Microsoft Windows Credential Provider Integration (Legacy OS)

Contents

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.

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.

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.

Baseline

Swivel 3.7

Windows 7, Windows 2008 Server R2

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, 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.

Swivel Integration Configuration

Configure a Swivel Agent

1. On the Swivel Management Console select Server/Agent

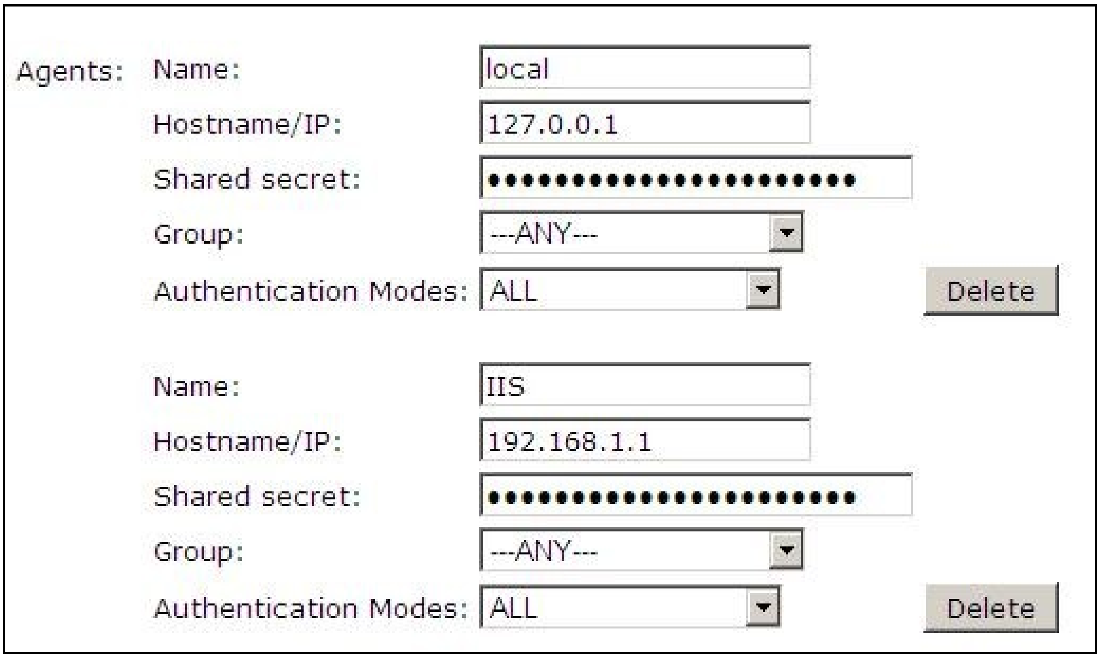
2. Enter a name for the Agent

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: local
Hostname/IP: 127.0.0.1
Shared secret: ••••••••••••••••••••••
Group: ---ANY---
Authentication Modes: ALL

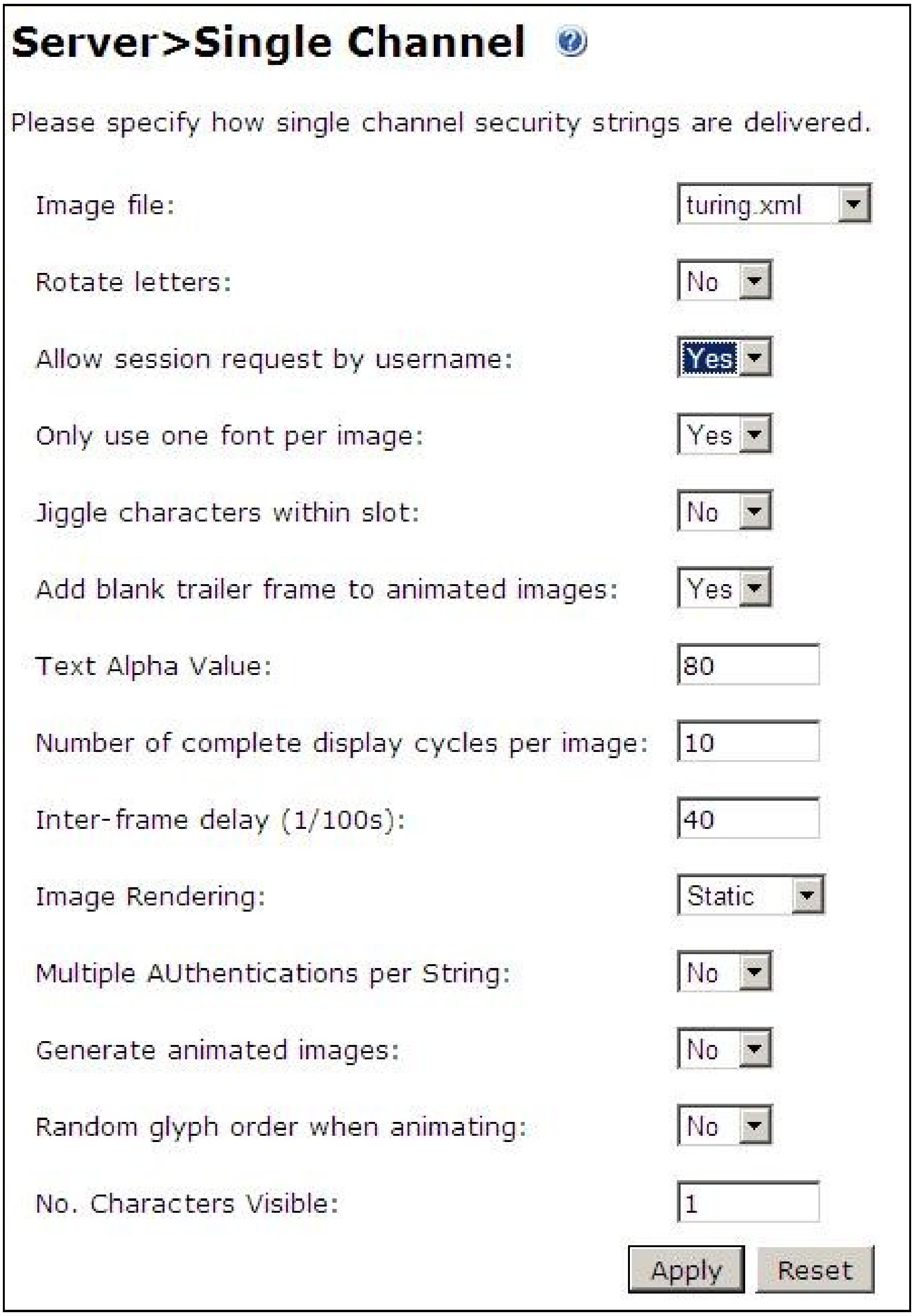
Name: IIS
Hostname/IP: 192.168.1.1
Shared secret: ••••••••••••••••••••••
Group: ---ANY---
Authentication Modes: ALL

