

Biometric Fingerprint for Windows Credential Provider

Contents

- 1 Overview
- 2 Prerequisites
 - ◆ 2.1 Supported models
- 3 Nitgen Reader vs Laptop Reader
- 4 Configuration for Nitgen Biometric Reader
 - ◆ 4.1 Configure Third Party Authentication Nitgen
 - ◆ 4.2 Configure Credential Provider
 - ◆ 4.3 Enrol the user with Nitgen
 - ◆ 4.4 Authenticating with Nitgen
- 5 Configuration for Laptop Biometric Reader
 - ◆ 5.1 Configure Third Party Authentication
 - ◆ 5.2 Disable Windows Hello
 - ◆ 5.3 Install Credential Provider with Fingerprint Enrolment
 - ◆ 5.4 Configure Credential Provider
 - ◆ 5.5 Enrol the user
 - ◆ 5.6 Authenticating
- 6 Configuration for Fujitsu PalmSecure-F Pro Biometric Reader
 - ◆ 6.1 Configure Third Party Authentication PalmSecure
 - ◆ 6.2 Configure Credential Provider PalmSecure
 - ◆ 6.3 Enrolment with PalmSecure
 - ◆ 6.4 Authenticating with PalmSecure
 - ◆ 6.5 Identification with PalmSecure
- 7 Biometric Identification
- 8 Removing user fingerprint
- 9 Troubleshoot

Overview

With Biometric for WCP, you can enrol the user's fingerprint or palm, use it as a 2FA, or just to identify the username.

Prerequisites

AuthControl Sentry v4.0.5 onwards

AuthControl Credential Provider v5.4.5 onwards

Windows 10

Nitgen biometric reader, Fujitsu PalmSecure-F Pro biometric reader or Laptop supporting biometric authentication (Windows Hello) with integrated fingerprint reader

Supported models

Nitgen Fingkey Hamster

Fujitsu PalmSecure-F Pro

Dell, HP and Lenovo Laptops with Windows 10 using Windows Biometric Framework

The following have been tested successfully:

- Dell Vostro 15 5568
- HP Probook 6550b
- Lenovo Thinkpad 13 Gen 2
- Lenovo Thinkpad T520

Nitgen Reader vs Laptop Reader

There are some relevant differences with both types of readers that need to be considered.

1) Enrolment

- Nitgen Reader: enrolment is done during the first login
- Laptop Reader: the user cannot be enrolled during login, so enrolment is done inside AuthControl Credential Provider Configuration

2) Authentication in multiple devices

- Nitgen Reader: allows to authenticate in several devices with only one enrolment
- Laptop Reader: enrolment in each one of the devices is necessary

Configuration for Nitgen Biometric Reader

Configure Third Party Authentication Nitgen

In AuthControl Sentry Management Console, add the following Third Party to Server > Third Party Authentication

Identifier: FingerprintNitgen

Class: com.swiveltechnologies.pinsafe.server.thirdparty.FingerprintNitgen

Enabled: yes

Server>Third Party Authentication

Please enter the details of any third party authentication methods to be used. Third party authentication all place on top of the standard Sentry traffic.

Third parties:

 [WindowsGINA](#)



Identifier:

Class:

Enabled:

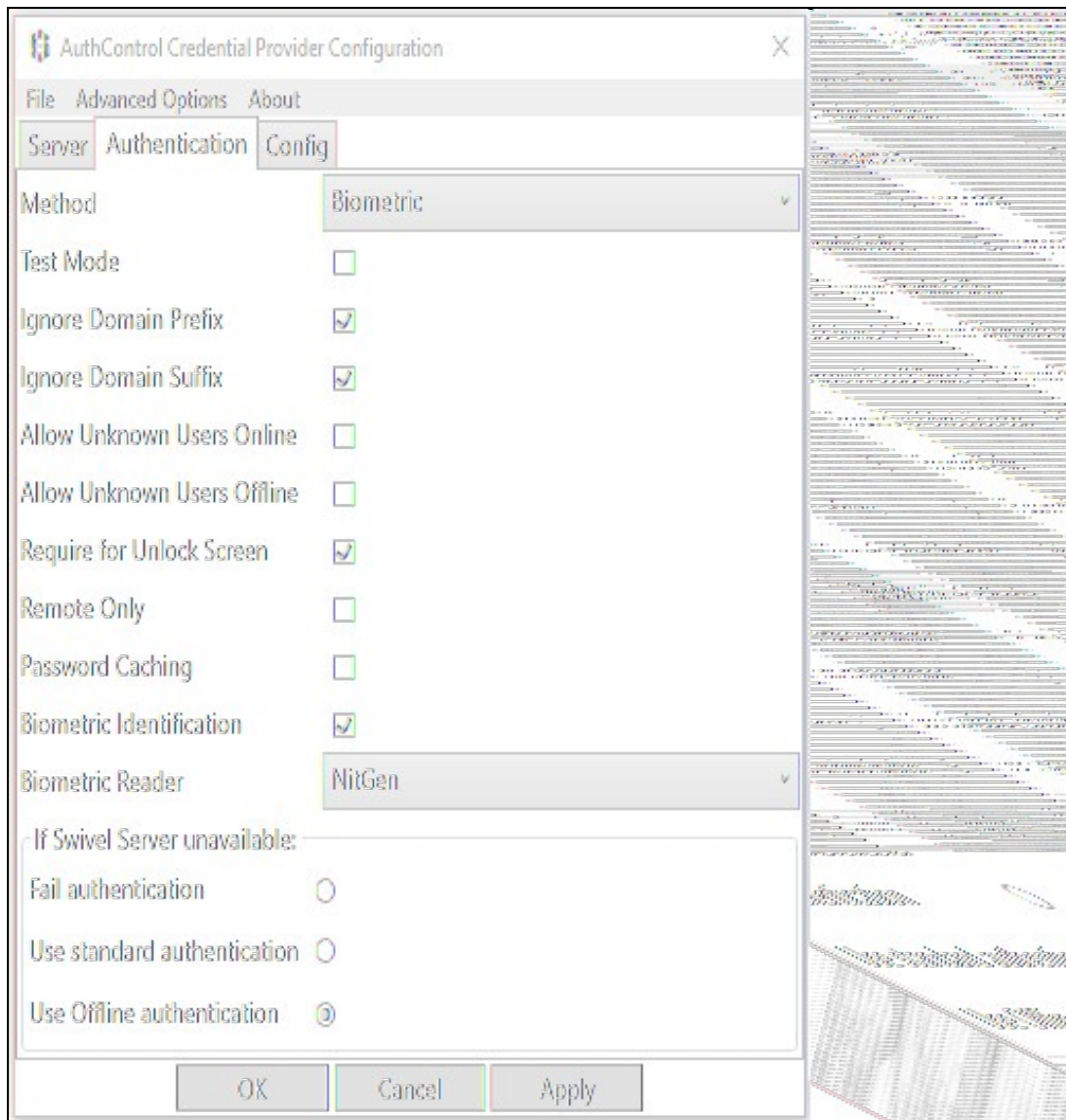
Group:

License key:

Configure Credential Provider

Select in Authentication -> Method the option "Biometric".

Select in Authentication -> Biometric Reader the option "Nitgen".



Enrol the user with Nitgen

When the user is not enrolled, the user is requested, after login with username and password, to enrol the fingerprint.

- 1) Select the finger to enrol
- 2) Place the finger on the sensor the necessary times untill the enrolment is successfull



Authenticating with Nitgen

After authenticating with username and password, when requested, place the finger on the sensor



Configuration for Laptop Biometric Reader

Configure Third Party Authentication

In AuthControl Sentry Management Console, add the following Third Party to Server > Third Party Authentication

Identifier: WinBioFingerprint

Class: com.swiveltechnologies.pinsafe.server.thirdparty.FingerprintNitgen

Enabled: yes

Server>Third Party Authentication

Please enter the details of any third party authentication methods to be used. Third party authentication all place on top of the standard Sentry traffic.

