
Installation Guide

Advanced Authentication Device Service

Version 6.1

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.netiq.com/company/legal/>.

Copyright © 2018 NetIQ Corporation, a Micro Focus company. All Rights Reserved.

Contents

About NetIQ Corporation	5
About this Book	7
1 System Requirements	9
Supported Card Readers and Cards	10
Supported Devices for PKI	11
Supported Fingerprint Readers	11
2 Installing and Uninstalling Device Service	13
Installing Device Service on Windows	13
Uninstalling Device Service on Windows	14
Uninstalling Device Service through Setup Wizard	14
Uninstalling Device Service through Control Panel	14
Installing Device Service on Linux	15
Upgrading Device Service on Linux	15
Uninstalling Device Service on Linux	16
Installing Device Service on Mac	16
Uninstalling Device Service on Mac	17
3 Configuring Device Service	19
Card Settings	19
Fingerprint Settings	20
PKI Settings	21
Configuring the PKI Device	22
Configuring e-Token PRO	23
Configuring the YubiKey PKI	23
Configuring OpenSC	25
Performing Bulk Replacement of Configuration File	26
4 Troubleshooting	27
Generic Issues	29
Card Related Issues	29
FIDO U2F Related Issues	30
Fingerprint Related Issues	30
PKI Related Issues	30
Issue with YubiKey PKI	30
Unable to Import a Certificate to the YubiKey Token	31
Bluetooth Issues	31
Configuring Gemalto Smart Card with Advanced Authentication	31
Installing the SafeNet Authentication Client 10	31
Generating the Customized MSI file	32
Configuring PKCS Path in the Device Service	32
Configuring the Virtual Machine for Working of the RF IDEas Readers	32

5 Developer Information35

Card Plug-in35

FIDO U2F Plug-in36

Fingerprint Plug-in.....37

PKI Plug-in38

Bluetooth Plug-in.....40

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- ♦ Identity & Access Governance
- ♦ Access Management
- ♦ Security Management
- ♦ Systems & Application Management
- ♦ Workload Management
- ♦ Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

About this Book

The *Advanced Authentication Device Service Guide* has been designed for all users and describes system requirements that must be fulfilled before the installation of Advanced Authentication Device Service.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

About Device Service

Device Service provides you with an ability to use compliant fingerprint devices, contact and contactless cards, PKI smart cards, crypto sticks, and FIDO U2F tokens during enrollment in Advanced Authentication Self-Service Portal and for further authentication.

1 System Requirements

The following table provides information about supported platforms for Device Service:

	Microsoft Windows	Apple MacOS X	Linux
Card plug-in	x	x	x
Face plug-in	x	x	x
FIDO U2F plug-in	x	x	x
Fingerprint plug-in	x		
PKI plug-in	x	x	x
Bluetooth	x	x	x
Windows Hello plug-in	x		

Device Service for Windows supports Card and PKI redirection to Remote Desktop and Citrix terminal sessions. You must have Device Service installed on the terminal server to perform the redirection.

Device Service also supports virtual channel and you must have the Device Service installed on the both the terminal client and terminal server.

NOTE: Local administrator (Windows)/ root (Mac OS X, Linux) privileges are required for installing and removing Device Service.

Ensure that the system meets the following requirements:

- ♦ **Operating system:** Any of the following operating systems is installed based on the platform.
 - ♦ **Windows**
 - ♦ Microsoft Windows 7 Service Pack1 (32-bit and 64-bit)
 - ♦ Microsoft Windows 8.1 (32-bit and 64-bit)
 - ♦ Microsoft Windows 10 (v1709/ v1803/ v1809 32-bit and 64-bit)
 - ♦ Microsoft Windows Server 2012 R2
 - ♦ Microsoft Windows Server 2016
 - ♦ **Apple Mac OS** 10.12 (Sierra), 10.13 (High Sierra)
 - ♦ **Linux**
 - ♦ CentOS 7 with KDE or Gnome desktop environment
 - ♦ SUSE Linux Enterprise Desktop 11 Service Pack 4
 - ♦ SUSE Linux Enterprise Desktop 12 Service Pack 3
 - ♦ SUSE Linux Enterprise Desktop 15
 - ♦ SUSE Linux Enterprise Server 11 Service Pack 4
 - ♦ SUSE Linux Enterprise Server 12 Service Pack 3

- ♦ SUSE Linux Enterprise Server 15
- ♦ Red Hat Enterprise Linux Workstation 7.5
- ♦ Red Hat Enterprise Linux Server 7.5
- ♦ Debian 9.5
- ♦ Ubuntu 16, 18
- ♦ **Browsers:** Any of the following browsers are installed.
 - ♦ Microsoft Internet Explorer 11
 - ♦ Google Chrome 65 and later
 - ♦ Mozilla Firefox 58 and later
 - ♦ Safari 11 and later
 - ♦ Microsoft Edge 20.0 and later

To run Device Service on Microsoft Edge, perform the following steps:

 1. Open the command prompt with elevated privileges.
 2. Run the command `CheckNetIsolation LoopbackExempt -a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe`
 3. Open **about:flags** and ensure that the **Allow localhost loopback** option is enabled.
- ♦ **Bluetooth:** Only Bluetooth is supported, BLE is not supported.

NOTE: It is not recommended to use the Bluetooth feature on VMware virtual machines, because false authentication can occur when Bluetooth device is disabled or it is out of range.

For more information about additional system requirements, see the following sections:

- ♦ [Supported Card Readers and Cards](#)
- ♦ [Supported Devices for PKI](#)
- ♦ [Supported Fingerprint Readers](#)

Supported Card Readers and Cards

Advanced Authentication stores the serial number of a card during enrollment and validates the serial number later during the user's authentication.

Advanced Authentication supports the following cards and card readers:

- ♦ **Contactless card readers**
 - ♦ ACS ACR122
 - ♦ Broadcom Corp Contactless SmartCard
 - ♦ Elatec RFID
 - ♦ HID OMNIKEY CardMan 5x25
 - ♦ HID OMNIKEY 5326
 - ♦ HID OMNIKEY 5x2x
 - ♦ RF IDEas pcProx series
 - ♦ NXP PR533

- ♦ **Non supported readers**
 - ♦ LEGIC AIR ID series
- ♦ **Contactless smart cards**
 - ♦ HID iClass series
 - ♦ HID Prox series
 - ♦ MIFARE Classic 1K/4K, Ultra Light, Ultra Light C, Plus
 - ♦ MIFARE DESFIRE 0.6, MIFARE DESFIRE EV1, MIFARE SE, DESFire

Supported Devices for PKI

Advanced Authentication supports the certificate-based PKCS#11 contact smart cards and USB tokens (crypto sticks).

Device Service supports the following devices:

- ♦ Aladdin eToken PRO 32k/72k with SafeNet Authentication Client 9
- ♦ ruToken
- ♦ SafeNet Authentication eToken on the Mac OS.

To use PKI, specify a PKCS#11 module for your PKI device. See [PKI Settings](#) for more information.

The following are the requirements for used certificates:

1. Certificate must contain the Authority Information Access (AIA) and Certificate Revocation List (CRL) link to check revocation status.
2. Certificate must contain a key pair: public and private key in the x509 format. The certificates that do not comply with the requirements are ignored (hidden during enrollment).

NOTE: The cards Cosmo polIC 64K V5.2 and Cyberflex Access 64K V1 SM 2.1 support the certificate-based enrollment only (generate a key pair mode is not supported).

To support the SafeNet Authentication eToken (PKI) on the Mac OS, perform the following steps:

- 1 Install the latest [Device Service 6.0](#) on Mac OS.
- 2 Install the `SafenetAuthenticationclient9.1.2.0.dmg` package.
You can download SafeNet Authentication Client from [Knowldege Symantec](#) website.
- 3 Run the following commands to restart the Device Service:
 1. `sudo launchctl unload /Library/LaunchDaemons/com.netiq.deviceservice.plist`
 2. `sudo launchctl load /Library/LaunchDaemons/com.netiq.deviceservice.plist`
- 4 Plug-in the SafeNet Authentication eToken (PKI) to Mac OS.