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

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

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)

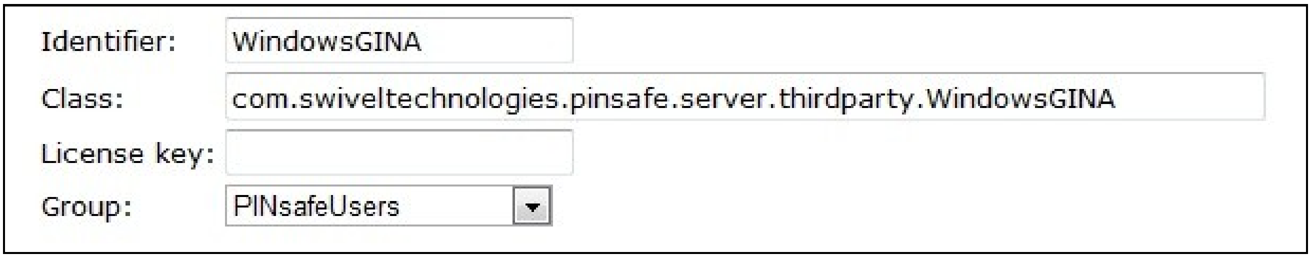
3. For the Class enter: com.swiveltechnologies.Swivel.server.thirdparty.WindowsGINA

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

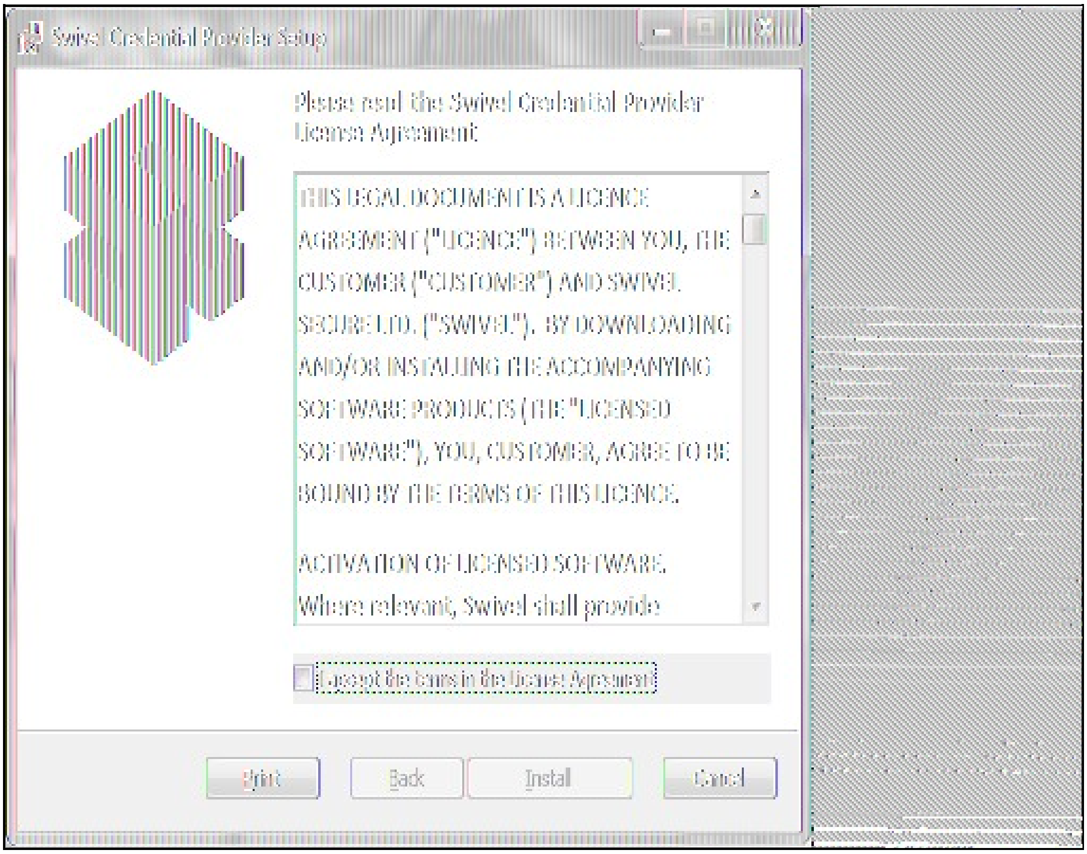
Microsoft Windows Swivel Credential Provider Installation

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

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 msiexec command.

