Microsoft Windows GINA login

Contents

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.

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.

Baseline

Architecture

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

Swivel Configuration

Configure a Swivel Agent

1. On the Swivel Management Console select Server/Agent

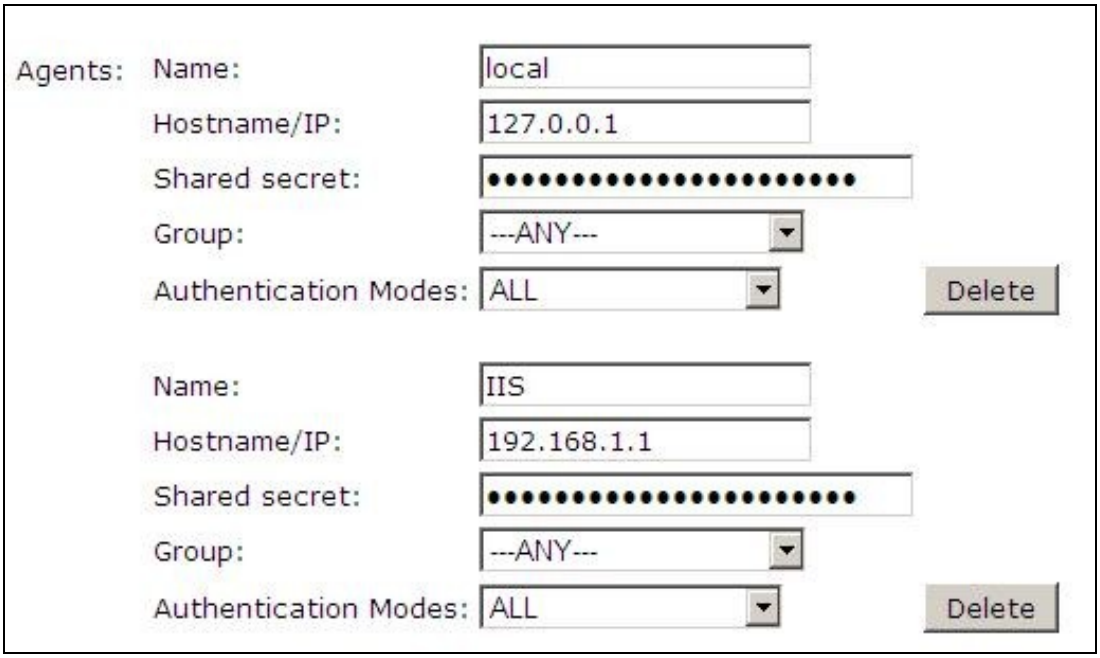
2. Enter a name for the Agent

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)

