Axidian CertiFlow Technical Documentation

Version: 7.1

Date: 29.05.2026

Contents

About Axidian CertiFlow 5

Components 6

Licensing 8

System requirements 10

- Server 11
- Client 13
- Networking 14
- Cards 16

Installation steps 18

Environment 20

- User catalog 21
  - LDAP 22
  - Internal catalog 28
- Data storage 32
- Microsoft CA 35
- Service certificates 44
- Web server 52
  - IIS 53
  - NGINX 54
  - Apache HTTP Server 74
- .NET 85

Install server components 87

- Axidian CertiFlow Server 88
- OpenID Connect server 93
- Configuration Wizard 100
- Unified Event log 117
- Axidian CertiFlow Agent 131

Install client components 143

- Middleware 144
- Client Tools 151
- Agent 155

Administrator guide 159

Start 160
Configuration 161
Manage policies 163
PKI settings 166
Microsoft CA 168
Common certificates 174
Axidian Access 175
Workflow 178
Issue 182
Authentication 185
Agents 186
Card printer 188
Notifications 189
Licenses 192
Card types 193
Organization structure 199
Roles 201
Tags 212
Print templates 213
Notifications 215
Custom logs 218
Management Console 221
Dashboard 223
Users 225
User profile 230
Card operations 233
Issue 238
Assign 242
Reset user PIN 244
Unlock 245
Disable and enable 253
Revoke 257
Withdraw 258
Replace 260
Update 264

Issue and print image or text 267
Document operations 268
Cards 273
Certificates 278
Events 280
Client agent 281
Assign tasks manually 287
Automatic operations 296
Custom Logs 300
Documents 301
User guide 303
Card operations 305
Issue 306
Update 318
Disable and enable 324
Revoke and clear 325
Reset and change PIN 326
View contents 327
Change answers to secret questions 328
Documents 329
Client agent 332
View files and links 334
API 335
Authentication 336
Cards 341
Troubleshooting 349
Collect logs 350
Technical support 358
Release notes 359

About Axidian CertiFlow

Axidian CertiFlow is a public key infrastructure (PKI) management solution.

Axidian CertiFlow handles all activities regarding smart card management and provides complete control over smart cards and digital certificates at all stages of their lifecycle. The solution allows to resolve user issues related to card management without the need to contact administrators.

Key features

- Digital certificate management throughout the entire lifecycle
- Smart card management
- Smart card operations control using a client agent installed on user workstations
- Internal electronic document management system
- Audit logging and monitoring
- Generating reports to meet regulatory compliance
- Sending system alerts to administrators and users
- Card management API
- Role-based access control and flexible settings for controlling permissions and privileges
- Self-service portal for users to work with cards and certificates independently and to cooperate with administrators

Compatibility

Operating systems	Windows OS Linux OS
User catalogs	LDAP directories – Active Directory, FreeIPA Internal user catalog in Microsoft SQL Server or PostgreSQL
Certification authorities	Microsoft CA
Data storage	Microsoft SQL Server PostgreSQL

Components

Axidian CertiFlow consists of server and client components.

Server components

The core of the system is Axidian CertiFlow Server. The server components include:

- **Management Console** – an administrator console.
- **Self-Service** – a user's personal account.
- **Remote Self-Service** – a remote service for users outside the domain.
- **API** – an API service for cards lifecycle management and integration with third-party systems.
- **CredProvAPI** – a service for online unlocking and disabling cards.
- **Card Monitor** – a service for monitoring card status (installed with the server).
- **Axidian CertiFlow Agent** (client agent) – a service for registering client agents and for cards remote management.
- **Axidian CertiFlow Configuration Wizard** – a web console for configuring Axidian CertiFlow operations settings.
- **OpenID Connect Server** – a server for user authentication in web applications via the OpenID Connect protocol.
- **MSCA Proxy** – an additional component for configuring integration with Microsoft Enterprise CA instances outside the domain where Axidian CertiFlow is deployed.
- **Event Log Proxy** – an additional component for recording events from multiple Axidian CertiFlow servers into Windows event log.
- **Axidian Log Server** – an additional component for recording events from multiple Axidian CertiFlow servers into Windows event log, Microsoft SQL or PostgreSQL databases, and SysLog.

> **TIP**
> The OpenID Connect Server, MSCA Proxy, Event Log Proxy, and Axidian Log Server web applications are mandatory for Linux-based installations and additional for Windows-based installations.

Auxiliary tools

- **Storage.sql** – a script for populating Microsoft SQL database.
- **Storage-Postgre.sql** – a script for populating PostgreSQL database.
- **Certiflow.CertEnroll.MsCA.exe** – a tool for issuing the Enrollment Agent certificate for a Microsoft Enterprise CA service account.

- **Certiflow.Agent.Cert.Generator** – a tool for creating client agent certificates.
- **Certiflow.Config.DataProtector** – a tool for encrypting the Axidian CertiFlow services configuration files.

Client components

Axidian CertiFlow Middleware – a component providing a single interface for managing cards connected to a workstation.

Axidian CertiFlow Client Tools

- **Credential Provider** – a component for online and offline unlocking of cards used for Windows authentication.
- **Axidian CertiFlow Unblock** – a component for unlocking cards in a user session.

Axidian CertiFlow Agent – a client agent for remote blocking, resetting the user PIN, updating the card content, clearing or initializing the card when it is revoked, and changing the administrator PIN.

Licensing

To work with Axidian CertiFlow, you must obtain a license key. Axidian offers the following license types for Axidian CertiFlow:

- General license
- Add-on licenses

How to manage licenses in Axidian CertiFlow

General license

General license lets you manage all cards supported by Axidian CertiFlow:

- Smart cards and USB tokens
- Virtual smart cards — TPM Virtual Smart Card and Windows Hello for Business
- Registry cards

You should purchase a general license for every Axidian CertiFlow user.

A license is locked when you assign or issue at least one card to a user. You can issue or assign two cards and more to a single user, and it will still lock only one license. If you store multiple certificates on one card, you should still get one license per user.

A license is released when you withdraw all cards from a user.

If all your licenses are locked, you can buy extra licenses. You can revoke a license from one user and reassign it to another one.

Add-on licenses

Add-on licenses cover the following components:

- Axidian AirCard Enterprise – a license that allows you to use virtual smart cards. License count is based on the number of AirCard users.
- Axidian CertiFlow agent (client agent) – a license that allows you to remotely manage cards using agents. License count is based on the number of workstations where agents are deployed.

License term

Based on the validity period, Axidian offers the following license types for Axidian CertiFlow:

- Perpetual – a permanent license
- Subscription-based – a license that expires at the end of the subscription term

You can also request a trial license to explore the features of Axidian CertiFlow during your evaluation period.

When licenses expire or all licenses are locked, you cannot perform the following operations:

- Issue new cards to new users
- Register new client agents

To renew your license, contact your Axidian sales representative.

> **INFO**
> A license also allows you to contact Axidian technical support and update Axidian CertiFlow when new software versions are released.

System requirements

Server

System requirements for server components

Client

System requirements for client components

Networking

Networking requirements for the Axidian CertiFlow components

Cards

Supported smart cards and USB tokens list

Server

Review the system requirements for the Axidian CertiFlow server components.

Hardware requirements

- 8 GB RAM
- 50 GB of free disk space

Software requirements

Operating system	• Windows Server 2012/2012 R2 • Windows Server 2016–2022 • Debian 9–12 • Ubuntu 18.04 LTS–25.04 LTS • Red Hat Enterprise Linux 8–9 • CentOS Stream 8–9
Web-server	• Internet Information Services (IIS) 7.0 and higher • Nginx 1.22.1 and higher • Apache 2.4.25 and higher
Microsoft additional packages	• Microsoft .NET 8.0 • URL Rewrite

Environment

User catalog	• LDAP directories: Active Directory, Samba AD DC, FreeIPA • Internal user catalog in Microsoft SQL Server or PostgreSQL
Certification authorities	Microsoft Enterprise CA: • Windows Server 2008 (Enterprise and higher) • Windows Server 2012/2012 R2 • Windows Server 2016–2022

Data storage	• Microsoft SQL Server 2012 SP2 and higher • PostgreSQL 13 and higher
Cryptographic Service Providers (CSP)	RSA • Card manufacturer's CSP • Microsoft Base Smart Card Cryptographic Service Provider

Client

Review the system requirements for the Axidian CertiFlow client components.

Hardware requirements	300 МБ of free disk space
Operating system	• Windows Vista SP2 x86/x64 • Windows 7 SP1 x86/x64 • Windows 8/8.1 x86/x64 • Windows 10 x86/x64 • Windows 11 x86/x64 • Windows Server 2008 SP2 x86/x64 (with KB980368) • Windows Server 2008 R2 SP1 • Windows Server 2012/2012 R2 • Windows Server 2016–2022 • Debian 10–11 • Ubuntu 18.04 LTS and higher • Red Hat Enterprise Linux 8–9 • CentOS Stream 8–9
Environment	• Installed drivers (PKI managers) for smart cards and USB tokens • Microsoft Edge 88.0.705.81 and higher • Google Chrome или Chromium 88.0.4324 and higher • Mozilla Firefox 109.0.1 and higher

Networking

Server

Web applications, HTTP, HTTPS	• 80 (TCP) • 443 (TCP) • 3001/3002 (TCP) for Axidian AirCard Enterprise • 3003 (TCP) for Axidian CertiFlow Agent
SMTP server for email notifications (outbound)	• 25 (TCP) • 465 (TCP) • 587 (TCP)
Active Directory	• 53 (TCP/UDP), outbound – DNS • 135 (TCP) – RPC • 389 (TCP/UDP) – LDAP • 636 (TCP) – LDAPS • 3268 (TCP) – LDAP Global Catalog • 3269 (TCP) – LDAP Global Catalog SSL • 88 (TCP/UDP) – Kerberos • 464 (TCP/UDP) – Kerberos Password Change
Microsoft SQL Server	• 135 (TCP) – Transact-SQL debugger/RPC • 1433 (TCP) – SQL Server default instance • 1434 (UDP) – SQL Server Browser service • 4022 (TCP) – Service Broker
PostgreSQL	5432 (TCP/UDP) - PostgreSQL default port

Microsoft Enterprise CA	• 135 (TCP) – RPC • 389 (TCP/UDP) – LDAP • 636 (TCP) – LDAPS • 49152 - 65535 – DCOM/RPC dynamic ports (TCP) **INFO** Microsoft CA uses DCOM technology. DCOM applications use random TCP port numbers from upper range by default. It is also possible to set the CA to use the defined TCP port.

User workstations

DNS	53 (TCP/UDP), outbound
Web applications, HTTP, HTTPS	• 80 (TCP) • 443 (TCP) • 3001/3002 (TCP) for Axidian AirCard Enterprise • 3003 (TCP) for Axidian CertiFlow Agent

Cards

Windows

Manufacturer	Card model
Axidian	Axidian AirCard Enterprise virtual smart card
ACS	ACOS5-64
Avest	Avest Key 256A
Bit4id	ID-One Cosmo
CRYPTAS	TicTok V2/V3
Cryptovision	ePasslet Suite v3.0, JCOP V3.0
Feitian	ePass2003 (A1+, A2) BioPass2003
HID	Crescendo C1150 Series Crescendo C1300 Series Crescendo C2300 Series
Microsoft	Local Computer Certificate Store User Certificate Store TPM Virtual Smart Card (Microsoft VSC) — Virtual Smart Card Trusted Platform Platform Module v.2.0 Windows Hello for Business (WHfB)
RSA	RSA SecurID 800

Manufacturer	Card model
Thales (SafeNet и Gemalto)	SafeNet eToken PRO 32k SafeNet eToken PRO 64k eToken PRO Java 72K OS755 SafeNet eToken 5105 SafeNet eToken 5110 SafeNet eToken 5110 CC (940) IDCore30B eToken 1.7.7 SafeNet eToken 5300 SafeNet eToken Fusion SafeNet eToken Fusion CC IDPrime MD 830 FIPS IDPrime MD 830B FIPS IDPrime MD 840B IDPrime 930 IDPrime 930nc IDPrime 940 IDPrime 940B IDPrime MD 3810 IDPrime MD 3811 IDPrime 3930 IDPrime 3940 IDPrime 3940 FIDO
Yubico	YubiKey 5 Series

Linux

Manufacturer	Card model
Thales (SafeNet и Gemalto)	SafeNet eToken PRO 32k SafeNet eToken PRO 64k eToken PRO Java 72K OS755 SafeNet eToken 5105 SafeNet eToken 5110 IDCore30B eToken 1.7.7

Installation steps

Prepare your environment and install the Axidian CertiFlow server and client components.

Follow the instructions for the operating system of the workstation where you plan to install the Axidian CertiFlow server.

Windows

Prepare the environment

1. Configure a user catalog.
2. Create and enroll a TLS/SSL certificate to configure a secure connection to Axidian CertiFlow services.
3. Install Internet Information Services (IIS).
4. Install .NET.
5. Create a data storage.
6. Configure integration with Microsoft Certification Authority.

Install and configure Axidian CertiFlow

1. Install and configure the Axidian CertiFlow server components.
    1. Server
    2. Configuration Wizard
2. Install and configure the Axidian CertiFlow client components.
    1. Client Tools
    2. Middleware
3. Install the Axidian CertiFlow Middleware extension in the browsers on the workstations of administrators, operators, and users.

Install and configure additional components

You can configure the following optional components:

- Axidian CertiFlow Event Log Proxy or Log Server to record events to a centralized log, if you plan to deploy multiple Axidian CertiFlow servers in your environment.
- Axidian CertiFlow MS CA Proxy to connect to Microsoft CA, if it is located outside the domain of the Axidian CertiFlow server.
- OpenID Connect server to configure authentication in Axidian CertiFlow web services using the OpenID Connect protocol.

- Axidian CertiFlow Agent to manage cards on user workstations remotely. The agent requires a separate license.

Linux

Prepare the environment

1. Configure a user catalog.
2. Create and enroll a TLS/SSL certificate to configure a secure connection to Axidian CertiFlow services.
3. Install a web server: NGINX or Apache HTTP Server.
4. Install .NET.
5. Create a data storage.
6. Configure integration with Microsoft Certification Authority. To connect to Microsoft CA, install Axidian CertiFlow MS CA Proxy.

Install and configure Axidian CertiFlow

1. Install and configure the Axidian CertiFlow server components.
    1. Server
    2. Configuration Wizard
    3. OpenID Connect server
    4. Event Log Proxy or Log Server to record events to a centralized log
2. Install and configure the Axidian CertiFlow Middleware client component.
3. Install the Axidian CertiFlow Middleware extension in the browsers on the workstations of administrators, operators, and users.

Optionally, install and configure Axidian CertiFlow Agent to manage cards on user workstations remotely. The agent requires a separate license.

Environment

User catalog

2 items

Data storage

Microsoft SQL and PostgreSQL

Microsoft CA

Integrate with Microsoft CA

Service certificates

Create TLS/SSL certificates to configure a secure connection to Axidian CertiFlow services

Web server

3 items

.NET

Install .NET

User catalog

Configure a user catalog to manage users in Axidian CertiFlow.

LDAP

Active Directory and FreeIPA

Internal catalog

Microsoft SQL or PostgreSQL database

INFO

Internal user catalog is auxiliary to the main LDAP catalog and is connected to a Microsoft SQL or PostgreSQL database.

LDAP

Axidian CertiFlow supports the following LDAP catalogs: Active Directory and FreeIPA.

A LDAP catalog can be compound. It can pull user information from different containers within a single domain or from multiple domains.

Configure a catalog

Active Directory

Create a service account

Create a service account for reading and writing user attributes.

Active Directory

1. Launch the Active Directory Users and Computers (ADUC) snap-in.
2. Expand the domain tree and select the container or organizational unit that you want to host the user account.
3. On the Action menu, select **Create** → **User**.
4. Enter the name of the service account.
5. Fill in the required fields and click Finish to create the account.

Configure permissions

1. Launch the Active Directory Users and Computers snap-in.
2. Go to the **Security** tab of the object which contains the Axidian CertiFlow users.
3. Click **Advanced→Add→Select a principal**.
4. In the **Enter the object names to select** text box, type the service account name and click **OK**.
5. In the **Apply to** dropdown list, select **Descendant User objects**.
6. In the **Permissions** list, select:
   - List contents.
   - **Read all properties**. By default, all domain service accounts have a permission to read all user properties.
   - **Reset password**
7. In the **Properties** list, select:
   - **Write pwdLastSet**
   - **Write thumbnailPhoto** or **Write jpegPhoto**
   - **Write userAccountControl**

- **Write userCertificate**

8. Click **OK** and **Apply**.

> **INFO**
> Grant the service account the same set of permissions for each object which contains the Axidian CertiFlow users.

Grant read permissions

If domain security policies prohibit reading all user properties, grant the service account permissions to read user attributes and attributes of the object which contains the Axidian CertiFlow users:

1. In the **ADSI edit** snap-in, right-click the relevant object and go to **Properties** → **Security**.
2. In the Apply onto list, select **This object and all descendant objects** and configure the following settings:
    1. In the **Permissions** list, check **List contents** box.
    2. In the **Properties** list, check the following boxes:
        - **Read canonicalName**
        - **Read Distinguished Name**
        - **Read objectClass**
        - **Read objectGuid**
        - **Read showInAdvancedViewOnly**
3. In the Apply onto list, select **Descendant user objects**:
    1. In the **Permissions** list, check **List contents**.
    2. In the **Properties** list, select read/write for the following properties and attributes:
        - **Read personal Information**
        - **Read general Information**
        - Read account restrictions
        - **Read public Information**
        - **Write pwdLastSet**
        - **Write thumbnailPhoto** or **Write jpegPhoto**
        - **Write userAccountControl**
        - **Write userCertificate**

Supported user attributes

> **INFO**
>
> The following table lists LDAP Display Names of the catalog attributes.
>
> It is recommended to grant access to property sets. For more information about property sets, see Microsoft's documentation.

Attribute (LDAP Display Name)	Common Name	Info
c	Country/Region or Country/Region Abbreviation	Personal Information property set
canonicalName	Canonical Name	Public Information property set
cn	Common Name	Public Information property set
company	Company	Public Information property set
**department	Department	Public Information property set
distinguishedName	Distinguished Name	Public Information property set
givenName	Given Name	Public Information property set
l	Locality Name	Personal Information property set
mail	E-mail Addresses	Public Information property set
manager	Manager	Public Information property set
objectClass	Object Class	Public Information property set

Attribute (LDAP Display Name)	Common Name	Info
objectGUID	Object GUID	Public Information property set
objectSid	Object Sid	General Information property set
otherMailbox	Other Mailbox	Public Information property set
proxyAddresses	Proxy Addresses	Public Information property set
pwdLastSet	Pwd Last Set	Account Restrictions property set
sAMAccountName	SAM Account Name	General Information property set
sn	Surname	Public Information property set
st	State or Province Name	Personal Information property set
streetAddress	Address (or Street)	Personal Information property set
telephoneNumber	Telephone Number	Personal Information property set
thumbnailPhoto or jpegPhoto	Picture	Personal Information property set
userAccountControl	User Account Control	Account Restrictions property set.
userCertificate	User Certificate	Personal Information property set
userPrincipalName	User Principal Name	Public Information property set

FreeIPA

To configure a user catalog in FreeIPA:

1. Sign in to the FreeIPA Web UI as an administrator.
2. On the **Identity** tab go to **Users**, click **Add** and create a user. By default, the created user is a member of the `ipausers` service domain group.
3. Create a permission to read and search data in the catalog:
    1. On the **IPA Server** tab, in the **Role-Based Access Control** list, select **Permissions** and click **Add**.
    2. Enter the permission name.
    3. In the **Bind rule type** string, select **permission**.
    4. In the **Granted Rights** string, select `read`, `search`.
    5. In the **Subtree** string, enter the Distinguished name of domain.
    6. Select **Effective attributes**: `entryUUID`.
4. Create a permission to write data to the catalog:
    1. On the **IPA Server** tab, in the **Role-Based Access Control** list, select **Permissions** and click **Add**.
    2. Enter the permission name.
    3. In the **Bind rule type** string, select **permission**.
    4. In the **Granted Rights** string, select `write`.
    5. In the **Type** list, select **User**.
    6. Select **Effective attributes**:
    - `userPassword`
    - `krbPasswordExpiration`
    - `userCertificate`
    - `jpegPhoto`
5. In the **Role-Based Access Control** list, select **Privileges** and click **Add**.
6. Create a privilege and add the created permissions to it.
7. In the **Role-Based Access Control** list, select **Roles**, click **Add** and create a role.
8. In the **Roles** section, go to the **Privileges** tab and add the created privilege to the role.
9. Assign the role to the service account:
    1. In the **Roles** section, select the created role.
    2. In the user list, click **Add** and select the created user.

Supported FreeIPA user attributes

User attribute	Description
entryUUID	Universally unique identifier assigned to the entry
entryDN	Entry's distinguished name
uid	User identifier
mail	Email address
telephoneNumber	Phone number
givenName	First name
sn	Last name
cn	Common name
krbPrincipalName	Kerberos user principal name (UPN)
jpegPhoto	Photo
userPassword	Password
krbPasswordExpiration	A given user's password expiration date
userCertificate	Certificate

Internal catalog

An internal catalog functionality allows to create accounts for external users in a separate database of Axidian CertiFlow. External users are outside an organization and may need access to specific information or features. You can configure an internal catalog in Microsoft SQL or PostgreSQL.

Internal user catalog is auxiliary to the main LDAP catalog.

Configure a database

1. Create a database.
2. Create a service account.
3. Populate the database with a script from the Axidian CertiFlow installation package.

Microsoft SQL

1. Create a database in SQL Server Management Studio:
    1. In the **Object Explorer** pane, right-click **Databases** and select **New Database**.
    2. Enter a database name and click **OK**.
2. Use a local SQL service account or an Active Directory service account and grant it the required permissions to manage the database. This service account is used to perform read and write operations in the database.
    1. In the **Object Explorer** pane, expand the **Security** section.
    2. Right-click the **Logins** folder and select the service account from the context menu.
    3. Go to the **User Mapping** tab and configure the account permissions.
    4. In the **Database role membership for** section, select the check boxes next to the **db_owner** and **public** permissions.
3. Populate the database:
    1. Go to the **File** menu and click **Open**.
    2. Select **File...**, specify the catalog path to the *UserCatalog.sql* file (*\AxidianCertiflow.WindowsServer\Misc*) and click **Open**.
    3. Before running the script, uncomment `--USE[<database name>]--GO` and specify the name of the database or select it from the list.
    4. Click **Execute**.

PostgreSQL

1. Create a database in pgAdmin:

1. Open pgAdmin and connect to the server.
2. In the **Browser** section, right-click **Databases** and select **Create** → **Database...**.
3. On the **General** tab, specify the database name in the **Database** field, select the service account from the **Owner** list, and click **Save**.

2. Create a service account:
   1. In the **Browser** section, right-click the **Login/Group Roles** menu item.
   2. Select **Create** → **Login/Group Role...**.
   3. On the **General** tab, specify a service account name in the **Name** field.
   4. On the **Definition** tab, specify the password in the **Password** field. Make sure the **Account Expires** field has the **No Expiry** value.
   5. On the **Privileges** tab, enable the **Can Login?** parameter and click **Save**.
3. Populate the database. Select the created database in the **Browser** section, execute the *UserCatalog-Postgre.sql* script and grant the service account the required permissions:
   1. Select **Tools** → **Query Tool**.
   2. Click  and specify the catalog path to the *UserCatalog-Postgre.sql* file (*\AxidianCertiflow.WindowsServer\Misc*). Click **Select**.
   3. Click **Execute/Refresh**  .
   4. Click  and select **Clear Query**.
   5. Enter the query text with the service account name:

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO "service account name";
```

   1. Click **Execute/Refresh**  .

Configure a remote connection to the database

1. Open the *pg_hba.conf* configuration file.

> **pg_hba.conf file location**
>
> Windows OS: *C:\Program Files\PostgreSQL<version number>\data*
> Linux OS: */etc/postgresql/<version number>/main*.

2. Add a string in the following format:

```
CONNECTIONTYPE DATABASE USER ADDRESS METHOD
```

   - `CONNECTIONTYPE` is the name of the connection type. Specify `host` to use TCP/IP connection.

- `DATABASE` is the name of the database.
- `USER` is name of the user who accesses the database.
- `ADDRESS` is the IP address of the remote Axidian CertiFlow server.
- `METHOD` is the user authentication method.

```
host AxidianStorage servicepg 192.200.1.0/24 md5
```

Supported user attributes

Axidian CertiFlow connects to an internal user catalog using the following attributes.

Basic attributes

User attribute	Common name
cn	Common Name
dn	Distinguished Name
givenName	First Name
sn	Last Name
sAMAccountName	Logon Name
email	E-mail

Additional attributes

User attribute	Display name
telephoneNumber	Phone number
countryName	Country/region
stateOrProvinceName	State
localityName	City
streetAddress	Address

User attribute	Display name
organizationName	Organization
organizationUnitName	Department
title	Position

You can edit additional attributes and add custom attributes In the Axidian CertiFlow Configuration Wizard.
How to configure additional attributes in an internal user catalog

After you create an internal catalog, configure a connection to the created database in the Axidian CertiFlow Configuration Wizard in the **User Catalog** section.

Data storage

You can configure a data storage in Microsoft SQL or PostgreSQL.

To configure a data storage for Axidian CertiFlow:

1. Create a database.
2. Create a service account.
3. Populate the database with a script from the Axidian CertiFlow installation package.

Microsoft SQL

1. Create a database in SQL Server Management Studio.
    1. In the **Object Explorer** pane, right-click **Databases** and select **New Database**.
    2. Enter a database name and click **OK**.
2. Use a local SQL service account or an Active Directory service account and grant it the required permissions to manage the database. This service account is used to perform read and write operations in the database.
    1. In the **Object Explorer** pane, expand the **Security** section.
    2. Right-click the **Logins** folder and select the service account from the context menu.
    3. Go to the **User Mapping** tab and configure the account permissions.
    4. In the **Database role membership for** section, select the check boxes next to the **db_owner** and **public** permissions.
3. Populate the database.
    1. Go to the **File** menu and click **Open**.
    2. Select **File...**, specify the catalog path to the *Storage.sql* file (*AxidianCertiflow.WindowsServer**Misc*) and click **Open**.
    3. Before running the script, uncomment `--USE[<database name>]--GO` and specify the name of the database or select it from the list.
    4. Click **Execute**.

PostgreSQL

1. Create a database in pgAdmin.
    1. Open pgAdmin and connect to the server.
    2. In the **Browser** section, right-click **Databases** and select **Create** → **Database...**.
    3. On the **General** tab, specify the database name in the **Database** field, select the service account from the **Owner** list, and click **Save**.
2. Create a service account.

1. In the **Browser** section, right-click the **Login/Group Roles** menu item.
2. Select **Create** → **Login/Group Role...**.
3. On the **General** tab, specify a service account name in the **Name** field.
4. On the **Definition** tab, specify the password in the **Password** field. Make sure the **Account Expires** field has the **No Expiry** value.
5. On the **Privileges** tab, enable the **Can Login?** parameter and click **Save**.

3. Populate the database. Select the created database in the **Browser** section, execute the *Storage-Postgre.sql* script and grant the service account the required permissions.
   1. Select **Tools** → **Query Tool**.
   2. Click  and specify the catalog path to the *Storage-Postgre.sql* file (*\AxidianCertiflow.WindowsServer\Misc*). Click **Select**.
   3. Click **Execute/Refresh**  .
   4. Click  and select **Clear Query**.
   5. Enter the query text with the service account name:

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO "service account name";
```

   1. Click **Execute/Refresh**  .

Configure a remote connection to the database

1. Open the *pg_hba.conf* configuration file.

> **pg_hba.conf file location**
>
> Windows OS: *C:\Program Files\PostgreSQL<version number>\data*
> Linux OS: */etc/postgresql/<version number>/main*.