Supported Fingerprint Readers

Device Service supports fingerprint readers that use [Windows Biometric Framework \(WBF\)](#), Lumidigm readers, and Digital Persona readers.

NOTE: After migrating from Advanced Authentication v5, users may need to re-enroll the Fingerprint authenticators if they have enrolled the authenticators on the WBF compliant readers. This is because, the previous authenticators may contain low quality fingerprint images. Re-enrollment for the Lumidigm and Digital Persona readers is not required.

Ensure that the system meets the following requirements for the WBF compliant readers:

- ♦ A reader must be available in Device Manager in the **Biometric devices** section.
- ♦ The **Windows Biometric Service** (in services.msc) must be set to `Automatic` and must be in a running state.
- ♦ The policies **Allow to use of biometrics**, **Allow users to log on using biometrics**, **Allow domain users to log on using biometrics** (Computer Configuration - Administrative Templates - Windows Components - Biometrics) must be enabled.

Device Service supports the following fingerprint readers:

- ♦ Lumidigm readers
- ♦ Digital Persona readers
- ♦ NEXT Biometrics NB-3010-UL
- ♦ Precise Biometrics 100 X with AuthenTec AES2501B
- ♦ Zvetco Verifi P2500 with AuthenTec AES2550
- ♦ Zvetco Verifi P5100
- ♦ Zvetco Verifi P5200 with TouchChip Fingerprint Coprocessor
- ♦ Zvetco Verifi P6000
- ♦ Synaptic FP Sensors (WBF) (VID=138A, PID=0011)
- ♦ Synaptic FP Sensors (WBF) (VID=138A, PID=0017)
- ♦ Validity Sensor (VFS495) (VID=138A, PID=003F)
- ♦ Validity Sensors (WBF) (VID=138A, PID=0050)
- ♦ SecuGen Hamster Plus (HSDU03P)

Device Service does not support the following devices:

- ♦ SecuGen Hamster IV (HFDU04)
- ♦ SecuGen Hamster (HFDU02R)
- ♦ Synaptics WBDI (Lenovo t460s laptops)
- ♦ Futronic FS80, FS88

IMPORTANT: Advanced Authentication Windows Hello authenticator supports all the fingerprint readers that are supported by Microsoft Windows Hello.

NOTE: It is recommended to use Microsoft Surface Pro type cover with the Fingerprint ID for the Windows Hello method.

Usage of fingerprint readers requires manual configuration. For more information, see [Fingerprint Settings](#).

NOTE: Swipe readers may face issues with fingerprint matching because of low quality sensors.

2 Installing and Uninstalling Device Service

Before installing Device Service, ensure that you close all the web browsers. The installation procedure varies for different operating systems.

NOTE: You can find the Device Service component in the Advanced Authentication Enterprise Edition or the Remote Access Edition distributive package.

Device Service on Microsoft Windows

- ♦ [Installing Device Service on Windows](#)
- ♦ [Uninstalling Device Service on Windows](#)

Device Service on Apple Mac OS X

- ♦ [Installing Device Service on Mac](#)
- ♦ [Uninstalling Device Service on Mac](#)

Device Service on Linux

- ♦ [Installing Device Service on Linux](#)
- ♦ [Upgrading Device Service on Linux](#)
- ♦ [Uninstalling Device Service on Linux](#)

NOTE: After installing or upgrading the web browser, ensure to reinstall the Device Service.

WARNING: During the upgrade of Device Service on Apple Mac OS X and Linux, the configuration file is overwritten with a default one. Ensure that you have a copy of the file and put it back to the folder after the Device Service upgrade.

Installing Device Service on Windows

1. Run `naaf-deviceservice-x86-release-<version>.msi`.
2. Click **Next**.
3. Read and accept the licence agreement.
4. Click **Next**.
 - ♦ To change the destination folder, click **Change** and select an applicable destination.
 - ♦ To continue, click **Next**.
5. Click **Install** and wait until the component is installed.
6. Click **Finish**.

NOTE: To upgrade Device Service on a Windows machine that has a McAfee virus protection software installed, ensure to disable the McAfee protection. For more information about how to disable McAfee protection for a temporary period, see [link1](#) and [link2](#).

Uninstalling Device Service on Windows

You can uninstall Device Service through the Setup Wizard or through Control Panel.

- ♦ [Uninstalling Device Service through Setup Wizard](#)
- ♦ [Uninstalling Device Service through Control Panel](#)

Uninstalling Device Service through Setup Wizard

1. Run `naaf-deviceservice-x86-release-<version>.msi`.
2. Click **Next**.
3. Select **Remove** and click **Next**.
4. Click **Remove**.

Uninstalling Device Service through Control Panel

To uninstall Device Service through Control Panel, select one of the following options that corresponds to your operating system:

- ♦ [Microsoft Windows 7](#)
- ♦ [Microsoft Windows 8.1](#)
- ♦ [Microsoft Windows 10](#)

Microsoft Windows 7

1. In the **Start** menu, select **Control panel** and then double-click **Programs and Features**.
2. Select **NetIQ Device Service** and click **Uninstall**.
3. Confirm the uninstallation.

Microsoft Windows 8.1

1. In the **Search** menu, select **Apps > Control Panel > Programs > Programs and Features**.
2. Select **NetIQ Device Service** and click **Uninstall**.
3. Confirm the uninstallation.

Microsoft Windows 10

1. Right-click **Start** and select **Control Panel > Programs > Programs and Features**.
2. Select **NetIQ Device Service** and click **Uninstall**.
3. Confirm the uninstallation.

Installing Device Service on Linux

IMPORTANT: To use Device Service for FIDO U2F tokens, you must allow the FIDO U2F usage on Linux. For more information, see [yubico FAQ](#).

To install Device Service on Linux operating system, run the following commands depending on your platform.

Ubuntu, Debian (deb package)

The components `libnss3-tools` are used for Card or PKI plug-in, `pcscd` for HID OMNIKEY reader, and `bluez` for Bluetooth plug-in.

```
sudo apt-get install pcscd
sudo apt-get install libnss3-tools
sudo apt-get install bluez
sudo dpkg -i naaf-deviceservice-linux64-release-<version>.deb
```

openSUSE, SUSE

The components `libpcsc-lite1` and `nss-tools` are for Card/PKI plug-in and `bluez` for Bluetooth plug-in.

```
sudo zypper install libpcsc-lite1
sudo zypper install mozilla-nss-tools
sudo zypper install bluez
sudo rpm -i naaf-deviceservice-linux64-release-<version>.rpm
```

Fedora, CentOS, RHEL

The components `nss-tools` are for Card/PKI plug-in and `bluez` for Bluetooth plug-in.

```
sudo yum install nss-tools
sudo yum install bluez
sudo rpm -Uvh naaf-deviceservice-linux64-release-<version>.rpm
```

NOTE: During the installation of Device Service on CentOS or RHEL operating system, there could be dependency issues related with the `pcsc-lite` package. Install the required package with `yum install pcsc-lite` and restart the installation of Device Service.

Upgrading Device Service on Linux

To upgrade Device Service on Linux operating system, run the following commands depending on your platform.

NOTE: Device Service has been renamed from `deviceservice` to `naaf-deviceservice` from Advanced Authentication 5.3 Hotfix 1.

Ubuntu, Debian (deb package)

To upgrade Device Service 5.3 or later, remove the old package and install a new package.