The first page is the licence agreement:



Swivel Credential Provider Setup

Please read the Swivel Credential Provider License Agreement

THIS LEGAL DOCUMENT IS A LICENCE AGREEMENT ("LICENCE") BETWEEN YOU, THE CUSTOMER ("CUSTOMER") AND SWIVEL SECURE LTD. ("SWIVEL"). BY DOWNLOADING AND/OR INSTALLING THE ACCOMPANYING SOFTWARE PRODUCTS (THE "LICENSED SOFTWARE"), YOU, CUSTOMER, AGREE TO BE BOUND BY THE TERMS OF THIS LICENCE.

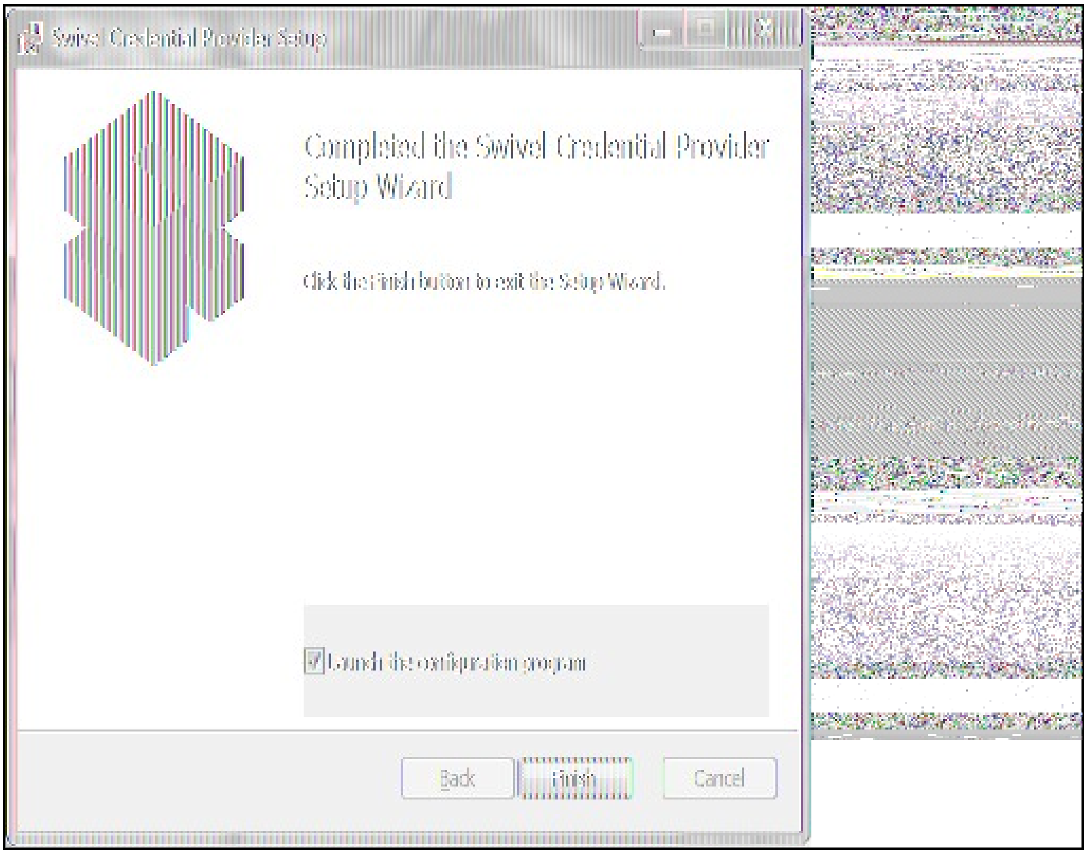
ACTIVATION OF LICENSED SOFTWARE. Where relevant, Swivel shall provide

□ I accept the terms in the License 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:


Swivel Credential Provider Setup

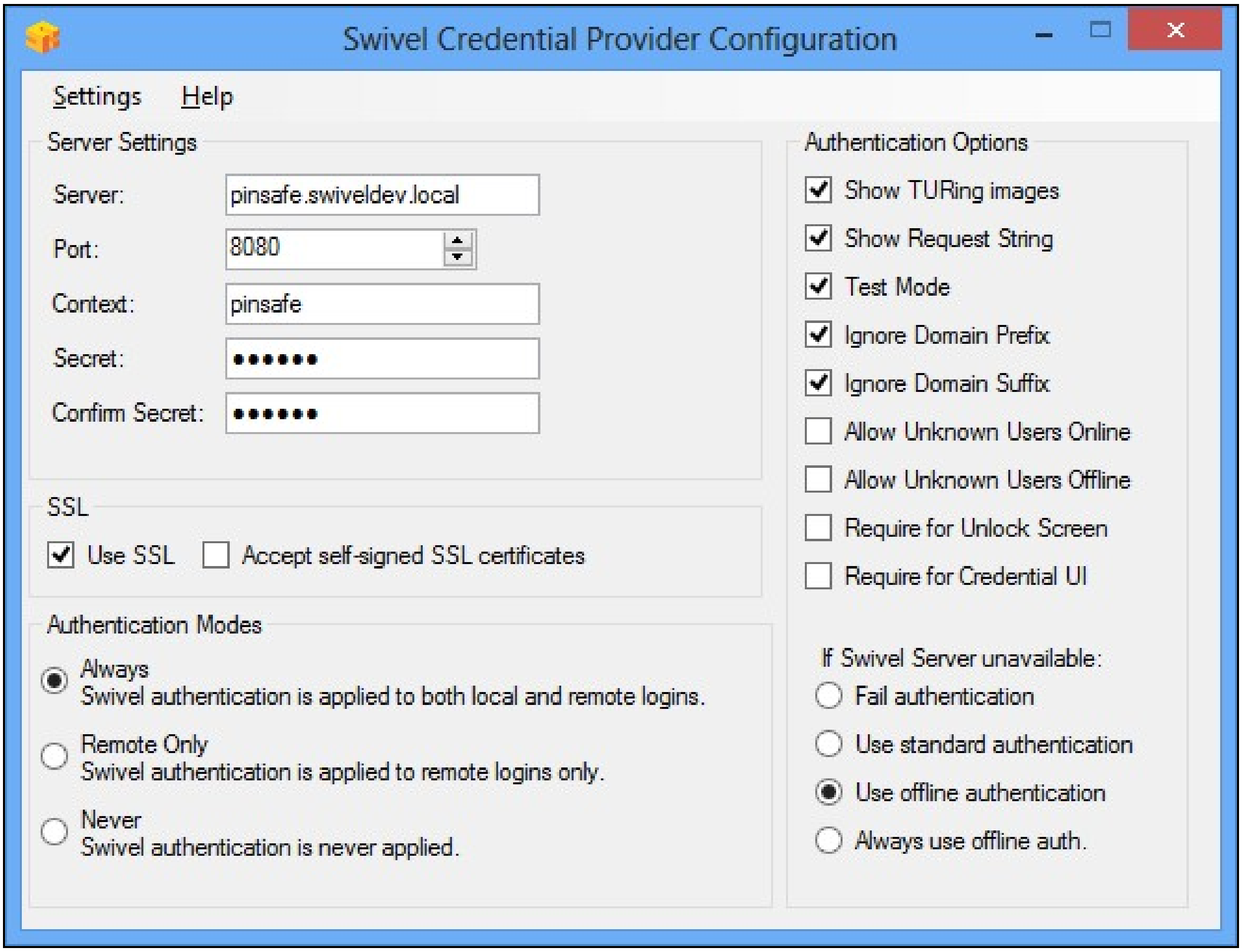
Completed the Swivel Credential Provider Setup Wizard

