Windows Credential Provider

Contents

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.

Downloads

Latest Release Versions:

Swivel AuthControl Desktop 64-bit version MSI 5.7.42.1 NOTE: this is the latest release. Documentation has not yet been updated to reflect the changes in this 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 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

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.
```

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.

Baseline

Swivel 3.11.3

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

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 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.

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.

Release Notes

AuthControl Desktop 5.7

New Features

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

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.

Proxy for Sentry connections

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

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.

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.

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.

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?.

Bug Fixes / Improvements

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.

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.

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.

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.

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.

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.

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.

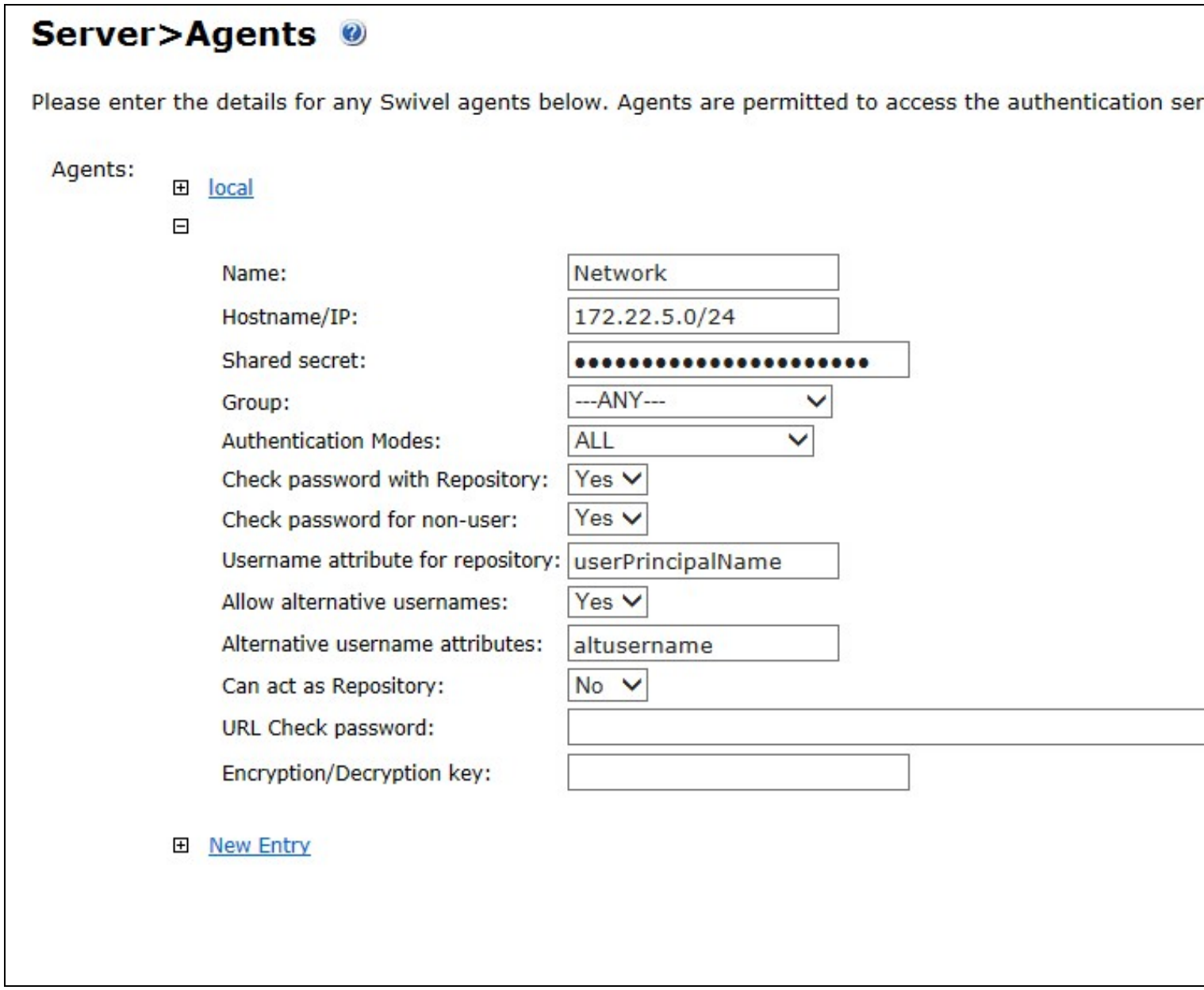
Offline Authentication

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.

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 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.

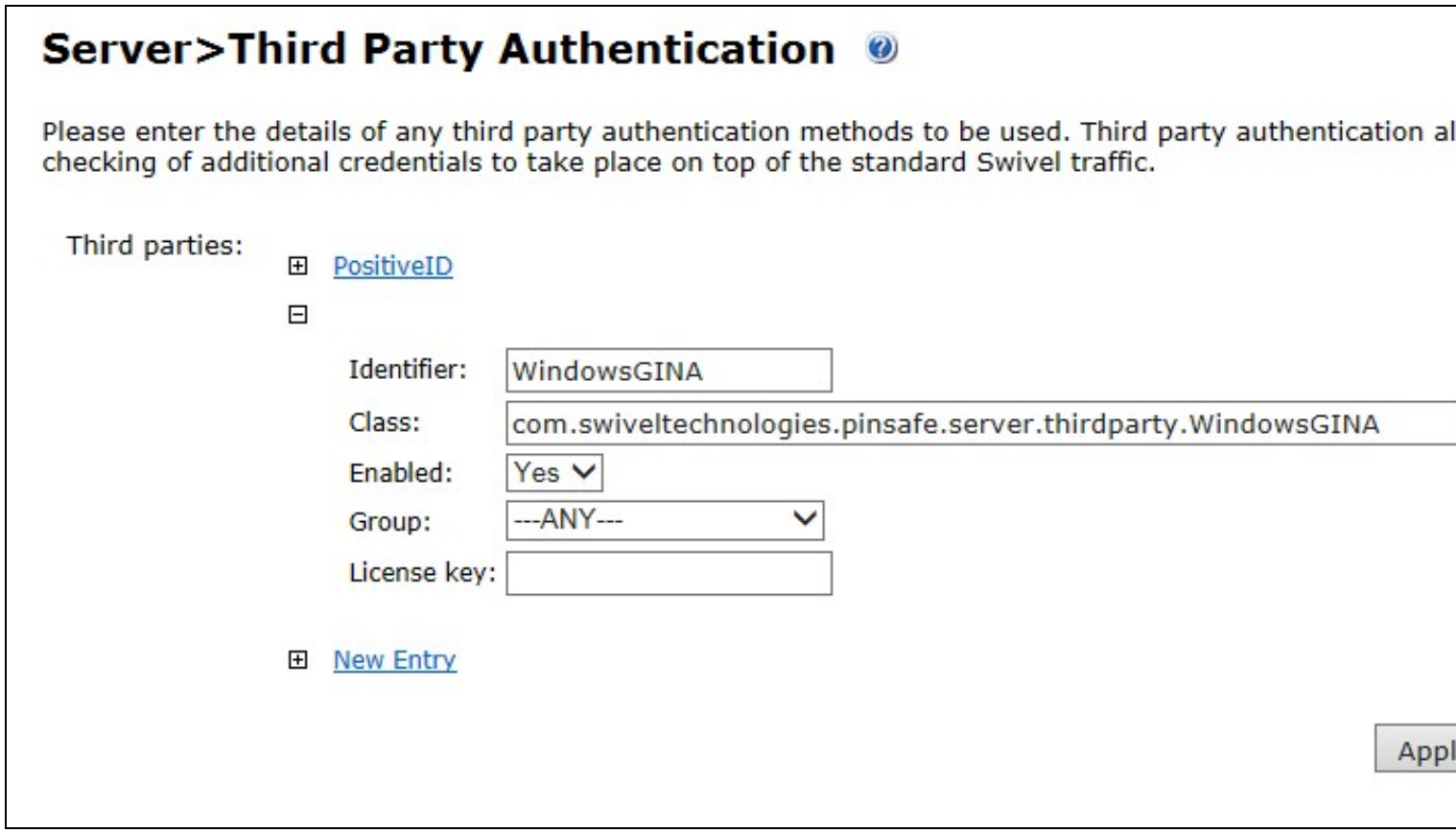


Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

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.