1. Remove device service package.

```
sudo apt-get remove deviceservice-<version>.x86_64
```

```
sudo apt-get install bluez
```

```
sudo dpkg -i naaf-deviceservice-linux64-release-<version>.deb
```

openSUSE, Fedora (rpm package)

To upgrade Device Service 5.3 or later, remove the old package and install a new package.

openSUSE

1. Remove device service package.

```
sudo rpm -e deviceservice-<version>.x86_64
```

```
sudo zypper install bluez
```

```
sudo rpm -i naaf-deviceservice-linux64-release-<version>.rpm
```

Fedora

1. Remove device service package.

```
sudo rpm -e deviceservice-<version>.x86_64
```

```
sudo yum install bluez
```

```
sudo rpm -Uvh naaf-deviceservice-linux64-release-<version>.rpm
```

Uninstalling Device Service on Linux

Run the following commands depending on your platform:

Ubuntu, Debian (deb package)

```
sudo dpkg --purge naaf-deviceservice-<version>.x86_64
```

openSUSE, Fedora

```
rpm -e naaf-deviceservice-<version>.x86_64
```

Installing Device Service on Mac

1. Double click the file naaf-deviceservice-macos-release-<version>.dmg.

The naaf-deviceservice.pkg and uninstall files are displayed.

2. Double click the file naaf-deviceservice.pkg.
3. Click **Continue**.
4. Read and accept the license agreement.
5. Select the disk where you want to install Device Service and click **Continue**.
6. Click **Install**.

A window is displayed to specify the local administrator credentials to install the software.

7. Specify **User name** and **Password**.

8. Click **Install Software**.
9. Click **Close**.

Uninstalling Device Service on Mac

You can uninstall the Device Service in two ways:

- ♦ [Using Uninstall Script](#) (recommended)
- ♦ [Manual](#)

Using Uninstall Script

- 1 Double click the file `naaf-deviceservice-macos-release-<version>.dmg`.
The `naaf-deviceservice.pkg` and `uninstall` files are displayed.
- 2 Click the `uninstall` file.
- 3 Specify sudo password.

Manual

- 1 Open the **Terminal** application.
- 2 Run the command to stop the Device Service.

```
sudo launchctl unload /Library/LaunchDaemons/com.netiq.deviceservice.plist
```
- 3 Delete the directory `Device Service` in `/Library/LaunchDaemons/NetIQ/`.

NOTE: If you uninstall Device Service manually, you must remove the NetIQ certificates for the following browsers.

- ♦ **Safari or Google Chrome:** Remove the NetIQ certificate in **Launchpad > Other > Keychain access**.
 - ♦ **Firefox:** Remove the NetIQ certificate in **Preferences > Privacy & Security > View certificates > Authorities**.
-

3 Configuring Device Service

Device Service contains the configuration file that is located in the following folder, depending on your platform:

- ♦ **Microsoft Windows:** `C:\ProgramData\NetIQ\Device Service\config.properties.`
- ♦ **Linux:** `/opt/NetIQ/Device Service/config.properties.`
- ♦ **Apple Mac OS X:** `/Library/LaunchDaemons/NetIQ/Device Service/config.properties.`

WARNING: During the upgrade of Device Service on Apple Mac OS X and Linux, the configuration file is overwritten with a default one. Ensure that you have a copy of the file and put it back to the folder after the Device Service upgrade.

NOTE: In the `host.ports` parameter, the supported ports are 8440, 8441, and 8442.

See the following settings for the Device Service configuration.

- ♦ [“Card Settings” on page 19](#)
- ♦ [“Fingerprint Settings” on page 20](#)
- ♦ [“PKI Settings” on page 21](#)
- ♦ [“Performing Bulk Replacement of Configuration File” on page 26](#)

To apply the changes, reboot the machine.

Card Settings

Advanced Authentication supports the Microsoft policy [Interactive logon: Smart card removal behavior](#), which allows you to select an action on a card event. You can configure it to perform a force log off or lock a user session when a user presents card to the reader.

To configure card settings, perform the following steps:

- 1 Open the configuration file depending on the platform:
 - ♦ **Microsoft Windows:** `C:\ProgramData\NetIQ\Device Service\config.properties.`
 - ♦ **Linux:** RF IDEas readers are not supported.
 - ♦ **Apple Mac OS X:** IDEas readers are not supported.
- 2 Set the parameters as follows:

Parameter	Description
<code>card.omnikeyEnabled</code>	Used for the omnikey type of readers. The default value is <code>true</code> . Set the value to <code>false</code> to disable the usage of the device.
<code>card.rfideasEnabled</code>	Used for the RF IDEas readers. The default value is <code>false</code> . Set the value to <code>true</code> to enable the usage of the device.

Parameter	Description
<code>card.rfideas.productType</code>	Used for RF IDEas readers. The possible values are <code>prox</code> , <code>sonar</code> , or <code>swipe</code> , or all. You can combine them as <code>prox;sonar;swipe</code> . The default value is <code>prox</code> .
<code>card.rfideas.deviceType</code>	The possible values are <code>usb</code> , <code>serial</code> , or <code>tcp</code> , or all. You cannot combine them. The default value is <code>usb</code> .
<code>card.forceVirtualChannels</code>	Used for RF IDEas readers to work in a terminal session. If you set <code>card.forceVirtualChannels</code> to <code>true</code> , the Device Service uses its own mechanism for card redirection through the virtual channels. You must install the Device Service on both the terminal server and terminal client. The default value is <code>false</code> .
<code>card.desfireEnabled</code>	Used for the desfire type of readers. The default value is <code>true</code> . Set the value to <code>false</code> to disable the usage of the device.

3 Save the changes.

4 Restart the Device Service.

Fingerprint Settings

Device Service supports the following modes for fingerprint readers:

- ♦ **fingerprint.mode: 1** to use the WBF API mode: In this mode, Advanced Authentication works with a processed fingerprint reader in [Windows Biometric Framework API](#).
- ♦ **fingerprint.mode: 2** to use the WBF Direct mode: In this mode, Advanced Authentication works directly with a device driver.

NOTE: Some WBF compliant readers may work only in the WBF Direct mode, for example, the [NEXT Biometrics](#) readers. You can download the NEXT Biometrics driver from the [link](#).

- ♦ **fingerprint.mode: 3** to use the Lumidigm mode. You must install the Lumidigm Drivers. You can download the drivers from the [HID Global](#) website. Some devices require that the Lumidigm Device Service is installed.
- ♦ **fingerprint.mode: 4** to use the DigitalPersona mode. You must install the DigitalPersona U.are.U RTE. You can download it from the [DigitalPersona](#) website.

Device Service supports multiple fingerprint modes. You can configure multiple modes in the following ways:

- ♦ Specify numeric values assigned to each mode.

For example: **fingerprint.mode: 1,2,3** to use WBF API, WBF Direct, and Lumidigm modes.
- ♦ Specify the mode names.

For example: **fingerprint.mode: WbfDirect,DigitalPersona** to use WBF Direct, and DigitalPersona modes.

- ◆ Specify the combination of numeric value and mode name.

For example: **fingerprint.mode:1,WbfDirect,3** to use WBF API, WBF Direct, and Lumidigm modes.

NOTE: The `fingerprint.mode: auto` is the default mode which enables Lumidigm, DigitalPersona, and WbfDirect modes.

To change the fingerprint settings, perform the following steps:

1. Open the configuration file depending on your platform:
 - ◆ **Microsoft Windows:** `C:\ProgramData\NetIQ\Device Service\config.properties`.
 - ◆ **Linux:** Fingerprint readers are not supported.
 - ◆ **Apple Mac OS X:** Fingerprint readers are not supported.

2. Add a string to configure single or multiple modes.

For example:

- ◆ **fingerprint.mode: 3** to use the Lumidigm mode
- ◆ **fingerprint.mode: 1,WbfDirect,3** to use the WBF API, WBF Direct, and Lumidigm modes.

3. Add optional parameters (if required):

- ◆ `fingerprint.captureTimeout: 15` of capture inactivity in seconds.

NOTE: The parameters are case-sensitive.

4. Save the changes.
5. Restart the Device Service.

NOTE: The parameter `fingerprint.isoSupported: true` (default value is `true`) helps Device Service to extract ISO from raw image that it gets from user who scanned his fingerprint for authentication. This parameter helps to eliminate this additional step on the server and improves the authentication speed on the server.