Click the Finish button to exit the Setup Wizard.

☑ Launch the configuration program

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

Windows Swivel Credential Provider configuration


Swivel Credential Provider Configuration

Server Settings

Server: pinsafe.swiveldev.local

Port: 8080

Context: pinsafe

Secret: ••••••

Confirm Secret: ••••••

SSL

☑ Use SSL ☐ Accept self-signed SSL certificates

Authentication Modes

● Always
Swivel authentication is applied to both local and remote logins.

○ Remote Only
Swivel authentication is applied to remote logins only.

○ Never
Swivel authentication is never applied.

Authentication Options

☑ Show TURing images

☑ Show Request String

☑ Test Mode

☑ Ignore Domain Prefix

☑ Ignore Domain Suffix

☐ Allow Unknown Users Online

☐ Allow Unknown Users Offline

☐ Require for Unlock Screen

☐ Require for Credential UI

If Swivel Server unavailable:

○ Fail authentication

○ Use standard authentication

● Use offline authentication

○ Always use offline auth.

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.

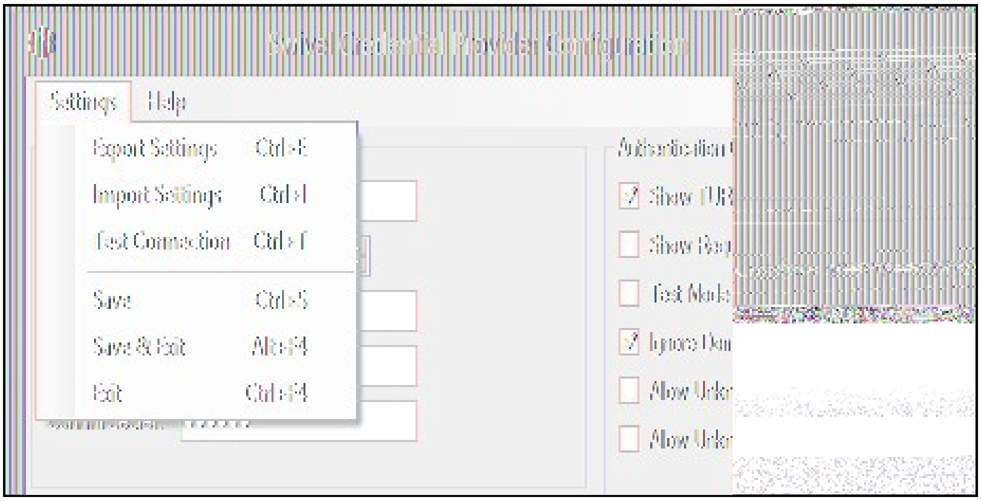
If Swivel unavailable, Fail authentication If the Swivel server cannot be contacted then authentication will fail

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:

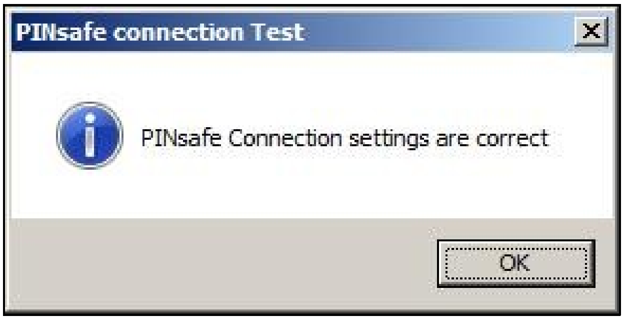


Export Settings Export settings as an XML file. These can be used to import settings elsewhere.

Import Settings Import settings from an XML file exported elsewhere.

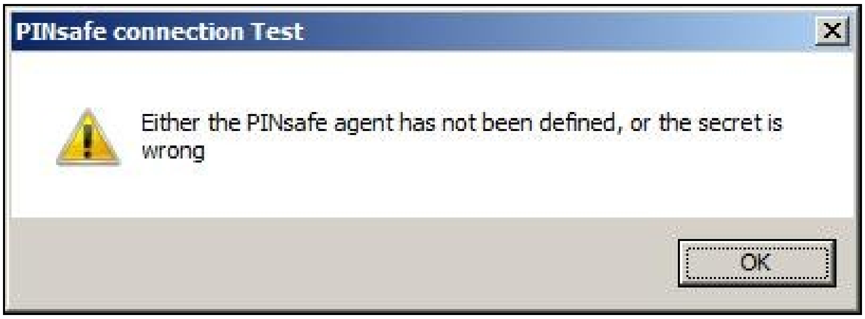
Test Connection Tests link to Swivel server:

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


PINsafe connection Test

PINsafe 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**


PINsafe connection Test

Either the PINsafe 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.