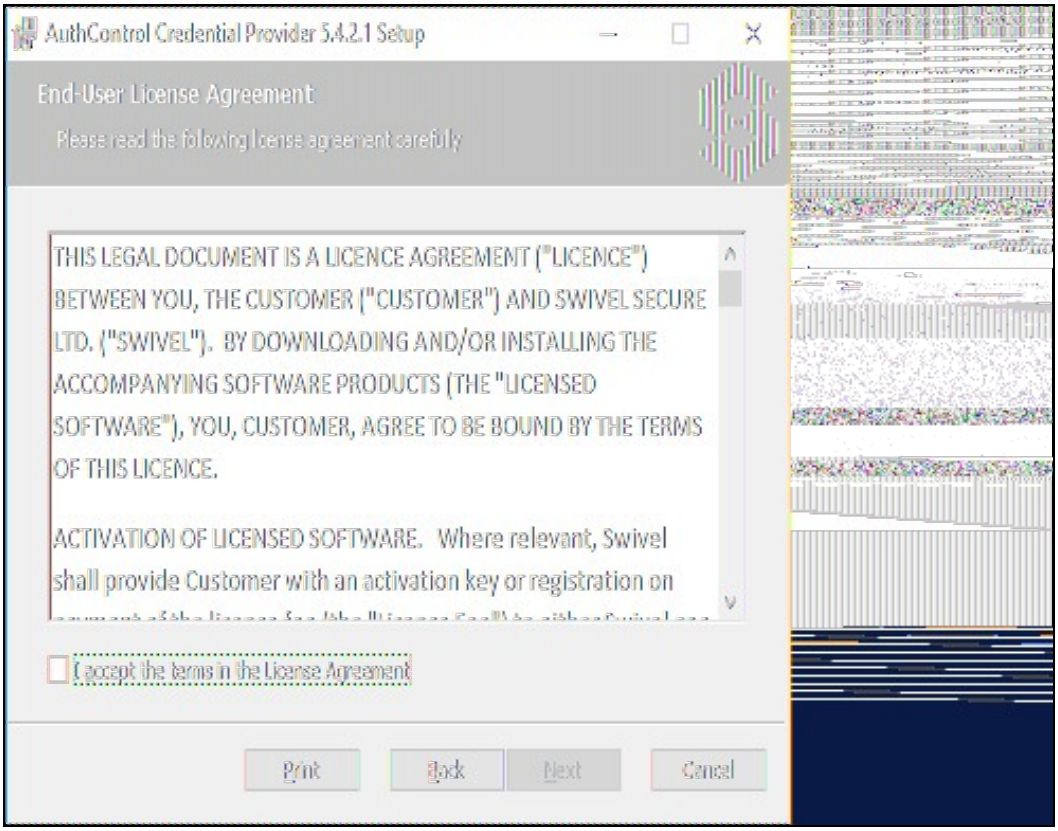


Microsoft Windows AuthControl Credential Provider Installation

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 msiexec command.