If you set the parameter to `false`, Device Service sends raw image to Advanced Authentication server and the server will need to extract ISO to compare it with a stored authenticator. This may cause performance issues in environments where hundreds of users perform fingerprint authentication at the same time.

PKI Settings

This section describes the following configurations:

- ◆ [Configuring the PKI Device](#)
- ◆ [Configuring e-Token PRO](#)
- ◆ [Configuring the YubiKey PKI](#)
- ◆ [Configuring OpenSC](#)

Configuring the PKI Device

To use PKI, you must specify a PKCS#11 module for your PKI device. To do this, perform the following steps:

1. Open the configuration file based on the operating system:
 - ♦ **Microsoft Windows:** C:\ProgramData\NetIQ\Device Service\config.properties.
 - ♦ **Linux:** /opt/NetIQ/Device Service/config.properties.
 - ♦ **Apple Mac OS X:** /Library/LaunchDaemons/NetIQ/Device Service/config.properties.
2. Remove the hash sign(#) before vendorModule to remove any comments from the parameter.
3. Set the vendor module specific dll file name to the parameter.

```
pki.vendorModule: <filename>.dll
```

For example, pki.vendorModule: rtPKCS11.dll.

NOTE: You can specify more than one PKCS#11 library with semicolon in the format:

```
pki.vendorModule: eToken.dll;rtPKCS11.dll
```

If a vendor module is not located in the **system32** directory, use \\ to specify the path. If there are any spaces in the path, ensure not to replace the space with \\ in the path.

For example, pki.vendorModule: C:\\Program Files\\ActivIdentity\\ActivClient\\acpkcs211.dll.

NOTE: If you have specified some pki.vendorModules separated by a semicolon, you must specify the same number of values for the parameter pki.blockingMode.

For example, pki.blockingMode: true;false.

PKI plugin of the Device Service supports the automatic mode, where a few known vendor modules are detected automatically. You must specify: pki.vendorModule: auto.

The following are the auto detectable vendor modules for different platforms.

4. (Optional) Specify the additional parameters:

- a. **Hash method**

```
pki.hashMethod: SHA256
```

The default value is SHA256 and you can specify this value, if a parameter is not presented. The following methods are also supported: SHA224, SHA384, SHA512. To set the methods, ensure that the PKCS#11 module supports the required hash method.

- b. **Padding**

```
pki.padding: PKCS#1
```

The default value is PKCS#1 and you can specify this value, if a parameter is not presented. The following options are also supported: **PSS**, **OAEP**.

- c. **Key size**

```
pki.modulusBits: 2048
```

The default value is 2048 bit. For example, eToken PRO 32k does not support it and you need to set 1024 to use it.

- d. **Blocking mode**

```
pki.blockingMode: true
```

This parameter is used to detect and monitor the token connected to your system. It is set to `true` by default. OpenSC does not support the 'waiting for card' mechanism and it requires to change the option to `False`. Most of the vendors module work appropriately in the default mode.

NOTE: If you specify both the parameters `pki.vendorModule: auto` and `pki.blockingMode`, the `pki.blockingMode` does not overwrite a blocking mode that is pre-defined for an auto-detectable vendor module.

5. Save the changes.
6. Restart the Device Service.

Configuring e-Token PRO

- 1 Navigate to one of the following paths and open the configuration file based on the operating system:
 - ♦ **Microsoft Windows:** `C:\ProgramData\NetIQ\Device Service\config.properties.`
 - ♦ **Linux:** `/opt/NetIQ/Device Service/config.properties.`
 - ♦ **Apple Mac OS X:** `/Library/LaunchDaemons/NetIQ/Device Service/config.properties.`
- 2 Remove the hash sign(#) before `vendorModule` to remove any comments from the parameter.
- 3 Set the vendor module specific dll file name to the parameter based on the operating system:
 - ♦ **Microsoft Windows:**
 - ♦ `pki.vendorModule: eToken.dll`
 - ♦ `pki.blockingMode: true`
 - ♦ **Linux:**
 - ♦ `pki.vendorModule: /usr/lib/libeTPkcs11.so`
 - ♦ `pki.blockingMode: true`
 - ♦ **Mac OS X:**
 - ♦ `pki.vendorModule: libeTPkcs11.dylib`
 - ♦ `pki.blockingMode: true`
- 4 Save the changes.
- 5 Restart the Device Service.

Configuring the YubiKey PKI

Before configuring the YubiKey PKI, ensure to download the [Yubico PIV \(https://developers.yubico.com/yubico-piv-tool/Releases/\)](https://developers.yubico.com/yubico-piv-tool/Releases/) tools. You can unpack the zip file and navigate to `bin` directory.

To configure the PIV compliant Yubikey for public key authentication with OpenSC through PKCS11, perform the following steps:

- 1 Open the configuration file based on the operating system:
 - ♦ **Microsoft Windows:** `C:\ProgramData\NetIQ\Device Service\config.properties.`

- ♦ **Linux:** /opt/NetIQ/Device Service/config.properties.
 - ♦ **Apple Mac OS X:** /Library/LaunchDaemons/NetIQ/Device Service/config.properties.
- 2 Add hash symbol (#) as prefix to the existing parameters that start with pki to set the parameter as comment.
- For example:
- ♦ #pki.vendorModule=auto
 - ♦ #pki.forceVirtualChannels=false
- 3 Add the following parameter specific to the operating system:
- ♦ **Microsoft Windows:**
 - ♦ pki.vendorModule=libykcs11-1.dll
 - ♦ pki.blockingMode=false
 - ♦ **Linux:**
 - ♦ pki.vendorModule=/usr/local/lib/libykcs11.so
 - ♦ pki.blockingMode=false
 - ♦ **Mac OS X:**
 - ♦ pki.vendorModule=/usr/lib/Libykcs11.1.dylib
 - ♦ pki.blockingMode=false
- 4 Save the changes.
- 5 Perform one of following based on the operating system:
- ♦ **Microsoft Windows:** Open the Services app and restart the Device Service.
 - ♦ **Linux:** Run the following commands:

```
sudo service deviceservice stop
sudo service deviceservice start
```
 - ♦ **Mac OS X:** Run the following commands:

```
sudo launchctl unload /Library/LaunchDaemons/com.netiq.deviceservice.plist
sudo launchctl load /Library/LaunchDaemons/com.netiq.deviceservice.plist
```

IMPORTANT: The YubiKey PKCS module supports only the **Generate a key pair** mode and does not work with the existing certificates on the PKI token or smart card.

NOTE: If you are not able to enroll the PKI method using YubiKey PKI or import a certificate to YubiKey token, see [PKI Related Issues](#) to resolve these issues.

NOTE

- ♦ Sometimes the vendor specific module may not respond and gets hanged on Mac OS.
 - ♦ Some certificates may not be accessible through the vendor specific module. The issue with certificate may display an error message Operation failed exception. This issue occurs when the vendor module does not retrieve the certificate body for some certificates.
-

Configuring OpenSC

OpenSC is a third party software that provides a set of libraries and utilities to work with different PKCS#11 tokens and cards. OpenSC implements the standard APIs to smart cards and tokens if these devices do not have the vendor specific PKCS module.

Before configuring the OpenSC on any PKCS#11 based tokens and cards, ensure that the following requirements are met:

- ♦ Download and install [OpenSC \(https://github.com/OpenSC/OpenSC/releases/\)](https://github.com/OpenSC/OpenSC/releases/).

NOTE: For Microsoft Windows, you must install and use a 32bit version of OpenSC.

- ♦ Import a certificate to the token or card.