Additional Installation Options

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

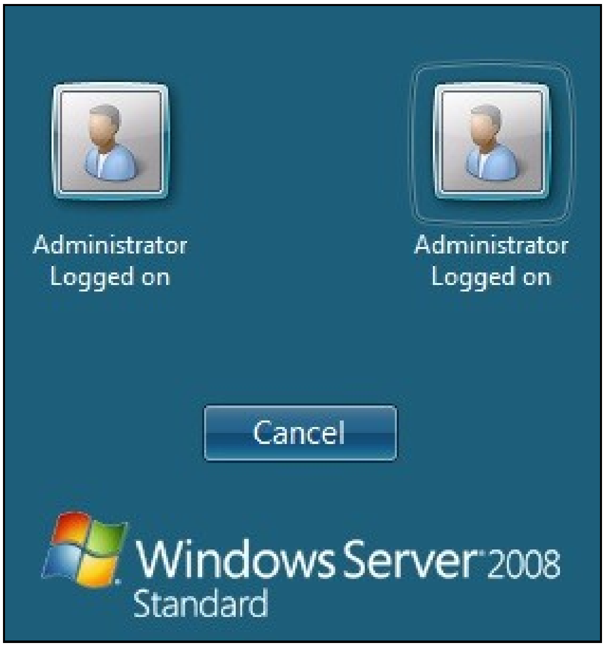
Directory

Uninstaller

Version

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.



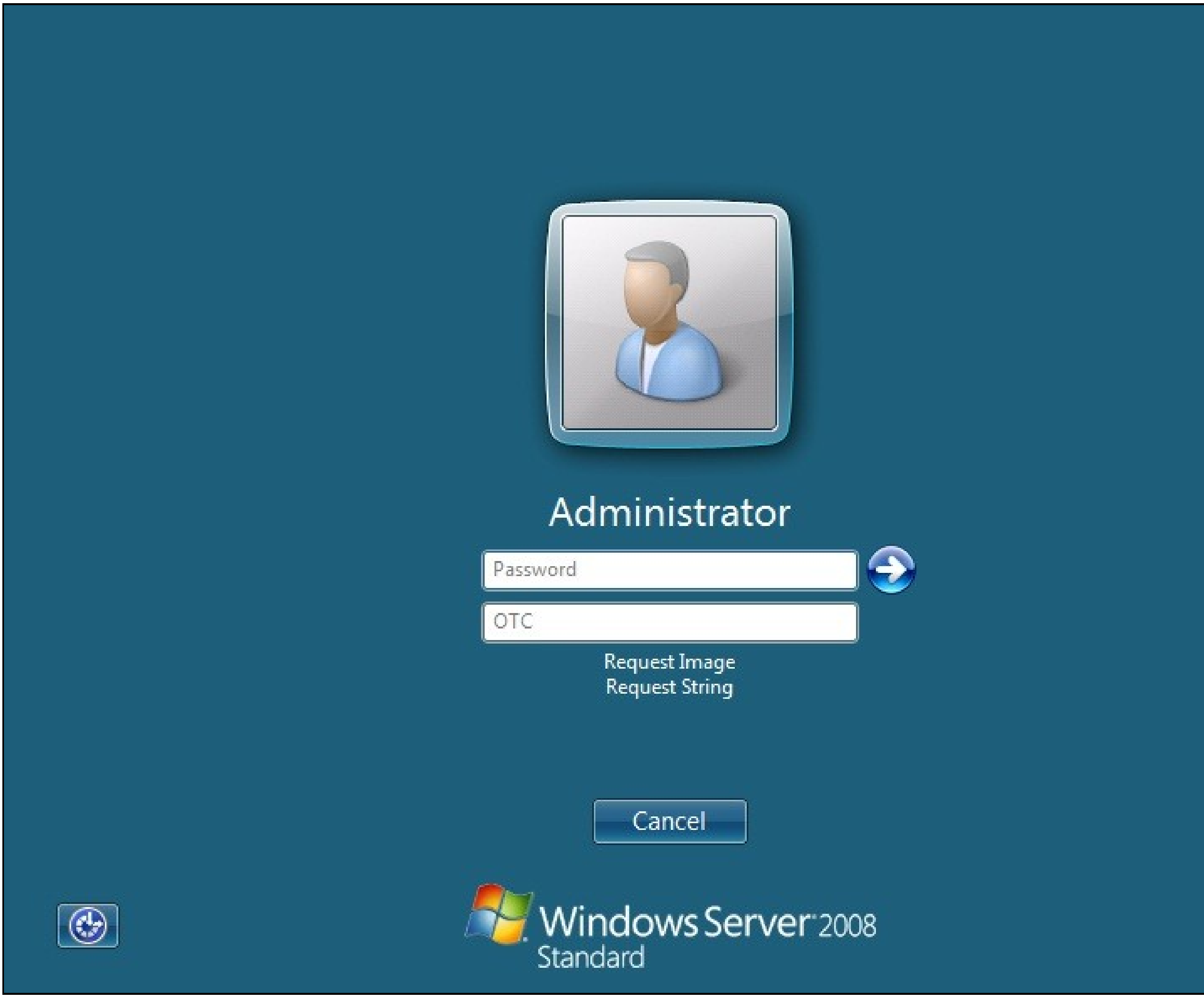
The Swivel credentials will always be on the left, the standard credentials on the right.