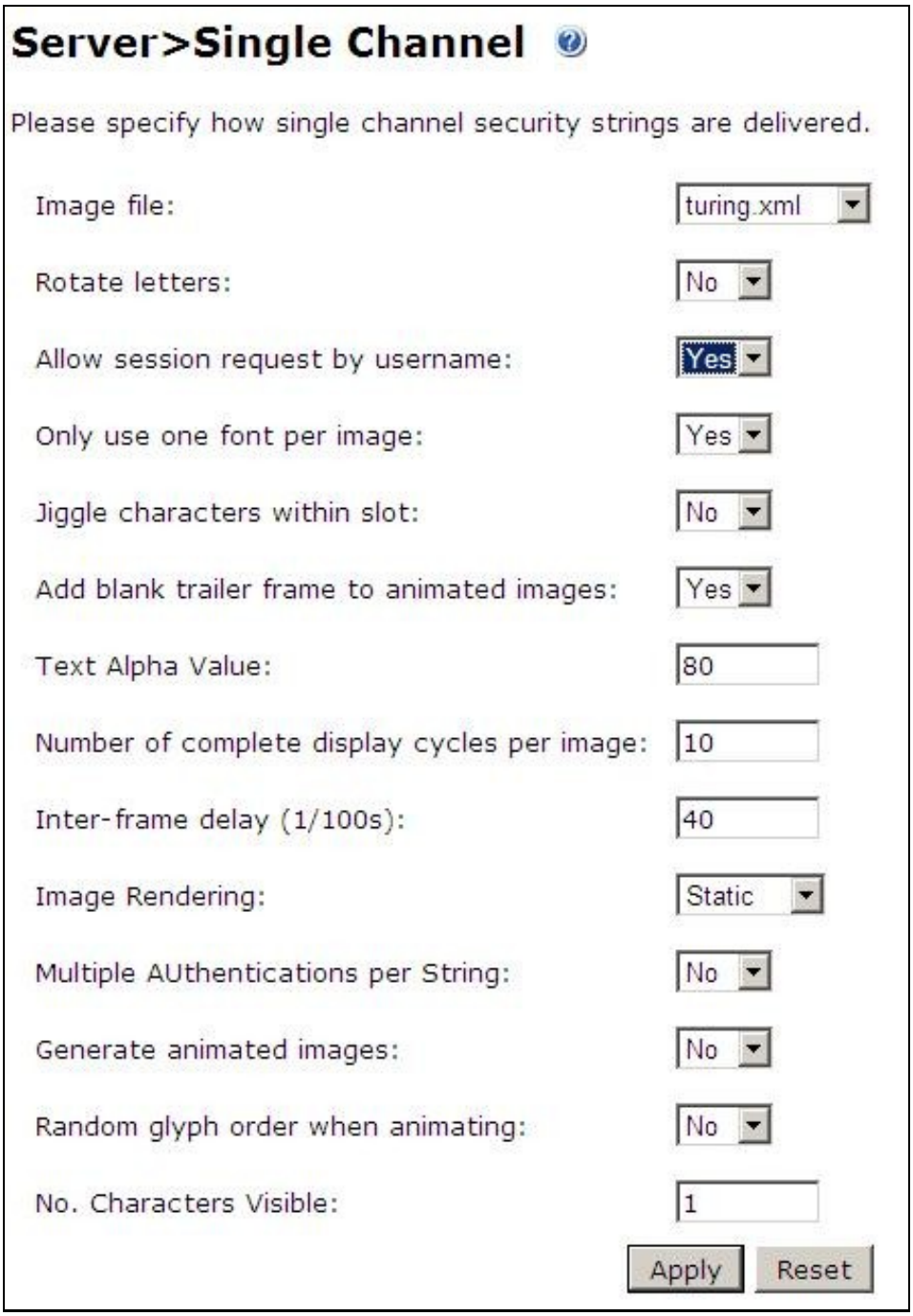
6. Click on Apply to save changes



Configure Single Channel Access

1. On the PINsafe Management Console select Server/Single Channel

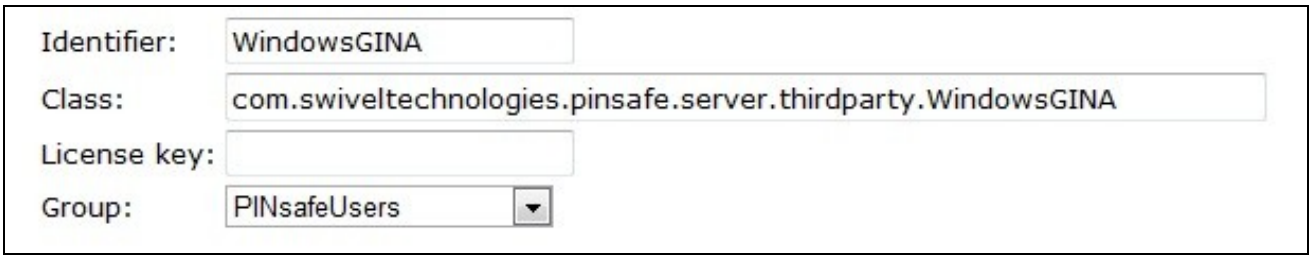
2. Ensure ?Allow session request by username? is set to YES



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



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

Terminal Services GINA Integration

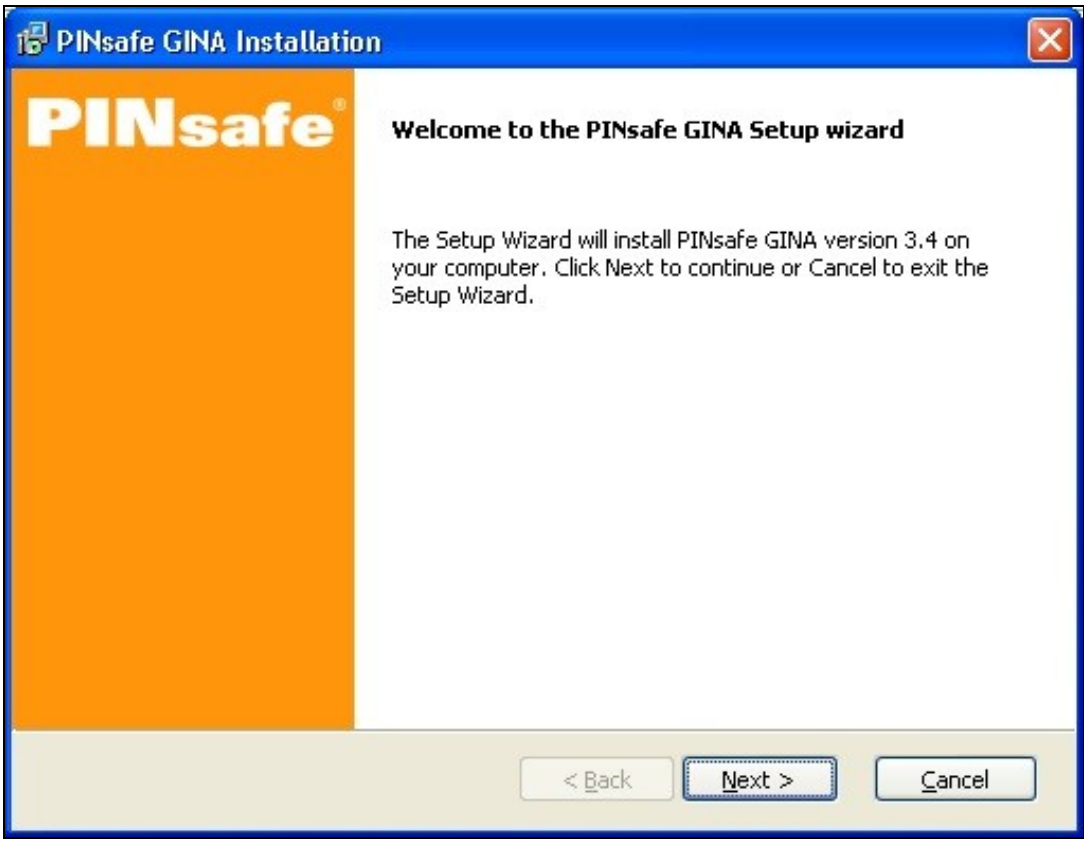
The PINsafe GINA Configuration utility provides a convenient means of configuring the installed PINsafe GINA.

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.