The first page is the licence agreement:

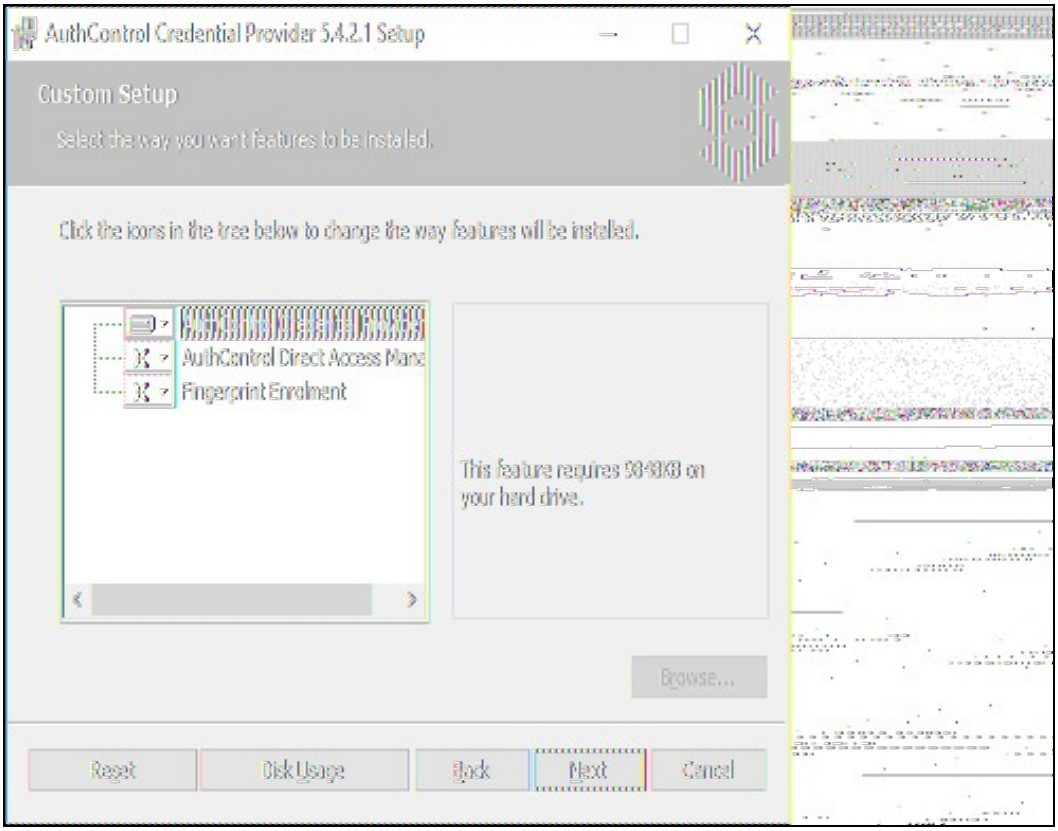


Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

Select the neccessary addons:

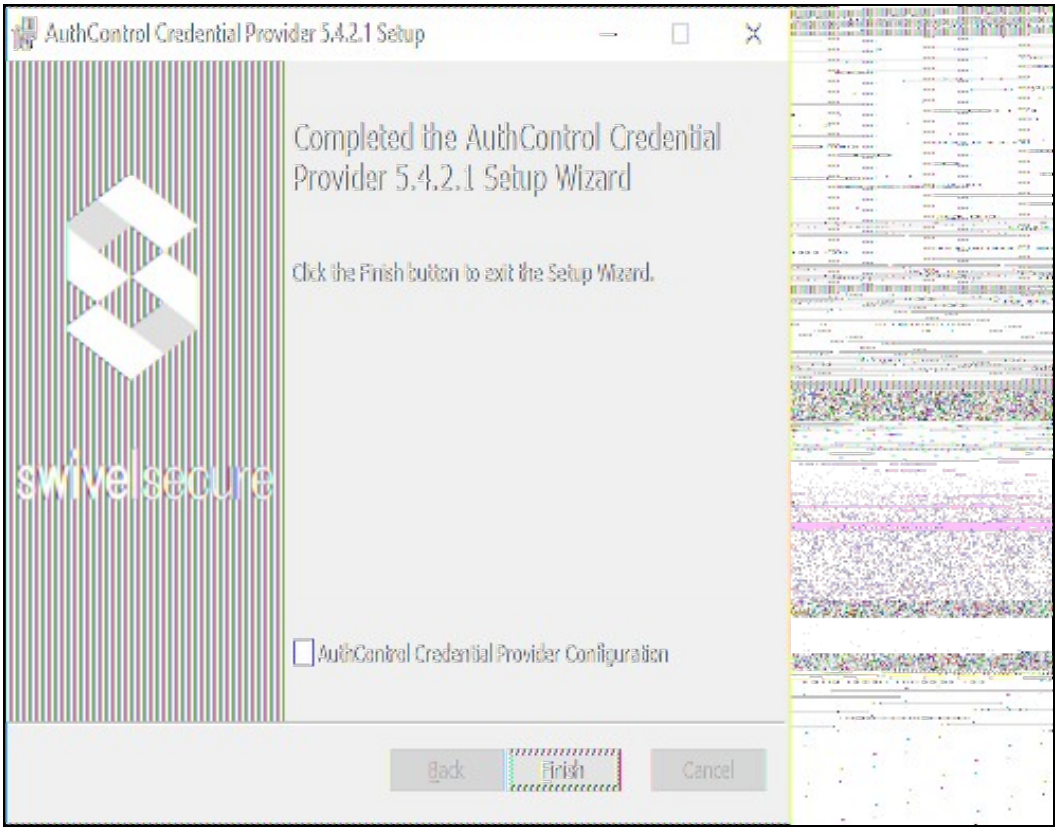
AuthControl Direct Access Manager - for integration with Direct Access

Fingerprint Enrolment - for Biometric Fingerprint enrolment and use Biometric authentication



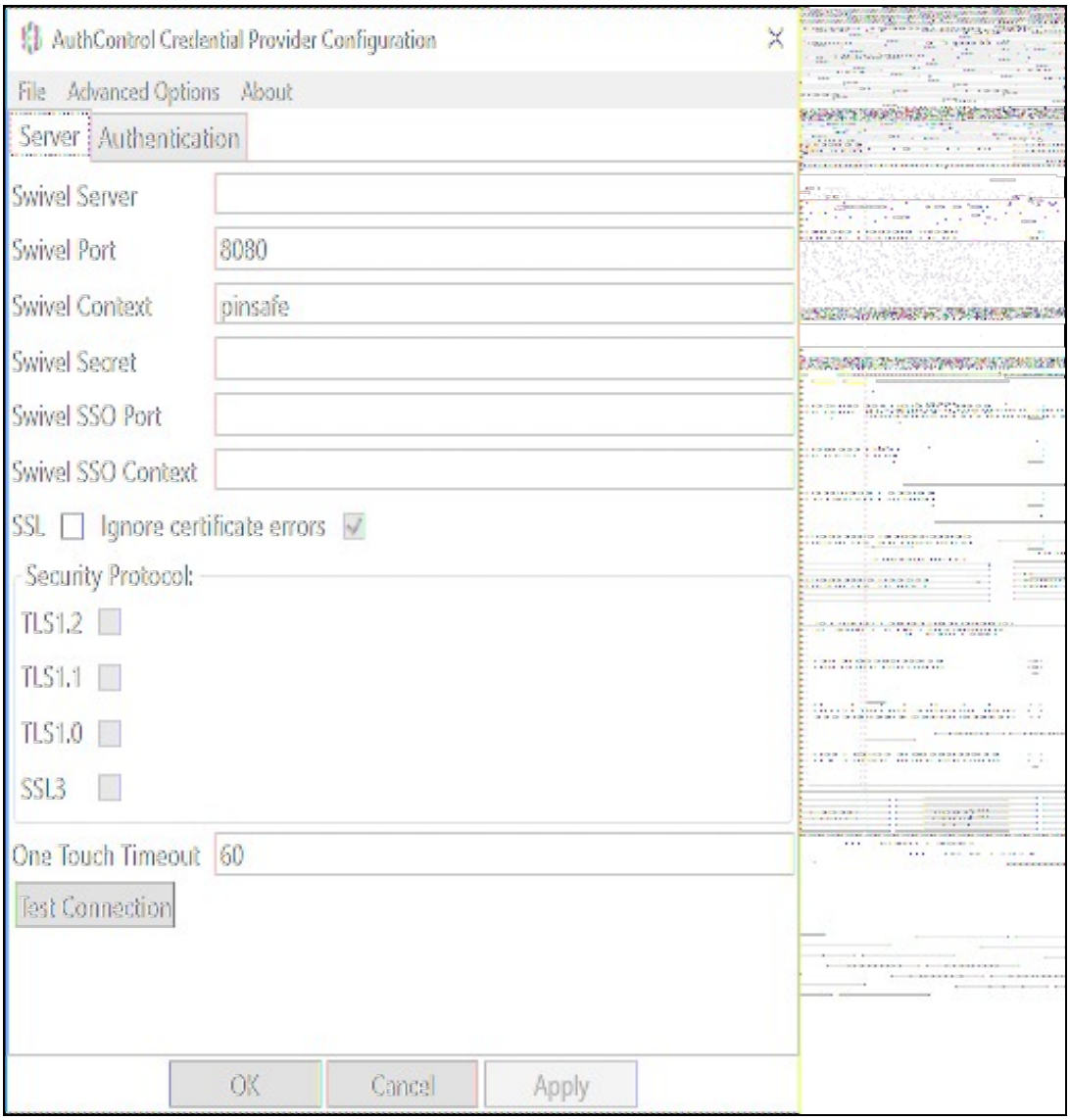
The application will be installed to C:\Program Files\Swivel Secure\Swivel Credential Provider. If you have reconfigured the program files directory elsewhere, it will be installed there, but otherwise you cannot control where the application is installed.