Importing Configurations

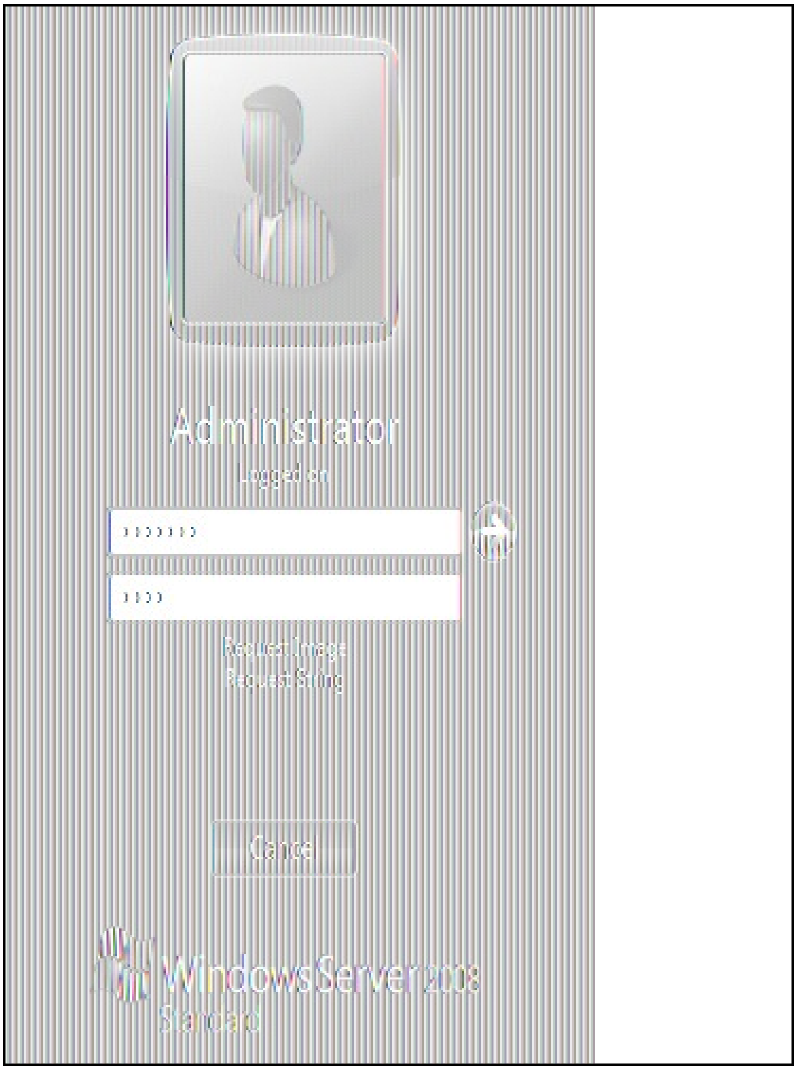
You can import credentials exported from other installations using the Import Settings menu item. Alternatively, if you need to install the Credential Provider on a large number of machines, you can modify the .msi file and replace the blank LoginSettings.xml file included with your own custom version.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

Verifying the Installation

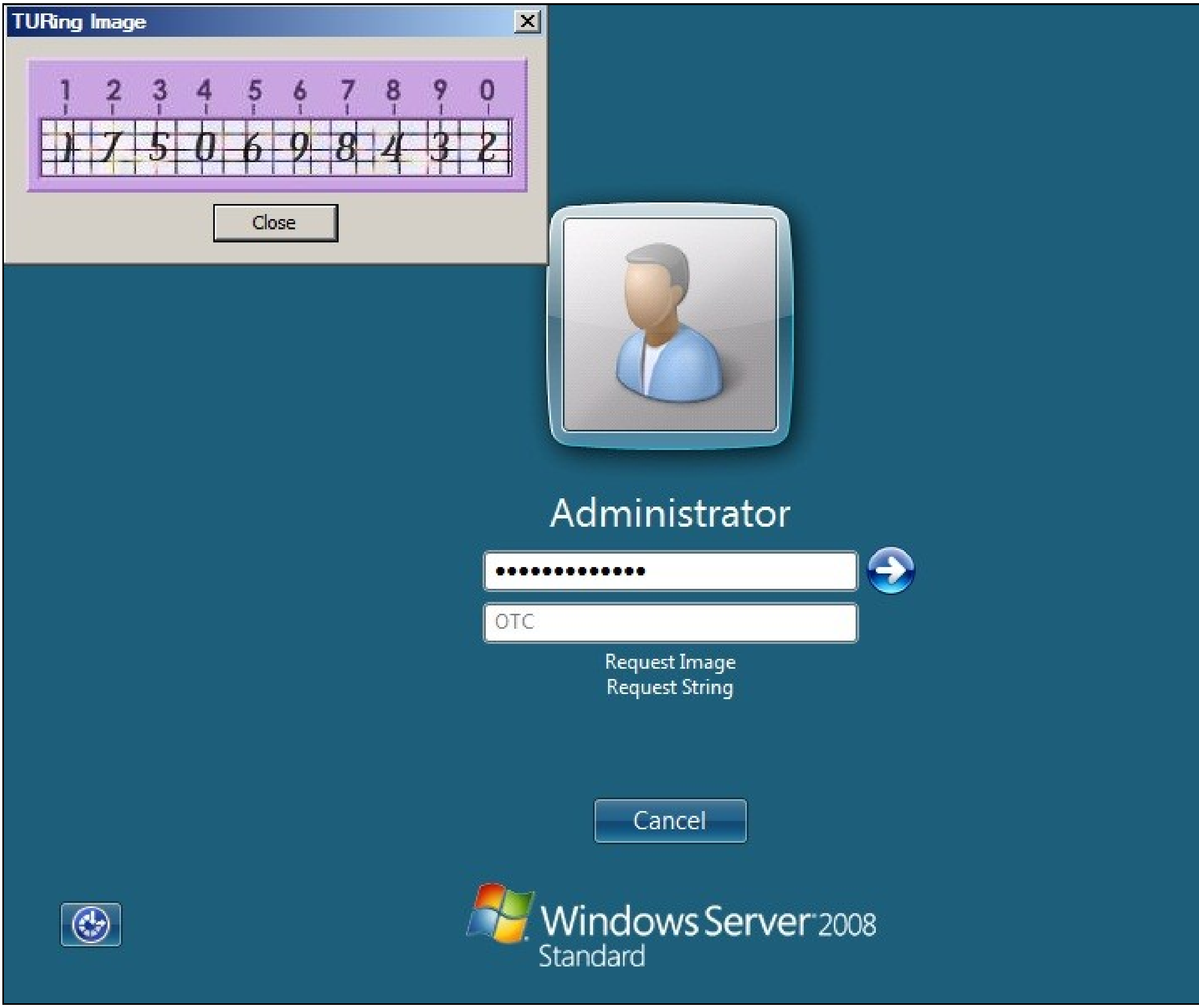
At the windows login a password and OTC login field should be available with Request Image and Request String options available.