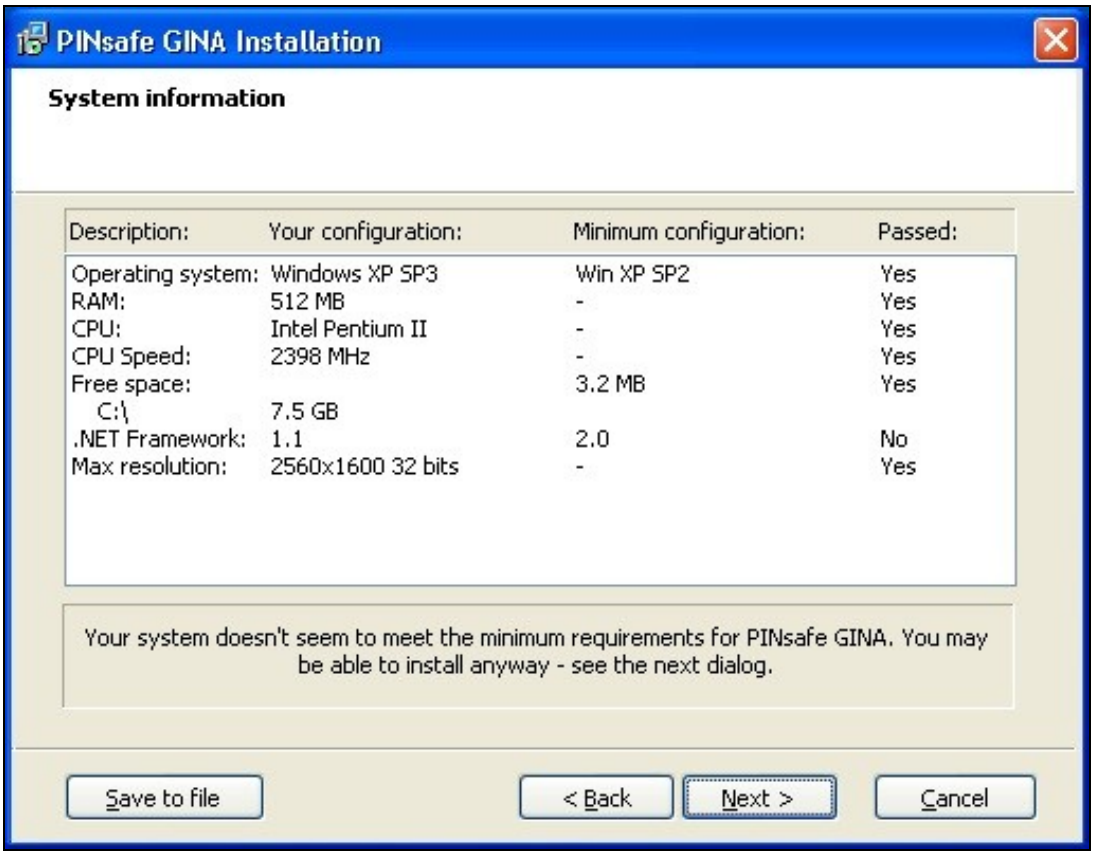
Install the GINA software on the Windows Terminal Server.