2. Add a string in the following format:

```
CONNECTIONTYPE DATABASE USER ADDRESS METHOD
```

   - `CONNECTIONTYPE` is the name of the connection type. Specify `host` to use TCP/IP connection.
   - `DATABASE` is the name of the database.
   - `USER` is name of the user who accesses the database.
   - `ADDRESS` is the IP address of the remote Axidian CertiFlow server.
   - `METHOD` is the user authentication method.

```
host AxidianStorage servicepg 192.200.1.0/24 md5
```

Microsoft CA

Configure Microsoft Enterprise CA integration with Axidian CertiFlow:

1. Create a service account.
2. Configure certificate templates.
3. Add the certificate templates to **Certificate Templates to Issue** list.
4. Issue an Enrollment Agent certificate for the service account.

Follow these steps to connect to Microsoft CA using the Axidian CertiFlow MS CA Proxy component in the following cases:

- If Microsoft CA is installed outside the domain where the Axidian CertiFlow server running Windows OS is deployed;
- If the Axidian CertiFlow server is installed on Linux OS.

Create a service account

Configure a service account that Axidian CertiFlow uses to request certificates from the CA:

1. Create a user account in Active Directory.
2. Open the **Certification Authority** snap-in, select the CA and go to **Properties**.
3. On the **Security** tab, click **Add** and specify the name of the created account.
4. Set the **Issue and Manage Certificates** permission. The **Request Certificates** permission is set by default.
5. Click **OK** to save the settings.

> ⓘ **INFO**
> Enable the **Manage CA** permission to be able to publish the certificate revocation list when you configure certificate templates for the CA in Axidian CertiFlow.

> ⚠ **CAUTION**
> If you plan to use Axidian CertiFlow with multiple CAs, ensure that the service account has the same set of permissions for all CAs.

Configure certificate templates

Configure the **Enrollment Agent** certificate template and user certificate templates.

Enrollment Agent

The Enrollment Agent certificate is used to request certificates on behalf of end users.

> ⚠ **CAUTION**
> The Enrollment Agent certificate is added to Axidian CertiFlow only once and is issued only for the service account.
> To prevent security issues, do not add the Enrollment Agent certificate to card usage policies in Axidian CertiFlow. Otherwise, users could bypass the normal procedure and generate their own certificates in the CA.

Create and configure the Enrollment Agent certificate template:

1. Open the **Certification Authority** snap-in and click the CA to expand the root folder.
2. Right-click the **Certificate Templates** section and select **Manage**.
3. Right-click the **Enrollment Agent** template and select **Duplicate Template**.
4. Go to the **General** tab and enter **Axidian Enrollment Agent** in the **Template display name** field. Change the **Validity period** according to your company's regulations.
5. Go to the **Cryptography** tab and set the required **key size**. The recommended key size is 2048 bits.
6. On the **Extensions** tab, select the **Application Policies** extension and click **Edit...**.
    1. Click **Add...**, select the Client Authentication application policy from the list and click OK.
    2. Select the **Client Authentication** application policy from the provided list.
    3. Click **OK**.
7. On the **Security** tab, click **Add...**.
    1. In the **Enter the object names to select** field, enter the service account name and click **OK**.
    2. In the **Permissions for** section, assign the **Read** and **Enroll** permissions.
8. Click **OK** to save the template settings.

User certificates

Prepare certificate templates for application policies that are used to issue certificates to Axidian CertiFlow end users.

Use the following instruction to create and configure the Smartcard Logon certificate template. The Smartcard Logon certificate template is used to issue certificates for logging into the operating system using a smart card.

1. Open the **Certification Authority** snap-in and click the CA to expand the root folder.
2. Right-click the **Certificate Templates** section and select **Manage**.
3. Right-click the **Smartcard Logon** template and select **Duplicate Template**.

4. Go to the **General** tab and enter *Axidian Smart Card Logon* in the **Template display name** field. Change the **Validity period** according to your company's regulations.
5. Go to the **Cryptography** tab and set the required **Key size**.

About minimum key size

The minimum key size can be configured for Microsoft CA 2008/2008R2 and higher. In previous versions, the minimum key size is configured on the **Request Handling** tab.

To prevent unauthorized access to confidential information, Microsoft issued an update (KB2661254) for all supported Microsoft Windows versions. This update blocks cryptographic keys that are less than 1024 bits long. This update is not supported in Windows 8 and higher or Windows Server 2012 and higher, since these systems can block weak RSA keys less than 1024 bits long.

6. On the **Issuance Requirements** tab, configure the following properties:
    1. Check the **CA Certificate manager approval** box.
    2. Check the **This number of authorized signatures** box. Type **1** in the text box.
    3. Select **Application policy** from the **Policy type required in signature** list.
    4. Select **Certificate Request Agent** from the **Application policy** list.
    5. Under **Require the following for reenrollment**, select **Same criteria as for enrollment**.
7. Go to the **Subject Name** tab. Depending on the certificate purpose, select:

- **Supply in the request** if certificates with Secure Email (OID 1.3.6.1.5.5.7.3.4) and Document Signing (OID 1.3.6.1.4.1.311.10.3.12) purposes are issued based on this template.

> **INFO**
> Certificate subject name is formed from the certificate request.
> You can define attributes for Subject and Subject Alternative Name in the Axidian CertiFlow Management Console. Go to **Configuration→Policies→PKI Settings→Microsoft→Templates**.

- **Built from this Active Directory information** if certificates with SmartCard Logon (OID 1.3.6.1.4.1.311.20.2) and Client Authentication (OID 1.3.6.1.5.5.7.3.2) purposes are issued based on this template. Follow these steps:

    i. Select **Fully distinguished name** from the **Subject name format** list.
    ii. Check the **User principal name (UPN)** box.
    iii. Clear the **Include e-mail name in subject name** and **E-mail name** check boxes if certificates based on this template are issued for users without email addresses defined in Active Directory.

8. Go to the **Security** tab and click **Add...**.

1. In the **Enter the object names to select** field, enter the service account name and click **OK**.
2. In the **Permissions for** section, assign the **Read** and **Enroll** permissions.

> ⚠ **CAUTION**
> Grant similar permissions to the service account for all certificate templates that are used in Axidian CertiFlow.

9. Click **OK** to save the template settings.

Add certificate templates

1. Open the Certification Authority snap-in and click the CA to expand the root folder.
2. Right-click the **Certificate Templates** section.
3. Select **New→Certificate Template to Issue**.
4. Select the **Axidian CertiFlow Enrollment Agent** certificate template and other required certificate templates.
5. Click **OK**.

Issue the Enrollment Agent certificate

There are two ways to create the Enrollment Agent certificate:

- Using the Certiflow.CertEnroll.MsCA tool
- Using the Certificates tool (certmgr.msc)

Certiflow.CertEnroll.MsCA

To issue an Enrollment Agent certificate:

1. Open the Axidian CertiFlow installation package and open the *AxidianCertiflow.WindowsServer\Misc* catalog.
2. Run *Certiflow.CertEnroll.MsCA.exe* on the Axidian CertiFlow server as local administrator with `/e userName password` and `/t templateName` parameters:
   - `userName` – a service account name
   - `password` – a service account password
   - `templateName` – Enrollment Agent certificate template name. Templates with any names that have the Certificate Request Agent EKU are supported.

   Command example

```
Certiflow.CertEnroll.MsCA.exe /e serviceca p@ssw0rd /t="AxidianEnrollmentAgent"
```

Results

```
CA: msca.demo.local\Axidian-Demo-CA
Certificate has been enrolled successfully.
```

3. If the certificate request is approved by a CA operator, the tool prompts to accept the request and continue, indicating the request serial number and the key container name:

```
CA: msca.demo.local\Axidian-Demo-CA
Certificate request is pending.
Request id: 27
Container name: lr-AxidianEnrollmentAgent-175d9490-7481-4a29-b567-503d39747354
Please accept request and then install certificate.
```

4. After approving the request in the CA, install the certificate in the certificate store. To install the certificate in the certificate store, run the Certiflow.CertEnroll.MsCA.exe with `/i userName password requestId containerName` parameters:

   - `userName` – a service account name
   - `password` – a service account password
   - `requestId` – a certificate request serial number
   - `containerName` – a key container name

Command example and results

```
Certiflow.CertEnroll.MsCA.exe /i serviceca p@ssw0rd 27 lr-AxidianEnrollmentAgent-
175d9490-7481-4a29-b567-503d39747354
CA: msca.demo.local\Axidian-Demo-CA
Certificate has been installed successfully.
```

As a result, the Certificate Request Agent (Enrollment Agent) certificate is installed in the certificate store of the machine where the Axidian CertiFlow server is installed.

If you need to issue an Enrollment Agent certificate from a specific CA (for example, if there are multiple CAs in the domain), run Certiflow.CertEnroll.MsCA.exe with the `/c` parameter. Specify the CA name in the `CAMachineName\CAName` format:

- `CAMachineName` – the DNS name of a server with the CA role
- `CAName` – the name of the CA

```
Certiflow.CertEnroll.MsCA.exe /e serviceca p@ssw0rd /t="AxidianEnrollmentAgent"
/c="msca.demo.local\Axidian-Demo-CA"
```

Certificate Manager

1. Log in to the OS under the service account and open the User Certificates snap-in (certmgr.msc).
2. Start the certificate request:
    1. Under Certificates, expand the Personal folder.
    2. Right-click Certificates and select All Tasks → Request New Certificate.
3. In the Certificate Enrollment wizard, select **Enrollment Agent**, expand the details and go to **Properties**.
4. Go to the **Private key** tab, expand the **Key options** menu and check the **Make private key exportable box**.
5. Save the issued certificate and its private key to the certificate store of the machine where the Axidian CertiFlow server is installed.
6. Grant the service account read permissions for the private key of the Enrollment Agent certificate:
    1. Go to the Computer Certificates snap-in and right-click the Enrollment Agent certificate.
    2. Select **All tasks→Manage Private Keys...**.
    3. Click **Add** and specify the service account.
    4. Assign the **Full control** permission.
    5. Click **Apply**.

Connect to Microsoft CA using Axidian CertiFlow MS CA Proxy

Axidian CertiFlow can work with CAs located outside the domain of the Axidian CertiFlow server using the Axidian CertiFlow MS CA Proxy component.

Configuration examples:

- There are several independent domains with separate CAs in each, Axidian CertiFlow is deployed in only one of these domains.
- Axidian CertiFlow is deployed on a non-domain Linux OS server and is used to request and issue certificates in a domain with Microsoft CA.

When issuing a certificate, Axidian CertiFlow uses the Enrollment Agent certificate to connect to the Axidian CertiFlow MS CA Proxy and forwards the request to the target CA.

Install and configure the Axidian CertiFlow MS CA Proxy

The Axidian CertiFlow MS CA Proxy application can only be installed on a machine running Windows OS. System requirements match the server requirements.

1. Create a service account for Microsoft CA in an external domain.
2. Configure the Enrollment Agent certificate template for the service account and issue the Enrollment Agent certificate. Install the Enrollment Agent certificate in the certificates store of a machine (Local computer) where you plan to install the Axidian CertiFlow MS CA Proxy.
3. Install the Axidian CertiFlow MS CA Proxy on a machine within the external CA domain:
    1. Open the Axidian CertiFlow installation package and open the *AxidianCertiflow.Server* catalog.
    2. Run the Axidian CertiFlow MS CA Proxy Installation Wizard *AxidianCertiflow.MSCA.Proxy-version number.x64.en-us.msi*.
4. In the Installation Wizard, select the authentication method depending on the OS of the machine where the Axidian CertiFlow server is installed, and specify the required settings in the configuration files:

Windows

1. Select the Windows authentication method. After the installation is complete, click **Finish**.
2. Open the *appsettings.json* file (*C:\inetpub\wwwroot\certiflow\mscaproxy*) in Notepad in administrator mode.
3. Specify the following settings in the `caProxySettings` section:

- `ca` – the CA name in the `CAMachineName\CAName` format. `CAMachineName` is the DNS name of the server with the CA role, `CAName` is the name of the CA.
- `userName` and `password` – login and password of the service account with an Enrollment Agent certificate.
- `enrollmentAgentCertificateThumbprint` – the thumbprint of the Enrollment Agent certificate.

```
"caProxySettings": {
"ca": "servercertiflow.external.com\\EXTERNAL-CA",
"userName": "EXTERNAL\\serviceca",
"password": "p@ssw0rd",
"enrollmentAgentCertificateThumbprint":
"dbd1859d27395860843643ebe17e2ee3fc463aba"
}
```

4. Save changes and close the *appsettings.json* file.

Linux

1. Select the certificate authentication method. After the installation is complete, click **Finish**.
2. Open the *appsettings.json* file (*C:\inetpub\wwwroot\certiflow\mscaproxy*) in Notepad in administrator mode.
3. Specify the following settings in the `caProxySettings` section:

- `ca` – the CA name in the `CAMachineName\CAName` format. `CAMachineName` is the DNS name of the server with the CA role, `CAName` is the name of the CA.
- `userName` and `password` – login and password of the service account with an Enrollment Agent certificate.
- `enrollmentAgentCertificateThumbprint` – the thumbprint of the Enrollment Agent certificate.

```
"caProxySettings": {
"ca": "servercertiflow.external.com\\EXTERNAL-CA",
"userName": "EXTERNAL\\serviceca",
"password": "p@ssw0rd",
"enrollmentAgentCertificateThumbprint":
"dbd1859d27395860843643ebe17e2ee3fc463aba"
}
```

4. In the `authSettings` section, specify the Enrollment Agent certificate thumbprint in the `allowedCertificateThumbprints` parameter. Make sure that the **Enhanced Key Usage** field of the certificate contains Client Authentication and the certificate is installed in the certificate store of the Axidian CertiFlow server.

```
"authSettings": {
"authorizeByCertificate": "true",
"allowedCertificateThumbprints": "aba8b93d73343f2182e3c1c40482b2ae2d75b6ec"
}
```

5. Save changes and close the *appsettings.json* file.

5. To apply changes, restart the Axidian CertiFlow MS CA Proxy application pool:

1. Open the Internet Information Services Manager (IIS). In the Connections pane, expand the server name, and then click **Application Pools**.

2. Select the Axidian CertiFlow MS CA Proxy application and click **Recycle...** under **Actions** on the right.

Service certificates

Create the following TLS/SSL certificates to configure a secure connection to Axidian CertiFlow services:

- Server authentication certificate for the web server and the OpenID Connect server
- Client authentication certificate for additional services: the Axidian CertiFlow Event Log Proxy and Axidian AirCard Enterprise

Server authentication certificate

Create and issue a TLS/SSL certificate to configure a secure connection to the website hosting Axidian CertiFlow. Use the same certificate as the signing certificate to configure the OpenID Connect server.

Certificate requirements

- **Subject** must include the **Common Name** attribute (the Axidian CertiFlow server FQDN).
- **Subject Alternative Name (SAN)** must include a **DNS Name** attribute (the Axidian CertiFlow server FQDN).
  For example: `server.domain.loc` or a corresponding wildcard entry `*.domain.loc`.
- **Enhanced Key Usage (EKU)** must include the **Server Authentication** value.

Create a certificate template

Prepare the certificate template. The following procedure details the configuration of a certificate template in Microsoft Certificate Authority (CA).

1. Open the Microsoft CA web interface (certsrv), right-click **Certificate Templates** and select **Manage**.
2. Copy the built-in **Web Server** template – right-click the template name and select **Duplicate Template**.
3. On the **General** tab of the template properties window, specify a name for the certificate template. If necessary, specify the certificate validity and renewal period.
4. On the **Request Handling** tab, enable the **Allow private key to be exported** option.
5. (Optional) On the **Cryptography** tab, edit the minimum key size.
6. On the **Security** tab, specify the server name for the certificate request:
   1. Click **Add** → **Object Types**, enable the **Computers** option, and click **OK**.
   2. Enter the name of the Axidian CertiFlow server and click **OK**.
7. In the permissions list, set **Allow** for the **Enroll** permission.
8. Click **Apply** and **OK**.
9. Publish the created certificate template.

1. In the certsrv console, right-click **Certificate Templates** and select **New → Certificate Template to Issue**.
2. In the **Enable Certificate Templates** window, select the created template. The template is published in the CA.

10. Close the certsrv console.

Enroll a certificate

Enroll the TLS/SSL certificate for the workstation where you plan to install the web server. You can either enroll the certificate in the CA or create a self-signed certificate.

Enroll the certificate in the CA

The following procedure details how to enroll a certificate in Microsoft CA.

1. Open the Certificates MMC snap-in (certs.msc) and go to the **Certificates (Local Computer)** store.
2. Right-click the **Personal** folder and select **All Tasks → Request New Certificate**.
3. In the **Certificate Enrollment** window, click **Next** twice and select the certificate template created earlier.
4. Click the link **More information is required to enroll for this certificate. Click here to configure settings** to specify additional certificate request details. This opens the certificate properties window.
5. In the certificate properties window, open the **Subject** tab.
    1. In the **Subject name** section, select **Common name** from the **Type** list.
    2. Enter the FQDN of the Axidian CertiFlow server and click **Add**.
    3. In the **Alternative name** section, select **DNS** from the **Type** list.
    4. Enter the FQDN of the Axidian CertiFlow server and click **Add**.
    5. (Optional) To create a domain wildcard for servers with various hostnames, select **DNS** from the **Type** list in the **Alternative name** section and enter a wildcard domain (for example, `*.demo.local`). Click **Add**.
6. Click **OK**.
7. Go to the **Private Key → Key Options** tab and ensure the **Make private key exportable** option is enabled. Click **OK**.
8. Click **Enroll**.

The certificate is installed in the local computer's certificate store (**Certificates → Personal → Certificates**) with the intended purpose of **Server Authentication**.

Install a certificate on a Linux workstation

To transfer and install the certificate on Linux workstations, export the certificate and split it into a certificate file and a private key file.

1. Follow the instructions provided in the previous section to enroll the certificate from a CA.

2. Right-click the certificate and select **All Tasks** → **Export**.

3. In the Certificate Export Wizard, click **Next**, select **Yes, export the private key**, and click **Next** twice.

4. Enable the **Password** option, enter and confirm the password. Click **Next**.

5. Select the destination folder for the exported certificate and click **Finish**.

6. Split the PFX file into a certificate file and a private key file. Replace `PFXFILE` with the name of the imported file.

   > ⚠ **CAUTION**
   > When executing the commands, the OpenSSL command line tool prompts you to set a password for the private key file. Leave the file without a password: press **Enter** twice.

   ```
   openssl pkcs12 -in PFXFILE.pfx -nokeys | sed -ne '/-BEGIN CERTIFICATE/,/END
   CERTIFICATE/p' > SSL.crt
   openssl pkcs12 -in PFXFILE.pfx -cacerts -nokeys | sed -ne '/-BEGIN
   CERTIFICATE-/,/-END CERTIFICATE-/p' > root-ca.crt
   openssl pkcs12 -in PFXFILE.pfx -nocerts -out SSLencrypted.key
   openssl rsa -in SSLencrypted.key -out SSL.key
   rm SSLencrypted.key
   ```

   The *SSL.crt* file must contain the following:

   ```
   -----BEGIN CERTIFICATE-----
   #Your certificate#
   -----END CERTIFICATE-----
   ```

Create a self-signed certificate

Create a self-signed root certificate using the OpenSSL command line tool.

1. Generate a private key and create the root certificate using the generated key.

   ```
   openssl genrsa -out ca.key 2048
   openssl req -x509 -new -nodes -key ca.key -out ca.crt -days 3650 -subj
   "/CN=selfCA"
   ```

2. Create an *SSL.conf* configuration file which contains the settings for generating the web server certificate request.

```
nano SSL.conf
```

SSL.conf example

```
[ req ]
default_bits = 2048
encrypt_key = no
default_md = sha256
utf8 = yes
string_mask = utf8only
prompt = no
distinguished_name = req_distinguished_name
req_extensions = req_ext
[ req_distinguished_name ]
commonName = <FQDN of the Axidian CertiFlow server>
[ req_ext ]
subjectAltName = @alt_names
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
basicConstraints = CA:FALSE
extendedKeyUsage = serverAuth
[alt_names]
DNS.1 = <FQDN of the Axidian CertiFlow server>
```

3. Create a certificate request and enroll the web-server certificate using the self-signed certificate.

```
openssl genrsa -out SSL.key 2048
openssl req -new -sha256 -out SSL.csr -key SSL.key -config SSL.conf
openssl x509 -req -days 365 -in SSL.csr -CA ca.crt -CAkey ca.key -CAcreateserial
-extfile SSL.conf -extensions req_ext -out SSL.crt
```

Client authentication certificate

The Axidian CertiFlow server can operate as a client for the Axidian CertiFlow Event Log Proxy and Axidian AirCard Enterprise services.

In this case, the Axidian CertiFlow server must have a client authentication certificate to access the services.

Certificate requirements

- **Subject** must include the **Common Name** attribute (the Axidian CertiFlow server FQDN).
- **Enhanced Key Usage (EKU)** must include the **Client Authentication** value.

Create a certificate template

Prepare the certificate template. The following procedure details the configuration of a certificate template in Microsoft Certificate Authority (CA).

1. Open the Microsoft CA web interface (certsrv), right-click **Certificate Templates** and select **Manage**.
2. Copy the built-in **Workstation Authentication** template – right-click the template name and select **Duplicate Template**.
3. On the **General** tab of the template properties window, specify a name for the certificate template. If necessary, specify the certificate validity and renewal period.
4. On the **Request Handling** tab, enable the **Allow private key to be exported** option.
5. (Optional) On the **Cryptography** tab, edit the minimum key size.
6. On the **Security** tab, specify the server name for the certificate request.
    1. Click **Add** → **Object Types**, enable the **Computers** option, and click **OK**.
    2. Enter the name of the Axidian CertiFlow server and click **OK**.
7. In the permissions list, set **Allow** for the **Enroll** permission.
8. Click **Apply** and **OK**.
9. Publish the created certificate template.
    1. In the certsrv console, right-click **Certificate Templates** and select **New** → **Certificate Template to Issue**.
    2. In the **Enable Certificate Templates** window, select the created template. The template is published in the CA.
10. Close the certsrv console.

Enroll a certificate

Enroll the TLS/SSL certificate for the workstation where you plan to install the web server. You can either enroll the certificate in the CA or create a self-signed certificate.

Enroll the certificate in the CA
The following procedure details how to enroll a certificate in Microsoft CA. 1. Open the Certificates MMC snap-in (certs.msc) and go to the **Certificates (Local Computer)** store. 2. Right-click the **Personal** folder and select **All Tasks** → **Request New Certificate**.

3. In the **Certificate Enrollment** window, click **Next** twice and select the certificate template created earlier.
4. Click the link **More information is required to enroll for this certificate. Click here to configure settings** to specify additional certificate request details. This opens the certificate properties window.
5. In the certificate properties window, open the **Subject** tab.
    1. In the **Subject name** section, select **Common name** from the **Type** list.
    2. Enter the FQDN of the Axidian CertiFlow server and click **Add**.
    3. In the **Alternative name** section, select **DNS** from the **Type** list.
    4. Enter the FQDN of the Axidian CertiFlow server and click **Add**.
    5. (Optional) To create a domain wildcard for servers with various hostnames, select **DNS** from the **Type** list in the **Alternative name** section and enter a wildcard domain (for example, `*.demo.local`). Click **Add**.
6. Click **OK**.
7. Go to the **Private Key** → **Key Options** tab and ensure the **Make private key exportable** option is enabled. Click **OK**.
8. Click **Enroll**.

The certificate is installed in the local computer's certificate store (**Certificates** → **Personal** → **Certificates**) with the intended purpose of **Client Authentication**.

Install a certificate on a Linux workstation

To transfer and install the certificate on Linux workstations, export the certificate and split it into a certificate file and a private key file.

1. Follow the instructions provided in the previous section to enroll the certificate from a CA.
2. Right-click the certificate and select **All Tasks** → **Export**.
3. In the Certificate Export Wizard, click **Next**, select **Yes, export the private key**, and click **Next** twice.
4. Enable the **Password** option, enter and confirm the password. Click **Next**.
5. Select the destination folder for the exported certificate and click **Finish**.
6. Split the PFX file into a certificate file and a private key file. Replace `PFXFILE` with the name of the imported file.

> ⚠ **CAUTION**
> When executing the commands, the OpenSSL command line tool prompts you to set a password for the private key file. Leave the file without a password: press **Enter** twice.

```
openssl pkcs12 -in PFXFILE.pfx -nokeys | sed -ne '/-BEGIN CERTIFICATE/,/END
CERTIFICATE/p' > client.crt
openssl pkcs12 -in PFXFILE.pfx -cacerts -nokeys | sed -ne '/-BEGIN
CERTIFICATE-/,/-END CERTIFICATE-/p' > root-ca.crt
openssl pkcs12 -in PFXFILE.pfx -nocerts -out clientencrypted.key
openssl rsa -in clientencrypted.key -out client.key
rm clientencrypted.key
```

The *client.crt* file must contain the following:

```
-----BEGIN CERTIFICATE-----
#Your certificate#
-----END CERTIFICATE-----
```

Create a self-signed certificate

Create a self-signed root certificate using the OpenSSL command line tool.

1. Generate a private key and create the root certificate using the generated key.

```
openssl genrsa -out ca.key 2048
openssl req -x509 -new -nodes -key ca.key -out ca.crt -days 3650 -subj
"/CN=selfCA"
```

2. Create a *client.conf* configuration file which contains the settings for generating the certificate request.

```
nano client.conf
```

Client.conf example

```
[ req ]
default_bits = 2048
encrypt_key = no
default_md = sha256
utf8 = yes
string_mask = utf8only
prompt = no
distinguished_name = req_distinguished_name
req_extensions = req_ext
[ req_distinguished_name ]
commonName = <FQDN of the Axidian CertiFlow server>
[ req_ext ]
subjectAltName = @alt_names
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
basicConstraints = CA:FALSE
extendedKeyUsage = clientAuth
[alt_names]
DNS.1 = <FQDN of the Axidian CertiFlow server>
```

3. Create a certificate request and enroll the client certificate using the self-signed certificate.

```
openssl genrsa -out client.key 2048
openssl req -new -sha256 -out client.csr -key client.key -config client.conf
openssl x509 -req -days 365 -in client.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -extfile client.conf -extensions req_ext -out client.crt
```

Web server

To run the Axidian CertiFlow server components on Windows, install the Internet Information Services (IIS) web server. For Linux, install either the Apache or Nginx web server.

Before you install the web server, create and issue a TLS/SSL certificate to configure a secure connection for the website that hosts Axidian CertiFlow.

IIS

Install and configure Internet Information Services

NGINX

Install and configure NGINX

Apache HTTP Server

Install and configure Apache

IIS

To run the Axidian CertiFlow server components on Windows, install and configure the Internet Information Services (IIS) web server.