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.*



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

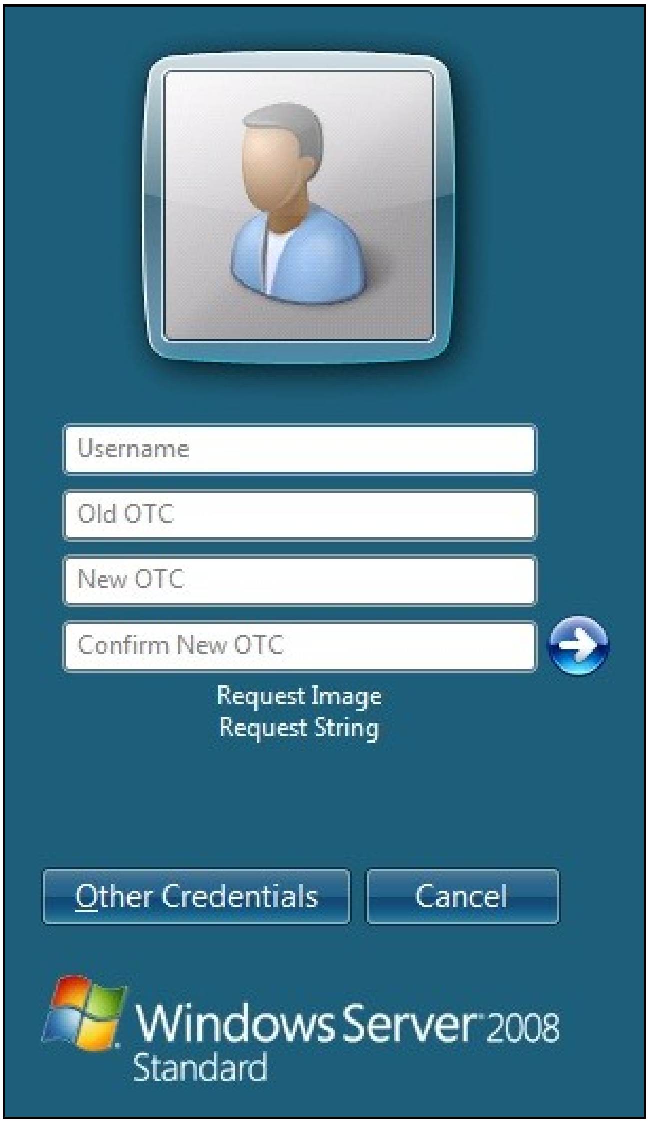
A failed login should not allow a login, and the following message should be displayed in the Swivel log: *Login failed for user: username*

ChangePIN

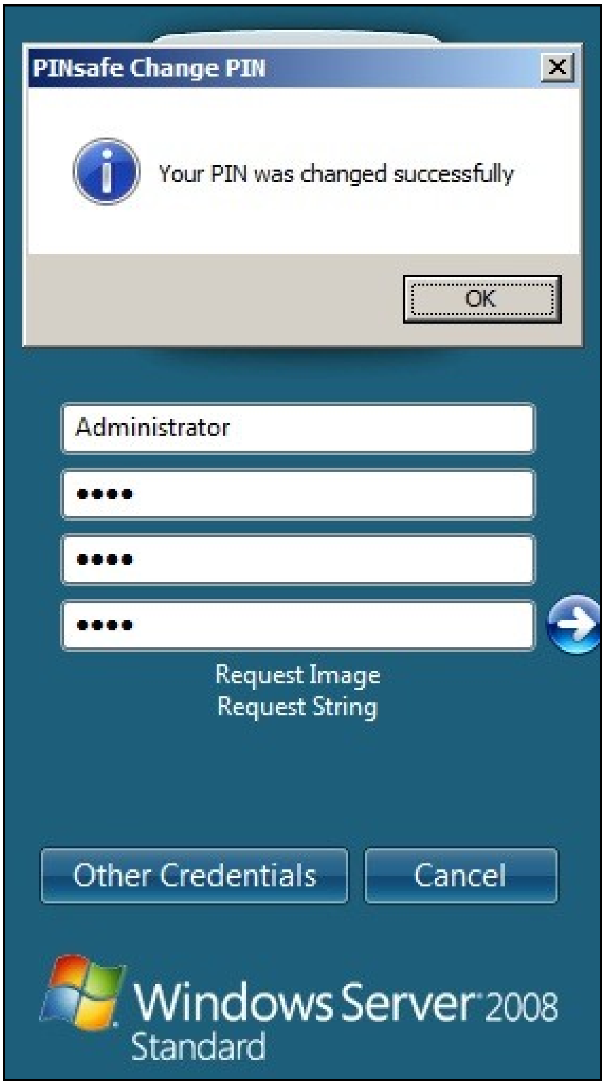
A user is usually able to change the password by using the Ctrl-Alt-Del keys (CTL-Alt-End for remote sessions). With the Windows Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the Other Credentials. This will not function for Offline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



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



PINsafe Change PIN

Your PIN was changed successfully

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

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.