Terminal Services GINA Installation

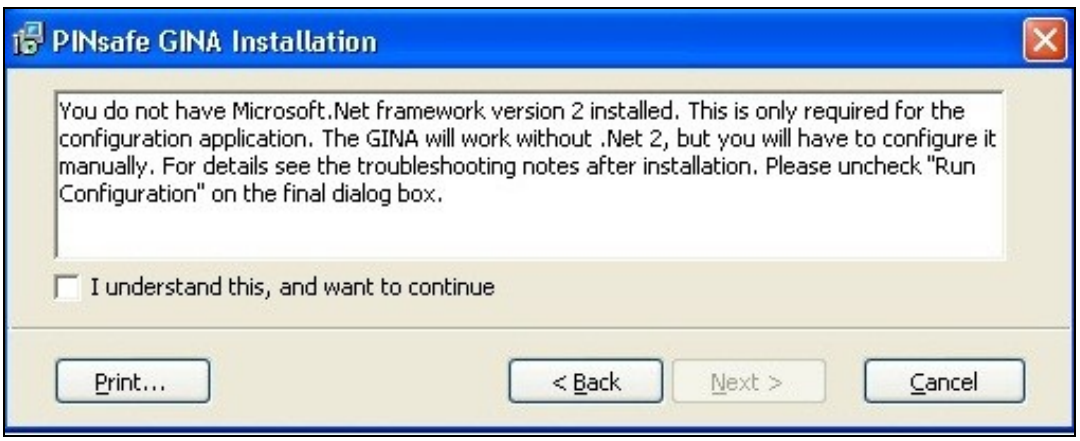
Start the PINsafe installation Wizard



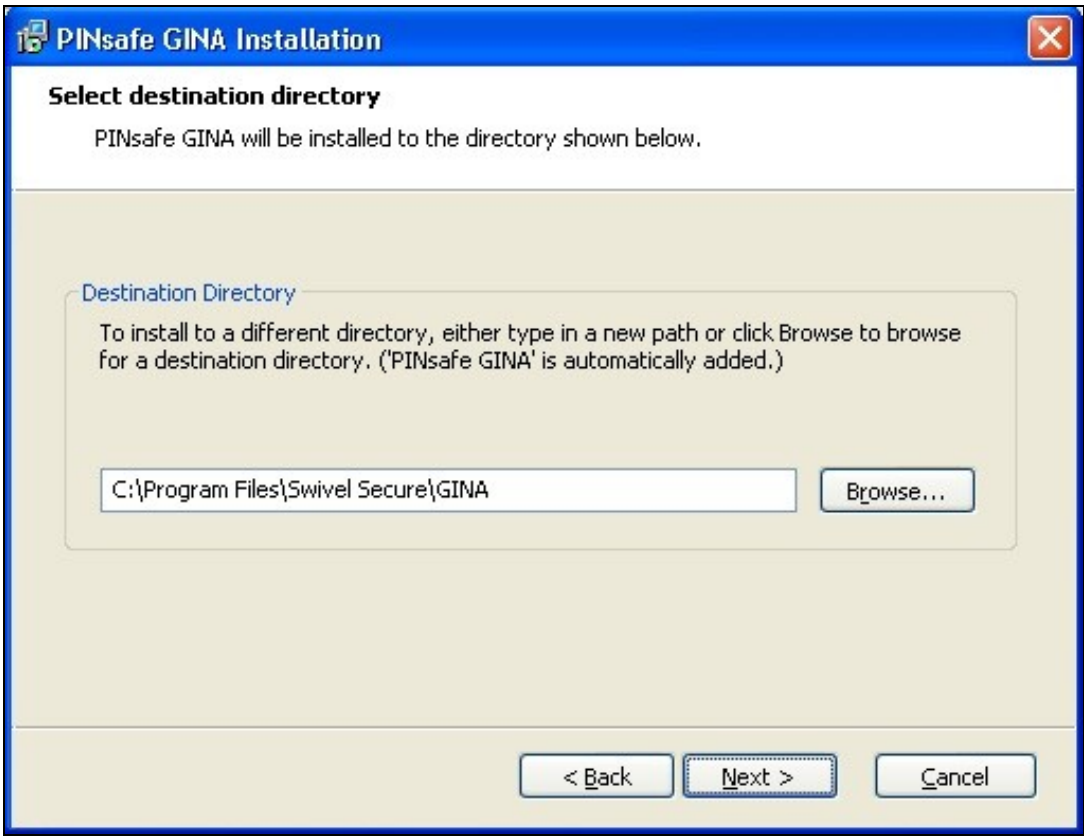
The system summary will report on any requirements which are not met, in this example .Net



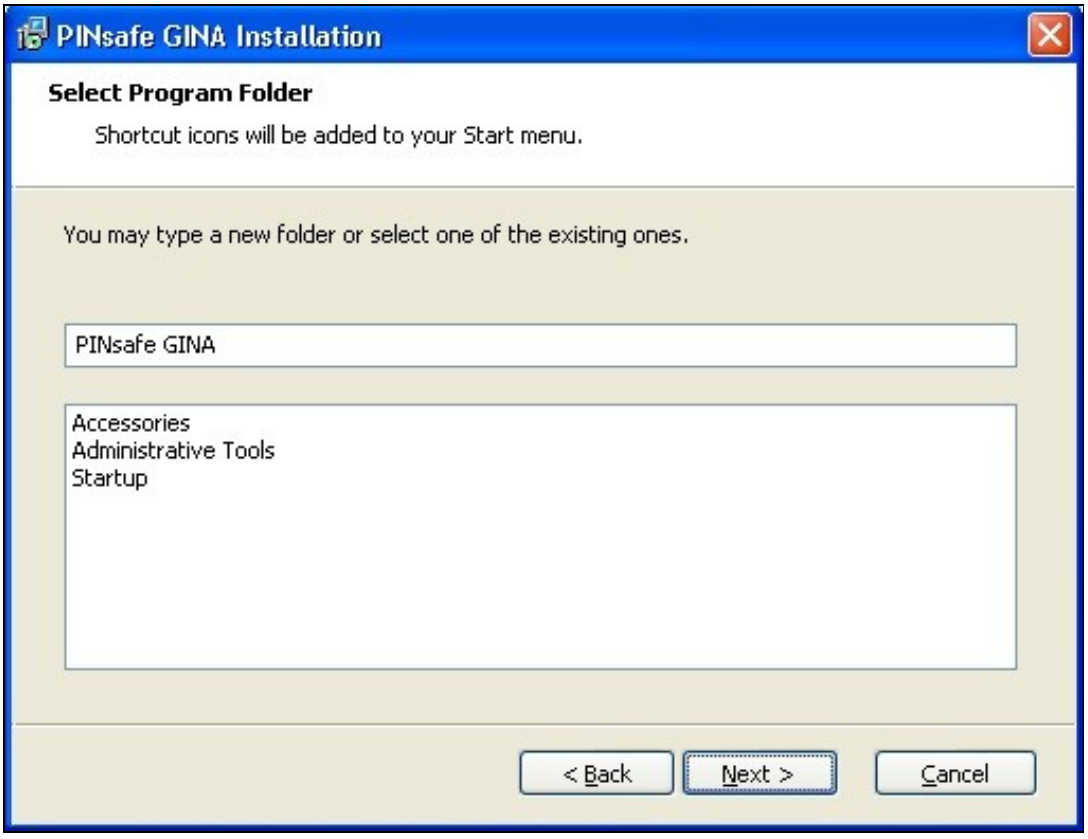
The PINsafe GINA may optionally be installed without .Net, the PINsafe GINA configuration utility requires .Net to install, but may be configured manually