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



AuthControl 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.

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

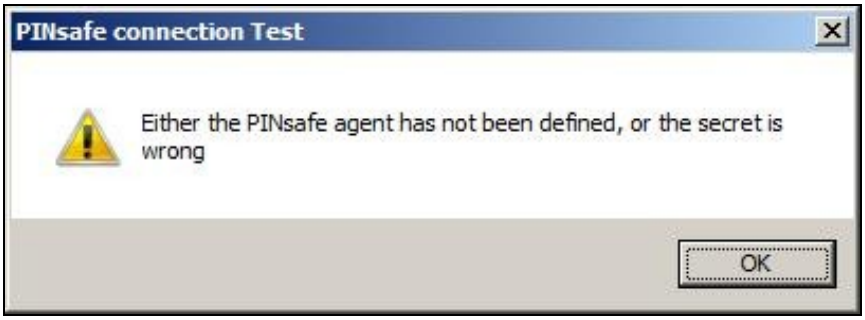
SSO Context: (Sentry v4.0.5 required) The AuthControl Sentry SSO context to allow RBA usage. (ex: sentry)

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

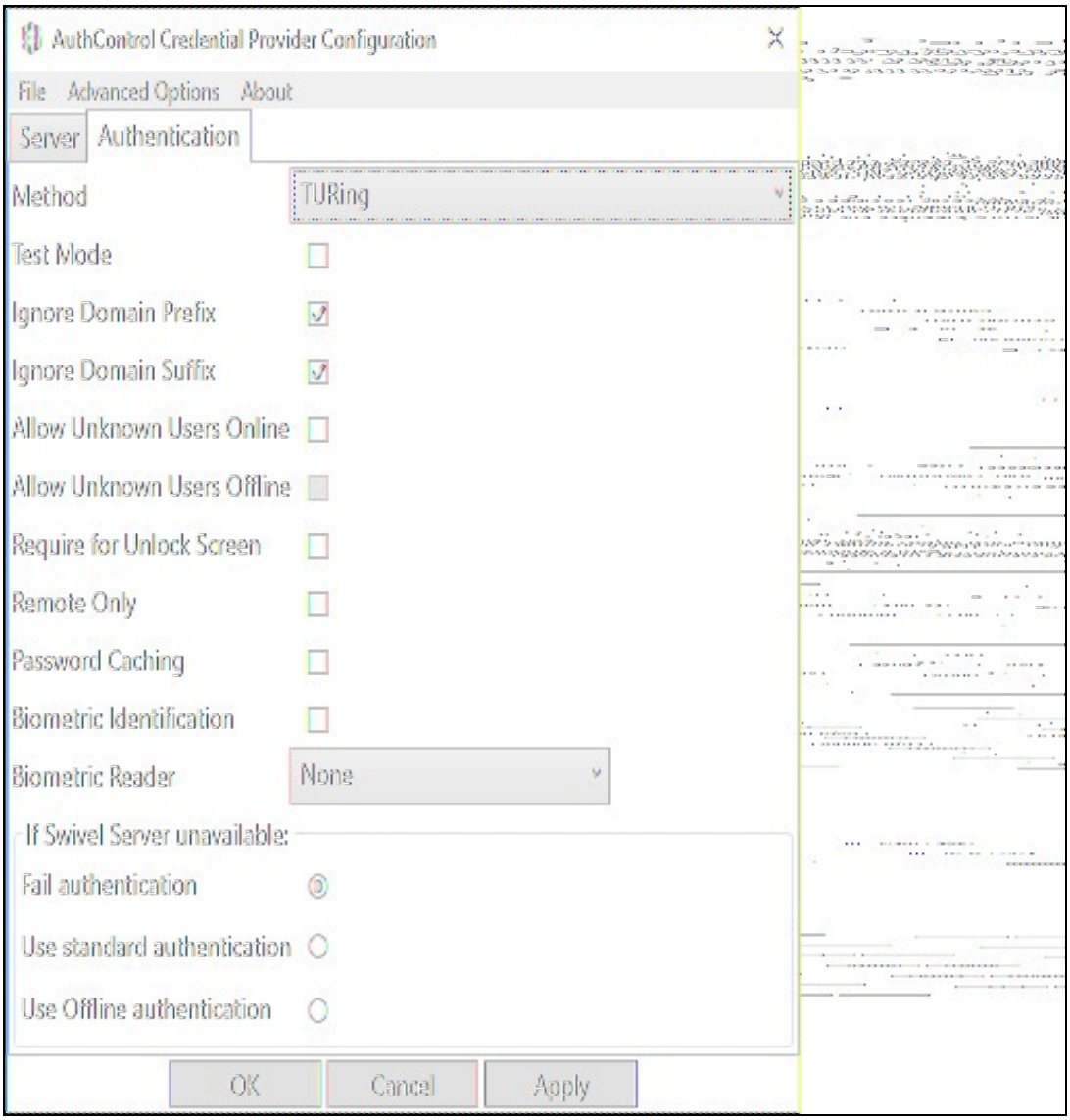
Accept self signed SSL certificates Check this box if Use SSL is enabled, and you do not have a commercial certificate on your Swivel server (or a certificate signed by an authority that the client machine trusts). You should also check this box if you are using IP address rather than host name, as recommended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



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.