Install IIS

Install Internet Information Services (IIS) version 7.0 or higher with the following modules:

- Static Content
- HTTP Redirection
- ASP.NET;
- .NET Extensibility
- ISAPI Extensions
- ISAPI Filters
- Basic Authentication
- URL Authorization
- Windows Authentication
- IIS Management Console

> **TIP**
> To quickly install Internet Information Services (IIS) with the required modules, use the PowerShell script from the *\IIS.Setup.Scripts* catalog of the Axidian CertiFlow installation package.
>
> To deploy the Axidian CertiFlow server, install Microsoft .NET 8.0 after you install and configuring the Internet Information Services (IIS) components.

Install a TLS/SSL certificate

How to issue a TLS/SSL certificate

Bind a TLS/SSL certificate to the Axidian CertiFlow website.

1. Open Internet Information Services (IIS) Manager.
2. Select the **Default Web Site** and go to **Bindings...**.
3. Click **Add...**, select **Type: https** and set **Port:** to **443**.
4. In the **SSL certificate:** list, select the appropriate certificate and click **OK**.

NGINX

To run the Axidian CertiFlow server components on Linux, configure the nginx web server as a reverse proxy server.

1. Install nginx.
2. Install a TLS/SSL certificate.
3. Configure the web server configuration file.

Follow the instructions for the operating system of the workstation where you plan to install nginx.

RHEL-based

Install nginx

Before you install nginx, set up the nginx packages repository. If the repository has not been set up automatically, add it manually.

1. Install the packages required to connect to the Yum repository:

```
sudo yum install yum-utils
```

2. To connect to the Yum repository, create a file named */etc/yum.repos.d/nginx.repo* with the following content.

```
[nginx-stable]
name=nginx stable repo
baseurl=http://nginx.org/packages/centos/$releasever/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://nginx.org/keys/nginx_signing.key
module_hotfixes=true

[nginx-mainline]
name=nginx mainline repo
baseurl=http://nginx.org/packages/mainline/centos/$releasever/$basearch/
gpgcheck=1
enabled=0
gpgkey=https://nginx.org/keys/nginx_signing.key
module_hotfixes=true
```

3. To install nginx, execute the following command.

```
sudo yum install nginx
```

If prompted to verify the GPG key, ensure its fingerprint matches `573B FD6B 3D8F BC64 1079 A6AB ABF5 BD82 7BD9 BF62`.

For more information about nginx installation, see the NGINX website.

Install a TLS/SSL certificate

How to issue a TLS/SSL certificate

Install a TLS/SSL certificate on the web server.

1. Copy the certificate and private key files to the catalogs specified in the nginx configuration file.

```
sudo cp ./SSL.crt /etc/ssl/certs/
sudo cp ./SSL.key /etc/ssl/private/
```

2. Add the root CA certificate to the trusted certificates store on the workstation running nginx.

```
sudo cp ./ca.crt /etc/pki/ca-trust/source/anchors/
sudo update-ca-trust extract
```

3. Make the certificate trusted across the domain. For example, distribute it through Group Policies.

4. Grant the nginx system user read access to the certificate files.

Edit the nginx configuration file

Configure Nginx to accept web requests and proxy them to the Axidian CertiFlow service.

Nginx and its modules operate according to the settings defined in the main configuration file, *nginx.conf*. Depending on your operating system, this file is located in the */usr/local/nginx/conf*, */etc/nginx*, or */usr/local/etc/nginx* catalog.

Recommended directives

Context	Directive	Default value	Recommended value	
http	proxy_buffer_size	4k | 8k	16k	Increase size to h informa request
	proxy_buffers	8 4k | 8 8k	4 16k	Increase size to h informa request
	types_hash_max_size	1024	4096	Increase size to s to the la proxied
	client_max_body_size	1m	10m	Increase maximu uploade

Context	Directive	Default value	Recommended value	
server	listen	80	443 ssl	Change to HTTF configu default.
	listen	—	3003 ssl	Port 30(addition when us CertiFlo
	ssl_certificate	—	/etc/ssl/private/SSL.crt	For HTT specifie certifica certifica root CA
	ssl_certificate_key	—	/etc/ssl/private/SSL.key	For HTT specifie certifica
	ssl_verify_client	off	optional_no_ca	Added f authenti client ag

Context	Directive	Default value	Recommended value	
	location	proxy_pass	—	*
include		—	/etc/nginx/conf.d/proxy.conf	Some d describe For a m configu recomm file with set of di it in eac writing t repeate
proxy_http_version		1.0	1.1	Version for keep and NTL
proxy_cache_bypass		—	$http_upgrade	Defines which a taken fr

Context	Directive	Default value	Recommended value	
proxy_set_header		—	Upgrade $http_upgrade	Specifie HTTP/1 after es connect
		—	Connection keep-alive	For usin connect
		—	Host $host	To pres name in passing CertiFlo
		—	X-Real-IP $remote_addr	By defa reverse non-sta the user requirin
		—	X-Forwarded-For $proxy_add_x_forwarded_for	Similar $remote formati correct Forwarc present header, $proxy_ = $remo
proxy_set_header		—	X-Forwarded-Proto $scheme	The wel request proxies Axidian for corr substitu
fastcgi_buffers		8 4k | 8k	16 16k	Defines of buffe respons server, p

Context	Directive	Default value	Recommended value	
fastcgi_buffer_size		4k | 8k	32k	Defines reading respons server.
proxy_set_header		—	x-ssl-client-cert $ssl_client_escaped_cert	Passes when pr client ac based a

Using multiple `location` blocks in the configuration leads to repeating the same set of directives. To simplify the configuration process, extract the common set of directives into a separate file. Then, use the `include` directive within each `location` context to reference that file.

1. Create a file for the reusable directives. You can place this file in CONF format in the */etc/nginx/conf.d/* catalog.

   Recommended proxy.conf file content for Axidian CertiFlow compatibility

   ```
   proxy_http_version 1.1;
   proxy_set_header   Upgrade $http_upgrade;
   proxy_set_header   Connection keep-alive;
   proxy_set_header   Host $host;
   proxy_cache_bypass $http_upgrade;
   proxy_set_header   X-Real-IP $remote_addr;
   proxy_set_header   X-Forwarded-For $proxy_add_x_forwarded_for;
   proxy_set_header   X-Forwarded-Proto $scheme;
   fastcgi_buffers 16 16k;
   fastcgi_buffer_size 32k;
   ```

2. Configure the main nginx configuration file. The `location` context names must match the path to the proxied service.

▼ **Nginx.conf example**

```
user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log notice;
events {    worker_connections 1024;    }

http {
 proxy_buffer_size   64k;
 proxy_buffers   4 64k;
 types_hash_max_size     4096;
 add_header X-Frame-Options sameorigin always;
 add_header X-Content-Type-Options nosniff;

 log_format  main  '[$time_local] $remote_addr VIA $scheme --- $status ---
$request \n $ssl_client_fingerprint';
 access_log  /var/log/nginx/access.log  main;
 sendfile                on;
 tcp_nopush              on;
 include                 /etc/nginx/mime.types;
 default_type            application/octet-stream;

 server {
     listen              443 ssl;
     server_name         $hostname;

     ssl_certificate     "/etc/ssl/certs/SSL.crt";
     ssl_certificate_key "/etc/ssl/private/SSL.key";

     location /certiflow/mc
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5001/certiflow/mc; }
     location /certiflow/ss
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5002/certiflow/ss; }
     location /certiflow/rss
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5003/certiflow/rss;    }
     location /certiflow/api
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5004/certiflow/api;    }
     location /certiflow/credprovapi
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5005/certiflow/credprovapi;    }
     location /certiflow/oidc
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5008/certiflow/oidc;   }
     location /certiflow/wizard
     {   proxy_pass http://localhost:5009;  }
     #location /api
     #{  include /etc/nginx/conf.d/proxy.conf;   proxy_pass
```

```
    http://localhost:5010/api;  }
     }

     server {
         listen              3003 ssl;
         server_name         $hostname;

         ssl_certificate     "/etc/ssl/certs/SSL.crt";
         ssl_certificate_key "/etc/ssl/private/SSL.key";
         ssl_verify_client   optional_no_ca;

         location /agentregistrationapi
         { include /etc/nginx/conf.d/proxy.conf;   proxy_pass
    http://localhost:5006/agentregistrationapi;  }
         location /agentserviceapi
         { include /etc/nginx/conf.d/proxy.conf;   proxy_pass
    http://localhost:5007/agentserviceapi;
                                                   proxy_set_header   x-ssl-client-
    cert $ssl_client_escaped_cert;  }
     }
    }
```

3. To apply the changes in the configuration file, reload the configuration or restart nginx. To reload the configuration, execute the following command.

```
sudo nginx -s reload
```

Debian-based

Install nginx

1. Install the packages required to connect to the Yum repository:

Ubuntu

```
sudo apt install curl gnupg2 ca-certificates lsb-release ubuntu-keyring
```

Debian

```
sudo apt install curl gnupg2 ca-certificates lsb-release debian-archive-keyring
```

2. Import the official GPG key used by apt to authenticate packages:

```
curl https://nginx.org/keys/nginx_signing.key | gpg --dearmor | sudo tee
/usr/share/keyrings/nginx-archive-keyring.gpg >/dev/null
```

3. Connect to the Yum repository.

```
echo "deb [signed-by=/usr/share/keyrings/nginx-archive-keyring.gpg]
http://nginx.org/packages/ubuntu `lsb_release -cs` nginx" | sudo tee
/etc/apt/sources.list.d/nginx.list
```

4. Execute the following commands.

```
sudo apt update
sudo apt install nginx
```

For more information about nginx installation, see the NGINX website.

Install a TLS/SSL certificate

How to issue a TLS/SSL certificate

Install a TLS/SSL certificate on the web server.

1. Copy the certificate and private key files to the catalogs specified in the nginx configuration file.

```
sudo cp ./SSL.crt /etc/ssl/certs/
sudo cp ./SSL.key /etc/ssl/private/
```

2. Add the root CA certificate to the trusted certificates store on the workstation running nginx:

```
sudo cp ./ca.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates -f
```

3. Make the certificate trusted across the domain. For example, distribute it through Group Policies.

4. Grant the www-data system user read access to the certificate files.

Edit the nginx configuration file

Configure Nginx to accept web requests and proxy them to the Axidian CertiFlow service.

Nginx and its modules operate according to the settings defined in the main configuration file, *nginx.conf*. Depending on your operating system, this file is located in the */usr/local/nginx/conf*,

/etc/nginx, or */usr/local/etc/nginx* catalog.

Recommended directives

Context	Directive	Default value	Recommended value	
http	proxy_buffer_size	4k | 8k	16k	Increase size to h informa request
	proxy_buffers	8 4k | 8 8k	4 16k	Increase size to h informa request
	types_hash_max_size	1024	4096	Increase size to s to the la proxied
	client_max_body_size	1m	10m	Increase maximu uploade

Context	Directive	Default value	Recommended value	
server	listen	80	443 ssl	Change to HTTF configu default.
	listen	—	3003 ssl	Port 30(addition when us CertiFlo
	ssl_certificate	—	/etc/ssl/private/SSL.crt	For HTT specifie certifica certifica root CA
	ssl_certificate_key	—	/etc/ssl/private/SSL.key	For HTT specifie certifica
	ssl_verify_client	off	optional_no_ca	Added f authenti client ag

Context	Directive	Default value	Recommended value	
	location	proxy_pass	—	*
include		—	/etc/nginx/conf.d/proxy.conf	Some d describe For a m configu recomm file with set of di it in eac writing t repeate
proxy_http_version		1.0	1.1	Version for keep and NTL
proxy_cache_bypass		—	$http_upgrade	Defines which a taken fr

Context	Directive	Default value	Recommended value	
proxy_set_header		—	Upgrade $http_upgrade	Specifie HTTP/1 after es connect
		—	Connection keep-alive	For usin connect
		—	Host $host	To pres name in passing CertiFlo
		—	X-Real-IP $remote_addr	By defa reverse non-sta the user requirin
		—	X-Forwarded-For $proxy_add_x_forwarded_for	Similar $remote formati correct Forwarc present header, $proxy_ = $remo
proxy_set_header		—	X-Forwarded-Proto $scheme	The wel request proxies Axidian for corr substitu
fastcgi_buffers		8 4k | 8k	16 16k	Defines of buffe respons server, p

Context	Directive	Default value	Recommended value	
fastcgi_buffer_size		4k | 8k	32k	Defines reading respons server.
proxy_set_header		—	x-ssl-client-cert $ssl_client_escaped_cert	Passes when pr client ac based a

Using multiple `location` blocks in the configuration leads to repeating the same set of directives. To simplify the configuration process, extract the common set of directives into a separate file. Then, use the `include` directive within each `location` context to reference that file.

1. Create a file for the reusable directives. You can place this file in CONF format in the */etc/nginx/conf.d/* catalog.

   Recommended proxy.conf file content for Axidian CertiFlow compatibility

   ```
   proxy_http_version 1.1;
   proxy_set_header   Upgrade $http_upgrade;
   proxy_set_header   Connection keep-alive;
   proxy_set_header   Host $host;
   proxy_cache_bypass $http_upgrade;
   proxy_set_header   X-Real-IP $remote_addr;
   proxy_set_header   X-Forwarded-For $proxy_add_x_forwarded_for;
   proxy_set_header   X-Forwarded-Proto $scheme;
   fastcgi_buffers 16 16k;
   fastcgi_buffer_size 32k;
   ```

2. Configure the main nginx configuration file. The `location` context names must match the path to the proxied service.

Nginx.conf example

```
user www-data;
worker_processes auto;
error_log /var/log/nginx/error.log notice;
events {    worker_connections 1024;    }

http {
 proxy_buffer_size   64k;
 proxy_buffers   4 64k;
 types_hash_max_size     4096;
 add_header X-Frame-Options sameorigin always;
      add_header X-Content-Type-Options nosniff;

 log_format  main  '[$time_local] $remote_addr VIA $scheme --- $status ---
$request \n $ssl_client_fingerprint';
 access_log  /var/log/nginx/access.log  main;
 sendfile                on;
 tcp_nopush              on;
 include                 /etc/nginx/mime.types;
 default_type            application/octet-stream;

 server {
      listen              443 ssl;
      server_name         $hostname;

      ssl_certificate     "/etc/ssl/certs/SSL.crt";
      ssl_certificate_key "/etc/ssl/private/SSL.key";

     location /certiflow/mc
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5001/certiflow/mc; }
     location /certiflow/ss
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5002/certiflow/ss; }
     location /certiflow/rss
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5003/certiflow/rss;    }
     location /certiflow/api
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5004/certiflow/api;    }
     location /certiflow/credprovapi
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5005/certiflow/credprovapi;    }
     location /certiflow/oidc
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5008/certiflow/oidc;   }
     location /certiflow/wizard
     {   proxy_pass http://localhost:5009;  }
     #location /api
     #{  include /etc/nginx/conf.d/proxy.conf;   proxy_pass
```

```
    http://localhost:5010/api;  }
     }

     server {
          listen              3003 ssl;
          server_name         $hostname;

          ssl_certificate     "/etc/ssl/certs/SSL.crt";
          ssl_certificate_key "/etc/ssl/private/SSL.key";
          ssl_verify_client   optional_no_ca;

          location /agentregistrationapi
          { include /etc/nginx/conf.d/proxy.conf;   proxy_pass
    http://localhost:5006/agentregistrationapi;  }
          location /agentserviceapi
          { include /etc/nginx/conf.d/proxy.conf;   proxy_pass
    http://localhost:5007/agentserviceapi;
                                                    proxy_set_header   x-ssl-client-
    cert $ssl_client_escaped_cert;  }
     }
    }
```

3. To apply the changes in the configuration file, reload the configuration or restart nginx. To reload the configuration, execute the following command.

```
sudo nginx -s reload
```

Apache HTTP Server

To run the Axidian CertiFlow server components on Linux, configure the Apache web server as a reverse proxy server.

1. Install Apache.
2. Install a TLS/SSL certificate.
3. Configure the modules.
4. Configure the Apache website.

Follow the instructions for the operating system of the workstation where you plan to install Apache.

RHEL-based

Install Apache

Install the Apache web server using the following commands.

```
sudo yum install httpd
sudo systemctl enable httpd
sudo systemctl start httpd
```

Alternatively, install the Apache web server from source. For more information, see the Apache website.

Install a TLS/SSL certificate

How to issue a TLS/SSL certificate

Install a TLS/SSL certificate on the web server.

1. Copy the certificate and private key files to the catalogs specified in the Apache configuration file.

   ```
   sudo mkdir /etc/ssl/private/
   sudo cp ./SSL.crt /etc/httpd/ssl/certs
   sudo cp ./SSL.key /etc/httpd/ssl/private
   ```

2. Add the root CA certificate to the trusted certificates store on the workstation running Apache.

   ```
   sudo cp root-ca.crt /usr/local/share/ca-certificates/
   sudo update-ca-certificates -f
   ```

3. Make the certificate trusted across the domain. For example, distribute it through Group Policies.

Install modules and edit configuration

1. Install the **mod_ssl** module.

```
sudo yum install -y mod_ssl
```

2. Add the following directives to the *httpd.conf* configuration file (default location: */etc/httpd/conf/httpd.conf*).

```
Listen 3003
LimitRequestLine 16384
LimitRequestFieldSize 16384
ServerName SERVER_FQDN
Header append X-FRAME-OPTIONS "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
```

   In this and the following sections, replace *SERVER_FQDN* with the hostname (FQDN) of your server.

Configure the Apache website

Configure Apache to accept web requests and proxy them to the Axidian CertiFlow service.

1. Create the website configuration file */etc/httpd/conf.d/SERVER_FQDN.conf*.

```
sudo touch /etc/httpd/conf.d/SERVER_FQDN.conf
```

2. Populate the file with the recommended content.

> ⚠ **CAUTION**
> The `SSLCertificateFile` and `SSLCertificateKeyFile` parameters contain the paths to the certificate and private key files created or imported in the previous steps. Verify the specified paths and filenames.

Recommended content for the SERVER_FQDN.conf file

```
<VirtualHost *:80>
   RewriteEngine On
   RewriteCond %{HTTPS} !=on
   RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI}/$1 [R=301,L]
</VirtualHost>

<VirtualHost *:443>
   Protocols h2 http/1.1
   SSLCertificateFile /etc/httpd/ssl/certs/SSL.crt
   SSLCertificateKeyFile /etc/httpd/ssl/private/SSL.key
   SSLCipherSuite @SECLEVEL=1:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-
ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384

   ErrorLog logs/error.log
   CustomLog logs/access.log combined

   SSLEngine on
   SSLProtocol -all +TLSv1.2
   SSLHonorCipherOrder off
   SSLCompression off
   SSLSessionTickets on
   SSLUseStapling off
   SSLProxyEngine on
   SetEnv nokeepalive ssl-unclean-shutdown
   RequestHeader set X-Forwarded-Proto https
   Header always set Strict-Transport-Security "max-age=63072000"

   ProxyPreserveHost On

       ProxyPass /certiflow/mc http://localhost:5001/certiflow/mc
       ProxyPassReverse /certiflow/mc http://localhost:5001/certiflow/mc

       ProxyPass /certiflow/ss http://localhost:5002/certiflow/ss
       ProxyPassReverse /certiflow/ss http://localhost:5002/certiflow/ss

       ProxyPass /certiflow/rss http://localhost:5003/certiflow/rss
       ProxyPassReverse /certiflow/rss http://localhost:5003/certiflow/rss

       ProxyPass /certiflow/api http://localhost:5004/certiflow/api
       ProxyPassReverse /certiflow/api http://localhost:5004/certiflow/api

       ProxyPass /certiflow/credprovapi
http://localhost:5005/certiflow/credprovapi
       ProxyPassReverse /certiflow/credprovapi
http://localhost:5005/certiflow/credprovapi

       ProxyPass /certiflow/oidc http://localhost:5008/certiflow/oidc
```

```
        ProxyPassReverse /certiflow/oidc http://localhost:5008/certiflow/oidc

        ProxyPass /certiflow/wizard http://localhost:5009/certiflow/wizard
        ProxyPassReverse /certiflow/wizard
http://localhost:5009/certiflow/wizard

        #ProxyPass /api http://localhost:5010/api
        #ProxyPassReverse /api http://localhost:5010/api

</VirtualHost>

<VirtualHost *:3003>
   protocols h2 http/1.1

   SSLCertificateFile /etc/httpd/ssl/certs/SSL.crt
   SSLCertificateKeyFile /etc/httpd/ssl/private/SSL.key
   SSLCipherSuite @SECLEVEL=1:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-
ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384

   ErrorLog ${APACHE_LOG_DIR}/error.log
   CustomLog ${APACHE_LOG_DIR}/access.log combined

   SSLEngine on
   SSLProtocol -all +TLSv1.2
   SSLHonorCipherOrder off
   SSLCompression off
   SSLSessionTickets on
   SSLUseStapling off
   SSLProxyEngine on
   RequestHeader set X-Forwarded-Proto https
   Header always set Strict-Transport-Security "max-age=63072000"

        ProxyPass /agentregistrationapi
http://localhost:5006/agentregistrationapi
        ProxyPassReverse /agentregistrationapi
http://localhost:5006/agentregistrationapi

   <Location "/agentserviceapi">
        SSLVerifyClient optional_no_ca
        SSLOptions +ExportCertData
        RequestHeader unset x-ssl-client-cert
        RequestHeader set x-ssl-client-cert "expr=%{escape:%{SSL_CLIENT_CERT}}"
        #RequestHeader set x-ssl-client-cert "expr=%{escape:%
{SSL_CLIENT_S_DN}}"

        ProxyPass http://localhost:5007/agentserviceapi
        ProxyPassReverse http://localhost:5007/agentserviceapi
```

```
    </Location>
  </VirtualHost>
```

3. Reload the configuration file.

```
sudo httpd -t
sudo systemctl restart httpd
```

Debian-based

Install Apache

Install the Apache web server using the following commands.

```
sudo apt install apache2
sudo systemctl enable apache2
sudo service apache2 start
```

Alternatively, install the Apache web server from source. For more information, see the Apache website.

Install a TLS/SSL certificate

How to issue a TLS/SSL certificate

Install a TLS/SSL certificate on the web server.

1. Copy the certificate and private key files to the catalogs specified in the Apache configuration file.

```
sudo cp ./SSL.crt /etc/ssl/certs
sudo cp ./SSL.key /etc/ssl/private
```

2. Add the root CA certificate to the trusted certificates store on the workstation running Apache.

```
sudo cp root-ca.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates -f
```

3. Make the certificate trusted across the domain. For example, distribute it through Group Policies.

Install modules and edit configuration

Apache consists of a core server with module components that can be loaded to extend its functionality as required.

1. Install the following modules.

```
sudo a2enmod proxy
sudo a2enmod proxy_http
sudo a2enmod ssl
sudo a2enmod headers
sudo a2enmod rewrite
sudo systemctl restart apache2
```

2. Add the following directives to the *apache2.conf* configuration file (default location: */etc/apache2/apache2.conf*).

```
Listen 3003
LimitRequestLine 16384
LimitRequestFieldSize 16384
ServerName SERVER_FQDN
Header append X-FRAME-OPTIONS "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
```

   In this and the following sections, replace *SERVER_FQDN* with the hostname (FQDN) of your server.

Configure the Apache website

Configure Apache to accept web requests and proxy them to the Axidian CertiFlow service.

1. Create the website configuration file */etc/apache2/sites-available/SERVER_FQDN.conf*.

```
sudo touch /etc/apache2/sites-available/SERVER_FQDN.conf
```

2. Populate the file with the recommended content.

> ⚠ **CAUTION**
> The `SSLCertificateFile` and `SSLCertificateKeyFile` parameters contain the paths to the certificate and private key files created or imported in the previous steps. Verify the specified paths and filenames.

Recommended content for the SERVER_FQDN.conf file

```
<VirtualHost *:80>
    RewriteEngine On
    RewriteCond %{HTTPS} !=on
    RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI}/$1 [R=301,L]
</VirtualHost>

<VirtualHost *:443>
    Protocols h2 http/1.1
    SSLCertificateFile /etc/ssl/certs/SSL.crt
    SSLCertificateKeyFile /etc/ssl/private/SSL.key
    SSLCipherSuite @SECLEVEL=1:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-
ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SSLEngine on
    SSLProtocol -all +TLSv1.2
    SSLHonorCipherOrder off
    SSLCompression off
    SSLSessionTickets on
    SSLUseStapling off
    SSLProxyEngine on
    SetEnv nokeepalive ssl-unclean-shutdown
    RequestHeader set X-Forwarded-Proto https
    Header always set Strict-Transport-Security "max-age=63072000"

    ProxyPreserveHost On

        ProxyPass /certiflow/mc http://localhost:5001/certiflow/mc
        ProxyPassReverse /certiflow/mc http://localhost:5001/certiflow/mc

        ProxyPass /certiflow/ss http://localhost:5002/certiflow/ss
        ProxyPassReverse /certiflow/ss http://localhost:5002/certiflow/ss

        ProxyPass /certiflow/rss http://localhost:5003/certiflow/rss
        ProxyPassReverse /certiflow/rss http://localhost:5003/certiflow/rss

        ProxyPass /certiflow/api http://localhost:5004/certiflow/api
        ProxyPassReverse /certiflow/api http://localhost:5004/certiflow/api

        ProxyPass /certiflow/credprovapi
http://localhost:5005/certiflow/credprovapi
        ProxyPassReverse /certiflow/credprovapi
http://localhost:5005/certiflow/credprovapi

        ProxyPass /certiflow/oidc http://localhost:5008/certiflow/oidc
```

```
        ProxyPassReverse /certiflow/oidc http://localhost:5008/certiflow/oidc

        ProxyPass /certiflow/wizard http://localhost:5009/certiflow/wizard
        ProxyPassReverse /certiflow/wizard
http://localhost:5009/certiflow/wizard

        #ProxyPass /api http://localhost:5010/api
        #ProxyPassReverse /api http://localhost:5010/api

</VirtualHost>

<VirtualHost *:3003>
    protocols h2 http/1.1

    SSLCertificateFile /etc/ssl/certs/SSL.crt
    SSLCertificateKeyFile /etc/ssl/private/SSL.key
    SSLCipherSuite @SECLEVEL=1:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-
ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SSLEngine on
    SSLProtocol -all +TLSv1.2
    SSLHonorCipherOrder off
    SSLCompression off
    SSLSessionTickets on
    SSLUseStapling off
    SSLProxyEngine on
    RequestHeader set X-Forwarded-Proto https
    Header always set Strict-Transport-Security "max-age=63072000"

        ProxyPass /agentregistrationapi
http://localhost:5006/agentregistrationapi
        ProxyPassReverse /agentregistrationapi
http://localhost:5006/agentregistrationapi

    <Location "/agentserviceapi">
        SSLVerifyClient optional_no_ca
        SSLOptions +ExportCertData
        RequestHeader unset x-ssl-client-cert
        RequestHeader set x-ssl-client-cert "expr=%{escape:%
{SSL_CLIENT_CERT}}"
        #RequestHeader set x-ssl-client-cert "expr=%{escape:%
{SSL_CLIENT_S_DN}}"

        ProxyPass http://localhost:5007/agentserviceapi
        ProxyPassReverse http://localhost:5007/agentserviceapi
```

```
    </Location>
</VirtualHost>
```

3. Reload the configuration.

```
sudo a2ensite SERVER_FQDN
sudo apachectl configtest
sudo systemctl restart apache2
```

.NET

To operate the server components, install .NET 8.0.

.NET is an open-source application platform supported by Microsoft on Windowsand Linux OS. For more information about .NET product versions, installation files, and source code, see the Microsoft .NET download page.

To install .NET, follow the instructions for the operating system of the workstation where the Axidian CertiFlow server is installed.