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.

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\WindowNT\CurrentVersion\WinLogon\ginadll" registry value

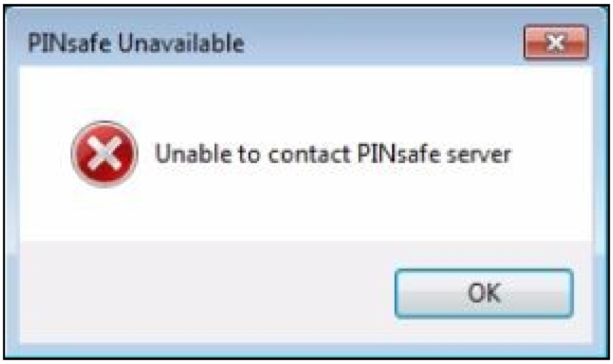
Reboot Windows

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

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.



PINsafe Unavailable

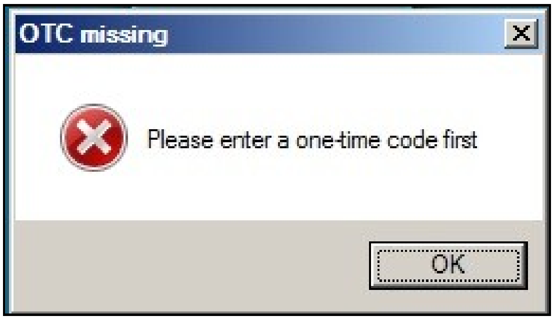
Unable to contact PINsafe server

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

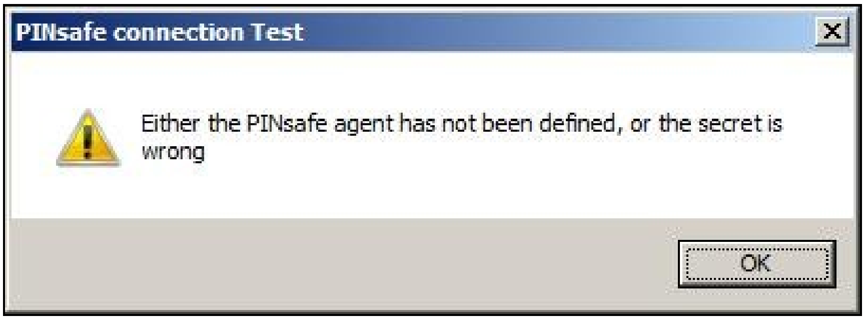


OTC missing

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



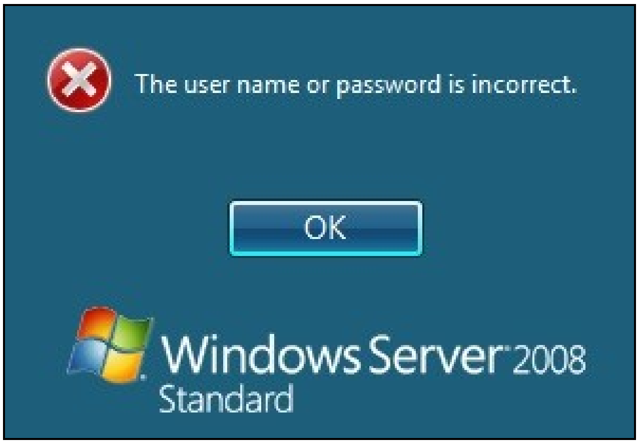
PINsafe connection Test

Either the PINsafe agent has not been defined, or the 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.



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

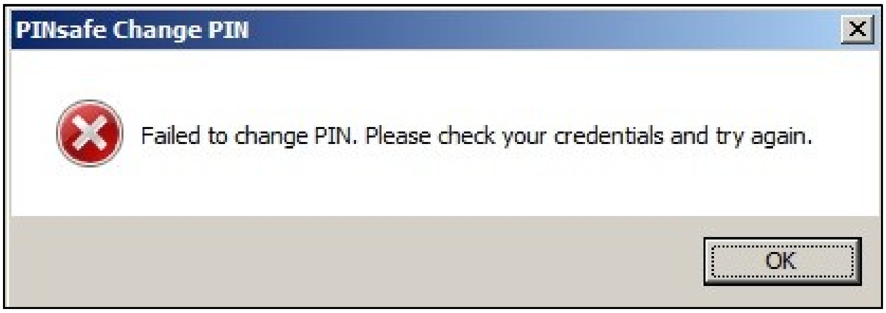
error: The third party class could not be found.

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.



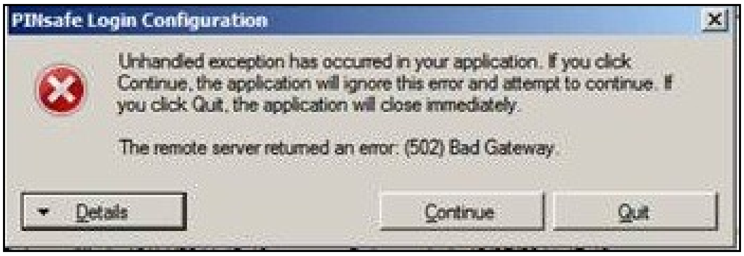
PINsafe Change PIN

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.



PINsafe Login Configuration

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.

Release Notes

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.

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.

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, who can create a custom installer for your organisation.

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.