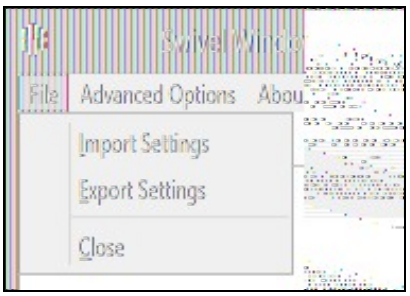
Biometric Reader The type of Biometric Reader: Nitgen or Native Laptop.

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)

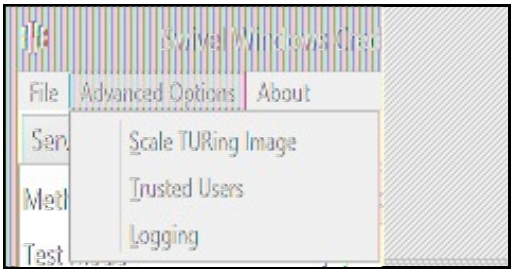
File menu



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.

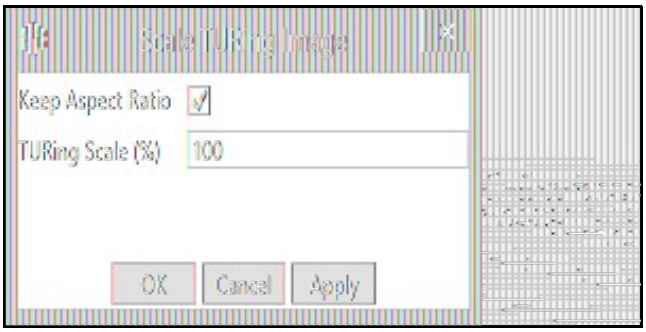
Advanced Options



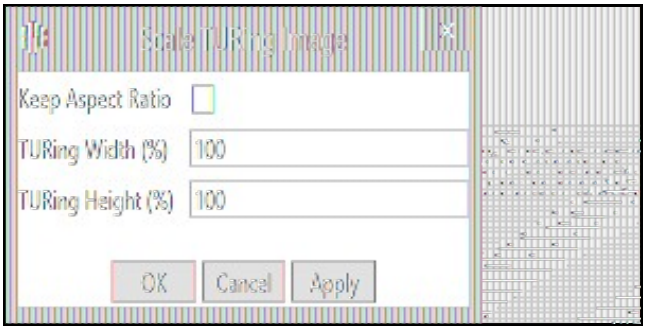
Scale TURing Image

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.

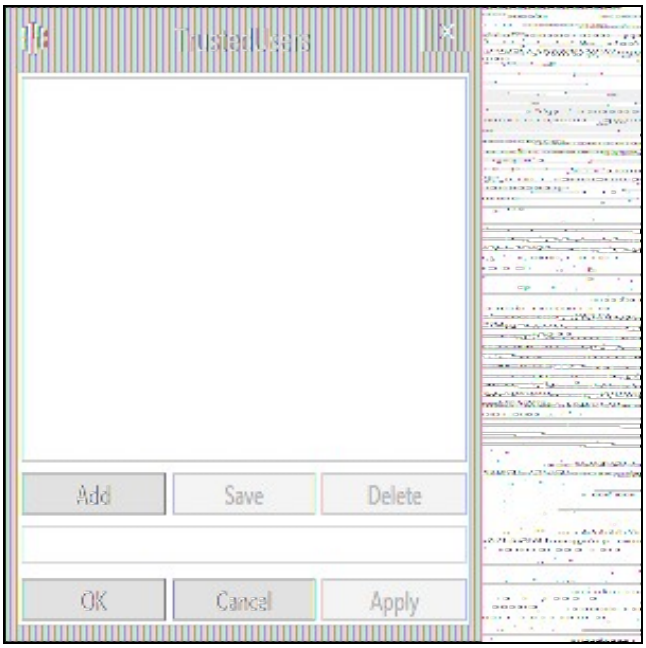


If its not selected then you can select the width and hight independently.



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.

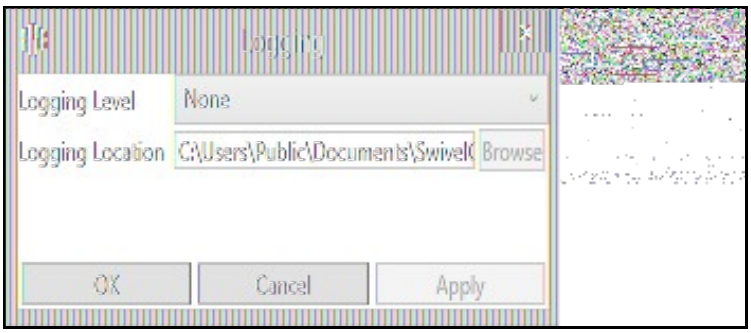
To edit a username select the username from the list, change the name in the text-box and click ""Save"".

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.