To configure token for public key authentication with OpenSC through PKCS11, perform the following steps:

- 1 Open the OpenSC configuration file based on the operating system:
 - ♦ **Microsoft Windows:** c:\Program Files (x86)\OpenSC Project\OpenSC\opensc.conf
 - ♦ **Linux:** /usr/local/etc/opensc.conf
 - ♦ **Apple Mac OS X:** /Library/OpenSC/etc/opensc.conf
- 2 Remove the hash symbol from following parameter to uncomment:
`pin_cache_ignore_user_consent = true;`
You can also see the following comments in the configuration file:
Older PKCS#11 applications not supporting CKA_ALWAYS_AUTHENTICATE
may need to set this to get signatures to work with some cards.
Default: false
- 3 Open the configuration file based on the operating system:
 - ♦ **Microsoft Windows:** C:\ProgramData\NetIQ\Device Service\config.properties
 - ♦ **Linux:** /opt/NetIQ/Device Service/config.properties
 - ♦ **Apple Mac OS X:** /Library/LaunchDaemons/NetIQ/Device Service/config.properties
- 4 Add the following parameters specific to the operating system:
 - ♦ **Microsoft Windows:**
 - ♦ `pki.vendorModule=C:\\Program Files (x86)\\OpenSC Project\\OpenSC\\pkcs11\\opensc-pkcs11.dll`
 - ♦ `pki.blockingMode=false`
 - ♦ **Linux:**
 - ♦ `pki.vendorModule=/usr/local/lib/opensc-pkcs11.so`
 - ♦ `pki.blockingMode=false`
 - ♦ **Mac OS X:**
 - ♦ `pki.vendorModule=/Library/OpenSC/lib/opensc-pkcs11.so`
 - ♦ `pki.blockingMode=false`
- 5 Save the changes.

6 Perform one of following based on the operating system:

- ♦ **Microsoft Windows:** Open the Services app and restart the Device Service.

- ♦ **Linux:** Run the following commands:

```
sudo service deviceservice stop
```

```
sudo service deviceservice start
```

- ♦ **Mac OS X:** Run the following commands:

```
sudo launchctl unload /Library/LaunchDaemons/com.netiq.deviceservice.plist
```

```
sudo launchctl load /Library/LaunchDaemons/com.netiq.deviceservice.plist
```

IMPORTANT: While using OpenSC, the **Generate a key pair** mode is not supported for Yubikeys and allows to work with the certificates that are existing on the PKI token or smart card.

Performing Bulk Replacement of Configuration File

To customize configuration of Device Service on multiple computers in domain, perform the following instructions:

- 1 Create a configuration file `config.properties` with the required parameters.
- 2 Copy this configuration file on a network folder.
- 3 Open **Group Policy Management** console.
- 4 Right-click the domain name and select **Create GPO in this domain, and Link it here.**
- 5 Specify a name for the **Group Policy Object**. It is used to update the Device Service configuration file. Click **OK**.
- 6 Right-click the created GPO and click **Edit**.
- 7 Browse **Computer Configuration > Preferences > Windows Settings**.
- 8 Right-click **Files** and select **New > File**.
- 9 Change **Action** to **Replace**.
- 10 In **Source file(s)** specify the full path of the configuration file located on the network folder.
- 11 In **Destination File**, specify the path: `C:\ProgramData\NetIQ\Device Service\config.properties`.
- 12 Clear all the **Attributes** options.
- 13 Click **OK**.
- 14 Create a group in the domain that contains computers on which you want to replace the Device Service configuration file.
- 15 In the **Security Filtering** section of the **Group Policy Management** console, for the used GPO remove the **Authenticated Users**.
- 16 Click **Add** and select the created group.
- 17 Click **Delegation**.
- 18 Right-click the added group and select **Edit settings, delete, modify security**.
- 19 Run `gpupdate /force` on the computer where you will replace the configuration file or wait till the policy is automatically applied.

4 Troubleshooting

This chapter provides information about troubleshooting Device Service.

- ♦ [“Generic Issues” on page 29](#)
- ♦ [“Card Related Issues” on page 29](#)
- ♦ [“FIDO U2F Related Issues” on page 30](#)
- ♦ [“Fingerprint Related Issues” on page 30](#)
- ♦ [“PKI Related Issues” on page 30](#)
- ♦ [“Bluetooth Issues” on page 31](#)
- ♦ [“Configuring Gemalto Smart Card with Advanced Authentication” on page 31](#)
- ♦ [“Configuring the Virtual Machine for Working of the RF IDEas Readers” on page 32](#)

To investigate the possible issues, you may be asked to provide the debug logs. The following information helps you to enable logging on different platforms.

Microsoft Windows

To enable debug logging for all Client components, follow the steps:

1. Run `DiagTool.exe` (the tool must have Microsoft .NET Framework 3.5 installed).
2. Click **Clear All** (if applicable) in the **Debug logs** tab.
3. Click **Enable**.
4. Restart the machine.
5. Reproduce your problem.
6. Run `DiagTool.exe`.
7. Click **Save logs** in the **Debug logs** tab.
8. Specify a file name and path. Click **Save** to save the logs.
9. Click **Disable** to disable the logging.
10. Click **Clear All**.

If you do not have the Diagnostic Tool, you can perform the steps manually:

1. Create a text file `C:\ProgramData\NetIQ\Logging\config.properties`.
2. Add a string to the file: `logEnabled=True` that ends by a line break.
3. Create a directory: `C:\ProgramData\NetIQ\Logging\Logs\`.
4. Restart the workstation.
5. Reproduce your problem.
6. Pack the logs located in `C:\ProgramData\NetIQ\Logging\Logs\` into a zip package.
7. Change `logEnabled=True` to `logEnabled=False` in `C:\ProgramData\NetIQ\Logging\config.properties`.

Apple Mac OS X

To collect the debug logs using the Diagnostic Tool, perform the following steps:

- 1 Run the file `DiagTool.app`.
- 2 Click **Enable**.
- 3 Restart your system.
- 4 Repeat the issue.
- 5 Run the file `DiagTool.app`.
- 6 Click **Save** in the **Debug logs** tab.

The logs file is saved in the `logs-year-month-date-hour:minute:seconds.zip` format in the `/tmp` directory.

For example, logs file is saved as `logs-2017-10-23-15:30:20.zip`.

- 7 Click **Save**.

You can perform the following in the **Debug logs** tab:

- ♦ Use **Disable** to disable the logging.
- ♦ Use **Refresh** to update the logs list.
- ♦ Use **Open** to open any specific log.
- ♦ Use **Clear All** to delete the existing logs.

To identify the Advanced Authentication servers on the domain, perform the following steps:

- 1 Run the file `DiagTool.app`.
- 2 Click **Servers**.
- 3 Specify the domain name in **Domain** and click **Search**. A list of servers is displayed, if the IP is either IPv4 or IPv6.

If you do not have the Diagnostic Tool, perform the following steps to collect the debug logs manually:

- 1 Create a directory `NetIQ` in the `/Library/Logs/` folder.
- 2 Create a text file `config.properties` in `/Library/Logs/NetIQ/`.
- 3 Add a string to the file `logEnabled=True` that ends with a line break.
- 4 Create a directory `Logs` in `/Library/Logs/NetIQ/`.
- 5 Restart the system.
- 6 Repeat the issue.
- 7 Pack the logs located in `/Library/Logs/NetIQ/Logs/` into a zip file.
- 8 Change `logEnabled=True` to `logEnabled=False` in the file `/Library/Logs/NetIQ/config.properties`.

Linux

To enable logging for the component, perform the following steps:

- 1 Create a text file `/opt/NetIQ/Logging/config.properties`.
- 2 Add a string to the file: `logEnabled=True` that ends by line break.
- 3 Save changes.

- 4 Create a Logs folder in `/opt/NetIQ/Logging/`.
- 5 Stop the service by running the command in the terminal: `sudo service deviceservice stop`.
- 6 Start the service: `sudo service deviceservice start`.

Logs are generated in the `/opt/NetIQ/Logging/Logs` directory.

Generic Issues

These issues could happen with any service such as Bluetooth, PKI, Fido or Fingerprint.

After you install a new browser and then try to enroll or test authenticator, an error message `Service is not available` is displayed.