Third parties:

- ☒ [WindowsGINA](#)
- ☒ [FingerprintNitgen](#)
- ☐

Identifier:

Class:

Enabled:

Group:

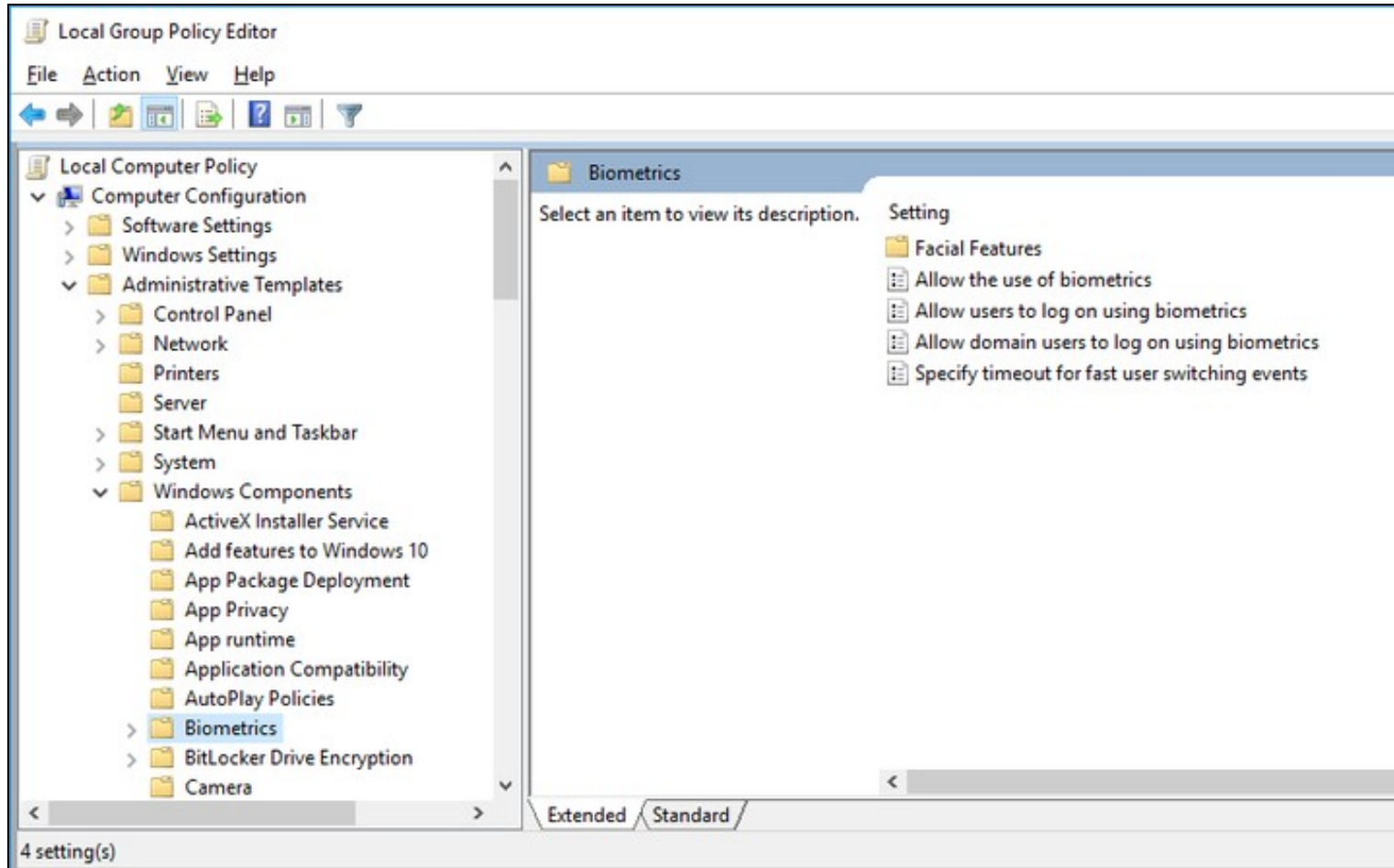
License key:

Disable Windows Hello

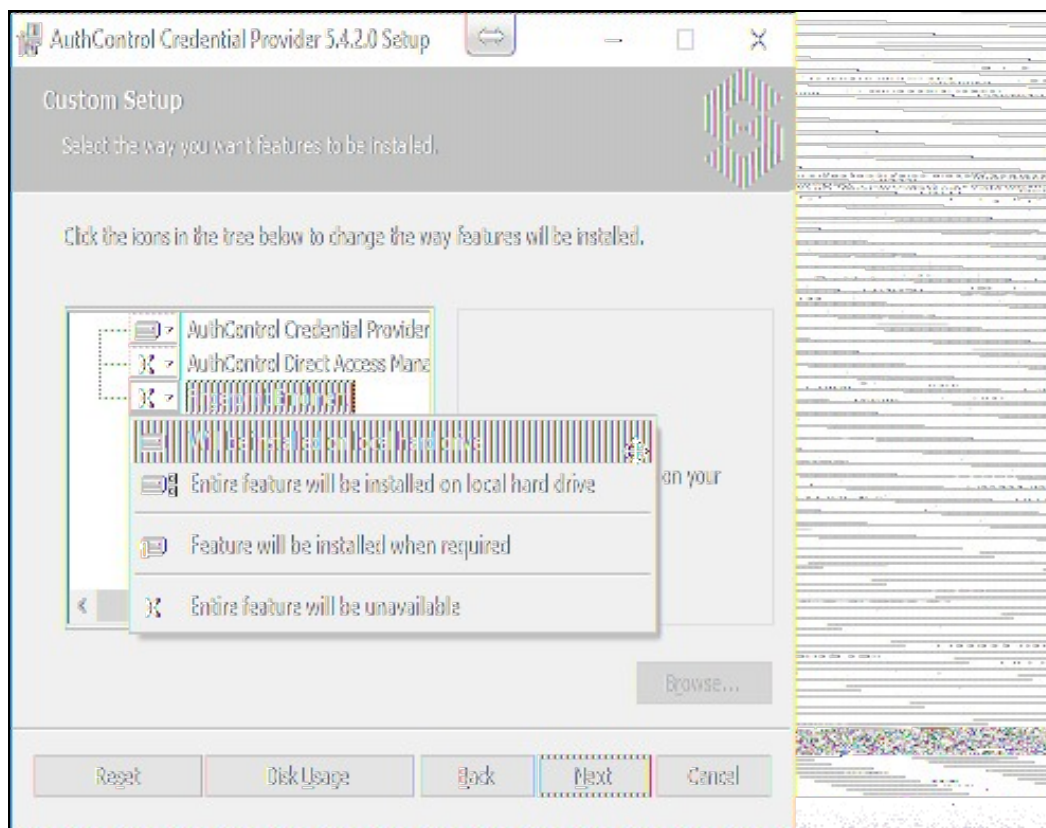
Windows Hello Biometric usage must be disabled in Local Group Policy:

- Access the Windows Local Group Policy Editor.

- Go to: Computer Configuration > Administrative Templates > Windows Components > Biometrics and disable the setting "Allow users to log on user biometrics".



