# Installation Guide

## Advanced Authentication Device Service

**Version 5.4**

MICRO FOCUS

## 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/.

# Contents

# 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 contains information about supported platforms for Device Service:

| | Microsoft Windows | Apple MacOS X | Linux |
|---|---|---|---|
| Card plugin | x | x | x |
| FIDO U2F plugin | x | x | x |
| Fingerprint plugin | x | | |
| PKI plugin | x | x | x |

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

Ensure that the system meets the following requirements:

- Microsoft Windows 7(x64/x86) SP1/Microsoft Windows 8.1(x64/x86)/Microsoft Windows 10(x64/x86)/ Microsoft Windows Server 2008 R2/ Microsoft Windows Server 2012 R2 is installed.
- Apple MacOS X 10.10 (Yosemite)/ 10.11 (El Capitan).
- The following versions of Linux are installed:
  - Debian 8
  - Ubuntu 15
  - Fedora 23
  - openSUSE 42
  - SUSE Linux Enterprise Desktop 12 SP1
  - SUSE Linux Enterprise Server 12 SP1
  - Red Hat Enterprise Linux Client 7.2
  - Red Hat Enterprise Linux Server 7.2
  - CentOS 7
- One of the following browsers:
  - Microsoft Internet Explorer 11
  - Google Chrome 45 and newer
  - Mozilla Firefox 40 and newer
  - Apple Safari 8.0-9.0

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

- Supported Card Readers and Cards
- Supported Devices for PKI
- Supported Fingerprint Readers

# 1.1 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:

| Card Reader | Supported Card |
|---|---|
| Contactless card readers | ◆ HID OMNIKEY CardMan 5x25.<br>◆ HID OMNIKEY 5326.<br>◆ HID OMNIKEY 5x2x.<br>◆ Broadcom Corp Contactless SmartCard.<br>◆ ACS ACR122.<br>◆ Contactless smart cards.<br>◆ HID iClass serie.<br>◆ HID Prox serie.<br>◆ MIFARE Classic 1K/4K, Ultra Light, Ultra Light C, Plus.<br>◆ MIFARE DESFIRE 0.6, MIFARE DESFIRE EV1, MIFARE SE, DESFire.<br>◆ LEGIC LM3000 (supported only for Microsoft Windows and requires installation with specific parameters and disabling of other card plug-ins).<br>◆ LEGIC LE-762-1N (supported only for Microsoft Windows and requires installation with specific parameters and disabling of other card plug-ins).<br>◆ RFIDeas pcProx serie (supported only for Microsoft Windows).<br>◆ Elatec RFID. |
| Non supported readers | LEGIC AIR ID serie. |

# 1.2 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

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 OCSP or 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).

## 1.3 Supported Fingerprint Readers

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

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.
- Validity Sensors (HP laptops).
- SecuGen Hamster Plus (HSDU03P).

Device Service does not support the following devices:

- SecuGen Hamster IV (HFDU04)
- SecuGen Hamster (HFDU02R)
- Synaptics WBDI (Lenovo t460s laptops)

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

Close all web browsers before installing Device Service. The installation procedure varies for different operating systems.

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

---

**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.

---

## 2.1 Installing Device Service on Windows

1. Run `naaf-deviceservice-x86-release-<version>.msi`.

   ---

   **IMPORTANT:** For LEGIC readers, you need to install Device Service by running the command line:

   `msiexec /i naaf-winclient-x86-release-<version>.msi TOKEN="XXX" KEY="YYY"`

   XXX - Token value (HEX <= 12 byte)

   YYY - 3Des Key (HEX 16 byte)

   If you leave the `TOKEN/KEY` parameters blank or enter invalid commands, Device Service does not detect the LEGIC reader.

   ---

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**.

## 2.2 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

### 2.2.1 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**.

### 2.2.2 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.

## 2.3 Installing Device Service on Linux

**IMPORTANT:** To use Device Service for FIDO U2F tokens, you need to 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)

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

### openSUSE, Fedora

### openSUSE

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

### Fedora

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

**NOTE:** During the installation of Device Service on 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.

## 2.4 Upgrading Device Service on Linux

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

**NOTE:** In Advanced Authentication 5.3 Hotfix 1 the name of the Device Service has been renamed from **deviceservice** to **naaf-deviceservice**.

### Ubuntu, Debian (deb package)

To upgrade Device Service 5.3 to 5.3 Hotfix 1 or later, you must remove the old package and install a new package.

1. Remove device service package.

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

2. Install new package.

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

To upgrade Device Service 5.3 Hotfix 1 to 5.4 you can upgrade the package:

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

### openSUSE, Fedora (rpm package)

To upgrade Device Service 5.3 to 5.3 Hotfix 1 or later, you must remove the old package and install a new package.

### openSUSE

1. Remove device service package.

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

2. Install new package

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

### Fedora

1. Remove device service package.

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

2. Install new package.

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

To upgrade Device Service 5.3 Hotfix 1 to 5.4 you can upgrade the package:

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

## 2.5 Uninstalling Device Service on Linux

Run the following commands depending on your platform:

### Ubuntu, Debian (deb package)

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

### openSUSE, Fedora

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

## 2.6 Installing Device Service on Mac

1. Run `naaf-deviceservice-macos-release-<version>.pkg`.
2. Click the Apple icon in the top-left corner and select **System Preferences.**
3. Click the **Security & Privacy** icon.
4. Click **Open Anyway** on the **General** tab.
5. Click **Continue**.
6. Read and accept the licence agreement.
7. Select the disk where you want to install Device Service and click **Continue**.
8. Click **Install.**
9. Specify the root account credentials and click **Install Software.**
10. Click **Close**.

