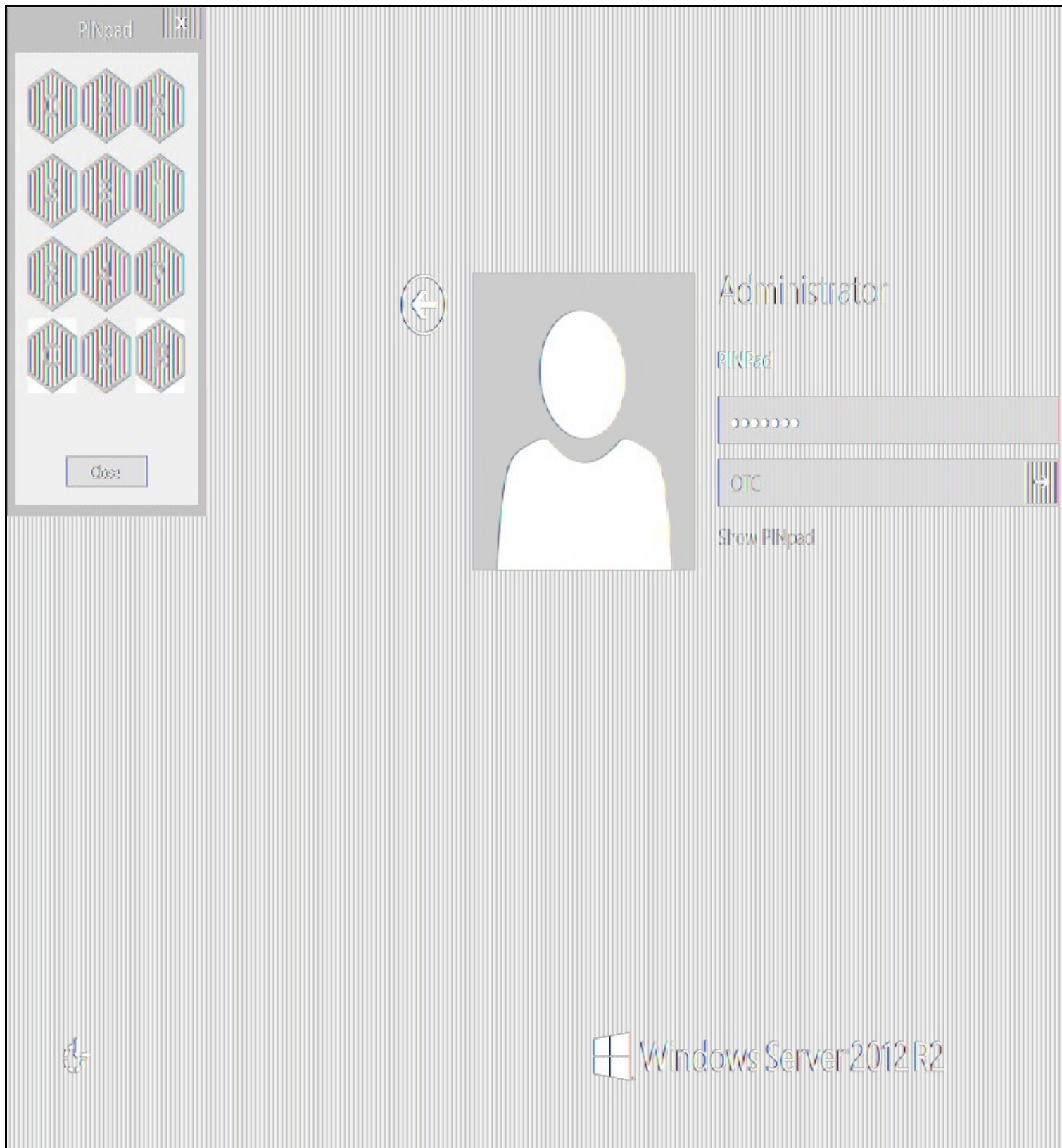
## Verifying the Installation

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.*

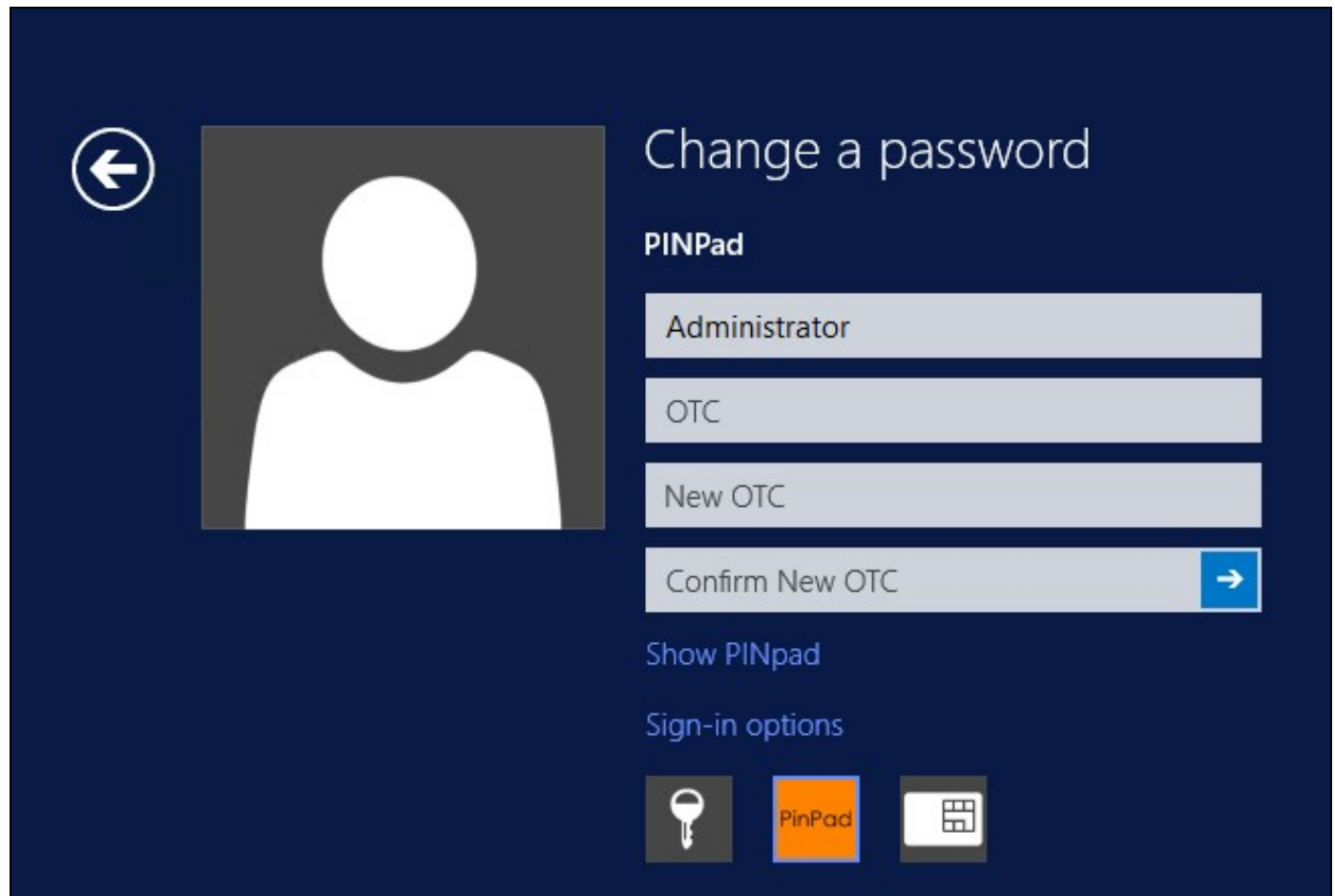
A failed login should not allow a login, and the following message should be displayed in the Swivel log: *Login failed for user: username.*