Install Credential Provider with Fingerprint Enrolment

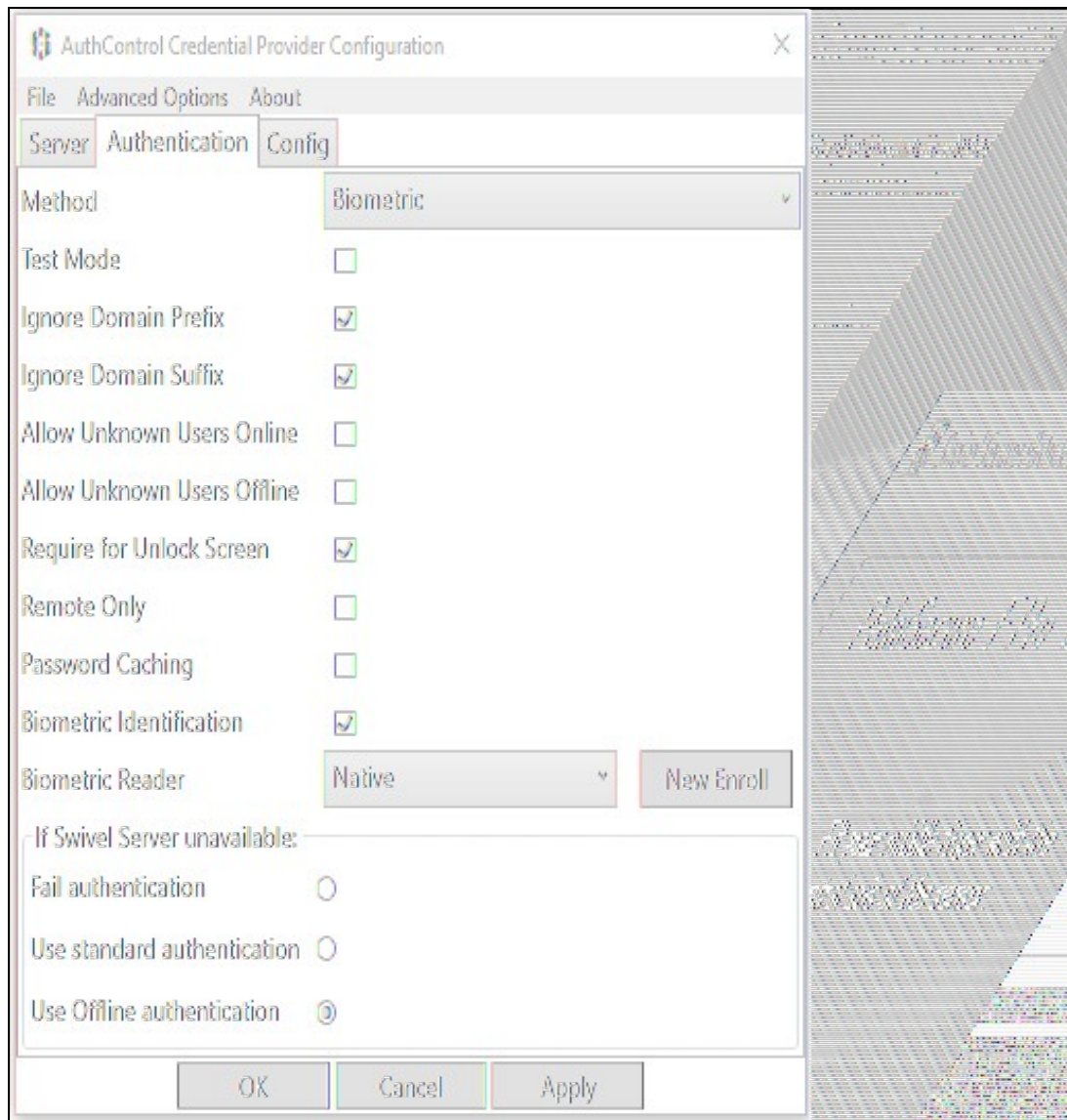


Configure Credential Provider

Select in Authentication -> Method the option "Biometric".

Select in Authentication -> Biometric Reader the option "Native".