The root cause for this issue is, device service keeps the certificates for itself during installation. So if the browser is installed after installing the device service, the browser will not have the required certificates.

To fix the issue, open a new browser window and access one of following URLs. Depending on the method used, apply the appropriate certificate.

- ♦ <https://127.0.0.1:8440/api/v1/card/getmessage?nowait>
- ♦ <https://127.0.0.1:8441/api/v1/fidou2f/abort>
- ♦ <https://127.0.0.1:8442/api/v1/fingerprint/capture>
- ♦ <https://127.0.0.1:8440/api/v1/pki/getmessage?nowait>
- ♦ <https://127.0.0.1:8440/api/v1/bluetooth/getdevices>

Card Related Issues

To troubleshoot the Card related issues you can check the link: <https://127.0.0.1:8440/api/v1/card/getmessage?nowait>.

The response format is as follows:

```
{
result: [<status>],
cardid: <card id>,
readerid: <reader id>
}
```

The following status is implemented:

- ♦ `NO_READER`: Indicates that the card service did not detect a card reader connected.
- ♦ `READER_ON`: Indicates that the card service detected a card reader connected.
- ♦ `NO_CARD`: Indicates that there is no card on the reader.
- ♦ `CARD_ON`: Indicates that a card is presented to the reader.

NOTE: Card ID can be used only with `CARD_ON` and `NO_CARD` status.

FIDO U2F Related Issues

To troubleshoot the FIDO U2F related issues, see: <https://127.0.0.1:8441/api/v1/fidou2f/abort>. The service should return: { "result": "ok" } when a FIDO U2F token is connected.

Fingerprint Related Issues

To troubleshoot the fingerprint related issues, see: <https://127.0.0.1:8442/api/v1/fingerprint/capture>. Open the URL while you are presenting your finger on the reader.

The following fields are included in the output:

- ♦ captureStatus: Can be 'Ok', 'Timeout', 'Error', 'NoReader'.
- ♦ Width, Height: Fingerprint image size (in pixels).
- ♦ Dpi: Dots per inch (used on matching side).
- ♦ BitsPerPixel: Bits per pixel (usually 8 bits).
- ♦ BytesPerLine: Bytes per one line in image (include align).
- ♦ Image: Fingerprint image encoded using base-64 in gray scale.

An example of a sample output:

```
{"BitsPerPixel":8,"BytesPerLine":256,"Dpi":508,"Height":360,"Image":"<fingerprintdata>","Width":256,"captureStatus":"Ok"}.
```

PKI Related Issues

To troubleshoot the PKI related issues you can check the URL: <https://127.0.0.1:8440/api/v1/pki/getmessage?nowait>.

The service returns:

- ♦ NO_READER if no reader is connected.
- ♦ NO_CARD if a card is not presented.
- ♦ CARD_ON if a card is presented.

Issue with YubiKey PKI

Issue: When you connect the PKI token to your system and initiate enrollment on the Self-Service portal, if an error message `Unexpected service status: PLUGIN_NOT_INITTED` is displayed. This issue occurs due to the invalid dll path in the configuration file.

Workaround: Ensure valid path to the dll file is specified in the configuration file. You can search for `opensc-pkcs11.dll` or `libykcs11-1.dll` in the C drive and specify the full path using `\\` in place of `\`.

You can plug the Yubikey token to your system and navigate to the URL <https://127.0.0.1:8441/api/v1/pki/getmessage?nowait> to view the status of the token. The status must display as `CARD_ON`.

When you import the certificate to the token, navigate to the URL <https://127.0.0.1:8441/api/v1/pki/getcertificates> to view the certificate data.

If you are unable to enroll PKI using YubiKey token on the Self-Service portal then try to export the logs to investigate the issue.

Unable to Import a Certificate to the YubiKey Token

Issue: When you try to import certificate to the YubiKey token using the yubico-piv-tool, an error message Failed authentication with the application is displayed.

Workaround: You must reset PIN of the token in one of the following ways:

- ♦ Specify incorrect PIN three times consecutively and then reset the PIN (default PIN is 123456).
- ♦ Specify incorrect PUK code (default PUK code is 12345678) of the same length (for example, 87654321) then reset the PIN.

You can import the certificate to the YubiKey token after resetting the PIN.

Bluetooth Issues

To troubleshoot the Bluetooth related issues, refer to the following URL: <https://127.0.0.1:8440/api/v1/bluetooth/getdevices>. It returns a list of the Bluetooth devices that have been discovered.

For more information on the Bluetooth, see “Bluetooth Plug-in” in the [Chapter 5, “Developer Information,” on page 35](#).

Configuring Gemalto Smart Card with Advanced Authentication

This section provides the configuration information of the following Gemalto smart cards:

- ♦ IDPrime .NET Smart cards
- ♦ SafeNet eToken 51x0

To configure the Advanced Authentication with Gemalto smart card, perform the following configuration tasks:

- ♦ “Installing the SafeNet Authentication Client 10” on page 31
- ♦ “Generating the Customized MSI file” on page 32
- ♦ “Configuring PKCS Path in the Device Service” on page 32

Installing the SafeNet Authentication Client 10

- 1 Download the SafeNet Authentication Client 10.
- 2 Navigate to the **Customization Package** folder and execute the `SACCustomizationPackage-10.0.msi` file.
The SafeNet Authentication Client Customization Package Installation wizard is displayed.
- 3 Click **Next**.
- 4 Read the license agreement, and select **I accept the terms in the license agreement**. Click **Next**.
- 5 Click **Change** to select a different destination folder or install the Customization Tool's into the default folder:
`C:\Program Files\SafeNet\Authentication\`
- 6 Click **Install**.
- 7 Click **Finish**.

Generating the Customized MSI file

- 1 Click **Start** and navigate to **Programs > SafeNet > SACAdmin > SAC Customization Tool**.
- 2 Select **Features to install** in the left pane.
- 3 Select **IDGo 800 Compatible Mode** from the list.
- 4 Click **Actions > Generate MSI**.
- 5 Specify the file name and save files in the preferred folder.
The generated msi files are as follows:
 - ♦ <file name>msi-x32-10.0
 - ♦ <file name>msi-x64-10.0
- 6 Install the msi file according to the bits of your Operating System.
The Installation wizard is displayed.
- 7 Follow the installation steps and click **Finish**.

NOTE: Ensure that the file IDPrimePKCS11.dll is available in one of the following paths:

- ♦ C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11
 - ♦ C:\Program Files\Gemalto\IDGo 800 PKCS#11
-

Configuring PKCS Path in the Device Service

- 1 Install NetIQ Advanced Authentication Device Service.
- 2 Navigate to C:\ProgramData\NetIQ\Device Service\config.properties.
- 3 Set the pki.vendorModule to the customized PKCS file path as follows:

```
pki.vendorModule= C:\\Program Files (x86)\\Gemalto\\IDGo 800  
PKCS#11\\IDPrimePKCS11.dll.
```

NOTE: Do not use a 64 bit library file (IDPrimePKCS1164.dll).

- 4 Save and Restart Device Service.

NOTE: If you have SafeNet Authentication Client (SAC) version v8.x, set the pki.vendorModule to auto. The SAC uses eToken.dll library for IDPrime cards.

Configuring the Virtual Machine for Working of the RF IDEas Readers

You must perform the following configuration steps to ensure that the RF IDEas reader work with the VMware Mac virtual machine.

- 1 Add the following lines to the .vmx file of the virtual machine.

```
usb.generic.allowHID=true  
usb.generic.allowLastHID=true
```


- 2 Set the following in the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`:
`card.rfideasEnabled:true`

You must perform the following configuration steps to ensure that the RF IDEas reader work with the VMware Windows virtual machine.

- 1 Add the following lines to the `.vmx` file of the virtual machine.

```
usb.generic.allowHID=true  
usb.generic.allowLastHID=true
```

If the above does not achieve the redirection, goto step 2.

- 2 Go to the following url: <http://kb.vmware.com/kb/1011600>.