## 2.7 Uninstalling Device Service on Mac

Delete the folder `DeviceService in /Library/LaunchDaemons/NetIQ/` to uninstall Device Service on Mac.

# 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
- Fingerprint Settings
- PKI Settings

To apply the changes, reboot the machine.

## 3.1 Card Settings

Advanced Authentication supports the Microsoft policy Interactive logon: Smart card removal behavior, which allows 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 use LEGIC LM3000 or LEGIC LE-762-1N readers, you must disable the other card plug-ins to avoid conflicts. To do this, perform the following steps:

1. Open the configuration file depending on the platform:
   - **Microsoft Windows**: `C:\ProgramData\NetIQ\Device Service\config.properties`.
   - **Linux**: LEGIC readers are not supported.
   - **Apple Mac OS X:** LEGIC readers are not supported.
2. Change the existing parameters based on the following scheme:
   - `card.omnikeyEnabled: false`
   - `card.rfideasEnabled: false`
   - `card.smarfidEnabled: true`
   - `card.desfireEnabled: false`
   - `card.isCardIdGenerated=true` to generate a new card identifier during enrollment. The default value is false and during each enrollment, the card identifier is not changed. The feature can be used only for LEGIC readers.

- `card.smarfidManualMode=true` Without the `card.smarfidManualMode` in the config file or when `card.smarfidManualMode=false`, the reader's LED is blue (read mode) by default and it always starts to blink when you put a card on it.

  When `card.smarfidManualMode=true` the reader's LED is green (ready mode) by default and does not blink when you put a card on the reader. It will blink only if you are on Logon/Unlock screen and Windows Client requests to put a card. 1:N has to be disabled to disable auto-waiting for a card for Logon/Unlock screen. For more information on disabling 1;N, refer to Disabling 1:N. Also **Interactive logon: Smart card removal behavior** policy must be disabled to disable auto-waiting for a card when a user is logged in. For more information on disabling **Smart card removal behavior** policy, refer to the link. You can use the feature only for LEGIC readers

3. Save the changes.
4. Restart the workstation.

## 3.2 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. This is the default mode.

  **NOTE:** Some WBF compliant readers may work only in the WBF Direct mode, for example, the NEXT Biometrics readers.

- **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.

To change the finger print 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 that specifies a mode. For example, **fingerprint.mode: 3** to use the Lumidigm mode.
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 your machine.

## 3.3 PKI Settings

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

1. Open a configuration file 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`.
2. Remove the hash sign(`#`) before `vendorModule` to remove any comments from the parameter.
3. Specify a path to a PKCS#11 module.
   - **Microsoft Windows**:
     - **for eToken PRO:** `pki.vendorModule: eToken.dll`.
     - **for ruToken**: `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 located out of the **system32** folder, use `\\`. The quotation marks are not needed even if there are spaces in the path. For example, `pki.vendorModule: C:\\Program Files\\ActivIdentity\\ActivClient\\acpkcs211.dll.`

     ---
   - **Linux**:
     - **for eToken PRO**: `pki.vendorModule: /usr/lib/libeTPkcs11.so`.
   - **Mac OS X**:
     - **for eToken PRO**: `pki.vendorModule: libeTPkcs11.dylib`.

   You can find a list of the known PKI modules from the link.

   ---

   **NOTE:** If you have specified some `pki.vendorModules` separated by a semicolon, you must specify the same number of values for `pki.blockingMode`. For example, `pki.blockingMode: true;false.`

   ---

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

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

   **Microsoft Windows**
   - `rtPKCS11.dll, the default pki.blockingMode: true`
   - `eToken.dll, the default pki.blockingMode: true`
   - `acpkcs211.dll, the default pki.blockingMode: false`

   **Linux**
   - `libeToken.so, the default pki.blockingMode: true`

   **Mac OS**
   - `libeToken.dylib, the default pki.blockingMode: true`
4. Specify the optional parameters (if required):
   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, RIPEMD160`. 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`

The default value is `True`. OpenSC does not support the 'waiting for card' mechanism completely and it requires to change the option to `False`. Most of the vendors should work fine with 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 autodetectable vendor module.

---

5. Save the changes.
6. Restart the workstation.

# 4 Troubleshooting

This chapter provides information about troubleshooting Device Service.

- Card Related Issues
- FIDO U2F Related Issues
- Fingerprint Related Issues
- PKI Related Issues

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 enable logging for the component, perform the following steps:

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

- Create a `Logs` folder in `/Library/LaunchDaemons/NetIQ/Logging/`.
- Stop the service by running the command in the terminal: `sudo launchctl unload /Library/LaunchDaemons/com.netiq.deviceservice.plist`
- Start the service: `sudo launchctl load /Library/LaunchDaemons/com.netiq.deviceservice.plist`

Logs are generated in the `/Library/LaunchDaemons/NetIQ/Logging/Logs` directory.

### Linux

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

- Create a text file `/opt/NetIQ/Logging/config.properties`.
- Add a string to the file: `logEnabled=True` that ends by line break.
- Save changes.
- Create a `Logs` folder in `/opt/NetIQ/Logging/`.
- Stop the service by running the command in the terminal: `sudo service deviceservice stop.`
- Start the service: `sudo service deviceservice start`.

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

## 4.1 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.

---

## 4.2 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.

## 4.3 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"}.

## 4.4 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.