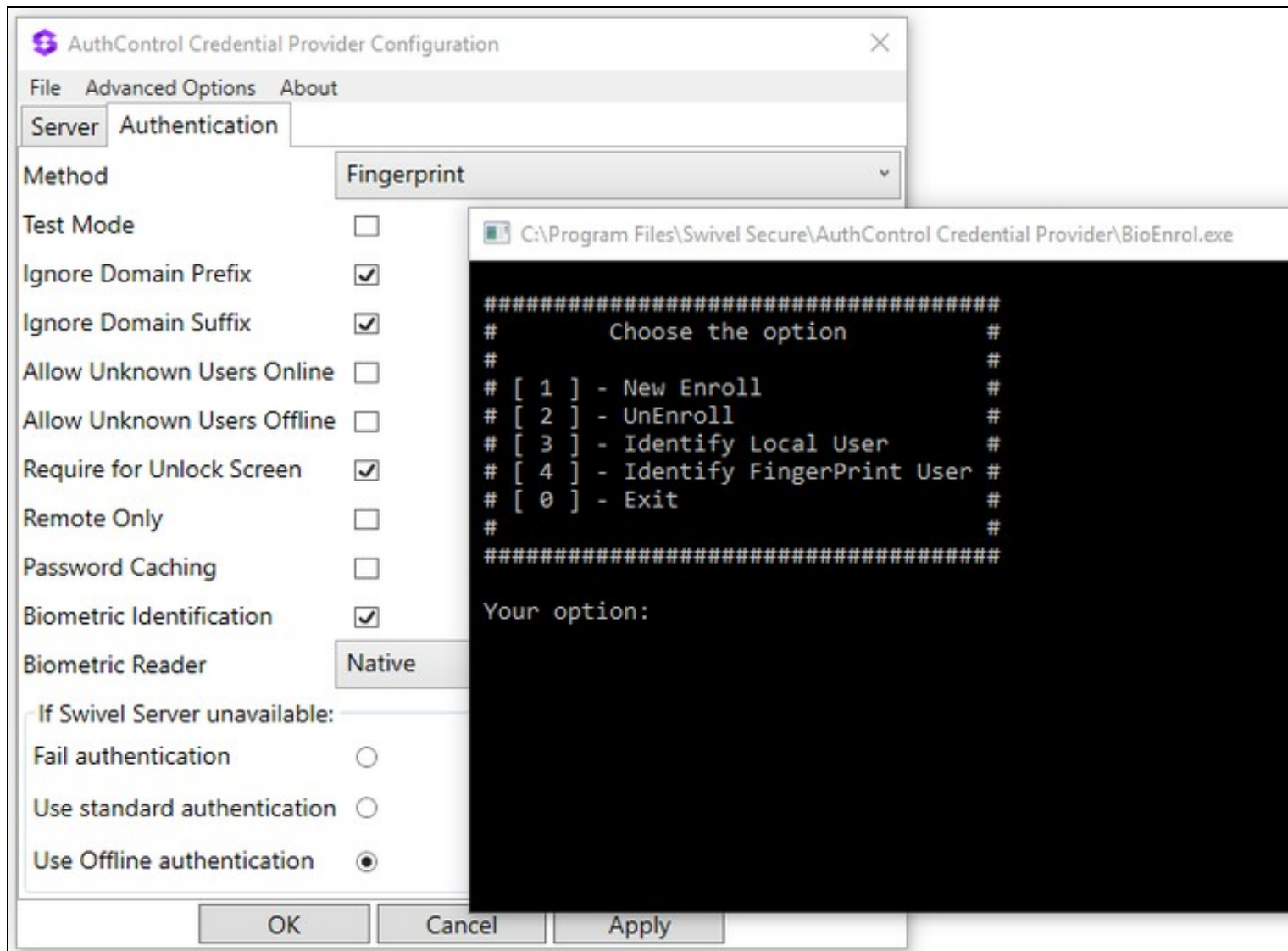
Click Apply.



Enrol the user

After selecting "Native" and clicking **Apply**, click in the button ?New Enroll? to open the "BioEnroll" executable.

Select option 1 to start a new enrol to current user and follow the steps presented.



Authenticating

With all configurations done, go to the Windows login page and access using your registered fingerprint when prompted.



Biometric Native



Swipe your finger

CCCC



Sign-in options



Configuration for Fujitsu PalmSecure-F Pro Biometric Reader

(This section is under construction / The Fujitsu PalmSecure-F Pro Biometric Reader is in Beta testing)

Configure Third Party Authentication PalmSecure

In AuthControl Sentry Management Console, add the following Third Party to Server > Third Party Authentication