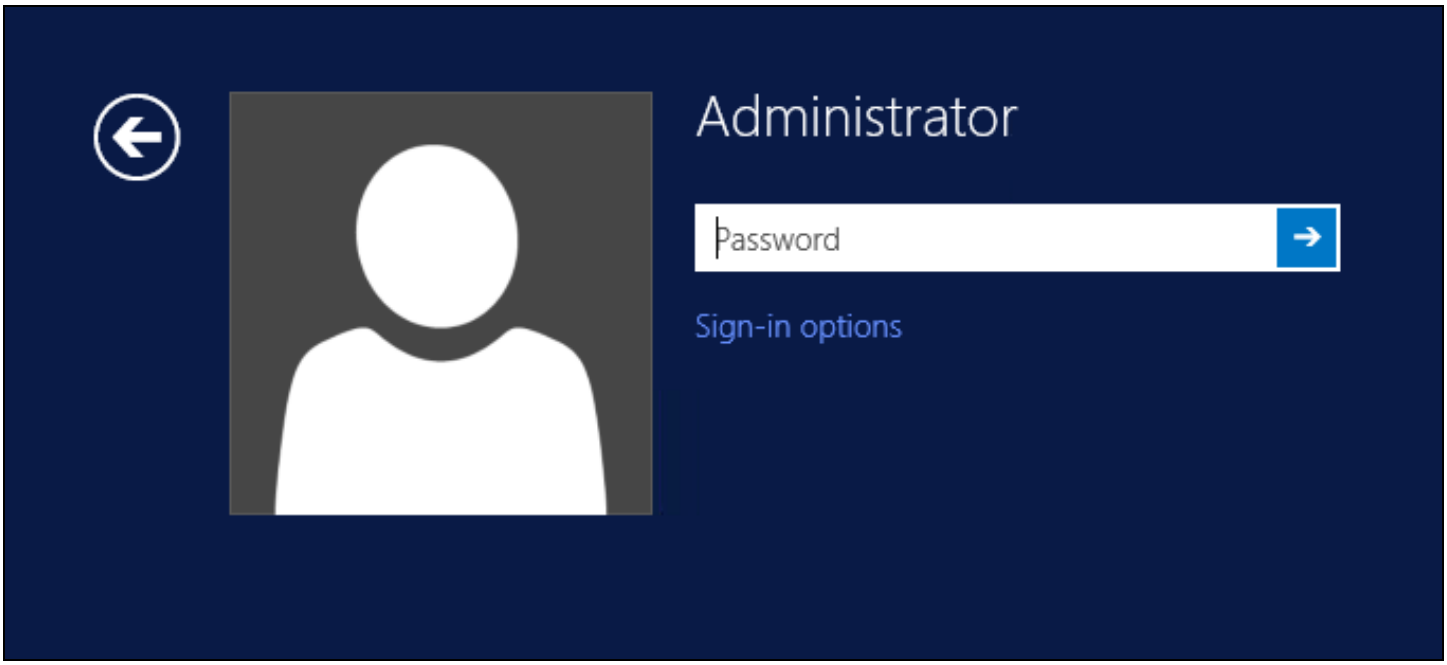


""Logging Level"" The account of message that will be logged.

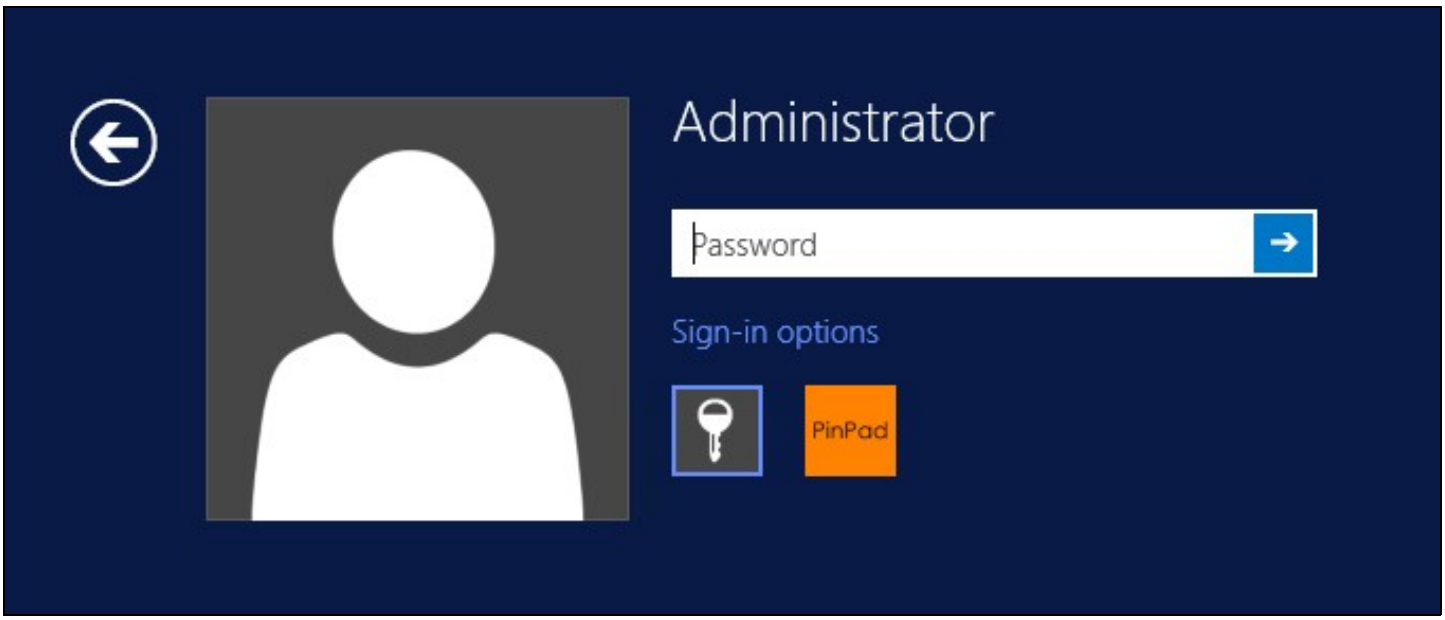
""Logging Location"" The location the logs will be created, this must be somewhere any account has access to.

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.