The VID (Vendor ID) and PID (Product ID) of the connected reader found in the Device Manager are generally listed as: `VID_0C27&PID_3BFA`. To ensure the VID and PID are included in the list, add the following to the registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMwareVDM\USB]  
AllowHardwareIDs=[REG_MULTI_SZ]"VID_0C27&PID_3BFA"
```

- 3 Set the following in the configuration file `C:\ProgramData\NetIQ\Windows Client\config.properties`.

```
card.rfideasEnabled:true
```


5 Developer Information

Currently the supported opened ports are 8440, 8441, 8442 but it is better to use 8440, as other ports may be deprecated in the future releases.

- ♦ “Card Plug-in” on page 35
- ♦ “FIDO U2F Plug-in” on page 36
- ♦ “Fingerprint Plug-in” on page 37
- ♦ “PKI Plug-in” on page 38
- ♦ “Bluetooth Plug-in” on page 40

Card Plug-in

To check the Card Service you may open the following URL: <https://127.0.0.1:8440/api/v1/card/getmessage?nowait>.

The response format:

```
{
  result: [<status>],
  cardid: <card id>,
  readerid: <reader id>
}
```

The following statuses are implemented:

- ♦ NO_READER means that the Card service didn't detect a card reader connected,
- ♦ READER_ON means that the Card service detected a card reader connected,
- ♦ NO_CARD means that there is no card on the reader,
- ♦ CARD_ON means that a card is presented to the reader.

NOTE: cardid is used only with CARD_ON and NO_CARD statuses.

Examples of commands:

- ♦ <https://127.0.0.1:8440/api/v1/card/getmessage?nowait> - immediately returns a current status. Possible values [NO_READER, NO_CARD, CARD_ON]
- ♦ <https://127.0.0.1:8440/api/v1/card/getmessage?wait> - waits for a next event (e.g. card presented or card removed)

NOTE: When you disconnect the reader with a card on, two messages will arrive: NO_CARD, NO_READER. But the first one will be caught with `getmessage?wait`. When you plug in a reader with a card on, there will be the two events: READER_ON, CARD_ON. And as a result READER_ON will be returned.

- ♦ <https://127.0.0.1:8440/api/v1/card/getreaderon?nowait> - immediately returns READER_ON if a reader is attached and NO_READER otherwise.

- <https://127.0.0.1:8440/api/v1/card/getreaderon?wait> - immediately returns `READER_ON` if a reader is attached or waits till it's attached
- <https://127.0.0.1:8440/api/v1/card/getcardon?nowait> - immediately returns `NO_READER` if a reader isn't attached, `NO_CARD` if a card isn't presented or `CARD_ON` if a card is presented
- <https://127.0.0.1:8440/api/v1/card/getcardon?wait> - immediately returns `NO_READER` if a reader isn't attached or wait till the card will be presented on a reader.

NOTE: It will wait the next tap of a card even if a card is already on a reader.

- <https://127.0.0.1:8440/api/v1/card/getcardoff?nowait&cardid=<cardid>> - immediately returns `NO_READER` if a reader isn't attached, `NO_CARD` if a card isn't presented on the reader or `CARD_ON` if a card is presented on the reader. Use `cardid` to wait when a specific card is removed.
- <https://127.0.0.1:8440/api/v1/card/getcardoff?wait> - returns immediately with `NO_READER` if a reader isn't attached. If there is no card presented on a reader, it returns `NO_CARD` immediately else waits till the card is removed from the reader
- <https://127.0.0.1:8440/api/abort?cancel-cookie=xxx> - all of the "wait" methods support `cancel-cookie=xxx` parameter. E.g. <https://127.0.0.1:8440/api/v1/card/getmessage?wait&cancel-cookie=xxx>. And by calling `abort` with a `cancel-cookie`, all waiting methods with the same specified cookie are terminated.

FIDO U2F Plug-in

To check the FIDO U2F Service you may open the following URL: <https://127.0.0.1:8441/api/v1/fidou2f/abort>. The service should return: `{ "result": "ok" }` when a FIDO U2F token is connected.

Available methods

FIDO U2F Service provides the following POST-methods:

<https://127.0.0.1:8441/api/v1/fidou2f/sign> - Performs the U2F Authenticate operation.

```
{
  "signRequests":
  [
    { "challenge": "tRiTY3C8YerfmH6IilfoCZjs5CMkKUWDrNhS7v5gCPQ",
      "version": "U2F_V2",
      "keyHandle": "knQD88Ue6ZT6tyutHr8ipZaiTRV2uT9qzwGqWjYo5HCwAiV5z2kc1vr08tWbd0LQ4S-
ODg09vpp62P6owh4qmQ",
      "appId": "https://demo.yubico.com"
    }
  ]
}
```

<https://127.0.0.1:8441/api/v1/fidou2f/register> - Performs the U2F Register operation.

```
{
  "registerRequests":
  [
    { "challenge": "tRiTY3C8YerfmH6IilfoCZjs5CMkKUWDrNhS7v5gCPQ",
      "version": "U2F_V2",
      "appId": "https://demo.yubico.com"
    }
  ],
  "signRequests": []
}
```

signRequest can be empty, or contain serial of for the key handle validation

```
{
  "challenge": "tRiTY3C8YerfmH6IilfoCZjs5CMkKUWDrNhS7v5gCPQ",
  "version": "U2F_V2",
  "keyHandle": "knQD88Ue6ZT6tyutHr8ipZaiTRV2uT9qzwGqWjYo5HCwAiV5z2kc1vr08tWbd0LQ4S-
ODg09vpp62P6owh4qmQ",
  "appId": "https://demo.yubico.com"
}
```

In case of success both methods above returns JSON reply in the U2F specification format:

or an error:

```
{ "errorCode"=1, "errorMessage"="Error Text" }
```

where:

errorCode - error code

errorMessage - additional error text

errorCode description:

1. Device other error. If the token is missing, errorMessage contains "Please connect a U2F token."
2. Device bad request. The visited URL doesn't match the App ID or not using HTTPS
3. Configuration unsupported
4. Token is not registers - for authentication process or token already registered - for register process, to enable this check, specify "signRequests" in the body of the register request).
5. Timeout - no answer from token. (if the user didn't press a button within a given timeout)

And the following GET-methods:

<https://127.0.0.1:8441/api/v1/fidou2f/abort> - Aborts all pending operations

Fingerprint Plug-in

To check the WBF Capture Service you may open the following URL: <https://127.0.0.1:8442/api/v1/fingerprint/capture>. Present your finger on the reader while the URL is loading.

The following fields are included into the output:

- captureStatus - can be 'Ok', 'Timeout', 'Error', 'NoReader'.
- Width, Height - fingerprint image size (in pixels).
- Dpi - dots per inch (used on matching side).
- BitsPerPixel - bits per pixel (usually 8 bits).

- BytesPerLine - bytes per one line in image (include align).
- Image - fingerprint image encoded using base-64 in gray scale.

E.g.