Identifier: PalmSecureReader

Class: com.swiveltechnologies.pinsafe.server.thirdparty.FingerprintNitgen

Enabled: yes

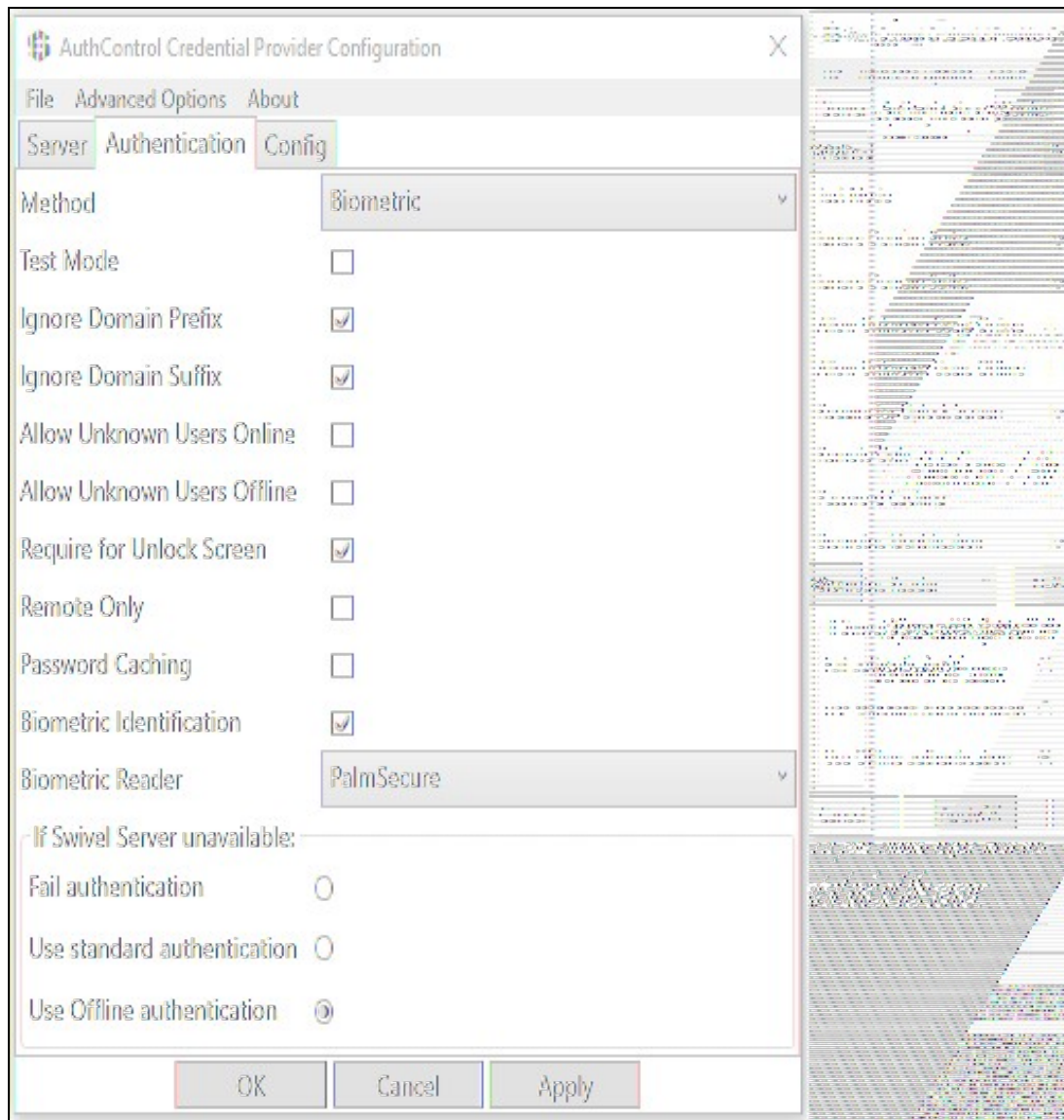
| | |
|--------------|---|
| Identifier: | <input type="text" value="PalmSecureReader"/> |
| Class: | <input type="text" value="com.swiveltechnologies.pinsafe.server.thirdparty.FingerprintNitgen"/> |
| Enabled: | <input type="button" value="Yes"/> |
| Group: | <input type="button" value="--ANY--"/> |
| License key: | <input type="text"/> |

Configure Credential Provider PalmSecure

Select in Authentication -> Method the option "Biometric".

Select in Authentication -> Biometric Reader the option "PalmSecure".

Click Apply.