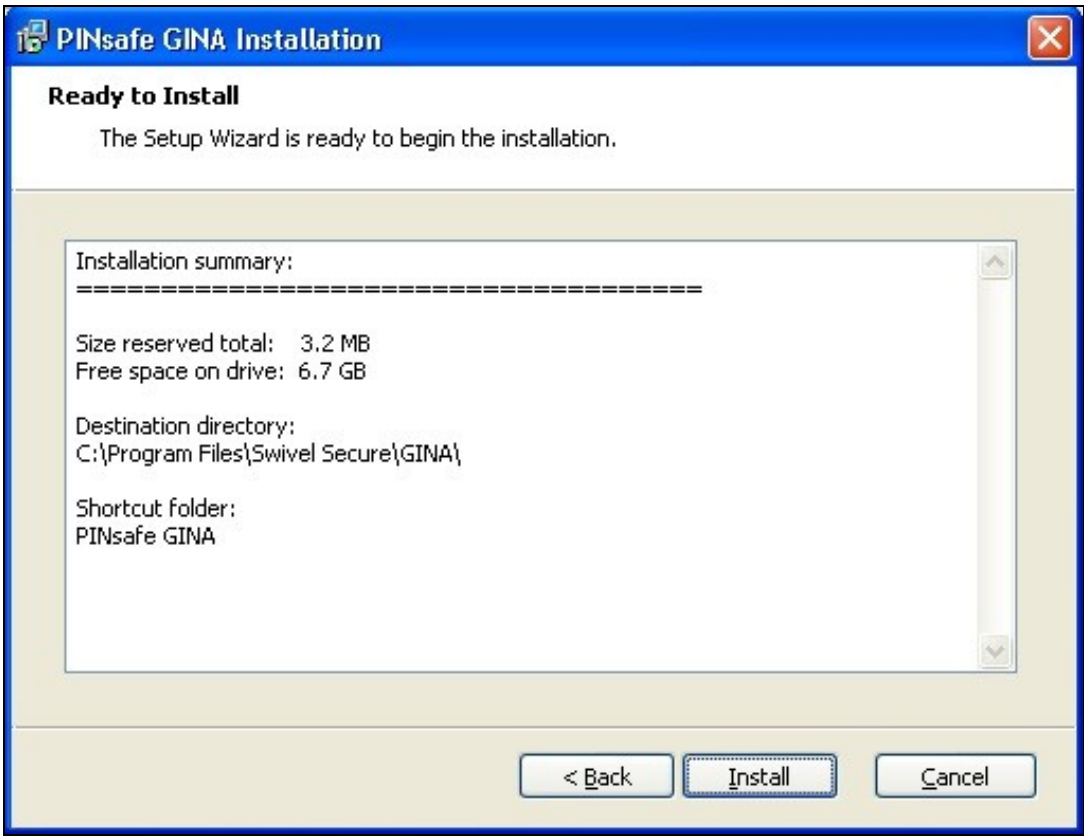
Select the install directory



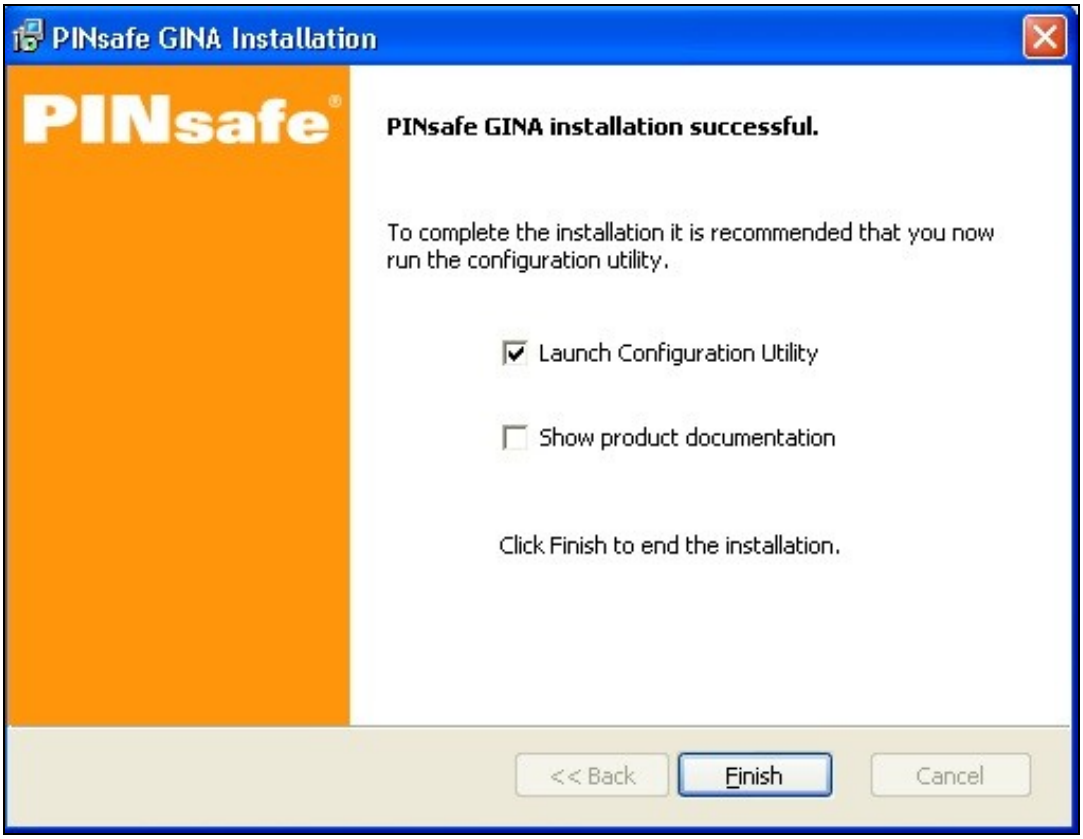
Select the Start Program files group



Check the installation details

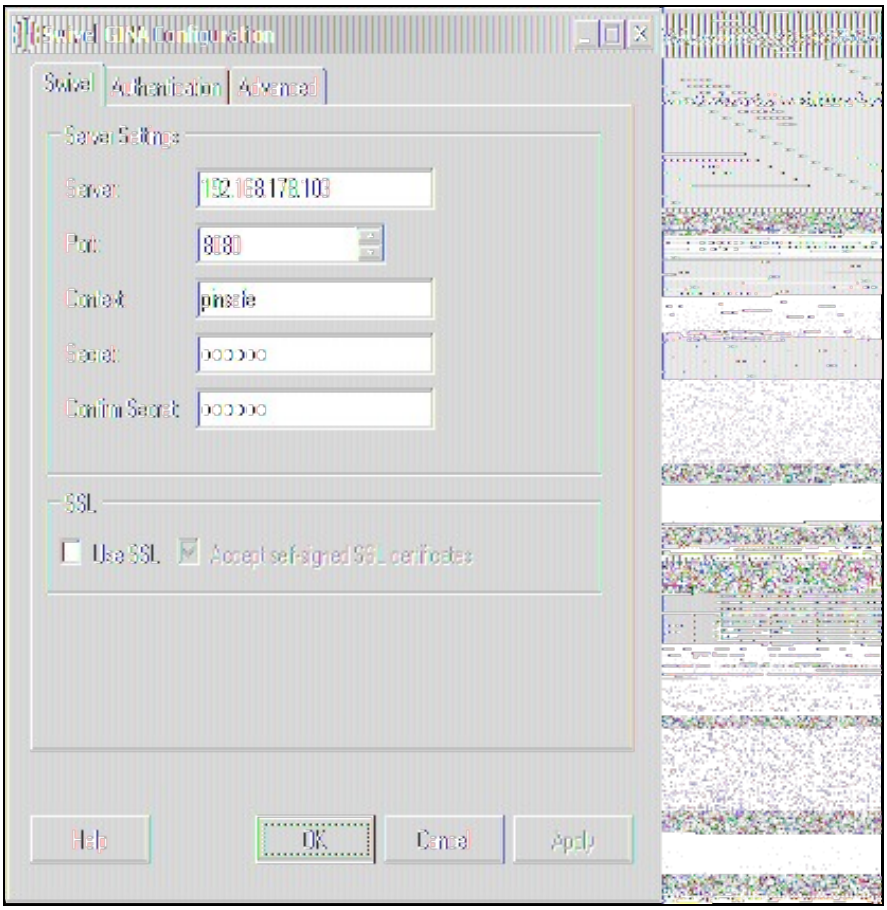


The PINsafe GINA installation reports when it is complete and allows the configuration utility to be run