Windows

Before you install .NET, make sure you have installed and configured the IIS components.

To install .NET:

1. Download the executable file from the Microsoft .NET download page under the **ASP.NET Core Runtime** → **Installers** → **Hosting bundle** section.
2. Run the file.

For operation on Windows OS, it is recommended to use the ASP.NET Core Runtime Hosting Bundle, which includes the .NET Runtime and IIS support.

Linux

> ⚠ **CAUTION**
> .NET installation on Linux OS requires root privileges.

To install .NET:

1. Download the ASP.NET Core Runtime archive for the required Linux OS from the **Binaries** section on the Microsoft .NET download page. For operation on Linux OS, the minimal .NET Core Runtime product version is sufficient.
2. Open a terminal, extract the downloaded archive to the `/usr/share/dotnet` catalog, and create a link to the executable file in the operating system's executable binaries catalog.

To confirm a successful .NET installation:

1. Run the terminal command: `dotnet --info`.
2. Verify the output shows version 8.0.22 and that no errors occurred.

Example

```
DOTNET_FILE=aspnetcore-runtime-8.0.22-linux-x64.tar.gz
sudo mkdir -p /usr/share/dotnet
sudo tar zxf $DOTNET_FILE -C /usr/share/dotnet
sudo ln -s /usr/share/dotnet/dotnet /usr/bin/dotnet
```

Install server components

1. Install the Axidian CertiFlow server.
2. Configure the Axidian CertiFlow settings in the Configuration Wizard.
3. For Linux installations, configure the OpenID Connect server.
4. For Linux installations, or multi-server configurations, configure a centralized event log.

Axidian CertiFlow Server

Install the server components

OpenID Connect server

Configure the OpenID Connect server

Configuration Wizard

Configure the Axidian CertiFlow services operation

Unified Event log

Record system events to the Unified Event Log

Axidian CertiFlow Agent

Configure client agent

Axidian CertiFlow Server

Axidian CertiFlow includes the following services:

- Management Console – the **mc** web application
- Self-Service – the **ss** web application
- Remote Self-Service – the **rss** web application
- Smart card unlock service – the **credprovapi** web application
- API – the **api** web application
- OpenID Connect server – the **oidc** web application
- Smart card monitoring service – the Card Monitor service
- Agent registration service – the **agentregistrationapi** web application
- Agent service for remote tasks – the **agentserviceapi** web application

> **INFO**
> Each service has its configuration files and access settings.

Install the server

Follow the instructions for the operating system of the workstation where you plan to install the Axidian CertiFlow server.

Windows

1. Run the *AxidianCertiFlow.Server-<version number>.x64.en-us.msi* file from the *AxidianCertiFlow.WindowsServer* catalog of the installation package.
2. Select the access control method: **Windows Authentication**, **OpenID Connect Authentication**, or **Certificate Authentication**.

   Windows

   c Windows Authentication, the following access control settings are configured automatically:

   - **Authentication**:
     - **Windows Authentication** is enabled for the mc, ss and api applications. Other methods are disabled.
     - **Anonymous Authentication** is enabled for the credprovapi, agentregistrationapi and agentserviceapi applications.

- **Anonymous Authentication** and **Forms Authentication** are enabled for the rss application.
- **SSL Settings**:
- **Require SSL** is enabled for all web applications.
- **Client certificates**:
  - **Ignore** for the mc, ss, rss, credprovapi, api and agentregistrationapi applications.
  - **Require** for the agentserviceapi application.

OpenID Connect

When you select OpenID Connect authentication, the following access control settings are configured automatically:

- **Authentication**:
  - **Anonymous Authentication** is enabled for all web applications. Other methods are disabled.
  - **Anonymous Authentication** and **Forms Authentication** are enabled for the rss application.
- **SSL Settings**:
  - **Require SSL** is enabled for all web applications.
  - **Client certificates**:
    - **Ignore** for the mc, ss, rss, credprovapi, api and agentregistrationapi applications.
    - **Require** for the agentserviceapi application.

Certificate

> ⚠ **CAUTION**
> If the user catalog is configured in Active Directory, the certificates used for authentication must contain a User Principal Name (UPN) attribute. Access to web applications is denied if the certificate does not contain a UPN attribute.

When you select user personal certificate authentication, the following access control settings are configured automatically:

- **Authentication**:
  - **Anonymous Authentication** is enabled for all web applications. Other methods are disabled.
  - **Anonymous Authentication** and **Forms Authentication** are enabled for the rss application.
- **SSL Settings**:

- **Require SSL** is enabled for all web applications.
- **Client certificates**:
  - **Ignore** for the rss, credprovapi and agentregistrationapi applications.
  - **Require** for the mc, ss, api and agentserviceapi applications.

After you install the Axidian CertiFlow server, you can edit the **SSL Settings** for each application in the Internet Information Services (IIS) Manager.

> ⚠ **CAUTION**
> Select the same authentication method when you configure access control for the Axidian CertiFlow web applications in the Configuration Wizard.

3. Issue an SSL/TLS certificate.

   SSL/TLS certificate requirements for IIS

   The certificate's **Subject** must contain the **Common Name (CN)** attribute (the FQDN of the Axidian CertiFlow server).

   The certificate's **Subject Alternative Name (SAN)** must contain the **DNS Name** attribute (the FQDN of the Axidian CertiFlow server). For example: *server.domain.loc* or a corresponding wildcard entry: **.domain.loc* (Wildcard certificate).

   The certificate's **Enhanced Key Usage (EKU)** must contain the **Server Authentication** value.

4. Add the SSL/TLS certificate to the **Default Web Site**:

   1. Launch the Internet Information Services (IIS) Manager.
   2. Select the **Default Web Site** and navigate to **Bindings...**.
   3. Click **Add...**, select **Type: https** and **Port: 443**.
   4. Select the **SSL certificate:** and click **OK**.

Linux

1. Install the server using the package manager from the Axidian CertiFlow installation package. Root privileges are required to use the package manager.

   Debian

```
sudo dpkg -i certiflow.-<version number>_amd64.deb
```

RHEL

```
sudo rpm -i certiflow.-<version number>.x86_64.rpm
```

2. Install Windows TrueType fonts for the proper operation of the Remote Self-Service.

Debian

```
wget http://ftp.ru.debian.org/debian/pool/contrib/m/msttcorefonts/ttf-
mscorefonts-installer_3.8.1_all.deb
sudo dpkg -i ttf-mscorefonts-installer_3.8.1_all.deb
fc-cache -f -v
```

RHEL

```
sudo yum install -y msttcore-fonts-installer
fc-cache -f -v
```

3. Configure application management.

   During server installation, systemd service files are created for managing the applications. Systemd allows applications to be launch automatically when the Axidian CertiFlow server starts and keeps them running without user interaction.

   By default, systemd launches Axidian CertiFlow applications under the **www-data** user account.

> **INFO**
> In RHEL-based operating systems, the **www-data** user account does not exist by default. You can add the **www-data** account using the `useradd` tool, or replace the active user account in the *certiflow-<service_name>.service* files located in the */etc/systemd/system* catalog.
>
> **Example command to create a www-data user**
>
> ```
> useradd -d /var/www -m www-data -s /sbin/nologin
> ```

Example of a Management Console service file running under the non-standard user account

```
[Unit]
Description=Axidian CertiFlow Management Console Application

[Service]
WorkingDirectory=/opt/axidian/certiflow/mc/
ExecStart=/opt/axidian/certiflow/mc/AxidianCertiFlow.Web.ManagementConsole
Restart=always
RestartSec=10
KillSignal=SIGINT
SyslogIdentifier=certiflow-mc
User=certiflow_adm
Environment=ASPNETCORE_URLS="http://localhost:5001"
Environment=ASPNETCORE_ENVIRONMENT=Production
Environment=DOTNET_PRINT_TELEMETRY_MESSAGE=false

[Install]
WantedBy=multi-user.target
```

To enable automatic launch of the applications, execute the *start-certiflow-services.sh* script file from the Axidian CertiFlow installation package:

```
chmod +x start-certiflow-services.sh
sudo ./start-certiflow-services.sh
```

> ⚠ **CAUTION**
> To execute a script file, that file must have execute permissions. Root privileges are required to run the script.

4. For the applications to function correctly, configure the Axidian CertiFlow settings using the Configuration Wizard (recommended) or manually.

5. To securely access the server from other workstations, configure the web server. The instructions cover binding SSL/TLS certificates and configuring HTTPS connection.

OpenID Connect server

OpenID Connect server allows to authenticate users in the Axidian Certiflow web applications using the OpenID Connect protocol.

It is mandatory for Axidian Certiflow Linux installations and optional for Windows installations. Install the OpenID Connect server before you install the Axidian Certiflow server.

> **INFO**
> OpenID Connect (OIDC) is an authentication and authorization protocol built on OAuth 2.0, which adds an identity layer to the OAuth framework. It enables applications to verify a user's identity and obtain basic profile information about them from an Identity Provider (IdP).

Follow the instructions for the operating system of the workstation where you plan to install the Axidian CertiFlow server.

Windows

1. To install the OIDC server, run the *AxidianCertiFlow.Oidc.Server-<version number>.x64.en-us.msi* file.
2. Install the Axidian CertiFlow server and select the **OpenID Connect Authentication** access control method in the server installation wizard.
3. Prepare a JWT signing certificate by following the instructions below.
4. Configure the OIDC server settings in the Configuration Wizard (**Access Control** → **OpenID Connect**).
5. Apply the settings on the Axidian CertiFlow server.

Prepare a JWT signing certificate

Use the web server certificate as the signing certificate.

To prepare the signing certificate:

1. Install the signing certificate in the **Local Computer – Personal** store.
2. Grant the IIS full access to the signing certificate's private key.
    1. Open the **Certificates** snap-in on the workstation where the OIDC server is installed.
    2. Right-click the certificate, select **All tasks** → **Manage Private Keys...** and click **Add**.
    3. In the **Location** menu, specify the server.
    4. In the **Enter the object names to select** field, specify the local group **IIS_IUSRS**, click **Check Names**, and **OK**.
    5. Set the permissions to **Full Control** and **Read**.
    6. Click **Apply**.

Edit database settings

By default, the OIDC server writes data to a local SQLite database. The SQLite database is intended for installations with a single Axidian CertiFlow server. The OIDC server's data is stored in the *C:\inetpub\wwwroot\certiflow\oidc\data* catalog.

Other than SQLite, you can use a Microsoft SQL or PostgreSQL database. To configure the connection to Microsoft SQL or PostgreSQL, edit the OIDC server's configuration file *appsettings.json*.

Microsoft SQL

1. Create a database in SQL Server Management Studio.
2. Open the OIDC server's configuration file *appsettings.json* and edit the `defaultConnection` and `provider` sections. The following example uses SQL authentication for the database connection.
   - `"defaultConnection": "Data Source=0;Initial Catalog=oidcdb;Persist Security Info=True;User ID=servicesql;Password=p@ssw0rd;TrustServerCertificate=True"`
   - `"provider": "mssql"`
3. Restart the Axidian CertiFlow OIDC application pool to apply the changes.
   1. Open the Internet Information Services (IIS) Manager and select **Application Pools** in the left menu.
   2. Select the Axidian CertiFlow OIDC application and click **Recycle** in the right menu.

Example parameters for connecting to Microsoft SQL

```
"connectionStrings": {
  "defaultConnection": "Data Source=0;Initial Catalog=oidcdb;Persist
Security Info=True;User
ID=servicesql;Password=p@ssw0rd;TrustServerCertificate=True"
},
"database": {
  "provider": "mssql"
},
```

PostgreSQL

1. Create a database in PostgreSQL.
2. Open the OIDC server's configuration file *appsettings.json* and edit the `defaultConnection` and `provider` sections. If you are using a .pgpass file, do not include the `Password` directive in the connection string.

- `"defaultConnection": "Host=172.17.0.11;Port=5432;Database=oidcdb;Username=servicepg;Password=p@ssw0rd"`
- `"provider": "pgsql"`

3. Restart the Axidian CertiFlow OIDC application pool to apply the changes.
   1. Open the Internet Information Services (IIS) Manager and select **Application Pools** in the left menu.
   2. Select the Axidian CertiFlow OIDC application and click **Recycle** in the right menu.

Example parameters for connecting to PostgreSQL

```
"connectionStrings": {
  "defaultConnection":
"Host=172.17.0.11;Port=5432;Database=oidcdb;Username=servicepg;Password=p@ssw(
},
"database": {
  "provider": "pgsql"
},
```

Linux

1. Install the Axidian CertiFlow server. The OIDC server is part of the Axidian CertiFlow server.
2. Prepare a JWT signing certificate by following the instructions below.
3. Configure the OIDC server settings in the Configuration Wizard (**Access Control**).
4. Apply the settings on the Axidian CertiFlow server.

Prepare a JWT signing certificate

Use the web server certificate as the signing certificate.

To prepare the signing certificate:

1. Create a subcatalog in the home catalog of the user account configured to run the OIDC server (**www-data** by default).

```
sudo mkdir -p /var/www/.dotnet/corefx/cryptography/x509stores/my/
```

How to check if the www-data user exists

1. To check if the www-data user exists, run the following command:

```
/etc/passwd | grep www-data
```

Example output if the www-data user exists

```
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

2. If the www-data user does not exist, you can create it or change the user for running the Axidian CertiFlow services.

   To create the www-data user and log in, run the following command:

```
sudo useradd -m -d /var/www -s /usr/sbin/nologin www-data
sudo su -s /bin/sh www-data
```

   To log in as any other user, run the following command and specify the username in the `User` directive.

```
/etc/systemd/system/certiflow-<service name>.service
```

2. Merge the certificate file and the key file into a PFX file. Place the PFX file in a subcatalog of the user's home catalog.

> ⚠ **CAUTION**
> When you run the command, the openssl utility prompts you to set a password for the PFX file. Leave the PFX file without a password: press **Enter** twice.

```
sudo openssl pkcs12 -export -out
/var/www/.dotnet/corefx/cryptography/x509stores/my/PFXFILE.pfx -inkey SSL.key -
in SSL.crt
```

3. Set the 600 permission for the PFX file.

```
sudo chmod 600 /var/www/.dotnet/corefx/cryptography/x509stores/my/PFXFILE.pfx
```

4. Obtain the signing certificate's thumbprint.

```
sudo openssl x509 -fingerprint -in SSL.crt -noout | tr -d ':'
```

Example of a certificate thumbprint output:

```
SHA1 Fingerprint=ADB613EC1A1692310D83C81F269C098A3DBD4EE0
```

Edit database settings

By default, the OIDC server writes data to a local SQLite database. The SQLite database is intended for installations with a single Axidian CertiFlow server. The OIDC server's data is stored in the */opt/axidian/certiflow/oidc/data* catalog.

Other than SQLite, you can use a Microsoft SQL or PostgreSQL database. To configure the connection to Microsoft SQL or PostgreSQL, edit the OIDC server's configuration file *appsettings.json*.

Microsoft SQL

1. Create a database in SQL Server Management Studio.
2. Open the OIDC server's configuration file *appsettings.json* and edit the `defaultConnection` and `provider` sections. The following example uses SQL authentication for the database connection.
   - `"defaultConnection": "Data Source=0;Initial Catalog=oidcdb;Persist Security Info=True;User ID=servicesql;Password=p@ssw0rd;TrustServerCertificate=True"`
   - `"provider": "mssql"`
3. Restart the OIDC service to apply the changes.

```
sudo systemctl restart certiflow-oidc.service
```

Example parameters for connecting to Microsoft SQL

```
  "connectionStrings": {
    "defaultConnection":
"Host=0;Port=5432;Database=oidcdb;Username=servicesql;Password=p@ssw0rd"
  },
  "database": {
    "provider": "mssql"
  },
```

PostgreSQL

1. Create a database in PostgreSQL.
2. Open the OIDC server's configuration file *appsettings.json* and edit the `defaultConnection` and `provider` sections. If you are using a .pgpass file, do not include the `Password` directive in the connection string.
   - `"defaultConnection": "Host=172.17.0.11;Port=5432;Database=oidcdb;Username=servicepg;Password=p@ssw0rd"`
   - `"provider": "pgsql"`
3. Restart the OIDC service to apply the changes.

```
sudo systemctl restart certiflow-oidc.service
```

Example parameters for connecting to PostgreSQL

```
  "connectionStrings": {
    "defaultConnection":
"Host=172.17.0.11;Port=5432;Database=oidcdb;Username=servicepsql;Password=p@s
  },
  "database": {
    "provider": "pgsql"
  },
```

Configuration Wizard

The Configuration Wizard automatically generates the configuration files for all Axidian CertiFlow services.

Install the Configuration Wizard and authenticate

The Configuration Wizard is a standalone component and is installed separately. Follow the instructions based on the operating system of the workstation where your Axidian CertiFlow server is installed.

Windows

1. Run the *AxidianCertiFlow.Wizard-<version number>.x64.en-us.msi* file from the *AxidianCertiFlow.WindowsServer* catalog of the Axidian CertiFlow installation package. The Configuration Wizard is installed to the *C:\inetpub\wwwroot\certiflow\wizard* catalog.
2. Obtain the authentication code. Start the AxidianCertiFlow Wizard IIS application pool. The code is saved to the *wizard_authentication_code.txt* file in the *C:\inetpub\wwwroot\certiflow\wizard\logs* catalog.
3. Open the *wizard_authentication_code.txt* file and copy the authentication code.
4. Open a web browser and navigate to `https://<Server FQDN>/certiflow/wizard`.
5. Enter the code in the **Authentication code** field and click **Login**.

> **INFO**
> If the authentication code is not generated, restart the IIS service.

Linux

1. Install the Configuration Wizard.

   Debian

   ```
   sudo dpkg -i certiflow.wizard-<version number>_amd64.deb
   ```

   RHEL

   ```
   sudo rpm -i certiflow.wizard-<version number>.x86_64.rpm
   ```

2. Open the Axidian CertiFlow server installation package and execute the `start-certiflow-wizard.sh` script.

```
sudo bash ./start-certiflow-wizard.sh
```

3. Obtain the authentication code. The authentication code is available in the output of the `start-certiflow-wizard.sh` script.

4. Open a web browser and navigate to `https://<Server FQDN>/certiflow/wizard`.

5. Enter the code in the **Authentication code** field and click **Login**.

Alternative ways for obtaining the authentication code

- Start the `certiflow-wizard.service`. The code is saved to the *wizard_authentication_code.txt* file in the */opt/axidian/certiflow/wizard/logs* catalog.
- Execute the `systemctl status` command:

```
sudo systemctl status certiflow-wizard.service | grep AuthenticationCode
```

- Retrieve the code from the application log of the `certiflow-wizard.service` systemd unit using the following command:

```
sudo journalctl -u certiflow-wizard.service | grep AuthenticationCode
```

The authentication code is output to the terminal screen.

System features

In the **Common features** section, configure the settings for the Management Console and the Self-Service.

Event Log

Configure Event Log operation.

1. Specify the attribute for users search in the event log. Default value is CN (Common Name).

2. Select:
   - **Use Windows Event Log** to record events from one or more servers in Windows Event Log.
   - **Use Log Server** to record events from multiple Axidian CertiFlow servers in Windows Event Log, SysLog, Microsoft SQL, or PostgreSQL database.

Use Windows Event Log

Events are recorded in Windows Event Log.

If multiple Axidian CertiFlow servers are deployed in your infrastructure, use the Axidian CertiFlow Event Log Proxy component to have all servers write events in Windows Event Log:

1. Install and configure the Axidian CertiFlow Event Log Proxy.
   How to install the Axidian CertiFlow Event Log Proxy
2. Activate the **Enable Event Log Proxy** option.
3. Specify the connection URL for the Event Log Proxy (for example, `https://server.domain.loc/certiflow/eventlogproxy`).
4. For Windows-based Axidian CertiFlow servers: Enter the credentials of an account with access rights to the unified event log (taken from the `authorization` section of the Event Log Proxy application's *Web.config* file).
   For Linux-based Axidian CertiFlow servers: In the **Certificate Thumbprint** field, specify the thumbprint of the client certificate presented by the Axidian CertiFlow server to connect to the Event Log Proxy (from the `allowedCertificateThumbprints` parameter in the Event Log Proxy application's *appsettings.json* file).

Use Log Server

If multiple Axidian CertiFlow servers are deployed in your infrastructure, use the Axidian Log Server application to have all servers write events to Windows Event Log, SysLog, Microsoft SQL, or PostgreSQL database.

1. Install and configure the Axidian Log Server application.
   How to install the Axidian Log Server

2. Specify the connection URL for the Axidian Log Server. For example:

   - `https://server.domain.loc/ls/api` for Windows servers
   - `https://server.domain.loc/api` for Linux servers

Certificate authorities

Configure integration with the Microsoft Enterprise Certificate Authority (CA).

AirCard Enterprise

Configure the integration with Axidian AirCard Enterprise:

1. Activate the **Enable integration with Axidian AirCard Enterprise** option.
2. Enter the connection URL for the AirCard Enterprise server (for example, `https://aircard.domain.loc:3002`). Make sure the specified port is open for incoming connections on the AirCard server.
3. Specify the client certificate thumbprint to establish a secure connection between the Axidian CertiFlow server and the AirCard Enterprise server.
4. Set the lifetime (in seconds) for unregistered AirCard smart cards. After this period expires, the Card Monitor service automatically deletes unregistered AirCard smart cards. The default value is 120 seconds.

For more information, see Axidian AirCard Enterprise docs.

Client agent

Configure client agents operation.

1. Install and configure the Axidian CertiFlow Agent.
   How to install the Axidian CertiFlow Agent

2. Activate the **Enable client agent** option.

3. Select the method for identifying an agent within the domain and outside the domain for registration in Axidian CertiFlow:

   - **Not set**. Default value.
   - **Machine GUID**. Use the workstation's `MachineGuid` value.
   - **Generate new GUID**. Select this option if multiple workstations share the same `MachineGuid` value.
   - **Computer domain SID**.
   - **Computer SID**. Select this option if the agent is installed on a non-domain workstation. The agent identifier is assigned the string value of `MachineGuid` from the workstation's registry key: *[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography]*.

Change the Agent ID generation strategy

To change the agent ID generation strategy after the initial Axidian CertiFlow configuration:

1. Stop the **agentregistrationapi** and **agentserviceapi**services on the Axidian CertiFlow server.
2. Delete all client agents in the **Agents** section of the Management Console, or execute a database query against the Axidian CertiFlow database to remove registered agents and their sessions.
3. Apply the changes in the Configuration Wizard and deploy the updated **agentregistrationapi** service configuration file to the Axidian CertiFlow server.
4. Start the **agentregistrationapi** and **agentserviceapi** services.

4. To enable agent registration without administrator approval, activate the **Automatic agent registration** option. After you install and configure the agent on a workstation, it appears in the **Agents** section of the Axidian CertiFlow Management Console with the *Registered* status.

5. Upload the agent certificate – the root certificate file for the agent services with the private key in JSON format (*agent_root_ca.json*).

6. From the **Level of agent's event log** list, select which agent events are recorded in the event log: all events, only errors, or only warnings and errors.

7. Fill in the **Frequency of receiving data from server (sec)** and **Interval of repeated performance of task canceled by user (sec)** fields.

8. The HTTP request certificate header name is set by default. If Axidian CertiFlow is used with a load balancer, enable the **Pass only certificate's Subject value in the HTTP request headers** option to reduce traffic.

User catalog

Configure the connection to the Axidian CertiFlow user catalog. You can connect several user catalogs.

How to configure a user catalog

LDAP
Click **Add** and select the user catalog type: Active Directory or FreeIPA.

Active Directory

1. Specify the credentials of an account with access rights to the user catalog: the name in the DOMAIN\UserName or UserName@DNSDomainName format and the password.
2. Specify the domain's NetBIOS name.
3. Specify the DNS name of the domain or the domain controller.
4. Specify the path to the user container in Distinguished Name format. To work with all users, select the domain root.
5. If you are using the LDAPS protocol to access the catalog, enable the **Use LDAPS** option.
6. To display the user's photo in the Axidian CertiFlow interface or print it on a smart card, select the attribute that contains the user's photo.
7. Click **Save**.

> **HOW TO FIND THE DNS NAME AND NETBIOS NAME OF A DOMAIN**
>
> Execute the following commands:
>
> - `set USERDNSDOMAIN` to find the **DNS domain name**.
> - `set USERDOMAIN` to find the **NetBIOS domain name**.

FreeIPA

1. Specify the credentials of an account with access rights to the user catalog: the name in the DOMAIN\UserName or UserName@DNSDomainName format and the password.
2. Specify the domain's NetBIOS name.
3. Specify the DNS name of the domain or the domain controller.
4. Specify the path to the user container in Distinguished Name format.
5. If you are using the LDAPS protocol to access the catalog, enable the **Use LDAPS** option.
6. Click **Save**.

> **HOW TO FIND THE DNS NAME AND NETBIOS NAME OF A DOMAIN**
>
> Execute the following commands:
>
> - `set USERDNSDOMAIN` to find the **DNS domain name**.
> - `set USERDOMAIN` to find the **NetBIOS domain name**.

Internal catalog

Use a Microsoft SQL or PostgreSQL database as the internal user catalog.

1. Click **Add** and select the storage type.
2. Configure the connection to the storage. Enter the server name, instance name (for Microsoft SQL), port number, and database name.
3. Select the authentication method for connecting to the database server:
   - **Microsoft SQL**: Windows Authentication or SQL Server Authentication. For SQL Server Authentication, enter the username and password.
   - **PostgreSQL**: Enter the username and password.
4. Click **Save**.

Custom attributes

To configure additional attributes for the internal user catalog:

1. Click **Add**.
2. Enter the **User attribute name** and **User attribute display name**.
3. To have the attribute appear when you create or edit a user in Axidian CertiFlow, enable the **Display in create/edit user form** option.
4. To make the attribute mandatory when you create or edit a user in Axidian CertiFlow, enable the **Required attribute** option.
5. Select the attribute type:
   - **Text**
     For a text attribute, specify the following settings:
     - **Maximum text length** – the maximum number of characters.
     - **Text format** – a regular expression for validating the attribute's text value.
     - **Invalid format message** – the text of the message that is displayed when you enter a text value that does not meet the regular expression requirements.
   - **Integer**
     Specify the minimum and maximum values. For example, for entering age information.
   - **Logical**
     The attribute can have a value of `true` or `false`.
   - **Values map**
     Specify the reference list that is used when you select attribute values. Format: `<attribute value #1>, <display value #1>; <attribute value #2>, <display value #2>;...`.
     For example: `red, Red color; green, Green color`.
6. Click **Save**.

Attribute mapping

You can configure a mapping between the Certificate Authority's attributes and the user attributes in the catalog.

If attribute mapping is configured, a new user can be registered in the Certificate Authority when issuing a card for that user in Axidian CertiFlow.

Tracked attributes

You can define a list of Active Directory user attributes that trigger a card certificate update if these attribute values are changed.

You can only track changes for attributes from the Subject and Subject Alternative Name (SAN) certificate fields.

> ⓘ **INFO**
> By default, Microsoft CA certificate template parameters track the Common Name, Email, and User Principal Name (UPN) attributes.

To track an attribute:

1. Click **Add**.
2. Specify the attribute name in the user catalog.
3. Specify the display name for the attribute.
4. Specify the X.500 name or OID of the attribute in the certificate. This value is used to locate the attribute within the certificate.
5. Click **Save**.

Access control

Select the access control method for Axidian CertiFlow services:

- **Windows Authentication**
  This method allows authentication using the user's Windows OS credentials and is used for Axidian CertiFlow installations on a domain workstation running Windows OS.

- **OpenID Connect Authentication**
  This method allows authentication using the OpenID Connect server and is used for Axidian CertiFlow installations on either domain or non-domain workstations running Windows or Linux OS.
  Navigate to the **OpenID Connect** section and specify the connection parameters for the OpenID Connect server.

> ⚠ **CAUTION**
> Make sure you select the same authentication method during the Axidian CertiFlow server installation on Windows OS.

Role administrator

Specify the role administrator UPN.

Role administrator is an account granted permission to manage roles in Axidian CertiFlow. When you launch Axidian CertiFlow for the first time, you must log in to the Management Console using this account.

The designated account must possess a **User Principal Name (UPN) attribute** and be a member of the user catalog.

Database

Configure the connection to the data storage.

How to create a data storage

1. Select the data storage type based on the environment where Axidian CertiFlow is deployed:
   - Microsoft SQL
   - PostgreSQL
2. Configure the connection to the database. Enter the server name, instance name (for Microsoft SQL), port number, and database name.
3. Select the authentication method for connecting to the database server:
   - **Microsoft SQL**: Windows Authentication or SQL Server Authentication. For SQL Server Authentication, enter the username and password.
   - **PostgreSQL**: Enter the username and password.
4. (Optional) Configure additional parameters:
   - Minimum pool size
   - Maximum pool size
   - Connection timeout
   - Connection lifetime
   - Number of connection retries
   - Connection retry interval

Encryption Key

Axidian CertiFlow data is stored and transmitted in encrypted form. From the dropdown list, select an encryption algorithm and click **Generate**. Save a backup copy of the encryption key.

Card Monitor service

Configure the Card Monitor service settings to monitor card usage.

<details>
<summary>More about the Card Monitor service</summary>

The Card Monitor service is automatically installed with the Axidian CertiFlow server and performs the following operations:

- Revokes and retrieves cards that belong to users with the accounts deleted from the user catalog
- Revokes temporary cards with expired validity period
- Disables cards that belong to users with disabled accounts
- Removes disabled user accounts from the user catalog
- Sets or resets the card content status
- Logs the *Agent connection lost* event in the event log
- Deletes inactive agents
- Sends email notifications to administrators and users

</details>

1. Specify the account for the Card Monitor service in the DOMAIN\UserName or UserName@DNSDomainName format. This account must meet the following requirements:
   - Be a member of the Axidian CertiFlow user catalog.
   - Belong to the **Administrators** group on the Axidian CertiFlow server.
   - Have the **Log on as a batch job** permission in the Active Directory policy.
2. Configure the Card Monitor service startup time.
3. In the **Manage users** section, you can configure the following settings:
   - **Disable cards assigned to users with disabled accounts**. Card Monitor disables cards that belong to users whose accounts have been disabled in the user catalog. If the **Revoke certificate when card is revoked or disabled** option is enabled in the Microsoft CA certificate template parameters, the validity of certificates stored on the devices is suspended and the certificates are revoked in the CA.
   - **Set filter to treat disabled users as removed**. Disabled user accounts that meet the filter condition are considered deleted from the user catalog. Cards that belong to deleted users are revoked. Specify the user attribute and its value. For example, the `DistinguishedName` attribute with the `OU=Fired users,DC=domain,DC=loc` value.

    - **Withdraw cards from removed users**. Cards that belong to deleted users are withdrawn.
4. In the **Agent Operations** section, you can configure the following settings:
    - **Log an event if agent is inactive for (min)**. If an agent loses communication with the server, Card Monitor logs this event in the system log after the specified time has elapsed.
    - **Remove agent if inactive for (days)**. If an agent loses communication with the server, Card Monitor deletes the agent from the database after the specified time has elapsed.

> **INFO**
> Create a separate service role for the Card Monitor service.

Confirmation

1. Review the settings in all sections of the Configuration Wizard.
2. Click **Apply**.

All configured parameters are written to the application configuration files and saved to the following catalogs:

- *C:\inetpub\wwwroot\certiflow\wizard\configs* for Windows OS
- */opt/axidian/certiflow/wizard/configs/* for Linux OS

Apply the configuration files to the Axidian CertiFlow server.

Results

Click **Download configuration files** to export the files.

If you install Axidian CertiFlow for the first time, it is recommended to save a copy of the configured parameters. Click **Backup current configuration settings** option and set a password for the file.

The backup copy contains all parameters defined during installation for all services, as well as the database encryption algorithm and key. Store the backup file in a secure location.

Restore configuration

You can restore Axidian CertiFlow configuration settings from a backup in the following scenarios:

- Upgrading the Axidian CertiFlow server.
- Migrating the server to a new workstation.
- Installing additional servers.

To restore the configuration from a file:

1. Go to the **Restore configuration** section of the Configuration Wizard.
2. Click **Restore configuration settings from backup**.
3. Upload the backup file.
4. If the backup file was encrypted, enter the password.

Apply the configuration files on the Axidian CertiFlow server

Apply the configuration files generated by the Configuration Wizard to the Axidian CertiFlow server.

Windows

1. Open PowerShell as an administrator.
2. Open the *C:\inetpub\wwwroot\certiflow\wizard\configs* catalog.
3. Run the `deploy_configuration.ps1` script.

   ```
   .\deploy_configuration.ps1
   ```

4. During the execution of the PowerShell script, enter the password for the account running the Card Monitor service.

> **TIP**
> It is recommended to specify the same local account for all Axidian CertiFlow web applications.

The configuration files for all Axidian CertiFlow services are located in the IIS web applications root catalog at *%SystemDrive%\inetpub\wwwroot\certiflow*. The configuration files for the Card Monitor service are located in the *%ProgramFiles%\Axidian CertiFlow\CardMonitor* catalog.

Linux

1. Open a terminal.
2. Open the `/opt/axidian/certiflow/wizard/configs` catalog.

3. Make sure the script file has execute permissions and run the bash script `deploy_configuration.sh`:

```
sh ./deploy_configuration.sh
```

4. During the execution of the bash script, specify the account running the Card Monitor service.

> **TIP**
> It is recommended to specify the same local account for all Axidian CertiFlow web applications.

If multiple Axidian CertiFlow servers are deployed in your infrastructure, apply the configuration files on each server. The configuration files for all Axidian CertiFlow services are located in the */opt/axidian/certiflow* catalog.

Encrypt/decrypt the configuration files

It is recommended to encrypt the Axidian CertiFlow configuration files using the Certiflow.Config.DataProtector tool. The tool supports the AES encryption algorithm with an effective key length of 256 bits. The encryption key is stored on the Axidian CertiFlow server.

The encryption key is located at:

- Windows OS: *C:\ProgramData\Axidian\certiflow\keys*
- Linux OS: */etc/axidian/certiflow/keys*

> **⚠ CAUTION**
> Create a backup copy of the encryption key to restore access to encrypted data in case the primary key is lost or corrupted. You can store the key copy alongside the Axidian CertiFlow configuration backup file.

Windows

Encryption

1. Open the *Misc\dataprotector* catalog in the axidian CertiFlow installation package.
2. Launch PowerShell as an administrator.
3. Execute one of the following commands:

- To encrypt all configuration files located in the standard catalogs (*C:\inetpub\wwwroot\<component name>\appsettings.json*):

```
.\Certiflow.Config.DataProtector.exe protect
```

- To encrypt a configuration file of a component:

```
.\Certiflow.Config.DataProtector protect --app <component name>
```

Example

```
.\Certiflow.Config.DataProtector protect --app ManagementConsole
```

- To encrypt a configuration file located outside the standard catalog:

```
.\Certiflow.Config.DataProtector protect --app <component name> --file
"appsettings.json file path"
```

Example

```
.\Certiflow.Config.DataProtector protect --app CardMonitor --file "C:\Program
Files\Axidian CertiFlow\CardMonitor\appsettings.json"
```

Decryption

1. Open the *Misc\dataprotector* catalog in the Axidian CertiFlow installation package.
2. Launch PowerShell as an administrator.
3. Execute one of the following commands:

- To decrypt all configuration files located in the standard catalogs (*C:\inetpub\wwwroot\<component name>\appsettings.json*):

```
.\Certiflow.Config.DataProtector.exe unprotect
```

- To decrypt a configuration file of a component:

```
.\Certiflow.Config.DataProtector unprotect --app <component name>
```

Example

```
.\Certiflow.Config.DataProtector unprotect --app ManagementConsole
```

- To decrypt a configuration file located outside the standard catalog:

```
.\Certiflow.Config.DataProtector unprotect --app <component name> --file
"appsettings.json file path"
```

Example

```
.\Certiflow.Config.DataProtector unprotect --app CardMonitor --file "C:\Program
Files\Axidian CertiFlow\CardMonitor\appsettings.json"
```

Linux

Encryption

1. Open the *Misc\dataprotector* catalog in the Axidian CertiFlow installation package.
2. Launch Linux Bash.
3. Execute one of the following commands:

- To encrypt all configuration files located in the standard catalogs (*/opt/axidian/certiflow/<component name>/appsettings.json*):

```
dotnet Certiflow.Config.DataProtector.dll protect
```

- To encryptnpm run lint:spell:fix a configuration file of a component:

```
dotnet Certiflow.Config.DataProtector.dll protect --app <component name>
```

Example

```
dotnet Certiflow.Config.DataProtector.dll protect --app ManagementConsole
```

- To encrypt a configuration file located outside the standard catalog:

```
dotnet Certiflow.Config.DataProtector.dll protect --app <component name> --file
"appsettings.json file path"
```

Example

```
dotnet Certiflow.Config.DataProtector.dll protect --app ManagementConsole --file
"/opt/axidian/certiflow/mc/appsettings.json"
```

Decryption

1. Open the *Misc\dataprotector* catalog in the Axidian CertiFlow installation package.
2. Launch Linux Bash.
3. Execute one of the following commands:

- To decrypt all configuration files located in the standard catalogs (*/opt/axidian/certiflow/<component name>/appsettings.json*):

```
dotnet Certiflow.Config.DataProtector.dll unprotect
```

- To decrypt a configuration file of a component:

```
dotnet Certiflow.Config.DataProtector.dll unprotect --app <component name>
```

Example

```
dotnet Certiflow.Config.DataProtector.dll unprotect --app ManagementConsole
```

- To decrypt a configuration file located outside the standard catalog:

```
dotnet Certiflow.Config.DataProtector.dll unprotect --app <component name> --
file "appsettings.json file path"
```

Example

```
dotnet Certiflow.Config.DataProtector.dll unprotect --app ManagementConsole --
file "/opt/axidian/certiflow/mc/appsettings.json"
```

Deactivate the Configuration Wizard

For security reasons, it is recommended to disable the Axidian CertiFlow Configuration Wizard web application after you complete the configuration process.

Windows

1. Open the Internet Information Services (IIS) Manager.
2. In the IIS server component tree, select **Application Pools**.
3. From the **Application Pools** list, choose AxidianCertiFlow Wizard.
4. In the **Actions** menu, select **Stop**.

Linux

1. Open a terminal emulator.
2. Execute the following command:

```
sudo systemctl stop certiflow-wizard.service
```

Unified Event log

You can use the Unified Event Log for Axidian CertiFlow Linux installations or in multi-server Windows configurations. It allows events from all servers to be recorded in a single, centralized log.

Configure the Unified Event Log using the Axidian CertiFlow Event Log Proxy or Log Server applications.

Axidian CertiFlow Event Log Proxy

The Axidian CertiFlow Event Log Proxy application enables logging events from one or more Axidian CertiFlow servers into a unified Windows Event Log. The Axidian CertiFlow Event Log Proxy can only be installed on a workstation running the Windows OS.

System requirements

To install and configure the Axidian CertiFlow Event Log Proxy:

1. Log in to the workstation as local administrator.
2. Open the Axidian CertiFlow installation package, navigate to the *AxidianCertiFlow.Server* catalog and run the *AxidianCertiFlow.EventLog.Proxy-<version-number>.x64.en-us.msi* installation file.
3. In the installation wizard, select an authentication method based on the operating system where the Axidian CertiFlow server is installed, and specify the required settings in the configuration files.

Windows

1. Select the Windows authentication method. When the installation is complete, click **Finish** and close the installation wizard.
2. Open the *web.config* file (C:\inetpub\wwwroot\certiflow\eventlogproxy) in Notepad as an administrator.
3. In the `allow users` parameter, specify a user account from the domain where the Event Log Proxy is installed. For example, the user catalog service account.

Example

```
<authorization>
     <clear />
     <add accessType="Allow" users="DOMAIN\servicecertiflow" />
</authorization>
```

4. Save and close the *web.config* file.

Linux

1. Select the Certificate authentication method. When the installation is complete, click **Finish** and close the installation wizard.
2. Open the *appsettings.json* file (*C:\inetpub\wwwroot\certiflow\eventlogproxy*) in Notepad as an administrator.
3. In the `authSettings` section, specify the thumbprint of a client certificate of the Axidian CertiFlow server in the `allowedCertificateThumbprints` parameter.
   Make sure the certificate's **Enhanced Key Usage** (EKU) field contains the **Client Authentication** value and the certificate is installed in the Axidian CertiFlow server's certificate store.

   Example

   ```
   "authSettings":{
   "authorizeByCertificate": "true",
   "allowedCertificateThumbprints": "aba8b93d73343f2182e3c1c40482b2ae2d75b6ec"
   }
   ```

   How to issue a client certificate
4. Save and close the *appsettings.json* file.

4. Restart the Axidian CertiFlow Event Log Proxy application pool to apply the changes.
   1. Open the Internet Information Services (IIS) Manager and select **Application Pools** in the left menu.
   2. Select the Axidian CertiFlow Event Log Proxy application and click **Recycle** in the right menu.

Log Server

With Log Server you can record events from one or more Axidian CertiFlow servers to a unified log in the following targets: Windows Event Log, Microsoft SQL Server, PostgreSQL Server, SysLog Server.

System requirements

The Log Server can be installed on a workstation running either Windows or Linux OS.

Windows

Install Log Server

Before installing the Log Server, install .NET 8.0 and URL Rewrite.

To install the Log Server:

1. Log in to the workstation as local administrator.
2. Run the *LogServer-<version number>.x64.en-us.msi* file from the *Log.Server* catalog of the Axidian CertiFlow installation package and follow the wizard's instructions.
3. Copy the following files from the *Log.Server* catalog*:
   - The *certiflowSchema.config* file to the *C:\inetpub\wwwroot\ls* catalog.
   - The *certiflowEventLogTarget.config*, *certiflowMsSqlTarget.config*, *certiflowPgSqlTarget.config*, and *certiflowSysLogTarget.config* files to the *C:\inetpub\wwwroot\ls\targetConfigs* catalog.

Configure event read/write operations

The Log Server supports reading events from only one storage target (`ReadTargetId`), while it can write events to multiple storage targets (`WriteTargets`) at the same time.

You can configure event reading and writing for the following storage types:

- Windows Event Log
- Microsoft SQL Server
- PostgreSQL Server
- Syslog Server

Windows Event Log

1. Open the *C:\inetpub\wwwroot\ls* catalog and edit the *clientApps.config* file.
   - In the `Applications` section, add the following parameters.

```
<Application Id="certiflow" SchemaId="certiflowSchema">
    <ReadTargetId>certiflowEventLogTarget</ReadTargetId>
    <WriteTargets>
        <TargetId>certiflowEventLogTarget</TargetId>
    </WriteTargets>
    <AccessControl>
        <!--<CertificateAccessControl CertificateThumbprint="001122...AA11"
Rights="Read" />-->
    </AccessControl>
</Application>
```

- In the `Targets` section, add a new element.

```
<Targets>
    <Target Id="certiflowEventLogTarget" Type="eventlog"/>
</Targets>
```

2. Save and close the file.

Microsoft SQL

1. Create a database in SQL Server Management Studio.
    1. In the **Object Explorer** pane, right-click **Databases** and select **New Database**.
    2. Enter a database name and click **OK**.
    3. In the **Owner:** field, specify the owner of the database.
    4. Click **OK** to save the database.

> **INFO**
> Create or select any existing internal Microsoft SQL or Active Directory account. For example, a service account for running Axidian CertiFlow.
>
> Once the database is created, the specified account is granted the *db_owner* and *public* roles. Axidian CertiFlow use this account for read/write operations.

2. Open the *C:\inetpub\wwwroot\ls\targetConfigs* catalog and edit the *certiflowMsSqlTarget.config* file. In the `<Settings>…</Settings>` section configure the following parameters:
    - `Data Source` – the Microsoft SQL Server name or the named Microsoft SQL Server instance in the `Server name\Instance name` format.
    - `Database` – the database name (ILS).
    - `User Id` – the service account for managing the Axidian CertiFlow database.
    - `Password` – the service account password.
    - `TrustServerCertificate` – the server certificate trust setting. Set the value to `True`.

```
<Settings>
    <ConnectionString>Data Source=MSSQL\SQLEXPRESS;Database=LogServer;User
Id=servicesql;Password=P@ssw0rd;TrustServerCertificate=True</ConnectionString>
</Settings>
```

3. Open the *C:\inetpub\wwwroot\ls* catalog and edit the *clientApps.config* file.

- In the `Application` section, add the following parameters.

```
<Application Id="certiflow" SchemaId="certiflowSchema">
    <ReadTargetId>certiflowMsSqlTarget</ReadTargetId>

    <WriteTargets>
        <TargetId>certiflowMsSqlTarget</TargetId>
    </WriteTargets>

    <AccessControl>
        <!--<CertificateAccessControl CertificateThumbprint="001122...AA11"
Rights="Read" />-->
    </AccessControl>
</Application>
```

- In the `Targets` section, add a new element.

```
<Targets>
    <Target Id="certiflowMsSqlTarget" Type="mssql"/>
</Targets>
```

4. Save and close the file.

PostgreSQL

1. Create a database in pgAdmin.
    1. Open pgAdmin and connect to the server.
    2. In the **Browser** section, right-click **Databases** and select **Create** → **Database...**.
    3. On the **General** tab, specify the database name in the **Database** field, select the service account from the **Owner** list, and click **Save**.
2. Grant the service account the permissions to manage the database.
    1. Select the database and select **Tools** → **Query Tool**.
    2. Enter the query with the service account name.

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO <service account
name>;
```

    3. Click **Execute/Refresh** (Execute/Refresh).
3. Follow these steps to add Universally Unique Identifiers (UUID) generation support.

1. Click  and select **Clear Query**.
2. Enter the query.

```
CREATE EXTENSION IF NOT EXISTS "uuid-ossp";
```

3. Click **Execute/Refresh** (Execute/Refresh).

4. Configure a remote connection to the database.

   1. Open the *pg_hba.conf* configuration file (*C:\Program Files\PostgreSQL\<version number>\data*).
   2. Add a string in the following format:

```
CONNECTIONTYPE DATABASE USER ADDRESS METHOD
```

   - `CONNECTIONTYPE` – the name of the connection type. To use TCP/IP connection, specify `host`.
   - `DATABASE` – the name of the database. To grant access to all databases, specify `ALL`.
   - `USER` – name of the user who accesses the database. To grant access to all users, specify `ALL`.
   - `ADDRESS` – the IP address of the remote Axidian CertiFlow server. To grant access from any IP address, specify `0.0.0.0/0`.
   - `METHOD` – the user authentication method. For example, `md5`, `scram-sha-256`.

   Example

```
host LogServer servicepg 192.200.1.0/24 md5
host ALL servicepg 10.0.0.0/8 md5
host ALL ALL 0.0.0.0/0 scram-sha-256
```

5. Open the *C:\inetpub\wwwroot\ls\targetConfigs* catalog and edit the *certiflowPgSqlTarget.config* file. In the `<ConnectionString>…</ConnectionString>` section, configure the following parameters:

   - `Host` – the PostgreSQL Server name.
   - `Port` – the PostgreSQL connection port. Default value is 5432.
   - `Database` – the database name.
   - `Username` – the service account for managing the Axidian CertiFlow database.
   - `Password` – the service account password.

```
<Settings>
    <ConnectionString>Host=SRV-
POSTGRESQL;Port=5432;Database=LogServer;Username=servicepg;Password=P@ssw0rd</C
</Settings>
```

6. Open the *C:\inetpub\wwwroot\ls* catalog and edit the *clientApps.config* file.

   - In the `Application` section add a new `TargetId` for `ReadTarget` and `WriteTarget`.

```
<Application Id="certiflow" SchemaId="certiflowSchema">
    <ReadTargetId>certiflowPgSqlTarget</ReadTargetId>

    <WriteTargets>
        <TargetId>certiflowPgSqlTarget</TargetId>
    </WriteTargets>

    <AccessControl>
        <!-- <CertificateAccessControl CertificateThumbprint="001122...AA11"
Rights="Read" /> -->
    </AccessControl>
</Application>
```

   - In the `Targets` section, add a new element.

```
<Targets>
    <Target Id="certiflowPgSqlTarget" Type="pgsql"/>
</Targets>
```

Syslog

Syslog only supports event writing (WriteTargets). The following configuration extends the PostgreSQL example.

1. Open the *C:\inetpub\wwwroot\ls\targetConfigs* catalog and edit the *certiflowSysLogTarget.config* file. In the `<ConnectionString>…</ConnectionString>` section, configure the following parameters:

   - `HostName` – the Syslog server name or IP.
   - `Port` – the Syslog server connection port. Default value is 514.
   - `Protocol` – the Syslog server connection type: UDP, TCP, TCPoverTLS.
   - `Format` – an optional parameter that configures log format: Plain, CEF, LEEF.
   - `SyslogVersion` – an optional parameter that configures the protocol: RFC3164, RFC5424.

```
<Settings HostName="SRV-SYSLOG" Port="514" Protocol="UDP"/>
```

2. Open the *C:\inetpub\wwwroot\ls* catalog and edit the *clientApps.config* file.

   - In the `Application` section, add a new `TargetId` for `WriteTarget`.

```
<Applications>
    <Application Id="certiflow" SchemaId="certiflowSchema">
        <ReadTargetId>certiflowPgSqlTarget</ReadTargetId>

        <WriteTargets>
            <TargetId>certiflowPgSqlTarget</TargetId>
            <TargetId>certiflowSysLogTarget</TargetId>
        </WriteTargets>

        <AccessControl>
            <!-- <CertificateAccessControl
CertificateThumbprint="001122...AA11" Rights="Read" /> -->
        </AccessControl>
    </Application>
</Applications>
```

   - In the `Targets` section, add a new element.

```
<Targets>
    <Target Id="certiflowPgSqlTarget" Type="pgsql"/>
    <Target Id="certiflowSysLogTarget" Type="syslog"/>
</Targets>
```

To apply the changes, restart the IIS application pool.

1. Open Internet Information Services (IIS) Manager and select **Application Pools** in the left menu.
2. Select the Log Server application pool and click **Recycle** in the right menu.

Linux

Install Log server

1. Run the installation package.

Debian

```
sudo dpkg -i axidian.logserver-<version number>_amd64.deb
```

RHEL

```
sudo rpm -i axidian.logserver-<version number>.x86_64.rpm
```

2. Open the *Log.Server* catalog and copy the *certiflowSchema.config* file to the */opt/axidian/ls* catalog.

```
sudo cp ./certiflowSchema.config /opt/axidian/ls/
```

Configure event read/write operations

The Log Server supports reading events from only one storage target (`ReadTargetId`), while it can write events to multiple storage targets (`WriteTargets`) at the same time.

You can configure event reading and writing for the following storage types:

- Microsoft SQL Server
- PostgreSQL Server
- Syslog Server

Microsoft SQL

1. Create a database in SQL Server Management Studio.
    1. In the **Object Explorer** pane, right-click **Databases** and select **New Database**.
    2. Enter a database name and click **OK**.
    3. In the **Owner:** field, specify the owner of the database.
    4. Click **OK** to save the database.

    > ⓘ **INFO**
    > Create or select any existing internal Microsoft SQL or Active Directory account. For example, a service account for running Axidian CertiFlow.
    >
    > Once the database is created, the specified account is granted the *db_owner* and *public* roles. Axidian CertiFlow use this account for read/write operations.

2. Open the */opt/axidian/ls/targetConfigs* catalog and edit the *certiflowMsSqlTarget.config* file. In the `<Settings>…</Settings>` section, configure the following parameters:
    - `Data Source` – the Microsoft SQL Server name or the named Microsoft SQL Server instance in the `Server name\Instance name` format.
    - `Database` – the database name (ILS).

- `User Id` – the service account for managing the Axidian CertiFlow database.
- `Password` – the service account password.
- `TrustServerCertificate` – the server certificate trust setting. Set the value to `True`.

```
<Settings>
    <ConnectionString>Data Source=MSSQL\SQLEXPRESS;Database=LogServer;User
Id=servicesql;Password=P@ssw0rd;TrustServerCertificate=True</ConnectionString>
</Settings>
```

3. Open the */opt/axidian/ls* catalog and edit the *clientApps.config* file.

   - In the `Application` section, add the following parameters.

```
<Application Id="certiflow" SchemaId="certiflowSchema">
    <ReadTargetId>certiflowMsSqlTarget</ReadTargetId>

    <WriteTargets>
        <TargetId>certiflowMsSqlTarget</TargetId>
    </WriteTargets>

    <AccessControl>
        <!--<CertificateAccessControl CertificateThumbprint="001122...AA11"
Rights="Read" />-->
    </AccessControl>
</Application>
```

   - In the `Targets` section, add a new element.

```
<Targets>
    <Target Id="certiflowMsSqlTarget" Type="mssql"/>
</Targets>
```

PostgreSQL

1. Create a database in pgAdmin.

   1. Open pgAdmin and connect to the server.
   2. In the **Browser** section, right-click **Databases** and select **Create** → **Database...**.
   3. On the **General** tab, specify the database name in the **Database** field, select the service account from the **Owner** list, and click **Save**.

2. Grant the service account the permissions to manage the database.

   1. Select the database and select **Tools** → **Query Tool**.

2. Enter the query with the service account name.

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO <service account
name>;
```

3. Click **Execute/Refresh** (Execute/Refresh).

3. Follow these steps to add Universally Unique Identifiers (UUID) generation support.

1. Click  and select **Clear Query**.
2. Enter the query.

```
CREATE EXTENSION IF NOT EXISTS "uuid-ossp";
```

3. Click **Execute/Refresh** (Execute/Refresh).

4. Configure a remote connection to the database.

1. Open the *pg_hba.conf* configuration file (*/etc/postgresql/<version number>/main*.).
2. Add a string in the following format:

```
CONNECTIONTYPE DATABASE USER ADDRESS METHOD
```

- `CONNECTIONTYPE` – the name of the connection type. To use TCP/IP connection, specify `host`.
- `DATABASE` – the name of the database. To grant access to all databases, specify `ALL`.
- `USER` – name of the user who accesses the database. To grant access to all users, specify `ALL`.
- `ADDRESS` – the IP address of the remote Axidian CertiFlow server. To grant access from any IP address, specify `0.0.0.0/0`.
- `METHOD` – the user authentication method. For example, `md5`, `scram-sha-256`.

Example

```
host LogServer servicepg 192.200.1.0/24 md5
host ALL servicepg 10.0.0.0/8 md5
host ALL ALL 0.0.0.0/0 scram-sha-256
```

5. Open the */opt/axidian/ls/targetConfigs* catalog and edit the *certiflowPgSqlTarget.config* file. In the `<ConnectionString>…</ConnectionString>` section, configure the following parameters:

- `Host` – the PostgreSQL Server name.
- `Port` – the PostgreSQL connection port. Default value is 5432.

- `Database` – the database name.
- `Username` – the service account for managing the Axidian CertiFlow database.
- `Password` – the service account password.