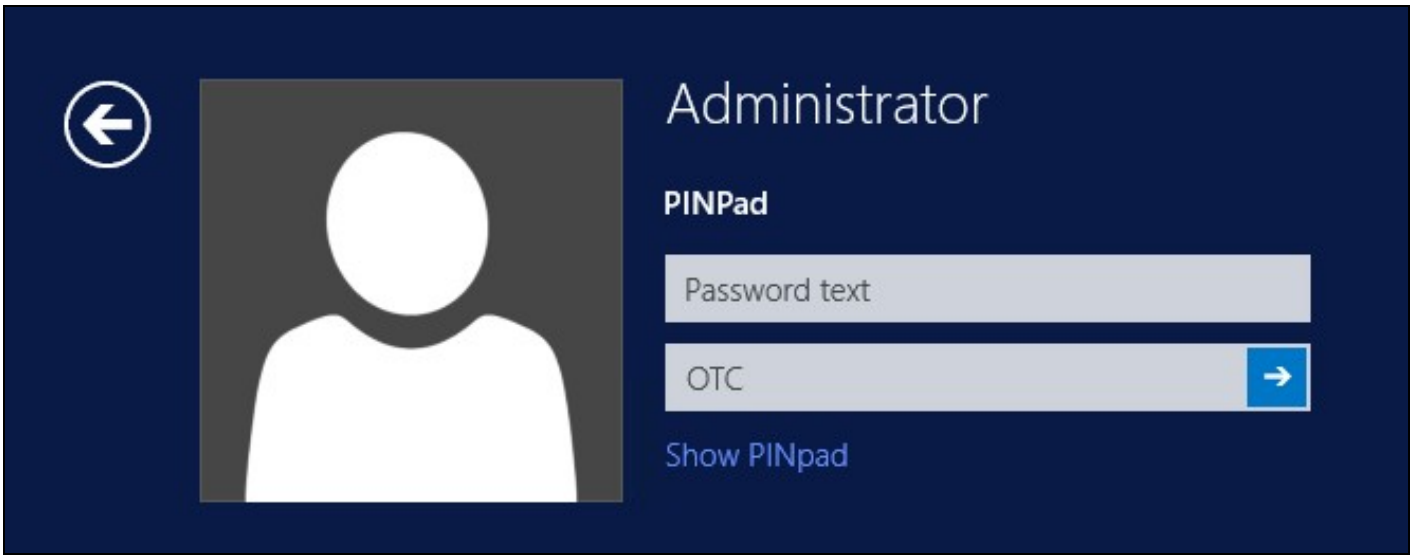
Importing Configurations

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

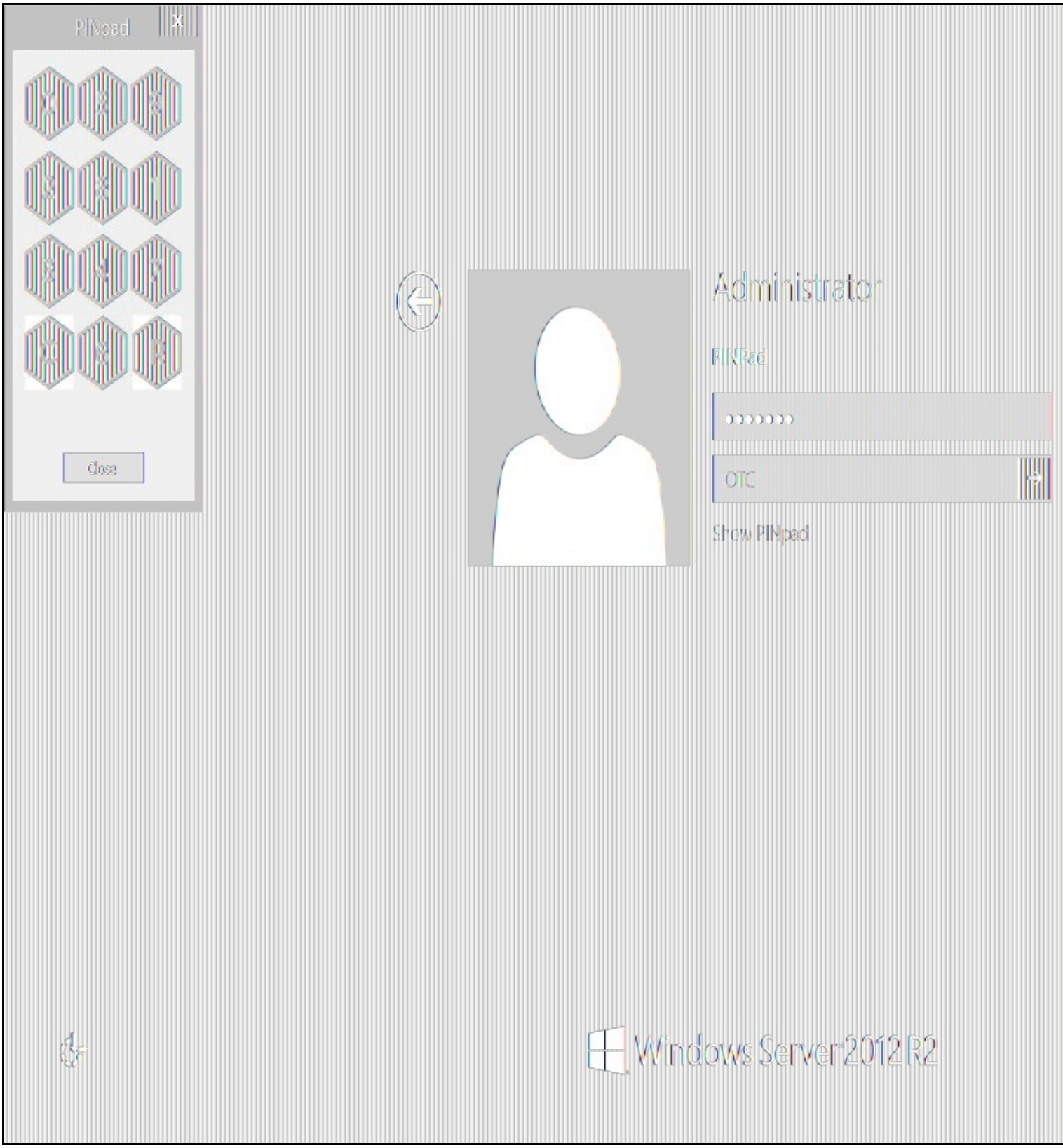
Verifying the Installation

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*.