Terminal Services GINA Configuration

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.

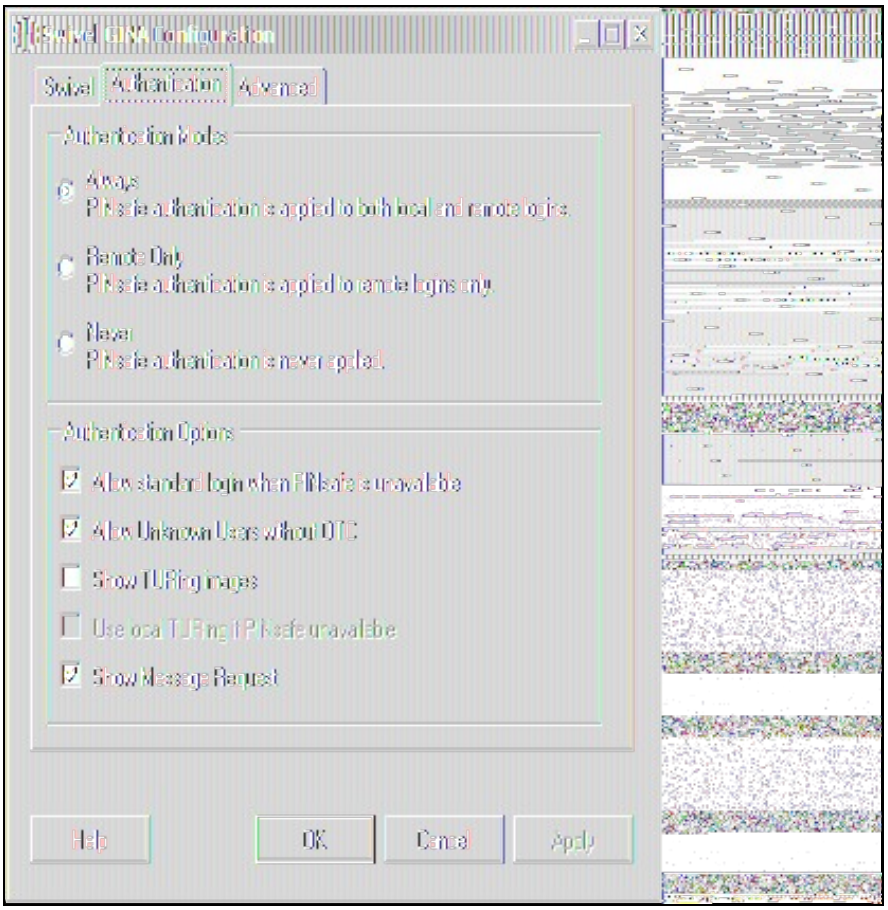
Confirm Secret Repeat the shared secret to ensure it has been entered correctly.

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.

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.