```
<Settings>
    <ConnectionString>Host=SRV-
POSTGRESQL;Port=5432;Database=LogServer;Username=servicepg;Password=P@ssw0rd</C
</Settings>
```

6. Open the */opt/axidian/ls* catalog and edit the *clientApps.config* file.

   - In the `Application` section add a new `TargetId` for `ReadTarget` and `WriteTarget`.

```
<Application Id="certiflow" SchemaId="certiflowSchema">
    <ReadTargetId>certiflowPgSqlTarget</ReadTargetId>

    <WriteTargets>
        <TargetId>certiflowPgSqlTarget</TargetId>
    </WriteTargets>

    <AccessControl>
        <!-- <CertificateAccessControl CertificateThumbprint="001122...AA11"
Rights="Read" /> -->
    </AccessControl>
</Application>
```

   - In the `Targets` section, add a new element.

```
<Targets>
    <Target Id="certiflowPgSqlTarget" Type="pgsql"/>
</Targets>
```

Syslog

Syslog only supports event writing (WriteTargets). The following configuration extends the PostgreSQL example.

1. Open the */opt/axidian/ls/targetConfigs* catalog and edit the *certiflowSysLogTarget.config* file. In the `<ConnectionString>…</ConnectionString>` section, configure the following parameters:

   - `HostName` – the Syslog server name or IP.
   - `Port` – the Syslog server connection port. Default value is 514.
   - `Protocol` – the Syslog server connection type: UDP, TCP, TCPoverTLS.

- `Format` – an optional parameter that configures log format: Plain, CEF, LEEF.
- `SyslogVersion` – an optional parameter that configures the protocol: RFC3164, RFC5424.

```
<Settings HostName="SRV-SYSLOG" Port="514" Protocol="UDP"/>
```

2. Open the */opt/axidian/ls* catalog and edit the *clientApps.config* file.

- In the `Application` section add a new `TargetId` for `WriteTarget`.

```
<Applications>
    <Application Id="certiflow" SchemaId="certiflowSchema">
        <ReadTargetId>certiflowPgSqlTarget</ReadTargetId>

        <WriteTargets>
            <TargetId>certiflowPgSqlTarget</TargetId>
            <TargetId>certiflowSysLogTarget</TargetId>
        </WriteTargets>

        <AccessControl>
            <!-- <CertificateAccessControl
CertificateThumbprint="001122...AA11" Rights="Read" /> -->
        </AccessControl>
    </Application>
</Applications>
```

- In the `Targets` section, add a new element.

```
<Targets>
    <Target Id="certiflowPgSqlTarget" Type="pgsql"/>
    <Target Id="certiflowSysLogTarget" Type="syslog"/>
</Targets>
```

Apply Log server settings

1. Open the web server configuration file for nginx or Apache and uncomment the strings for processing the api application.

nginx example

```
  location /api
 {  include /etc/nginx/conf.d/proxy.conf;    proxy_pass
http://localhost:5010/api;    }
```

Apache example

```
ProxyPass /api http://localhost:5010/api
ProxyPassReverse /api http://localhost:5010/api
```

2. Restart the web server.

3. Restart the Log Server service.

```
sudo systemctl restart axidian-ls.service
```

Configure Axidian CertiFlow to use the Unified Event log

1. Configure connection to the event log in the Configuration Wizard.
2. Test the event log functionality. Go to the Management Console, open the **Log** section, and search for events.

> **TIP**
> The log search might return no results if the log on the remote server contains no events. Perform any action in the Axidian CertiFlow web applications. For example, disable a card, add or modify a comment, and then repeat the event search.

Axidian CertiFlow Agent

With Axidian CertiFlow Client Agent you can manage cards on user workstations remotely.

After configuring the Axidian CertiFlow server components, install the agents on user workstations alongside the Axidian CertiFlow Middleware component.

The agent performs the following operations:

- Add and assign cards
- Issue empty or pre-assigned cards
- Continue issue and update operations for cards in a *Pending* state.
- Request a user PIN change after a specified time period
- Block and reset user PIN
- Update card contents
- Clear and initialize cards within revocation
- Change administrator PIN
- Control card usage and block user sessions and cards
- Detect cards with blocked user or administrator PINs, incorrect PIN entry attempts, and connections of unregistered cards

Configure agent environment

Follow the instructions for the operating system of the workstation where the Axidian CertiFlow server is installed.

Windows

1. Create certificates for agent services.
2. Configure a secure connection to the agent services website.
3. Configure Axidian CertiFlow to work with agents.
4. Install and configure agents on user workstations.

Create agent certificates

The agent requires the following certificates:

- **CertiFlow Agent CA** – the root certificate for the agent services. CertiFlow Agent CA certificate is used to issue certificates to user workstations with agents.

- **CertiFlow Agent SSL** – an authentication certificate signed by the root certificate. CertiFlow Agent SSL certificate is required to establish a secure TLS connection between the server and a workstation with an agent. The certificate is issued for the workstation hosting the Axidian CertiFlow server.
- **Workstation certificate** – a certificate that is issued automatically when an agent is registered. When connecting to the Axidian CertiFlow server, the client workstation uses this certificate to authenticate. Once the server verifies the connection, the workstation is added to the trusted list and can receive tasks from the server.

Use the CertiFlow.Agent.Cert.Generator tool to create the agent certificates.

CertiFlow.Agent.Cert.Generator tool parameters

Parameters for generating root and SSL certificates

Parameter	Description
`/root`	Generates the root certificate for agent services.
`/rootKeySize`	(Optional) Specifies the private key size (in bits) for the root certificate. Default: `4096`. Valid range: `512` to `8192`.
`/sn <server_DNS_name>`	Generates the SSL certificate for the specified server DNS name.
`/csn`	Generates the SSL certificate for the server where the tool is running.
`/sslKeySize`	(Optional) Specifies the private key size (in bits) for the SSL certificate. Default: `2048`. Valid range: `512` to `4096`.
`/pwd`	(Optional) Specifies the password for the SSL certificate.
`/installToStore`	(Optional) Publishes the certificates generated by the tool to the server's certificate stores: - The CertiFlow Agent CA certificate to the Trusted Root Certification Authorities store. - The CertiFlow Agent SSL certificate to the Personal certificate store of the workstation hosting the Axidian CertiFlow server.

Parameters for generating only an SSL Certificate using an existing CertiFlow Agent CA root certificate

Parameter	Description
`/rootKey`	The file path to the existing root certificate.
`/ssl`	Generates the SSL certificate for agent services.
`/sn <server_DNS_name>`	Generates the SSL certificate for the specified server DNS name.
`/csn`	Generates the SSL certificate for the server where the tool is running.
`/pwd`	(Optional) Specifies the password for the SSL certificate.

Parameter	Description
`/sslKeySize`	(Optional) Specifies the private key size (in bits) for the SSL certificate. Default: `2048`. Valid range: `512` to `4096`.
`/installToStore`	(Optional) Publishes the SSL certificate generated by the tool to the Personal certificate store of the workstation hosting the Axidian CertiFlow server.

Follow these steps to create agent certificates:

1. Navigate to the *AxidianCertiFlow.WindowsServer\Misc\AgentCertGenerator* catalog on the Axidian CertiFlow server.
2. Launch the command prompt as administrator and run the CertiFlow.Agent.Cert.Generator tool with the required parameters.

```
CertiFlow.Agent.Cert.Generator.exe /root /csn /installToStore
```

The tool creates the following files *AxidianCertiFlow.WindowsServer\Misc\AgentCertGenerator* catalog:

- *agent_root_ca.json* – the agent root certificate with its private key in JSON format
- *agent_root_ca.cer* – the agent root certificate
- *agent_root_ca.key* – the private key for the agent root certificate
- *agent_ssl_cert.cer* – the SSL certificate for the agent website
- *agent_ssl_cert.key* – the private key for the SSL certificate
- *agent_ssl_cert.pfx* – the agent SSL certificate with its private key in PFX format

> ⓘ **INFO**
> Install the CertiFlow Agent CA certificate (*agent_root_ca.cer*) into the Trusted Root Certification Authorities store on the Axidian CertiFlow server.

Multi-server deployments

For deployments with multiple Axidian CertiFlow servers using agents, issue a unique SSL certificate for each server. Use a shared CertiFlow Agent CA root certificate for all servers in your environment.

Follow these steps to create an SSL certificate for an additional server or to renew an expired certificate.

1. Copy the Cm.Agent.Cert.Generator tool catalog and the agent root certificate with the private key (*agent_root_ca.json*) to the target server.
2. Run the following command.

```
Cm.Agent.Cert.Generator.exe /rootKey <path_to_agent_root_ca.json> /ssl /sn
<server_DNS_name> /installToStore
```

Example

```
Cm.Agent.Cert.Generator.exe /rootKey "C:\AgentCertGenerator\agent_root_ca.json"
/ssl /sn server.domain.loc /installToStore
```

Configure a secure connection to the agent website

1. Open the Internet Information Services (IIS) Manager.
2. Select the Axidian CertiFlow Agent Site and go to **Bindings...**.
3. Select the binding for port 3003.

   > **INFO**
   > Port 3003 is set by default. If you use another port, create and configure a new binding for this port. The port must be open to incoming connections in the firewall.

4. Click **Edit...**.
5. In the **SSL certificate** field, select the CertiFlow Agent SSL certificate or another SSL/TLS certificate issued by a trusted Certificate Authority (CA) in your environment for the Axidian CertiFlow server's hostname, and click **OK**.

SSL certificate requirements

The SSL/TLS certificate can be an RSA certificate issued by any trusted Certificate Authority (CA) for the Axidian CertiFlow server.

- **Subject** must include the **Common Name** attribute (the server FQDN).
- **Subject Alternative Name (SAN)** must include a **DNS Name** attribute (the server FQDN). For example: `server.domain.loc` or a wildcard entry `*.domain.loc`.
- **Enhanced Key Usage (EKU)** must include the **Server Authentication** value.

Linux

1. Create certificates for agent services.
2. Configure a secure connection to the agent services website.
3. Configure Axidian CertiFlow to work with agents.
4. Install and configure agents on user workstations.

Create agent certificates

The agent requires the following certificates:

- **CertiFlow Agent CA** – the root certificate for the agent services. CertiFlow Agent CA certificate is used to issue certificates to user workstations with agents.
- **CertiFlow Agent SSL** – an authentication certificate signed by the root certificate. CertiFlow Agent SSL certificate is required to establish a secure TLS connection between the server and a workstation with an agent. The certificate is issued for the workstation hosting the Axidian CertiFlow server.
- **Workstation certificate** – a certificate that is issued automatically when an agent is registered. When connecting to the Axidian CertiFlow server, the client workstation uses this certificate to authenticate. Once the server verifies the connection, the workstation is added to the trusted list and can receive tasks from the server.

Use the CertiFlow.Agent.Cert.Generator tool to create the agent certificates.

CertiFlow.Agent.Cert.Generator tool parameters

Parameters for generating root and SSL certificates

Parameter	Description
`/root`	Generates the root certificate for agent services.
`/rootKeySize`	(Optional) Specifies the private key size (in bits) for the root certificate. Default: `4096`. Valid range: `512` to `8192`.
`/sn <server_DNS_name>`	Generates the SSL certificate for the specified server DNS name.
`/csn`	Generates the SSL certificate for the server where the tool is running.
`/sslKeySize`	(Optional) Specifies the private key size (in bits) for the SSL certificate. Default: `2048`. Valid range: `512` to `4096`.
`/pwd`	(Optional) Specifies the password for the SSL certificate.
`/installToStore`	(Optional) Publishes the certificates generated by the tool to the server's certificate stores: - The CertiFlow Agent CA certificate to the Trusted Root Certification Authorities store. - The CertiFlow Agent SSL certificate to the Personal certificate store of the workstation hosting the Axidian CertiFlow server.

Parameters for generating only an SSL Certificate using an existing CertiFlow Agent CA root certificate

Parameter	Description
`/rootKey`	The file path to the existing root certificate.
`/ssl`	Generates the SSL certificate for agent services.
`/sn <server_DNS_name>`	Generates the SSL certificate for the specified server DNS name.
`/csn`	Generates the SSL certificate for the server where the tool is running.
`/pwd`	(Optional) Specifies the password for the SSL certificate.

Parameter	Description
`/sslKeySize`	(Optional) Specifies the private key size (in bits) for the SSL certificate. Default: `2048`. Valid range: `512` to `4096`.
`/installToStore`	(Optional) Publishes the SSL certificate generated by the tool to the Personal certificate store of the workstation hosting the Axidian CertiFlow server.

Follow these steps to create agent certificates:

1. Open a terminal on the Axidian CertiFlow server, navigate to the *AxidianCertiFlow.LinuxServer/Misc/AgentCertGenerator* catalog, and grant execute permission to the Cm.Agent.Cert.Generator file:

   ```
   sudo chmod +x CertiFlow.Agent.Cert.Generator.dll
   ```

2. Run the tool with the `/root /csn` parameters.

   ```
   dotnet CertiFlow.Agent.Cert.Generator.dll /root /csn
   ```

The tool creates the following files *AxidianCertiFlow.WindowsServer\Misc\AgentCertGenerator* catalog:

- *agent_root_ca.json* – the agent root certificate with its private key in JSON format
- *agent_root_ca.cer* – the agent root certificate
- *agent_root_ca.key* – the private key for the agent root certificate
- *agent_ssl_cert.cer* – the SSL certificate for the agent website
- *agent_ssl_cert.key* – the private key for the SSL certificate
- *agent_ssl_cert.pfx* – the agent SSL certificate with its private key in PFX format

> **INFO**
> Install the CertiFlow Agent CA certificate (*agent_root_ca.cer*) into the Trusted Root Certification Authorities store on the Axidian CertiFlow server.

Multi-server deployments

For deployments with multiple Axidian CertiFlow servers using agents, issue a unique SSL certificate for each server. Use a shared CertiFlow Agent CA root certificate for all servers in your environment.

Follow these steps to create an SSL certificate for an additional server or to renew an expired certificate.

1. Copy the Cm.Agent.Cert.Generator tool catalog and the agent root certificate with the private key (*agent_root_ca.json*) to the target server.
2. Run the following command.

```
dotnet CertiFlow.Agent.Cert.Generator.dll /rootKey <path_to_agent_root_ca.json>
/ssl /sn <server_DNS_name> /installToStore
```

Example

```
dotnet CertiFlow.Agent.Cert.Generator.dll /rootKey ./agent_root_ca.json /ssl /sn
domain.loc1
```

Configure a secure connection to the agent website

Follow the instructions for the operating system of the workstation where the Axidian CertiFlow server is installed.

RHEL-based

1. Copy the agent website SSL certificate and its private key to the */etc/ssl/* catalog on the Axidian CertiFlow server, and the agent root certificate – to the trusted root certificates store.

```
sudo cp ./agent_ssl_cert.cer /etc/ssl/
sudo cp ./agent_ssl_cert.key /etc/ssl/
sudo cp ./agent_root_ca.cer /etc/pki/ca-trust/source/anchors/
```

2. Run the following command to update the trusted root certificates store.

```
sudo update-ca-trust extract
```

3. Specify the paths to the certificate and the private key in the configuration file of your web server, in the section that defines the agent website.

Debian-based

1. Copy the agent website SSL certificate and its private key to the corresponding catalogs on the Axidian CertiFlow server, and the agent root certificate – to the trusted root certificates store. Convert the agent's root certificate format from CER to CRT.

```
sudo cp ./agent_ssl_cert.cer /etc/ssl/certs/
sudo cp ./agent_ssl_cert.key /etc/ssl/private/
sudo cp ./agent_root_ca.cer /usr/local/share/ca-
certificates/agent_root_ca.crt
```

2. Run the following command to update the trusted root certificates store.

```
sudo update-ca-certificates -f
```

3. Specify the paths to the certificate and the private key in the configuration file of your web server, in the section that defines the agent website.

Port 3003 is set by default. If you use another port, create and configure a new binding for this port. The port must be open to incoming connections in the firewall.

Nginx configuration example

```
server {
        listen              3003 ssl;
        server_name         server.domain.loc;

        ssl_certificate     "/etc/ssl/certs/agent_ssl_cert.cer";
        ssl_certificate_key "/etc/ssl/private/agent_ssl_cert.key";
        ssl_verify_client   optional_no_ca;

        location /agentregistrationapi
             {   include /etc/nginx/conf.d/proxy.conf;
                proxy_pass http://localhost:5006/agentregistrationapi;  }
        location /agentserviceapi
         {   include /etc/nginx/conf.d/proxy.conf;
                proxy_pass http://localhost:5007/agentserviceapi;
                proxy_set_header x-ssl-client-cert $ssl_client_escaped_cert;
}
    }
```

Apache configuration example

```
<VirtualHost *:3003>
    protocols h2 http/1.1

    SSLCertificateFile /etc/apache2/ssl/agent_ssl_cert.cer
    SSLCertificateKeyFile /etc/apache2/ssl/agent_ssl_cert.key
    SSLCipherSuite @SECLEVEL=1:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-
ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384

    ErrorLog logs/error.log
    CustomLog logs/access.log combined

    SSLEngine on
    SSLProtocol -all +TLSv1.2
    SSLHonorCipherOrder off
    SSLCompression off
    SSLSessionTickets on
    SSLUseStapling off
    SSLProxyEngine on
    RequestHeader set X-Forwarded-Proto https
    Header always set Strict-Transport-Security "max-age=63072000"

        ProxyPass /agentregistrationapi
http://localhost:5006/agentregistrationapi
        ProxyPassReverse /agentregistrationapi
http://localhost:5006/agentregistrationapi

    <Location "/agentserviceapi">
        SSLVerifyClient optional_no_ca
        SSLOptions +ExportCertData
        RequestHeader unset x-ssl-client-cert
        RequestHeader set x-ssl-client-cert "expr=%{escape:%
{SSL_CLIENT_CERT}}"
        #RequestHeader set x-ssl-client-cert "expr=%{escape:%
{SSL_CLIENT_S_DN}}"

        ProxyPass http://localhost:5007/agentserviceapi
        ProxyPassReverse http://localhost:5007/agentserviceapi
    </Location>
</VirtualHost>
```

INFO

The SSL/TLS certificate can be an RSA certificate issued by any trusted Certificate Authority (CA) for the Axidian CertiFlow server.

- **Subject** must include the **Common Name** attribute (the server FQDN).
- **Subject Alternative Name (SAN)** must include a **DNS Name** attribute (the server FQDN). For example: `server.domain.loc` or a wildcard entry `*.domain.loc`.
- **Enhanced Key Usage (EKU)** must include the **Server Authentication** value.

Install client components

Middleware

Component for managing USB tokens and smart cards

Client Tools

Component for unlocking cards

Agent

Component for managing cards remotely

Middleware

With Axidian CertiFlow Middleware you can manage cards in Axidian CertiFlow.

> **INFO**
> To use Axidian CertiFlow Middleware, install card and reader drivers and other service tools on user workstations. This software is not included in the Axidian CertiFlow installation package.

Install Middleware on Windows

Different card types require different Axidian CertiFlow Middleware files.

Run the *AxidianCertiFlow.<card type name>.Middleware.<version number>.en-us.msi* file from the *AxidianCertiFlow.Client* catalog of the Axidian CertiFlow installation package and follow the wizard instructions.

The following table shows which Axidian CertiFlow Middleware file corresponds to each manufacturer and card model.

Manufacturer	Card model	Middleware file
ACS	ACOS5-64	*AxidianCertiFlow.ACOS.Middleware-<version number>.en-us.msi*
Avest	Avest Key 256A	*AxidianCertiFlow.Avest.Middleware-<version number>.en-us.msi*
Axidian	AirCard virtual smart card	*AxidianCertiFlow.AirCard.Middleware-<version number>.en-us.msi*
Bit4id	ID-One Cosmo	*AxidianCertiFlow.Bit4Id.Middleware-<version number>.en-us.msi*
CRYPTAS	TicTok V2/V3	*AxidianCertiFlow.TicTok.Middleware-<version number>.en-us.msi*
Cryptovision	ePasslet Suite v3.0, JCOP V3.0	*AxidianCertiFlow.Cryptovision.Middleware-<version number>.en-us.msi*

Manufacturer	Card model	Middleware file
Feitian	ePass2003 (A1+, A2) BioPass2003	*AxidianCertiFlow.ePass.Middleware-<version number>.en-us.msi*
HID	Crescendo C1150 Series Crescendo C1300 Series Crescendo C2300 Series	*AxidianCertiFlow.HID.Middleware-<version number>.en-us.msi*
Microsoft	Local Computer Certificate Store User Certificate Store	*AxidianCertiFlow.Registry.Middleware-<version number>.en-us.msi*
	TPM Virtual Smart Card (Microsoft VSC)	*AxidianCertiFlow.TPM.Middleware-<version number>.en-us.msi*
	Windows Hello for Business (WHfB)	*AxidianCertiFlow.WHfB.Middleware-<version number>.en-us.msi*
RSA	RSA SecurID 800	*AxidianCertiFlow.RSA.Middleware-<version number>.en-us.msi*

Manufacturer	Card model	Middleware file
Thales (SafeNet and Gemalto)	SafeNet eToken PRO 32k SafeNet eToken PRO 64k eToken PRO Java 72K OS755 SafeNet eToken 5105 SafeNet eToken 5110 IDCore30B eToken 1.7.7	*AxidianCertiFlow.eToken.Middleware-<version number>.en-us.msi*

Manufacturer	Card model	Middleware file
	IDPrime MD 830 FIPS IDPrime MD 830B FIPS IDPrime MD 840B IDPrime 930 IDPrime 930nc IDPrime 940 IDPrime 940B IDPrime MD 3810 IDPrime MD 3811 IDPrime 3930 IDPrime 3940 IDPrime 3940 FIDO SafeNet eToken 5300 SafeNet eToken Fusion SafeNet eToken Fusion CC SafeNet eToken 5110 CC (940)	*AxidianCertiFlow.IDPrime.Middleware-<version number>.en-us.msi*
Yubico	YubiKey 5 Series	*AxidianCertiFlow.YubiKey.Middleware-<version number>.en-us.msi*

Install Middleware on Linux

To install Axidian CertiFlow Middleware, run the following command.

Debian

```
sudo dpkg -i certiflow.middleware_<version number>_amd64.deb
```

RHEL

```
sudo rpm -i certiflow.middleware-<version number>.x86_64.rpm
```

Axidian CertiFlow for Linux supports SafeNet eToken cards using a single Middleware component.

Manufacturer	Card model
Thales (SafeNet и Gemalto)	SafeNet eToken PRO 32k SafeNet eToken PRO 64k eToken PRO Java 72K OS755 SafeNet eToken 5105 SafeNet eToken 5110 IDCore30B eToken 1.7.7

Install Middleware browser extension

Install the Axidian CertiFlow Middleware browser extension on administrator, operator, and user workstations for access to Axidian CertiFlow web applications.

Google Chrome, Chromium

1. Launch your browser and navigate to the extensions page: `chrome://extensions` for Google Chrome and Chromium.
2. Open the *AxidianCertiFlow.Client-v<version number>\certiflow.middleware.chrome.extension* catalog.
3. Upload the CRX file in the browser's extensions page.
4. Click **Add extension** in the pop-up window.

Mozilla Firefox

1. Launch your browser and navigate to the add-ons page: `about:addons`.
2. Click  and select **Install Add-on from file…**.
3. Upload the *certiflow.middleware-1.0.xpi* file from the *AxidianCertiFlow.Client-<version number>\certiflow.middleware.chrome.extension* catalog and click **Open**.
4. Click **Add** in the pop-up window.

Configure Registry cards support

Configure Registry cards support using Windows Group Policies or the Windows Registry (for workstations outside a Windows domain).

Windows Group Policies

To enable Axidian CertiFlow users to issue Registry cards in the Self-Service and write the certificates to the Local Computer Certificate Store or User Certificate Store, configure a Group Policy Object (GPO). This procedure installs the necessary administrative templates and applies the policy to the user workstations.

1. Copy the contents of the *AxidianCertiFlow.Client\Misc* catalog to your central ADMX file store. The standard location on a domain controller is *C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions*.

   > ⓘ **INFO**
   > If you use a local ADMX store instead, copy the files to *C:\Windows\PolicyDefinitions*.

2. Open the Group Policy Management console.
3. In the console tree, create a new GPO or select an existing GPO that applies to the target user workstations.
4. Right-click the GPO and select **Edit**.
5. In the Group Policy Management Editor, go to **Computer Configuration** → **Policies** → **Administrative Templates** → **Axidian CertiFlow** → **Client**.
6. Enable the following policies:
   - **Enable 'Registry' card (Machine)** to issue certificates to the Local Computer Certificate Store.
   - **Enable 'Registry' card (User)** to issue certificates to the User Certificate Store
7. Link the edited GPO to the Organizational Unit (OU) or security group that contains the workstations of the Axidian CertiFlow users.
8. Select **Apply**.
9. Force a policy update on the target workstations or wait for the next refresh cycle.

Windows Registry

If the Axidian CertiFlow server and user workstations are outside a Windows domain, configure the registry on each client workstation.

Create a REG file:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\AxidianCertiFlow\Client]
"MachineRegistryCardEnabled"=dword:00000000
"UserRegistryCardEnabled"=dword:00000000
```

- `MachineRegistryCardEnabled`: Set the value to **1** (dword:00000001) to enable certificate issuance to the Local Computer Certificate Store.
- `UserRegistryCardEnabled`: Set the value to **1** (dword:00000001) to enable certificate issuance to the User Certificate Store.