```
{"BitsPerPixel":8,"BytesPerLine":256,"Dpi":508,"Height":360,"Image":"<fingerprintdata>","Width":256,"captureStatus":"Ok"}.
```

PKI Plug-in

PKI plug-in supports the following options:

- vendorModule=eTPKCS11.dll - PKCS#11 implementation library of a needed vendor.
- hash=SHA1 or SHA224, SHA256 (this is a default value if not presented), SHA384, SHA512.
- padding=PKCS#1 (this is a default value if not presented) or PSS, OAEP.
- modulusBits=2048 - key size (this is a default value if not presented). E.g. eToken PRO 32k doesn't support it and you need to set 1024 to use it.
- blockingMode=True. The default value is True. OpenSC supports the 'waiting for card' mechanism not completely and it requires to change the option to False. The most of vendors should work fine with the default mode.

PKI plugin uses the simulator API for card / token detection and two new POST methods pki/enroll, pki/login:

Available methods:

Card service provides the following POST-methods

- https://127.0.0.1:8440/api/v1/pki/getcertificates - GET method to get all certificates from a token

```
{ "readerid":0, "certificates" : [{
  "keypairid": "9beb", "certificate": "30820371308202daa00...0b90d7290a1a76b0450264dd536d2cb057230f8dbfa8cfda05"}] }
```

slotid - slot ID

keypairid - id of the key pair in the certificate. Save it and use later for future logon operations.

certificate - certificate value in DER format.

- https://127.0.0.1:8440/api/v1/pki/generatekeypair- POST method, Request Body:

```
{"pin":"your_pin"}
```

// Replace with your token pin or empty if there is no pin

```
{ "readerid"=your_reader_id, "keypairid":"6f4712e554544ac3",
  "modulus": "a1709fb049c35fdc6695193e9dd980c713c...91daaa9d2604eeaaad73d13b1",
  "exponent": "010001" }
```

keypairid - id of the key pair in the certificate. save it and use later for future logon operations.

modulus - modulus

exponent - big exponent

- https://127.0.0.1:8440/api/v1/pki/signchallenge - POST method, Request Body:

```
{"challenge": "3128", "pin":"your_pin", "keypairid": "9beb" }
```

challenge in hex-string format(even length, since one byte is two hex symbols)

pin - pin to the token

keypairid - id of the keypair from token, you can get it from previous enroll operation

in case of success it returns signature for the given challenge in the hex format{

```
"readerid":your_reader_id, "hash":"SHA1", "padding":"PKCS#1",  
"signature":"58ad84f3a9b7244031aa55c0d0ad753b1a480ae709a37210d48...493130d7b11f12  
8ea2be1fcc42d123bdb715a153974e992b16d022" }
```

hash - used hash method

padding - used padding

- <https://127.0.0.1:8440/api/v1/pki/verifychallenge> - POST method, Request Body

```
{"challenge":"3128", "pin":"your_pin", "keypairid":"9beb",  
"signature":"58ad84f3a9b72....bdb715a153974e992b16d022" }
```

in case of an error two methods above returns an error:

```
{ "errorCode"="ERROR_ID" }
```

Possible values of ERROR_ID:

PLUGIN_NOT_INITTED - not inittd library, etc. dll was not provided

METHOD_NOT_FOUND - method not found

NO_CARD - no token or no card are presented. Use wait methods to get an event.

JSON_PARSE_FAILED - bad request body

WRONG_PIN- Wrong PIN

GET_PRIVATE_KEY_FAILED - error getting a private key from a token

OPERATION_FAILED- general operation failure

- <https://127.0.0.1:8440/api/v1/pki/getmessage?nowait> - returns immediately the current status. Possible values [NO_READER, NO_CARD, CARD_ON].

- <https://127.0.0.1:8440/api/v1/pki/getmessage?wait> - waits till the next event occurs.

NOTE: When you plug off the reader with a card on, two messages are displayed: NO_CARD, NO_READER. But the first one will be catch with getmessage?wait.

When you plug in a reader with a card on, occurs READER_ON, CARD_ON. And as a result READER_ON will be returned.

- <https://127.0.0.1:8440/api/v1/pki/getreaderon?nowait> - returns immediately with READER_ON if it's attached and NO_READER otherwise.

- <https://127.0.0.1:8440/api/v1/pki/getreaderon?wait> - returns immediately with READER_ON if a reader is attached or waits till it's attached.

- <https://127.0.0.1:8440/api/v1/pki/getcardon?nowait> - returns immediately with NO_READER if a reader isn't attached, NO_CARD if a card isn't inserted or CARD_ON if a card is inserted.

- <https://127.0.0.1:8440/api/v1/pki/getcardon?wait> - returns immediately with NO_READER if a reader isn't attached or wait till the card will be on a reader.

NOTE: It will wait the next tap of a card even if a card is already on a reader.

- `https://127.0.0.1:8440/api/v1/pki/getcardoff?nowait&cardid=<cardid>` - returns immediately with `NO_READER` if a reader isn't attached, `NO_CARD` if a card isn't inserted or `CARD_ON`

if a card is inserted. Use `cardid` to wait when a specific card is removed.

- `https://127.0.0.1:8440/api/v1/card/getcardoff?wait` - returns immediately with `NO_READER` if a reader isn't attached. if there is no card on a reader return `NO_CARD` immediately else waits till the card is removed from the reader

- `https://127.0.0.1:8440/api/abort?cancel-cookie=xxx` - all of the wait methods support `cancel-cookie=xxx` parameter.

For example, `https://127.0.0.1:8440/api/v1/card/getmessage?wait&cancel-cookie=xxx`.

And by calling `abort` with a `cancel-cookie`, all waiting methods with the same specified cookie are terminated.

Response format:

Response format

```
{
  result: [NO_READER, READER_ON, NO_CARD, CARD_ON],
  cardid: <card id>,
  readerid: <reader id>
}
```

`cardid` is used only with `CARD_ON`, and `NO_CARD` result.

Bluetooth Plug-in

To troubleshoot the Bluetooth related issues you can use the following instructions.

The Bluetooth plugin supports the following methods:

1. `https://127.0.0.1:8440/api/v1/bluetooth/getdevices`

This GET method returns a JSON array of all discovered bluetooth devices or an error code if Bluetooth is turned off.

Sample response:

```
{ "devices":
  [ { "name": "MagicKeyboard", "address": "9cd746e1234", "type": "peripheral", "hash": "9
    b67e2d07088a1f0bd64bde8c44ab7cdc279463bd6d93735ab778afda79d0bde" },
    { "name": "MagicMouse", "address": "1abcd22dafae", "type": "peripheral", "hash": "dbf7
    5830268ab5516a0d658d28105761b6d6ec062a42317a84b3a82e8e4d643f" },
    { "name": "Lex's iPhone", "address": "40cd0150cf58", "type": "phone", "hash": "ac904cc2
    e2626ca27eb7f4100166e0ae07957da89a5a3aa52f0a5d182b6ba42e" } ] }
```


Fields:

- ♦ name - bluetooth device name
- ♦ address - bluetooth address of the device
- ♦ type - device type [possible types: computer, phone, lan_access, audio, peripheral, imaging, unclassified]\

2. <https://127.0.0.1:8440/api/v1/bluetooth/detectdevice>

POST method, used to test the device presence by its address

The POST body:

```
{"address":"[RSA encoded address]"}
```

RSA encoded address - a bluetooth address encoded with an RSA public key (from certificate) in a hex-string format.

If the device is in range, the service returns:{"result":"CONNECTED","address":"40cd0150cf58"}

or if the device is absent or the bluetooth is off on the device:{"result":"DISCONNECTED"}

Other possible result values for this method:

- ♦ FAILED - general failure
- ♦ DECRYPT_FAILED - decoding failure
- ♦ INVALID_ADDRESS - not a valid value for the address
- ♦ hash - SHA256 hash of the address

If Bluetooth is off, the call returns the error: { "result": "BLUETOOTH_DISABLED" }

3. <https://127.0.0.1:8440/api/v1/bluetooth/getpublickey>

This GET method returns the public certificate in a PEM format. Encode the bluetooth address with the public key in that certificate.

```
{"publicKey": "[PUBLIC_CERT]"}
```

PUBLIC_CERT - the public certificate in a PEM format.

Currently the following is always same:

```
"-----BEGIN RSA PUBLIC KEY-----\n"
"MIGHAoGBAKqGJxyB/ZgrTESfqmMdE4GRwGH+XOioOa0EiQ8+HYcR8Pcg57j1Cc5k\n"
"D1TrGNKpayWUWW7YEsXvfSpc5a5x9qwsEe06Iak5eP/PcGNLUViLwy2CN9oy5mSM\n"
"lzpd607GNBUzEwWg0slpm3FBEvtFFDxBb7PzE9W4hE//t0LQkGcTAgED\n"
"-----END RSA PUBLIC KEY-----";
```