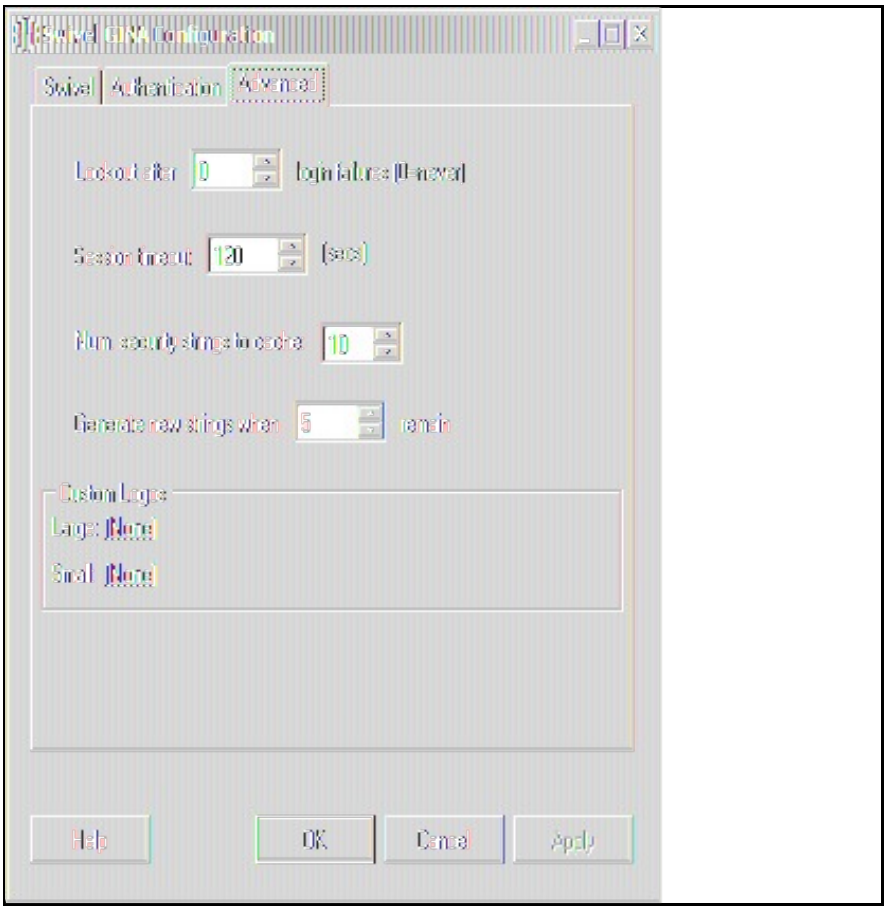
Allow unknown users without OTC When enabled, if a user is not known to PINsafe, they are not required to enter a one-time code to authenticate. There is no visible indication that the user is not known to PINsafe.

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.

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.

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.

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.

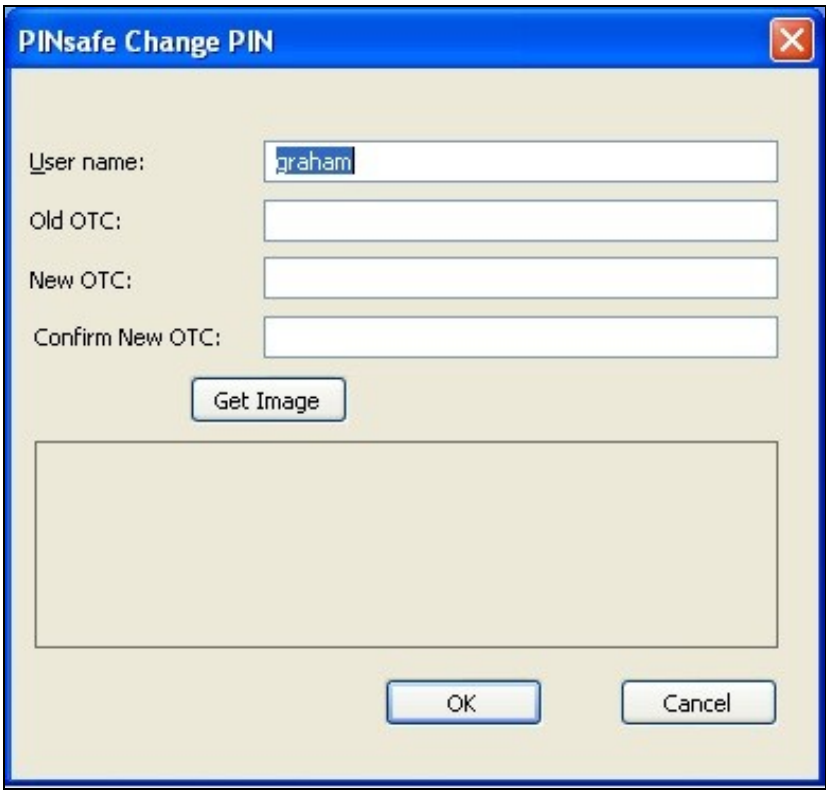
ChangePIN using dual channel or mobile phone client