REG file example

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\AxidianCertiFlow\Client]
"MachineRegistryCardEnabled"=dword:00000001
"UserRegistryCardEnabled"=dword:00000001
```

In this example, Registry cards are configured to be issued to both the Local Computer Certificate Store and the User Certificate Store.

Client Tools

With Axidian CertiFlow Client Tools you can unlock cards that are used for Windows OS authentication in online and offline modes, as well as cards not used for OS logon.

Install Client Tools

To install Axidian CertiFlow Client Tools on user workstations, run the *AxidianCertiFlow.Client.Tools-<version number>.en-us.msi* file from the *AxidianCertiFlow.Client* catalog and follow the wizard instructions.

Card unlock modes

You can unlock a card using two modes: online and offline. For more information, see Administrator guide.

Online
Online mode requires a connection between the user's workstation (where the locked card is connected) and the Axidian CertiFlow server. This connection is used to authenticate the user by verifying their answers to security questions. We recommend using a secure HTTPS connection for communication between user workstations and the Axidian CertiFlow server for online unlock.

Offline
In offline mode, an Axidian CertiFlow operator unlocks the card using a challenge-response authentication mechanism. When the PIN retry limit is reached, the user receives a card lockout message along with a unique 16-character challenge code. The user must contact an Axidian CertiFlow operator (for example, by phone) to verify their identity.

Configure online card unlock

Configure card unlock using Windows Group Policies or the Windows Registry (for workstations outside a Windows domain).

Windows Group Policies

To enable the online card unlock feature, configure a Group Policy Object (GPO). This procedure installs the necessary administrative templates and applies the policy to the user workstations.

1. Copy the contents of the *AxidianCertiFlow.Client\Misc* catalog to your central ADMX file store. The standard location on a domain controller is *C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions*.

   > ⓘ **INFO**
   > If you use a local ADMX store instead, copy the files to *C:\Windows\PolicyDefinitions*.

2. Open the Group Policy Management console.
3. In the console tree, create a new GPO or select an existing GPO that applies to the target user workstations.
4. Right-click the GPO and select **Edit**.
5. In the Group Policy Management Editor, go to **Computer Configuration** → **Policies** → **Administrative Templates** → **Axidian CertiFlow** → **Client**.
6. Enable the **Smart card unlocking server** policy and configure the following parameters:

- In the `Service URL` parameter, specify the link to the **credprovapi** component hosted on the Axidian CertiFlow server: `https://<Server FQDN>/certiflow/credprovapi`.
- In the `Verify server certificate` parameter, set the value to `Yes` if server certificate authentication is required. Set it to `No` (default) if no authentication is required.

7. Link the edited GPO to the Organizational Unit (OU) or security group that contains the workstations of the Axidian CertiFlow users.
8. Select **Apply**.
9. Force a policy update on the target workstations or wait for the next refresh cycle.

Optional settings of the smart card unlocking service

Policy	Description
Set explanations for offline unlocking	This policy applies to user workstations. If the policy is disabled or not defined, the explanation text for offline card unlock is not displayed in the Credential Provider. This text could provide the contact phone number of the Axidian CertiFlow administrator.
Credential Providers: Disable smart card standard provider wrapping	This policy applies to user workstations. If the policy is disabled or not defined, the user can unlock the smart card using the standard Windows OS smart card logon interface. If the policy is enabled, a separate smart card unlock option appears on the OS logon screen. This setting is useful when third-party software is installed on the workstation that prevents card unlock using the standard Credential Provider.
Credential Providers: Hide the "Disable the smart card" option	This policy applies to user workstations. If the policy is disabled or not defined, the user can disable the smart card from the Windows OS logon interface. If the policy is enabled, the option to disable the smart card is hidden on the OS logon screen.

Windows Registry

If the Axidian CertiFlow server and user workstations are outside a Windows domain, enter the path to the **credprovapi** application in the registry of each client workstation.

Create a REG file:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\AxidianCertiFlow\Client]
"CredProvAPIURL"=""
"AdminDetails"=""
"DisableServerCertificateChecking"=dword:00000000
"DisableSuspendCP"=dword:00000000
"DisableWrapperCP"=dword:00000000
```

- `CredProvAPIURL`: Specify the address of the **credprovapi** application on the Axidian CertiFlow server.

- `AdminDetails`: Specify the explanation text for the user.
- `DisableServerCertificateChecking`: Set the value to **0** (default) if authentication of the Axidian CertiFlow server certificate is required. Set it to **1** (dword:00000001) if authentication is not required.
- `DisableSuspendCP`: Set the value to **0** (default) to display the **Disable smart card** option in the OS logon interface. Set it to **1** (dword:00000001) if the **Disable smart card** option should not be displayed.
- `DisableWrapperCP`: Set the value to **0** (default) to perform smart card unlock using the standard Credential Provider. Set it to **1** (dword:00000001) to use a different Credential Provider.

REG file example

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\AxidianCertiFlow\Client]
"CredProvAPIURL"="https://server.domain.loc/certiflow/credprovapi"
"AdminDetails"="Contact the administrator at extension 1607"
"DisableServerCertificateChecking"=dword:00000000
"DisableSuspendCP"=dword:00000001
"DisableWrapperCP"=dword:00000001
```

In this example, the machine name is *server.domain.loc*, server certificate authentication is enabled, **Disable smart card** button is hidden, the smart card unlock option is enabled using a different Credential Provider on the OS logon screen.

Agent

With Axidian CertiFlow Client Agent you can manage cards on user workstations remotely.

Install Agent

Install Axidian CertiFlow Agent along with Axidian CertiFlow Middleware on user workstations.

To install an agent, run the *AxidianCertiFlow.Agent-<version number>.en-us.msi* file from the *AxidianCertiFlow.Client* catalog and follow the wizard instructions. The agent starts automatically after installation.

Configure server connection

Configure the settings for connecting agents to the Axidian CertiFlow server using Windows Group Policies or the Windows Registry.

Windows Group Policies

1. Copy the contents of the *AxidianCertiFlow.Client\Misc* catalog to your central ADMX file store. The standard location on a domain controller is *C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions*.

   > **INFO**
   > If you use a local ADMX store instead, copy the files to *C:\Windows\PolicyDefinitions*.

2. Open the Group Policy Management console.

3. In the console tree, create a new GPO or select an existing GPO that applies to the target user workstations.

4. Right-click the GPO and select **Edit**.

5. In the Group Policy Management Editor, go to **Computer Configuration** → **Policies** → **Administrative Templates** → **Axidian CertiFlow** → **Agent**.

6. Enable the **Agent's URL Settings** policy and configure the following parameters:

- In the `Agents registration service URL` parameter, specify the web address and port for connecting to the **agentregistrationapi** application hosted on the Axidian CertiFlow server. For example, `https://server.domain.loc:3003/agentregistrationapi/`.

- In the `Agents service URL` parameter, specify the web address and port for the **agentserviceapi** service. For example, `https://server.domain.loc:3003/agentserviceapi/`.

7. Link the edited GPO to the Organizational Unit (OU) or security group that contains the workstations of the Axidian CertiFlow users.
8. Select **Apply**.
9. Force a policy update on the target workstations or wait for the next refresh cycle.

▼ **Optional agent settings**

Policy	Description
Agent's timeouts settings	Request timeout to agent services (default: 30 sec.) Agent status check request interval (default: 300 sec.) Settings, bindings, tasks, and sessions update request interval (default: 30 sec.) Agent disconnect request timeout (default: 3 sec.)
Events caching settings	Number of minutes the agent attempts to send cached events to the server (default: 10 min.) Number of events transferred at once from the user workstation cache to the server (default: 500 events)
Proxy server settings	This policy defines the use of a proxy server when connecting to the Axidian CertiFlow server. If the policy is not set or disabled, a proxy server is not used. The **Proxy server** parameter specifies the proxy server address.
Event log settings	This policy sets the event logging level to the server log: All (default) Errors only Errors and warnings only
Tasks caching settings	Interval for updating the task cache and sending task execution status to the server if it could not be reported immediately (default: 60 sec.) Timeout after which tasks are removed from the cache during the next cache update (default: 300 sec.) Timeout before a user-canceled task can be executed again (default: 60 sec.)
Smart card status update settings	This policy sets the interval for checking card status (default: 30 sec.): User/Administrator PIN lock Incorrect User/Administrator PIN entry attempts

Windows Registry

Create a REG file:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\AxidianCertiFlow\Agent]
"AgentRegistrationServiceUrl"=""
"AgentServiceUrl"=""
"ProxyEnable"=""
"ProxyServer"=""
```

> **TIP**
> For 32-bit operating systems, configure the parameters in the following registry key: *[HKEY_LOCAL_MACHINE\SOFTWARE\AxidianCertiFlow\Agent]*

- `AgentRegistrationServiceUrl`: Specify the link and port for connecting to the **agentregistrationapi** application.
- `AgentServiceUrl`: Specify the web address and port for connecting to the **agentserviceapi** application.
- `ProxyEnable` and `ProxyServer`: If a proxy is used on the workstations where the client agent is installed, specify the proxy server URL.

Example proxy server parameters

```
`"ProxyEnable"=dword:00000000` – proxy is not used
`"ProxyEnable"=dword:00000001` and `"ProxyServer"=""` – default proxy settings are used
`"ProxyEnable"=dword:00000001` and `"ProxyServer"="<proxy server URL>"` – the proxy server specified in the setting is used
```