## 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.



Change a password

**PINPad**

Administrator

OTC

New OTC

Confirm New OTC →

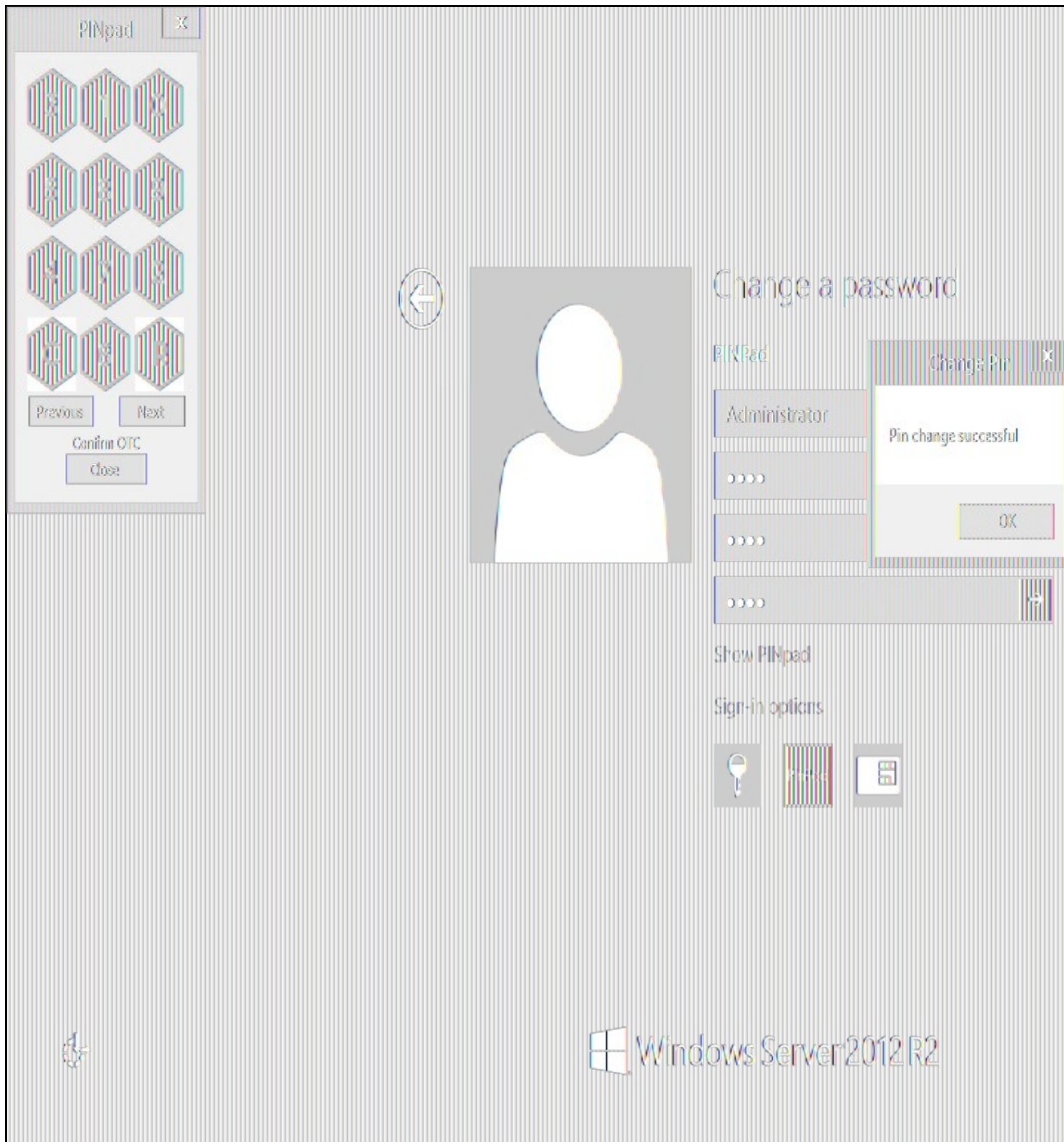
[Show PINpad](#)

[Sign-in options](#)

Key icon, PinPad icon, Security card icon

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.

## 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.

## 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}"

## 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.