Enrolment with PalmSecure



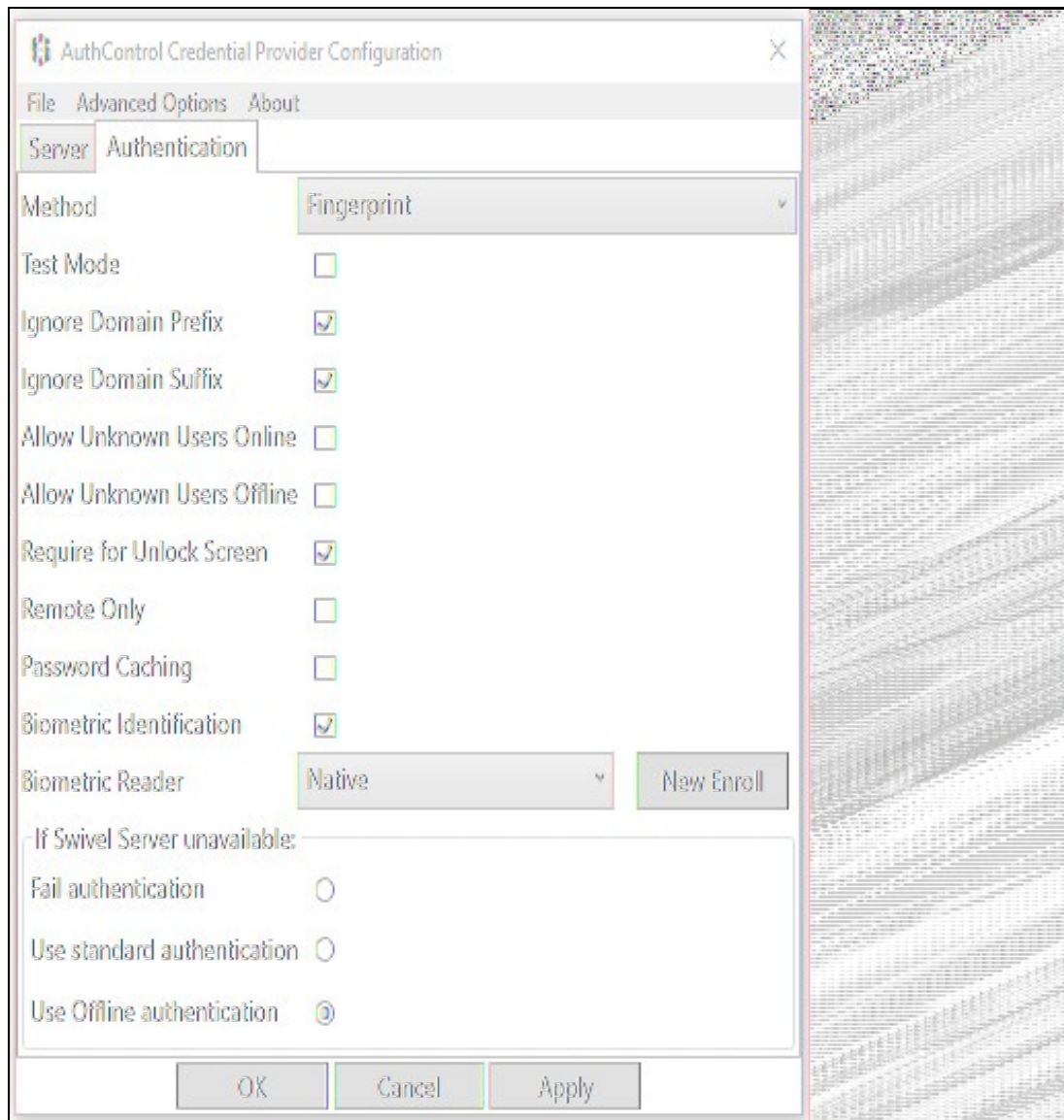
Authenticating with PalmSecure

Identification with PalmSecure



Biometric Identification

It's possible to use Biometric Identification instead of entering the username. First enable "Biometric Identification" under "Authentication" inside the Configuration.



When authenticating, select option "Read Fingerprint" and place your finger on the sensor when requested. If the fingerprint is enrolled, the username is automatically filled.




Removing user fingerprint

To remove a user fingerprint from the appliance, the administrator can go to User Administration, Select View -> Attributes, click the user and select "Remove fingerprint".

Sentry User Administration

Max No. Users: (121 users in this repository)

Users per page:

Repository: 


State: 

username  Contains  user

Members of group: 

View: 

Search

| Username | SAPUsername | altusername | email | familyname | fingerprint | give |
|--|-------------|-------------|----------------|--------------------|--|------|
| user  | | | | | 01 05 00 00 00 00 00 05 15 00 00 00 e0 8d 7d 1f 19... | |
| Edit | Policy | Reset PIN | Reset Password | Remove fingerprint | View ST | |

Troubleshoot

If you have issues with enrolment on the Integrated Laptop Reader, you might need to stop "Windows Biometric Service" or "WbioSrv" under your Windows Services and then delete the files located at "WinBioDatabase" in C:\Windows\System32\WinBioDatabase.