ChangePIN using TURing

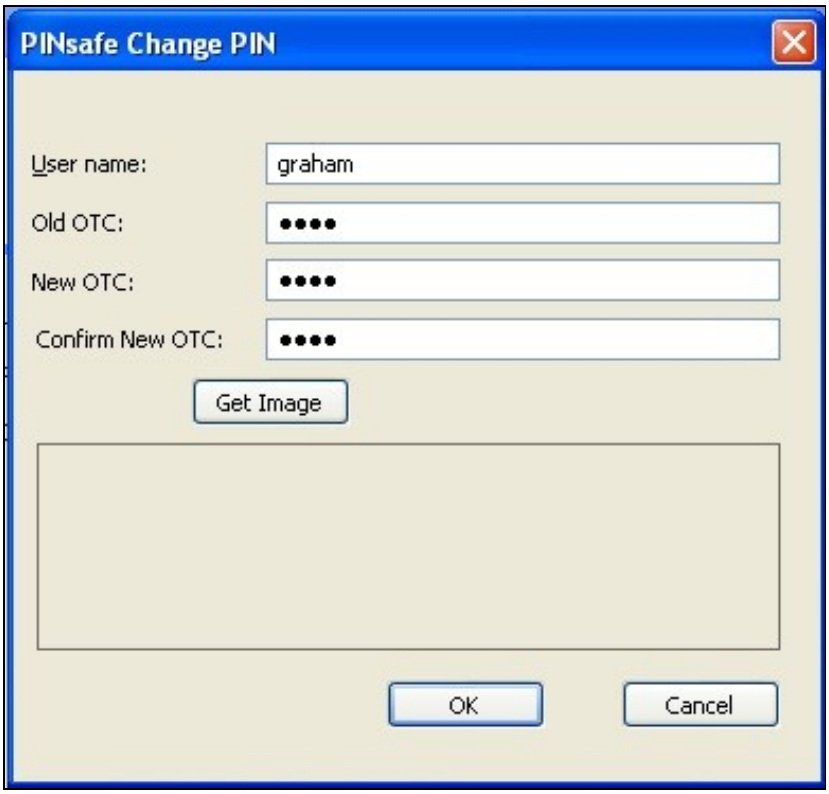
ChangePIN successful

ChangePIN redirect at login

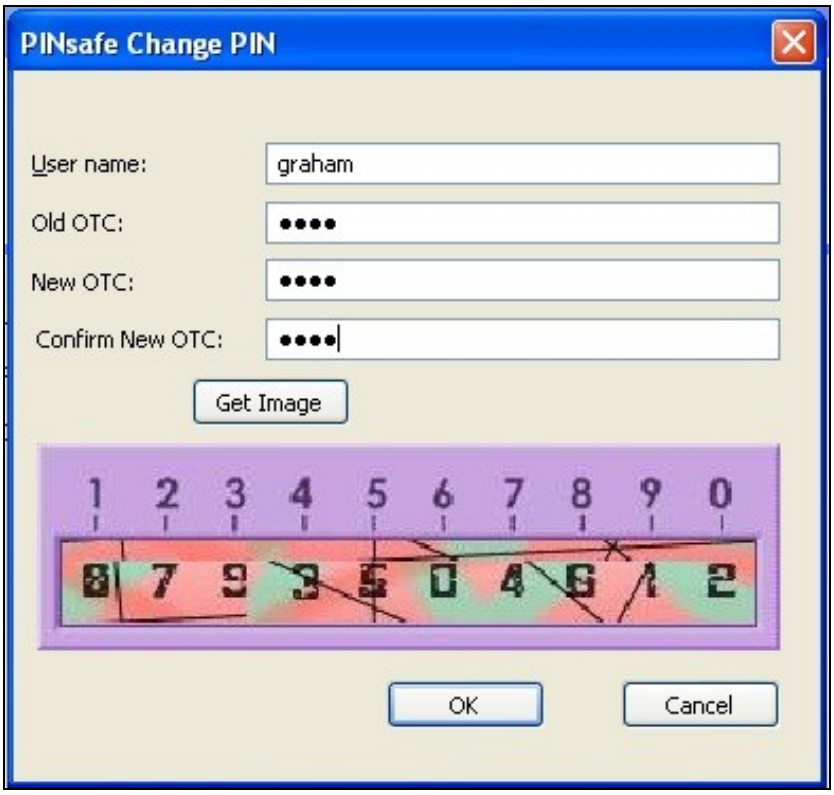
Where the user is required to ChangePIN the user is redirected at login.



ChangePIN using dual channel or mobile phone client



ChangePIN using TURing



ChangePIN successful

Additional Installation Options

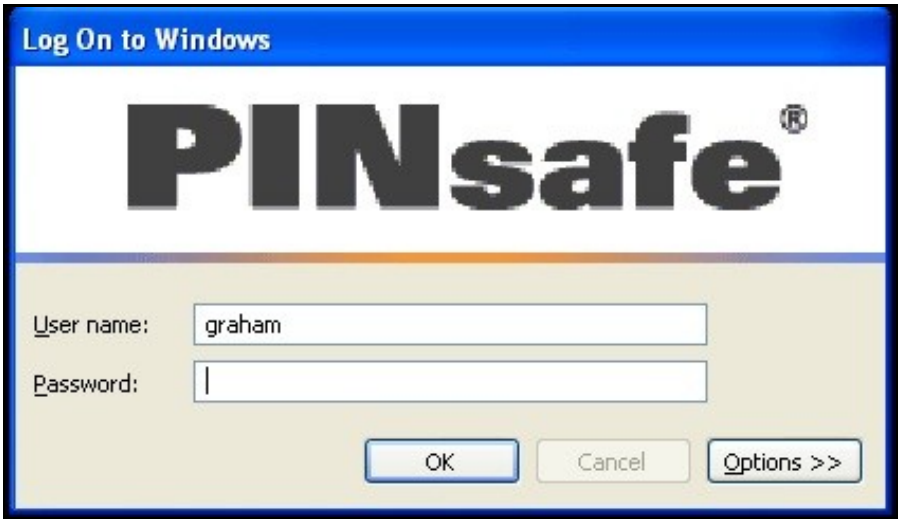
Verifying the Installation

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

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

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

Standard authentication when the PINsafe server cannot be contacted.



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.

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\WindowNT\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\WindowNT\CurrentVersion\WinLogon\ginadll" registry value

Reboot Windows

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

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.

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.

Additional Information