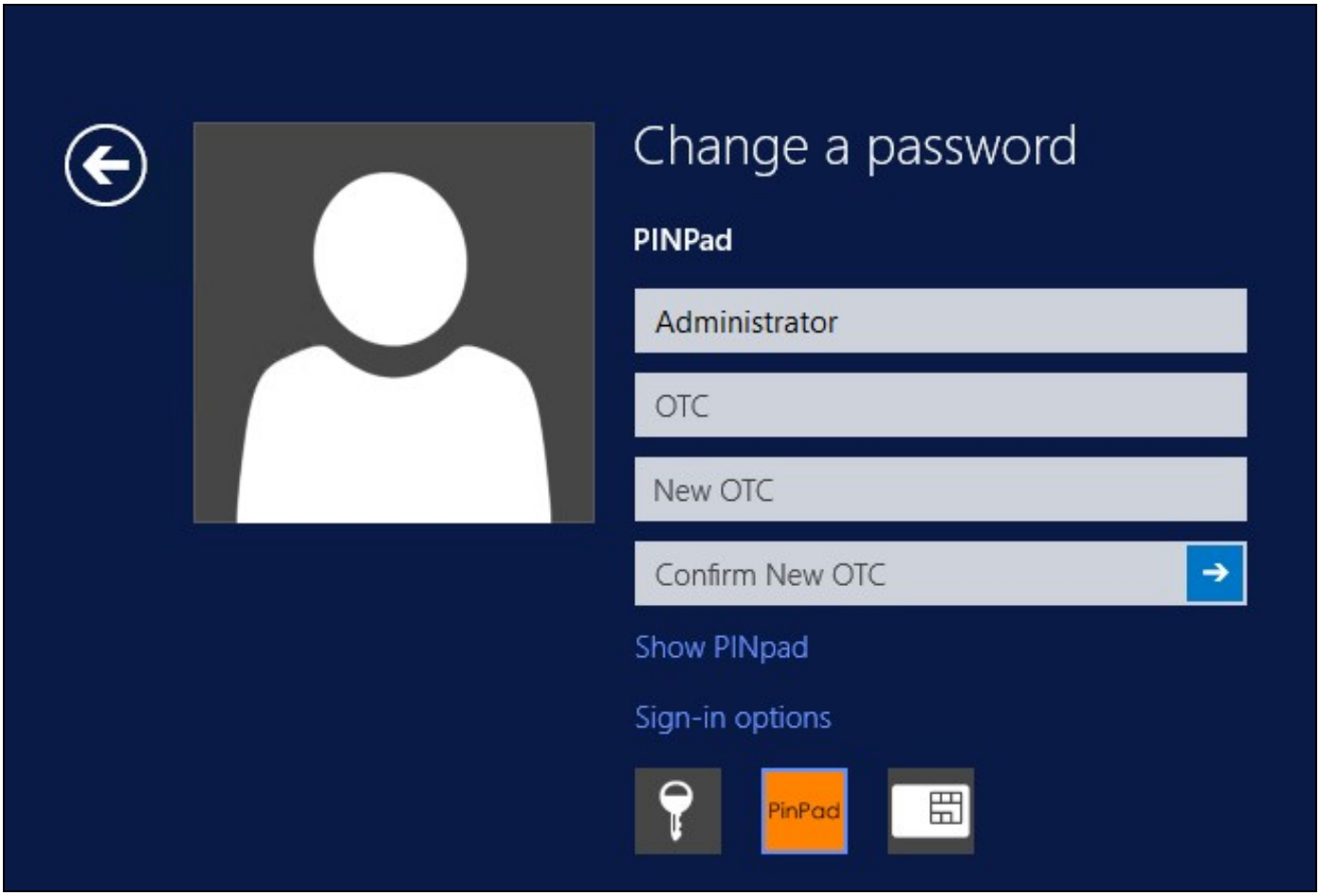
A failed login should not allow a login, and the following message should be displayed in the Swivel log: *Login failed for user: username*.

ChangePIN

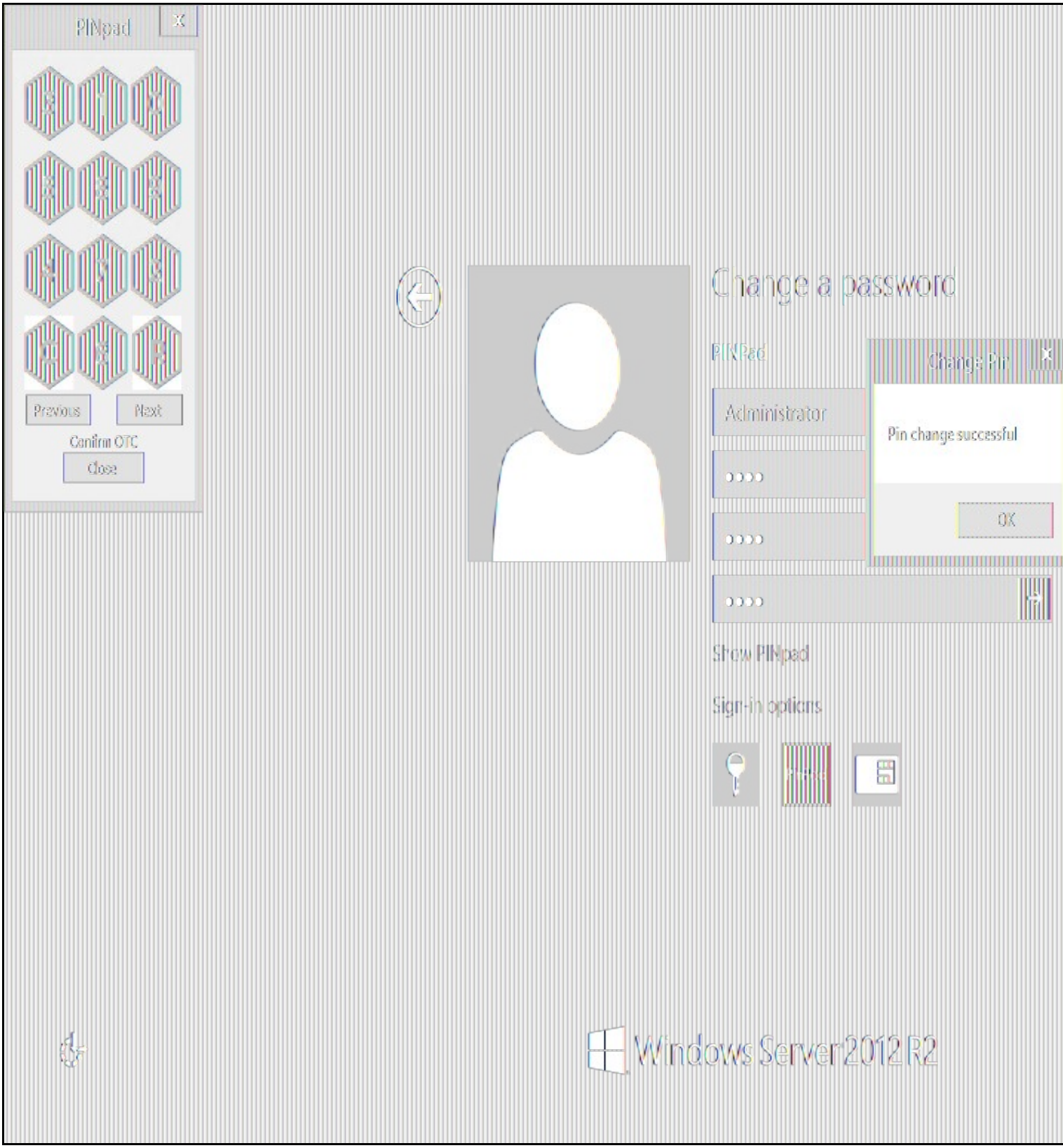
A user is usually able to change the password by using the Ctrl-Alt-Del keys (Ctrl-Alt-End for remote sessions). With the Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the "Sign-in options" button and selecting the Swivel credential. 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.



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 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.

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.

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.

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.

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.

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-A3D6-9D26255DA
 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
}
```

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.

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-A3D6-9D26255DA
 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 }
```

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.