## **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:	<u>     WindowsGINA</u> □	
	Identifier:	FingerprintNitgen
	Class:	com.swiveltechnologies.pinsafe.server.thirdparty.FingerprintNitgen
	Enabled:	Yes •
	Group:	ANY
	License key:	

### **Configure Credential Provider**

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

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

🚯 AuthControl Credential Provide		
File Advanced Options About		
Server Authentication Conf	iq	
Method	Biometric	
Test Mode		
Ignore Domain Prefix		
Ignore Domain Suffix	Z	
Allow Unknown Users Online		
Allow Unknown Users Offline		- i mar i
Require for Unlock Screen		
Remote Only		The All States and States and States
Password Caching		
<b>Biometric Identification</b>	2	
Biometric Reader	NitGen	
-If Swivel Server unavailable: -		The second secon
Fail authentication	0	MANANA SA
Use standard authentication	0	- set situation
Use Offline authentication	٢	
OX	Cancel Apply	

## 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 authenticationg 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

 ${\it Class: } com. swive ltechnologies. pinsafe. server. third party. Finger print Nitgen$ 

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:	Đ	WindowsGINA	
	Ð	<u>FingerprintNito</u>	<u>jen</u>
		Identifier:	WinBioFingerprint
		Class:	com.swiveltechnologies.pinsafe.server.thirdparty.FingerprintNitgen
		Enabled:	Yes T
		Group:	ANY •
		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".

Local Group Policy Editor			
<u>File</u> <u>Action</u> <u>View</u> <u>H</u> elp			
🗢 🔿 📶 🗟 🖬 🍸			
<ul> <li>Local Computer Policy</li> <li>Computer Configuration</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Administrative Templates</li> <li>Control Panel</li> <li>Control Panel</li> <li>Network</li> <li>Printers</li> <li>Server</li> <li>Start Menu and Taskbar</li> <li>System</li> <li>Windows Components</li> <li>ActiveX Installer Service</li> <li>Add features to Windows 10</li> <li>App Package Deployment</li> <li>App Privacy</li> <li>App runtime</li> <li>Application Compatibility</li> </ul>		Biometrics Select an item to view its description.	Setting Facial Features Allow the use of biometrics Allow users to log on using biometrics Allow domain users to log on using biometrics Specify timeout for fast user switching events
<ul> <li>AutoPlay Policies</li> <li>Biometrics</li> <li>BitLocker Drive Encryption</li> <li>Camera</li> </ul>	*		٢
< >		Extended Standard	
4 setting(s)			

Install Credential Provider with Fingerprint Enrolment

AuthControl Crede	ntial Provider 5.4.2.0 Setup	-		
Custom Setup				
Select the way you	want features to be installed.			an a
Click the icons in the	e tree below to change the way	features wil be installed.		
	hControl Credential Provider hControl Direct Access Mana Statistics of the states for the state of the states of the feature will be installed o	n local hard drive	en your	
Fei Rei Rei Fei	ature will be installed when n tire feature w <mark>il</mark> l be unavailabl	equired Ie		
			Browse	
Reget	Disk Usage	gət teg	Cencel	

## **Configure Credential Provider**

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

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

Click Apply.

1 AuthControl Credential Provide	er Configuration X	· · · · · · · · · · · · · · · · · · ·
File Advanced Options About		
Server Authentication Conf	ig	indiain arit ante
Method	Biometric	
Test Mode		
Ignore Domain Prefix	2	
Ignore Domain Suffix	2	
Allow Unknown Users Online		A Shine was
Allow Unknown Users Offline		
Require for Unlock Screen	~	
Remote Only		1 Robertown Sta
Password Caching		
<b>Biometric Identification</b>	2	
Biometric Reader	Native Mew Enroll	
-If Swivel Server unavailable: -		Austral Charach
Fail authentication	0	องว่าอ่างได้ระดอา
Use standard authentication	0	
Use Offline authentication	٥	1998
ОХ	Cancel Apply	

### Enrol the user

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

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

S AuthControl Credential Provi	der Configurati	ion X
Server Authentication		
Method	Fingerprint	v
Test Mode		C:\Program Files\Swivel Secure\AuthControl Credential Provider\BioEnrol.exe
Ignore Domain Prefix	<b>v</b>	
Ignore Domain Suffix	<b>v</b>	######################################
Allow Unknown Users Online		# # #
Allow Unknown Users Offline		# [ 2 ] - UnEnroll #
Require for Unlock Screen	<b>v</b>	<pre># [ 3 ] - Identify Local User # # [ 4 ] - Identify FingerPrint User #</pre>
Remote Only		#[0]-Exit #
Password Caching		***************************************
Biometric Identification	<u> </u>	Your option:
Biometric Reader	Native	
If Swivel Server unavailable:		
Fail authentication	0	
Use standard authentication	0	
Use Offline authentication	0	
	•	
ОК	Cand	cel Apply

## Authenticating

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



# 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:	PalmSecureReader	
Class:	com.swiveltechnologies.pinsafe.server.thirdparty.FingerprintNitgen	
Enabled:	Yes 7	
Group:	ANY	
License key:		e e e e e e e e e e e e e e e e e e e

### **Configure Credential Provider PalmSecure**

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

 $\label{eq:select} Select \ in \ Authentication \ -> \ Biometric \ Reader \ the \ option \ "PalmSecure".$ 

Click Apply.

B AuthControl Credential Provide	er Configuration X	is the same instance with a
File Advanced Options About		Selicity of the second
Server Authentication Confi	g	
Method	Biometric v	
Test Mode		
Ignore Domain Prefix	<i>s</i> /	
Ignore Domain Suffix	J.	
Allow Unknown Users Online		
Allow Unknown Users Offline		
Require for Unlock Screen	s.	513 013 103 103 103 103 103 103 103 103 1
Remote Only		Warnin, Anin 11.7
Password Caching		
Biometric Identification	<b>1</b>	1.00 0000 0000 000 000 000 000 000 000 0
Biometric Reader	PalmSecure	
- If Swivel Server unavailable: -		
Fail authentication	0	a vini vilitani
Use standard authentication	0	
Use Offline authentication	0	1000
OK	Cancel 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.

🚯 AuthControl Credential Provid	der Configuration X	
File Advanced Options About		
Server Authentication		Martin Carl
Method	Fingerprint v	and the second
Test Mode		10.2
Ignore Domain Prefix	V	
Ignore Domain Suffix		
Allow Unknown Users Online		
Allow Unknown Users Offline		
Require for Unlock Screen		
Remote Only		and the second secon
Password Caching		
Biometric Identification	2	
Biometric Reader	Native • New Enroll	
-If Swivel Server unavailable:		
Fail authentication	0	
Use standard authentication	0	
Use Offline authentication	٢	
OX	Cancel Apply	

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".

Max No. User	2: 2221 (-)(11)	200	(121	users in this re	pository)	
Users per pag	8:	100				
Repository:		Local XML			7	
State:		All			7	
usemame	7	Contains 7	Iser			
View:	roup.	Attributes 7			Se	arch
Usemame	SAPUsername	altusername	email	familyname	fingerprint	give
					01 05 00 00 00 00 00 05 15 00 00 00 e0 8d 7d 1f	
user 🔼					19	

# Troubleshoot

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