REG file example

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\AxidianCertiFlow\Agent]
"AgentRegistrationServiceUrl"="https://server.domain.loc:3003/agentregistrationapi/"
"AgentServiceUrl"="https://server.domain.loc:3003/agentserviceapi/"
"ProxyEnable"=dword:00000001
"ProxyServer"="https://192.168.10.10:443"
```

⚠ **CAUTION**

Distribute the registry file and apply the changes to user workstations. To apply the changes, restart the workstation with the Axidian CertiFlow Agent or restart the Agent Service.

Administrator guide

Start

Log in to Management Console

Configuration

9 items

Management Console

8 items

Start

You can manage Axidian CertiFlow in the Management Console.

The Management Console is available at *https://<Server FQDN>/certiflow/mc*.

You can access the Management Console according to the authentication settings configured during the Axidian CertiFlow server installation.

Before you start working with Axidian CertiFlow:

1. Run the Management Console as the role administrator. You can assign the role administrator in the Configuration Wizard (**Access control→Role administrator**).
2. Go to **Configuration→Roles** and assign the **Administrator** role to the current user (role administrator). Create the required roles and configure permissions.
3. Upload the license file in **Licenses**.
4. Upload the card types files in **Card types**.
5. Configure policy settings in **Policies**.
6. Assign policies on user groups in **Policy links**.

Configuration

Manage policies

8 items

Licenses

How to get, add and remove licenses

Card types

How to manage card types files

Organization structure

How to apply a single policy across multiple catalog objects

Roles

How to manage administrator and operator permissions

Tags

How to assign tags to cards

Print templates

How to manage print templates

Notifications

How to configure alerts about Axidian CertiFlow events

Custom logs

How to configure custom logs

Manage policies

Policies define allowed and prohibited user actions when they manage cards.

Create a policy

To create a policy:

1. In the Management Console side panel, go to **Configuration** → **Policies**.
2. Click **Create policy**.
3. Specify the display name for the policy in the **Name** field, or copy settings from a previously created policy using the **Copy from** field.
4. Click **Create**.

Delete a policy

To delete a policy, select it from the list and click ✖ → **Delete**. You can delete a policy if no cards issued using this policy are registered in Axidian CertiFlow.

Link a policy

Configure policy links to centrally apply policies to objects or users.

You can apply policies to the following objects:

- **User catalog**: Domain, Container, Organizational Unit
- **Organization structure**: Domain, Container, Organizational Unit, users, or groups from the user catalog

For more information, see Organization structure

> ⓘ **INFO**
> You can apply a policy to an entire object (domain, container, or organizational unit) or to specific user groups within that object.
>
> Policies applied to the LDAP user catalog take precedence over policies applied to the Axidian CertiFlow Organization structure.

To assign a policy to an object:

1. In the Management Console side panel, go to **Configuration** → **Policy links**.

2. Click **Create policy link** and select the required policy from the **Policy** list.
3. Define the following parameters:
    - **Container** – The scope of the policy. A container can be an Organizational Unit from the user catalog or a node in the Axidian CertiFlow Organization Structure.
    - **Groups** – An optional filter for applying the policy. For example, multiple policies can be assigned to a single container containing organizational users. These policies apply only to users who belong to catalog groups within that container.
    - **Priority** – A value that determines which policy takes effect if a user falls under the scope of multiple policies at the same time (for example, when a user belongs to two groups located within the same Organizational Unit).
    - **Roles** – Local roles that are granted permissions to manage the policy.
4. Click **Create**.

Policy settings

PKI settings

2 items

Axidian Access

Configure integration with Axidian Access

Workflow

Configure the available operations for Axidian CertiFlow administrators, operators, and users

Issue

Configure card issue and initialization settings

Authentication

Configure security questions

Agents

Configure Axidian CertiFlow Agent parameters

Card printer

Configure integration with card printer

Notifications

Configure alerts about Axidian CertiFlow local events

PKI settings

In the PKI Settings section, you can define parameters for user logon to the operating system.

- **Import CA certificates**

  The root certificate or certificate chain of the Certification Authority (CA) is written to the card when it is issued. These certificates are not removed from the card when it is withdrawn from Axidian CertiFlow.

  > **INFO**
  > Make sure that the card supports writing the root certificate or certificate chain.

- **Enforce smart card logon**

  When a card is issued, the **Smart card is required for interactive logon** setting is applied to the user properties in the catalog.

  Prerequisites for the Enforce smart card logon option

  - The user catalog service account must have *Write:userAccountControl* permissions in Active Directory. For more information, see Active Directory user catalog configuration.
  - If you enable the **Smart card is required for interactive logon** option in the user's Active Directory profile, the user's domain password changes to a random value with an unlimited expiration date.
  - Before you enable the **Enforce smart card logon** option, ensure that the **Smartcard Logon** certificate template is added to the policy.

Integrate Axidian CertiFlow with a CA. You can add several CAs for a single policy or create multiple policies, each with its own designated CA.

Microsoft CA

Configure integration the Microsoft Ca

Common certificates

Add common certificates

Microsoft CA

Configure connection to Microsoft CA and create certificate templates.

Prerequisites

To allow access to the **Microsoft CA** section:

1. Launch the Axidian CertiFlow Configuration Wizard and go to **Certification authorities**.
2. Enable integration with Microsoft Enterprise CA.

Connect to a CA

Follow the instructions for the operating system of the workstation where the Axidian CertiFlow server is installed.

Windows

1. Click **Add CA**.
2. In the **Server address** field, specify the CA address if it was not detected automatically.
3. Enter the login in `DOMAIN\Username` format and the password of the service account holding the Enrollment Agent certificate.
4. Click **Add**.

> ⚠ **CAUTION**
> An Enrollment Agent certificate is required for Axidian CertiFlow to integrate with the CA. The user account holding the Enrollment Agent certificate is used to send certificate enrollment requests to the CA on behalf of Axidian CertiFlow users. You can change the user's credentials after you add the CA to Axidian CertiFlow.

Add a CA located outside the Axidian CertiFlow users domain

1. Click **Add CA**.
2. In the **Server address** field, specify the address of the Axidian CertiFlow MS CA Proxy application. If Axidian CertiFlow is deployed in a domain forest, using Axidian CertiFlow MSCA Proxy is optional.
3. In the **Username** field, enter the login in `DOMAIN\Username` format and the password of the service account holding the Enrollment Agent certificate.
4. Enable the **Issue certificates for users from external associated catalog** option.
5. Specify the path to the external user catalog in the **LDAP** field.

6. In the **Username** field, enter the login of a user with read permissions for all user properties in the external domain. You can use the account specified earlier.

   > **TIP**
   > To configure permissions to read only a specific set of properties, go to the **Permissions** list of the specified user profile and select the required properties.

7. In the **Catalogs associating attribute** field, specify the attribute that is used to determine the uniqueness of a user who has accounts in each domain. You can select one of the following attributes: Common name, Email, or Login (sAMAccountName).

Linux

1. Click **Add CA**.
2. In the **Server address** field, specify the address of the Axidian CertiFlow MS CA Proxy application.
3. In the **Client certificate** field, select a client authentication certificate to connect to Axidian CertiFlow MS CA Proxy.
4. Click **Add**.

Add a CA located outside the Axidian CertiFlow users domain

4. Enable the **Issue certificates for users from external associated catalog** option.
5. Specify the path to the external user catalog in the **LDAP** field.

3. In the **Username** field, enter the login of a user with read permissions for all user properties in the external domain.

   > **TIP**
   > To configure permissions to read only a specific set of properties, go to the **Permissions** list of the specified user profile and select the required properties.

4. In the **Catalogs associating attribute** field, specify the attribute that is used to determine the uniqueness of a user who has accounts in each domain. You can select one of the following attributes: Common name, Email, or Login (sAMAccountName).

Certificate templates

Before you configure certificate templates in Axidian CertiFlow, make sure that the required templates are configured and published in the CA. For more information, see CA certificate templates.

To create a certificate template:

1. Open policy settings and go to **Microsoft CA** → **Templates** section.
2. Click **Create certificate template**.
3. Configure the required parameters and click **Create**.

Parameter	Description
Name	Certificate template name
CA	CA name
Microsoft CA certificate template	Template is uploaded automatically from the connected CA
Key name prefix	If you do not specify a key name prefix, the name of the container with the key pair is generated automatically. If you specify a prefix, it is added in front of the container name. The prefix value is displayed in Axidian CertiFlow and in third-party software for managing private key containers.

Parameter	Description
Include in subject name	Specify the attributes to form the certificate Subject name: **Attribute list** • Fully distinguished name (default value) • Common name • First name • Last name • Initials • E-mail • Title • Organization unit • Organization • Street • Locality • State • Country To form the certificate's Subject and Subject Alternative Name from the attribute list, open the Microsoft CA template properties, go to the **Subject Name** tab and select **Supply in the request**.
Include in alternative subject name	Specify the attributes to form the certificate Subject Alternative Name: **Attribute list** • E-mail • Additional e-mail addresses • User principal name Configure the attribute for reading additional email addresses from the user catalog. The default attribute is `proxyAddresses`.
Backup key	When a key pair is generated on a card, its backup copy is saved on the Axidian CertiFlow server. A key pair copy can only be saved once. If this option is disabled, the key pair is generated on the card directly.
Copy backup key to temporary card	Certificate and private key copies are written to the card during a temporary replacement.

Parameter	Description
Reuse key	When certificates are renewed, the existing encryption key is reused.
Import certificate if exists	Axidian CertiFlow uses the certificate from the card instead of issuing a new certificate (for the specified user, CA, and template). If the card is initialized before issuance, the certificate is removed.
Do not remove certificate at card updating/cleaning	When a card is updated or cleared, the expiring or expired certificates are not removed from the card and the certificates are not revoked in the CA. When a card is updated, a new certificate with a new private key is requested and written to the card. If the **Reuse key** option is enabled, the expiring or expired certificates are removed from the card. New certificates with old private keys are written to the card. The expiring or expired certificates are removed if the card is withdrawn and initialized.
Revoke certificate at card revoking/disabling	Certificates are revoked when a card is disabled or revoked.
Install certificate to local store	When a card is issued or updated in the Self-Service, the certificates written to the card are added to the user's local certificate store.
Publish CRL	When cards are disabled, enabled, or revoked, the Certificate Revocation List (CRL) is published. This prevents users from signing documents with a revoked certificate. This option is available if the Microsoft CAservice account has the **Manage CA** permission.
Accept certificate request automatically	The certificate request is approved automatically. If this option is disabled, you must wait for the CA to approve the request.
Accept signed certificate renewal request automatically	The certificate renewal request is approved automatically. If this option is disabled, you must wait for the CA to approve the request to renew the certificate.

Parameter	Description
Require signed certificate document before continuing card issuing/updating	The certificate is written to the card after the user provides a signed certificate form to the administrator for verification. After the CA approves the request, the certificate form becomes available to the user in the Self-Service. The user can download the certificate form, sign and submit it for review.
Tracked user attributes	Specify user attributes that trigger a certificate renewal: Common Name, Email, or User Principal Name (UPN). Changing the e-mail causes the certificate renewal if this attribute is included in the Microsoft CA certificate template properties on the **Subject Name** tab of the **Include e-mail name in subject name** and **E-mail name** options.
Print templates	Upload the document templates in the **Configuration → Print templates** section. If there are no document templates, the default print templates are used.
Default	This certificate is used by default for logging in to third-party software.
Optional certificate	When a card is issued or updated, you can select which optional certificates to write to the card. If this option is disabled, certificates are written to the card by default.

Common certificates

A common certificate is issued by a third-party CA and shared among multiple users. Axidian CertiFlow allows you to write common certificates and their private keys to multiple users' cards at the same time.

You cannot suspend or revoke common certificates, but you can update them: delete the old PFX file and add a new one. Common certificates cannot be published to a user catalog, file storage, or user certificate store.

Add a common certificate

To add a common certificate to Axidian CertiFlow:

1. Open policy settings and go to **PKI settings** → **Common certificates**.
2. Click **Add common certificate** and select the required PFX file.
3. Enter the password to access file contents.
4. (Optional) To configure a permission to write common certificates to cards, enable the **Optional certificate** option.
   If the **Optional certificate** option is not enabled, the common certificate is considered mandatory and is written to the card during issuance or update.
5. Click **Add**.

Configure common certificates expiration alerts

To send notifications about common certificates expiration:

1. Open policy settings and go to **Notifications**.
2. Create a notification for the *Common certificates expiring* event.

Notifications are not sent for certificates that have already expired.

Axidian Access

Axidian CertiFlow features integration with Axidian Access.

The integration combines the following operations:

- Card issuance
- Certificate request
- Writing the certificate to the card
- Registration of the *SmartCard + PIN Provider* in Axidian Access

When you issue a card in Axidian CertiFlow, the *Smart card + PIN* authentication method is registered in Axidian Access, and a certificate is written to the card. The issued card can then be used for domain authentication, SSO access, digital signatures, and accessing resources using personal certificates.

When you revoke and withdraw a card, both the authenticator and the certificates stored on the card are deleted. Deactivating a card makes the authenticator inactive, while activating it makes the authenticator active again.

Prerequisites

To allow access to the **Axidian Access** section:

1. Launch the Axidian CertiFlow Configuration Wizard.
2. Go to **Common features**.
3. Activate the **Enable integration with Axidian Access** option.

Configure integration

Select the instructions based on your Axidian Access version.

Axidian Access 6

1. Install and configure the following Axidian Access components:
    - Axidian Administration Tools (or Axidian Admin Pack) on each Axidian CertiFlow server.
    - Axidian Extended Security Provider on each Axidian Access server.
    - Axidian Access Smart Card + PIN Provider on each Axidian Access server and on user workstations.

> **TIP**
> Axidian Administration Tools is included in the Axidian Access 6 installation package. To obtain the Axidian Extended Security Provider and Axidian Access Smart Card + PIN Provider components, contact Axidian technical support.

2. Configure the Extended Security Provider:

    1. Create the **Axidian Access Enrollment Admins** security group.
    2. Add the service account to the **Axidian Access User Admins** and **Axidian Access Enrollment Admins** security groups.

3. In the Axidian CertiFlow Management Console, open the **Configuration** section.

4. Open policy settings and go to **Axidian Access**.

5. Activate the **Enable integration with Axidian Access** option and select **Axidian Access 6**.

6. Configure the following parameters.

Parameter	Description
Use Axidian Access proxy server	Axidian CertiFlow connects to the Axidian Access proxy server, which forwards the request to the Axidian Access servers. Use a proxy server if the Axidian CertiFlow servers are located outside the domain where Axidian Access server is installed.
Proxy server address	The URL of the Axidian Access proxy server.
Username **Password**	The domain credentials for a user who is a member of both the **Axidian Access User Admins** and **Axidian Access Enrollment Admins** security groups.
Allow usage of Axidian Access Windows Logon	When you issue a card in Axidian CertiFlow, the user can authenticate to the domain using the Axidian Access Windows Logon provider.
Allow usage of Axidian Access Enterprise Single Sign-On	When you issue a card in Axidian CertiFlow, the user can authenticate to applications using the Axidian Access Enterprise Single Sign-On provider.
Generate Windows account random password	When you issue a card in Axidian CertiFlow, a random domain password is generated for the user. When the password expires, a new one is generated. The new password is saved in the Axidian Access database.

> **INFO**
> If the user's last registered authenticator is deleted, the permissions for using Axidian Access Windows Logon, Axidian Access Enterprise Single Sign-On, and random password generation are disabled.

Axidian Access 8.2

1. Install and configure the Axidian Access Smart Card + PIN Provider component on each Axidian Access server and on the user workstations.
2. In the Axidian CertiFlow Management Console, open the **Configuration** section.
3. Open policy settings and go to **Axidian Access**.
4. Activate the **Enable integration with Axidian Access** option and select **Axidian Access 8.2**.
5. In the **Server address** field, enter the address of the Axidian Access server. For example, `https://server.domain.loc/am/core`.
6. To connect to the Axidian Access server, enter the UPN of the user account (for example, admin@domain.loc) and its password.

   > **INFO**
   > Axidian CertiFlow and Axidian Access must be connected to the same user catalog.
   > The account must be a member of the Axidian Access local or global administrators group and have the following privileges:
   >
   > - *Register any authenticator*
   > - *Enable authenticator*
   > - *Disable authenticator*
   > - *Delete authenticator*

7. Click **Save**.

Axidian CertiFlow tests the connection to the Axidian Access server.

Workflow

In the **Workflow** section, you can define the available operations for administrators and operators in the Management Console and for users in the Self-Service.

General

Add cards automatically when they are issued or assigned	Cards are automatically registered in Axidian CertiFlow at the moment of issuance or assignment. If this option is disabled, you cannot issue or assign unregistered cards.
Allow user to add cards when they are issued	Users can issue unregistered cards. Cards are registered automatically during the issuance process.
Search for certificates when card is issued or updated to track validity period	When a card is issued or updated, Axidian CertiFlow checks for third-party certificates and private keys and registers the certificates to manage the validity period. For more information, see Tracked certificates.
Record tracked certificates in custom logs	Tracked certificates information is recorded in custom logs. This option is available if the **Custom logs** option is enabled in the **Common features** section of the Axidian CertiFlow Configuration Wizard.
Allow user to select tracked certificates	When a card is issued or updated in the Self-Service, users can select third-party certificates and record them in Axidian CertiFlow.

Administrator permissions

Reset user PIN	If a user forgets or locks their card PIN, you can reset it.
Unblock card offline	You can unlock a card in offline mode, even if there is no connection between the user's workstation and the Axidian CertiFlow server.

Validate answers to security questions	To unlock a card in offline mode, you must receive correct answers to the security questions from the user. For more information, see Offline unlock operation.
Cancel card update operation	If a user starts updating a card by mistake, you can cancel the update.

> **INFO**
> Make sure the role members have the privileges to cancel card updates, reset PINs, and unlock card. Configure these privileges in the **Configuration** → **Roles** section.

User permissions

General

Require to set answers to security questions when logging in to self-service	When users log in to the Self-Service, they must select security questions and set their answers. To authenticate in the Remote Self-Service, users must enter answers to security questions. If this option is disabled, the form for setting up security questions and answers is not displayed when users log in to the Self-Service. Users can configure security questions and answers at any time.
Change answers to security questions	Users can edit answers to security questions. If this option is disabled, users cannot edit answers to security questions. You can reset answers to security questions for users to set them again.
Issue AirCard	Users can issue AirCard virtual smart cards. Issuing AirCard cards is possible if you configured integration with Axidian AirCard Enterprise.

Card issuing operations

Assign	When users issues cards in a *Clean* status, cards are automatically assigned. If this option is disabled and a card is not assigned to a user, they cannot issue cards in the Self-Service.
Select optional certificates when card is issued	When users issue cards, a list of templates for optional certificates is displayed. Users can select which certificates to write to the card. In the **Message text** field, you can specify a warning message.

Issued card operations

View contents	Users can view the **Contents** tab in the card menu, displaying all certificates stored on the card.
Update	Users can update certificates stored on the card if their validity has expired or is about to expire.
Select optional certificates when card is updated	When users update cards, a list of templates for optional certificates is displayed. Users can select which certificates to add or remove. In the **Message text** field, you can specify a warning message.
Reset user PINs	If users forget or lock their card PINs, they can reset PINs.
Enable	Users can enable cards, if cards were disabled.
Disable	Users can disable cards to temporarily block access to them.
Revoke	Users can revoke cards if they are damaged, lost or compromised.

Clear	After a card is revoked, the **Clear card** option is in the card menu. Users can clear cards. After a card is cleared, it remains assigned to the user.

Document operations

Delete	Users can delete documents in the **Your documents** section in the Self-Service.

Issue

In the **Issuance** section, you can configure the card issue and initialization settings.

Card issue

Option	Description
Maximum number of cards per user	A number that limits the number of cards a user can have. The default value is 1.
Initialize card	The card is initialized before it is issued. All data stored on the card is erased. During the card issue process, you can enable or disable initialization for a specific card.

Set random user PIN	A random user PIN is generated during the card issue process.
	The random PIN is generated using non-repeating characters.
	
	Configure the **User PIN generation settings.**
	
	▼ **User PIN generation settings**
	
	1. Select at least one character group to be used in PIN generation:
	  ◦ Numeric characters
	  ◦ Uppercase letters
	  ◦ Lowercase letters
	  ◦ Special characters
	2. (Optionally) Specify up to 16 forbidden characters.
	3. Set the PIN length. The minimum length is 4 characters, the maximum – 31. The maximum PIN length also depends on the selected character groups.
	4. To allow an administrator to view the card PIN in the Management Console, enable the **Show generated user PIN to administrator** option.
	5. To allow a user to view the card PIN in the Self-Service, enable the **Show generated user PIN to user** option.
	
	You can send the random user PIN to the user or their manager in an email notification.

User PIN must be changed on first logon	When a user connects a card to their workstation for the first time, the user is prompted to change the card PIN. This option is only supported for eToken and IDPrime cards.

Option	Description
Lock card	The card is locked after it is issued. Before the user can manage the card, they are prompted to unlock it and set a new PIN.
Generate card name automatically	The card name can be set using one of the user's attributes – Common name, Logon name, Last name, E-mail, Organizational unit, or a specified string. The selected value is automatically inserted into the card name field. If the **Allow editing card name** option is active, the user can change the card name before the card is issued.
Require a comment to the card	When you issue a card in the Management Console, you must enter a comment.
Require tags to the card	When you issue a card in the Management Console, you must assign tags to the card.

> ⚠ **CAUTION**
> The following options are mutually exclusive:
>
> - **Lock card** and **Set random user PIN**
> - **Lock card** and **User PIN must be changed on first logon**

Card initialization

The set of initialization parameters depends on the card type. If you have not configured initialization parameters in the policy, Axidian CertiFlow applies the default parameters from the Card type settings.

Axidian CertiFlow applies the PIN complexity policies when you issue and initialize a card, and stores the policies on the card until the next initialization.

To set card initialization parameters:

1. Go to **Issuance** → **Card initialization** and click **Add initialization parameters**.
2. Select the card type and click **OK**.
3. Configure the initialization parameters.
4. Click **Add**.

> ⓘ **INFO**
> If you specify the different PIN length values in the **Issuance** and **Card initialization** sections, Axidian CertiFlow applies the larger value when you issue the card.

Supported card types

By default, you can issue all types of cards registered in Axidian CertiFlow.

To define a policy for issuing cards of a specific type:

1. Go to **Issuance** → **Allowed cards**.
2. Click **Add card type**, select the card type name, and click **Add**.

The number of supported card types is not limited. To remove a card type from the allowed list, click ✖ .

Authentication

In the **Authentication** section, you can configure the following user authentication settings:

- **Number of questions to ask**
  Determines how many questions a user must answer to complete authentication. The default value is 1.
- **Maximum authentication retry count**
  Determines the number of authentication attempts before the user is blocked. The default value is 3.

Security questions

Users can authenticate using security questions in the following cases:

- Card unlock
- Disabling a card without performing an OS login
- Accessing the Remote Self-Service
- Executing the Reset user PIN task on a client agent

To create a security question:

1. In the Axidian CertiFlow Management Console, go to **Configuration** and open policy settings.
2. Go to **Authentication** → **Security questions** and click **Create security question**.
3. Enter the question.
4. Set the minimum answer length. The default value is 3 characters.
5. Click **Create**.

> **INFO**
> If you have not created security questions, users cannot set answers to them in the Self-Service.

Agents

The Axidian CertiFlow Client Agent allows you to control cards on user workstations.

In the **Agents** section, you can configure card usage settings, specify messages for users when the agent completes a task, define available automatic operations, and set administrator PINs for different card types.

Control card usage

Parameter	Description
The action to be taken when the bound card and agent do not match	Select the action the agent performs if a user connects a card to a workstation not approved by the administrator. • Write event • Lock user session, write event • Lock card, write event • Lock user session and card, write event
Message to the user when the bound card and agent do not match	Enter the message the user receives when they connect a card to a workstation not approved by the administrator.
Enable user card binding	When the user connects a card to a workstation, the agent verifies whether the card is assigned to the user.
The action to be taken when the bound card and user do not match	Select the action the agent performs if a user connects a card to a workstation in another user's session. • Write event • Lock user session, write event • Lock card, write event • Lock user session and card, write event
Message to the user when the bound card and user do not match	Enter the message the user receives when they connect a card to a workstation in another user's session.
Timeout before locking the user session (sec.)	Define the time delay before the user session is locked, if session locking is the selected action for card usage policy violations. The allowed range is 0 to 5 seconds.

User messages

The agent can notify users about the following card operations:

- Locking a card
- Changing the administrator PIN
- Cleaning a card
- Detecting an unregistered card

By default, messages are not displayed to the user. To send a notification to the user, enter text in the **User messages** section. When the user connects the card to a workstation, the message appears in a pop-up window.

Workflow

Configure the settings that define the operations available to agents installed on user workstations. For more information, see Agent automatic operations

Administrator PINs

Set administrator PINs for the supported card types. When you add a card to Axidian CertiFlow, the agent uses the value specified for its card type as the current administrator PIN.

To add an administrator PIN:

1. Click **Add administrator PIN**.
2. Select the card type and click **OK**.
3. Enter a value in the **Administrator PIN** field.
4. Click **Add**.

Card printer

Integrating Axidian CertiFlow with the EDIsecure XID 8300 printer enables the following scenarios:

- Issuing cards to users using the printer's readers without printing cards
- Issuing cards to users using the printer's readers with an image or text printed on cards
- Printing an image or text on cards without issuing them to users

You can configure the following card printer settings:

Enable card printer support	When you issue a card, you can choose between the workstation reader and the printer's built-in reader to connect a card.
Read RFID tag of card	Axidian CertiFlow reads the card's tag and saves it to the storage, associating it with the user. When the card is revoked, the tag value remains in Axidian CertiFlow storage as long as the card is registered. When the card is issued to another user, the tag value is assigned to them.
Enable card printing	When you issue a card using a printer, an image or text is printed on it according to the uploaded print template.

To upload a print template:

1. Go to **Card printer** → **Card design template**and click **Load card design template**.
2. Select the XML file and click **Load**.

To obtain a print template file, contact Axidian technical support.

Notifications

In the **Notifications** section of the policy settings, you can configure email notifications to administrators and users about local events related to the policy.

To configure notifications:

1. Set up the mail server.
2. Define notification recipient groups.
3. Create event notifications.
4. (Optional) Configure a custom notification template for each event.

Mail server

Configure the mail server for local notifications:

1. Go to policy settings and open the **Notifications** → **Mail Server** section.
2. To use global mail server settings, select **Use global settings**.
   To use local mail server settings, select **Specify the mail server settings**, specify the mail server settings and click **Save**.
3. Click **Send test e-mail** to verify the mail server's operation.
4. Enter the recipient's email address and click **Send**.

If you have not received a test message, check the mail server settings and send the message again.

Recipient groups

Configure notification recipient groups.

For global administrators, you can select global recipient groups configured in **Configuration** → **Notifications** → Recipient Groups. For local administrators, you can create separate recipient groups for notifications about events related to a specific policy.

To add a recipient group:

1. Click **Create group**.
2. Enter the group name and the recipient email addresses.
3. Click **Create**.

You can edit or delete recipient groups.

> ⚠ **CAUTION**
> You can only delete a recipient group if it is not currently used for sending notifications.

Administrator notifications

Configure email notifications for Axidian CertiFlow administrators:

1. Click **Create notification**.
2. Select an event and specify the **Event type**: Information, Error, or Warning.
3. Select recipients:
   - **Recipient group** – a group created in the **Recipient Groups** section.
   - **Security group** – an Active Directory security group.
4. Click **Create**.

Repeat interval (days)

In the **Repeat interval (days)** field, you can specify the time interval before a notification is sent again.

This field is available for the following events:

- User attributes changed
- Common certificates expiring
- Accept card issuing
- Accept card replacing
- Accept card updating
- Deny card issuing
- Deny card replacing
- Deny card updating
- Traced certificates expiring
- Policy updated
- Changing policy
- Managed certificates expiring

User notifications

Configure email notifications for Axidian CertiFlow users. Ensure that an email address is specified in the catalog profile for each user account.

1. Select **Create notification**.

2. Select an event and specify the **Event type**: Information, Error, or Warning.
3. To send a copy of the notification to the user's manager, enable the **Send copy to manager** option. The manager's email address is specified on the **Organization** tab of the user's catalog profile under **Manager**.
4. Click **Create**.

Repeat interval (days)

In the **Repeat interval (days)** field, you can specify the time interval before a notification is sent again.

This field is available for the following events:

- User attributes changed
- Common certificates expiring
- Accept card issuing
- Accept card replacing
- Accept card updating
- Deny card issuing
- Deny card replacing
- Deny card updating
- Traced certificates expiring
- Policy updated
- Changing policy
- Managed certificates expiring

Notification templates

In the **Administrator Templates** and **User Templates** sections, you can configure email notification templates. Use the default templates or edit them to create customized notifications.

A set of objects with parameters is embedded into the default template for each event. Axidian CertiFlow inserts these parameter values into the notification text. You can only use parameters that are built in the template in the notification text; you cannot add new ones. You can remove parameters you do not need.

To customize a notification, make your edits and click **Save**. To revert to the default template, click **Reset**.

Licenses

For more information about the Axidian CertiFlow license types, see Licensing.

Get a license

1. Open the Management Console at `https://<Server FQDN>/certiflow/mc` and go to **Configuration** → **Licenses**.
2. Copy the value from the **System identifier** field and send it to your Axidian representative or to Axidian technical support.

> **INFO**
> System identifier is a unique code generated from the file paths of the Axidian CertiFlow user catalogs. If a catalog has been moved, all licenses are no longer valid. Contact Axidian technical support to get a new license.

Add a license

1. Open the Management Console and go to **Configuration** → **Licenses**.
2. Click **Add license**, upload the license file and click **Add**.

Remove a license

1. Open the Management Console and go to **Configuration** → **Licenses**.
2. Click ✖ next to the license.

Card types

Supported card types include USB tokens, smart cards, and hybrid cards.

In the **Card types** section, you can configure the following settings for each card type:

- Administrator and user PIN values
- A new administrator PIN value to be set on a card when the card is added to Axidian CertiFlow
- Card initialization settings
- Card model parameters

If your organization adopts a new type of card or stops using a previously supported one, update the card type settings in Axidian CertiFlow.

Add a card type

1. Open the Management Console and go to **Configuration** → **Card types**.
2. Click **Add card type**, upload the card type file.
3. (Optional) To replace an existing card type file, enable the **Replace existing** option.
4. Click **Add**.

> **TIP**
> You can find the configuration files for different card types in the *\Misc\CardTypes* catalog of the Axidian CertiFlow server installation package.

Card types and models

Manufacturer	Card model	Card type file
ACS	ACOS5-64	Acos5-64.xml
Avest	Avest Key 256A	AvestKey-256-A.xml
Axidian	AirCard Virtual Smart Card	AirCard.xml
Bit4id	ID-One Cosmo	Bit4Id.xml
CRYPTAS	TicTok V2	TicTok_v2.xml
	TicTok V3	TicTok_v3.xml
Cryptovision	ePasslet Suite v3.0, JCOP V3.0	cv-ePassletSuite3.0-JCOP3.0.xml
Feitian	ePass2003 (A1+, A2) BioPass2003	ePass2003.xml
HID	Crescendo C1150 Series	CrescendoC1150.xml
	Crescendo C1300 Series	CrescendoC1300.xml
	Crescendo C2300 Series	CrescendoC2300.xml
Microsoft	Local Computer Certificate Store User Certificate Store	Registry.xml
	TPM Virtual Smart Card (Microsoft VSC)	Tpm.xml
	Windows Hello for Business (WHfB)	Whfb.xml
RSA	RSA SecurID 800	RSASecurID.xml

Manufacturer	Card model	Card type file
Thales Group	SafeNet eToken PRO 32k	eTokenPro32K.xml
	SafeNet eToken PRO 64k	eTokenPro4.2B.xml
	SafeNet eToken PRO Java 72K OS755 IDCore30B eToken 1.7.7	eTokenProJava72K.xml
	SafeNet eToken 5300 SafeNet eToken Fusion SafeNet eToken Fusion CC	eToken 5300.xml
	IDPrime MD 830 FIPS IDPrime MD 830B FIPS IDPrime MD 840B IDPrime 940 IDPrime 940B IDPrime MD 3810 IDPrime MD 3811 IDPrime 3930 IDPrime 3940	IDPrimeMD T=0.xml
	SafeNet eToken 5110 CC (940)	IDPrimeMD T=1.xml
	IDPrime 930 IDPrime 930nc	IDPrimeMD v2 T=0.xml
	IDPrime 3940 FIDO	IDPrimeMD Fido T=1.xml
Yubico	YubiKey 5 Series	YubiKey5.xml

Delete a card type

1. Open the Management Console and go to **Configuration** → **Card types**.
2. Click ✖ next to the required card type.

You can delete a card type only if no cards of that type are currently registered in Axidian CertiFlow.

Edit a card type

1. Open the Management Console and go to **Configuration** → **Card types**.
2. Click  next to the required card type.

The card type configuration file contains the default administrator and user PIN values.

> **INFO**
>
> - When you delete a card from Axidian CertiFlow, the administrator PIN is reset to the value specified in this file.
> - When you withdraw a card from a user, the user PIN is reset to the value specified in this file.

When you edit a card type, you can do the following:

- View and modify the administrator and user PIN values
- Specify initialization and PIN configuration parameters, which manage the issue process for cards of this type.

View and change administrator and user PINs

To view the current administrator and user PIN values, click  . To change the PIN values, enter the new values and click **Save**.

Configure card registration parameters

You can configure how cards are registered in Axidian CertiFlow by setting the following parameters:

Initialize card while adding

When you add a card, Axidian CertiFlow performs the following actions:

- Clears the card — all certificates added through Axidian CertiFlow are removed.
- Changes the card name to *Empty*.
- Changes theadministrator PIN to a random value written only in Axidian CertiFlow, or to the value specified in the **Set a non-random administrator PIN** option.
- Sets the administrator PIN entry limit to 3 attempts before the PIN is blocked.
- Changes the user PIN, its minimum length, and its entry limit before blocking to the values specified in the card type file.

> **INFO**
> The eToken cards support initialization with any state and any administrator PIN value.

Set non-random administrator PIN

When you add a card, Axidian CertiFlow changes the administrator PIN to the value specified in the **Set non-random administrator PIN** field.

If the option is disabled, Axidian CertiFlow changes the administrator PIN to a random value written only in Axidian CertiFlow.

Specify card model settings

You can configure specific parameters for adding different models od cards. This feature is supported for eToken PRO Java 72K and IDPrime MD.

> **INFO**
> - If the card model is not found or if model-specific settings are not configured, the card is added using the default settings.
> - If your company uses card models not listed in the system requirements, contact Axidian technical support.

To add card model settings:

1. Select the required card type from the list and click ✎.

2. Click **Add model settings** at the bottom of the editing window.
3. Select the required model from the list and click **Add**.
4. Configure the initialization and PIN parameters, and click **Save**.

Organization structure

You can issue cards according to the defined rules. These rules are configured in card usage policies, which are applied to a specified node (set of objects). The policy node is a user catalog object, such as an Active Directory domain organizational unit.

The organization structure feature allows you to consolidate different user catalog objects under a single card usage policy.

Prerequisites

To allow access to organization structure management:

1. Launch the Axidian CertiFlow Configuration Wizard and go to **Common features**.
2. Activate the **Organization structure** option.
3. Open the Management Console and navigate to **Configuration** → **Roles**.
4. Grant role members the privileges for working with the organization structure:
    - *Viewing the organization structure*
    - *Editing the organization structure*

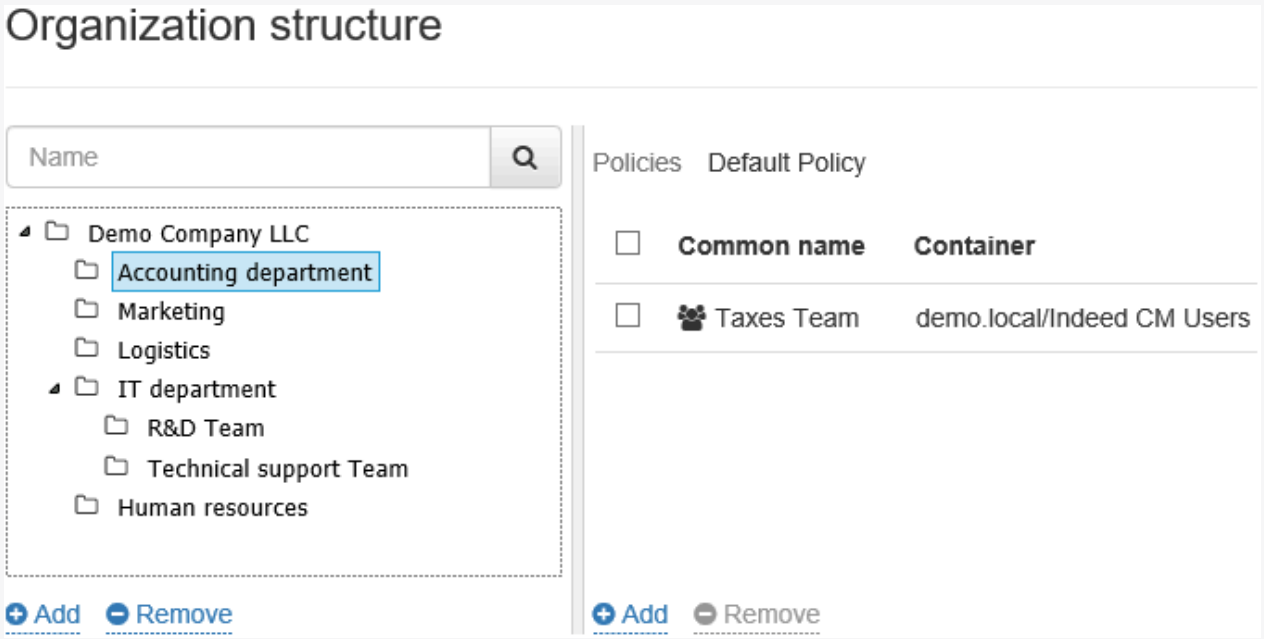
Manage organization structure objects

You can manage organization structure objects in **Configuration** → Organization structure**.

To add a new node, click **Add** and enter the node name. To delete a node, select it in the nodes list and click **Remove**.

To add objects to a node, select **Add** in the right pane of the organization structure editing window. The structure is built using user catalog objects.

Example


Organization structure
Name
Demo Company LLC
Accounting department
Marketing
Logistics
IT department
R&D Team
Technical support Team
Human resources
Add
Remove
Policies
Default Policy
Common name
Container
Taxes Team
demo.local/Indeed CM Users
Add
Remove

Roles

The role-based model in Axidian CertiFlow provides flexible control over administrator and operator access to Management Console features. Each role is assigned a set of privileges that determine which actions its members can perform.

You can configure roles and privileges in **Configuration** → **Roles**. Until you assign the roles, all actions are prohibited.

Prerequisites

During the initial setup of Axidian CertiFlow, access to the Management Console is granted only to a dedicated role administrator account. You can specify the role administrator in the Axidian CertiFlow Configuration Wizard (**Access Control** → Role Administrator).

> **INFO**
> The role administrator account must have a User Principal Name (UPN) attribute and be a member of the user catalog.

To perform the initial access rights configuration, use the role administrator account to grant Axidian CertiFlow management rights to other users:

1. Log in to the Management Console under the role administrator account.
2. Go to **Configuration** → **Roles**.
3. Click  next to the *Administrator* role.
4. In the **Role membership** list, select **Add**.
5. Add all users who require full access to Management Console features, including role management. Select:
   - **Group** to add a user group. In the search bar, enter the group's **Common Name** to find it.
   - **User** to add a specific user. In the search bar, enter the user's **Common Name** or **Login** to find them.
6. Click **Save**.

All users with the *Administrator* role can create new roles, assign privileges, and add users to roles.

Default roles

Axidian CertiFlow includes the *Administrator** and* Operator** roles by default.

Administrator	• Maximum set of privileges • Access to all sections This role is intended for specialists responsible for the configuration and operation of Axidian CertiFlow
Operator	• Limited set of privileges • No access to modify settings in the **Configuration** section This role is intended for specialists responsible for managing Axidian CertiFlow objects

Privileges

Privilege	Administrator	Operator
User		
Finding users	✓	✓
Viewing user	✓	✓
Unlocking user	✓	✓
Resetting security questions	✓	✓
Setting photo	✓	✓
Resetting user password	✓	✓
Assigning CA user	✓	✓
Configuration		
Viewing policy	✓	✗
Creating policy	✓	✗
Changing policy	✓	✗
Removing policy	✓	✗
Viewing policy link	✓	✗
Creating policy link	✓	✗
Changing policy link	✓	✗

Privilege	Administrator	Operator
Removing policy link	✓	✗
Viewing license	✓	✗
Adding license	✓	✗
Removing license	✓	✗
Viewing card type	✓	✗
Adding card type	✓	✗
Changing card type	✓	✗
Removing card type	✓	✗
Viewing role	✓	✗
Creating role	✓	✗
Changing role	✓	✗
Removing role	✓	✗
Viewing tag	✓	✗
Creating tag	✓	✗
Changing tag	✓	✗
Removing tag	✓	✗
Viewing print template	✓	✗

Privilege	Administrator	Operator
Adding print template	✓	✗
Changing print template	✓	✗
Removing print template	✓	✗
Viewing mail server settings	✓	✗
Changing mail server settings	✓	✗
Viewing recipient groups	✓	✗
Creating recipient groups	✓	✗
Changing recipient groups	✓	✗
Removing recipient groups	✓	✗
Viewing administrator notifications	✓	✗
Creating administrator notifications	✓	✗
Changing administrator notifications	✓	✗
Removing administrator notifications	✓	✗
Viewing administrator templates	✓	✗
Changing administrator templates	✓	✗
Viewing custom log dictionary	✓	✗
Creating custom log dictionary	✓	✗

Privilege	Administrator	Operator
Changing custom log dictionary	✓	✗
Removing custom log dictionary	✓	✗
Viewing custom log template	✓	✗
Creating custom log template	✓	✗
Changing custom log template	✓	✗
Removing custom log template	✓	✗
Event log		
Viewing event log	✓	✓
Dashboard		✓
Viewing dashboard	✓	✓
Card		
Viewing card repository	✓	✓
Viewing card details	✓	✓
Adding card	✓	✓
Changing comment	✓	✓
Changing tags	✓	✓
Showing administrator PIN	✓	✗

Privilege	Administrator	Operator
Changing administrator PIN	✓	✗
Setting administrator PIN	✓	✗
Initializing card	✓	✓
Assigning card	✓	✓
Issuing card	✓	✓
Enabling card	✓	✓
Disabling card	✓	✓
Updating card	✓	✓
Canceling card updating	✓	✓
Replacing card	✓	✓
Resetting PIN	✓	✗
Changing PIN	✓	✗
Locking card	✓	✗
Unlocking card	✓	✓
Printing card	✓	✓
Revoking card	✓	✓
Cleaning card	✓	✓

Privilege	Administrator	Operator
Unassigning card	✓	✓
Removing card	✓	✓
Certificates		
Viewing certificate repository	✓	✓
AirCard		
Change AirCard bindings	✓	✓
Removing AirCard	✓	✓
Agents		
Viewing agent repository	✓	✓
Changing agent card bindings	✓	✓
Updating agent status	✓	✓
Removing agent	✓	✗
Updating agent name	✓	✓
Updating agent comment	✓	✓
Removing task	✓	✓
Documents		
Viewing document repository	✓	✓

Privilege	Administrator	Operator
Adding document	✓	✓
Changing document	✓	✓
Removing document	✓	✓
Approving document	✓	✓
Custom logs		
Viewing custom log	✓	✓
Adding record to custom log	✓	✓
Changing record in custom log	✓	✓
Removing record from custom log	✓	✓

Role types

Global	Permissions apply to all card usage policies.
Local	Permissions apply only to the specific policies to which this role is bound. Members of a local role can manage only those users who fall under the scope of its assigned policies.

> **INFO**
> You cannot change a role's type after it has been created.

Create a role

Global

To create a global role:

1. In the **Roles** section, click **Create role**.

2. Specify the role's name.
3. Select the **Global** role type.
4. To add role members, select **Add** in the **Role Membership** parameter.
5. Select one the options:

- **Group** to add a user group. In the search bar, enter the group's **Common Name** to find it.
- **User** to add a specific user. In the search bar, enter the user's **Common Name** or **Login** to find them.

6. Click **Save**.
7. Assign privileges to the role members.
8. Click **Create**.

Local

To create a local role:

1. In the **Roles** section, select **Create role**.
2. Specify the role's name.
3. Select the **Local** role type.
4. Assign privileges to the role members.
5. Click **Create**.
6. To add role members, go to **Configuration** → **Policy Assignments**.
7. Click  next to the required policy.
8. In the **Roles** parameter, click **Add role**.
9. Select the local role you created and click **Add**.
10. Click **Save**.

For more information, see Policy assignment.

Card Monitor service role

To run the Card Monitor service, create a dedicated service role containing the account used by the service, and grant it the following privileges:

- *Disabling card*
- *Updating card*
- *Canceling card updating*
- *Revoking card*

- *Cleaning card*
- *Unassigning card*
- *Removing card*
- *Removing agent*
- *Removing task*
- *Removing record from custom log*

If Axidian CertiFlow is integrated with Axidian AirCard Enterprise, assign the *Deleting AirCard* privilege.

Tags

You can use tags for more flexible card management.

To create a tag:

1. Open the Management Console and go to **Configuration** → **Tags**.
2. Click **Create Tag**, specify a name, and click **Create**.

You can assign tags to a card during the following operations:

- Bulk card registration
- Card issue
- Viewing card contents
- Editing tags in the **Cards** section
- Managing a user's profile

Tags can help you find cards in the Management Console (**Cards** → Advanced search).

Print templates

You can use print templates to populate and print certificate requests, certificate forms, and user documents.

Add a print template

1. Open the Management Console and go to **Configuration** → **Print templates**.
2. Click **Add print template**.
3. Enter the template name in the **Name** field.
4. Select the document type:
   - **Certificate** – for certificate requests, certificate forms, and certificate revocation requests.
   - **User** – for user documents.
5. Upload the print template file.
6. Click **Add**.

> **INFO**
> Axidian CertiFlow supports only XSL-format templates .
> You can upload the print templates in policy settings (**PKI settings** → **Templates**).

You can edit or delete templates.

Edit default print template files

You can edit the files of the default print templates.

The print template files are stored in the following catalogs for each service.

Print templates for the Management Console

`C:\inetpub\wwwroot\certiflow\mc\wwwroot\content\request\_ru.xsl` – certificate request print template.
`C:\inetpub\wwwroot\certiflow\mc\wwwroot\content\cert\_ru.xsl` – certificate form print template.
`C:\inetpub\wwwroot\certiflow\mc\wwwroot\content\revocationRequest\_ru.xsl` – certificate revocation request print template.

Print templates for the Self-Service

`C:\inetpub\wwwroot\certiflow\ss\wwwroot\content\request\_ru.xsl` – certificate request print template.
`C:\inetpub\wwwroot\certiflow\ss\wwwroot\content\cert\_ru.xsl` – certificate form print template.
`C:\inetpub\wwwroot\certiflow\ss\wwwroot\content\revocationRequest\_ru.xsl` – certificate revocation request print template.

You can use different print templates in each card usage policy:

1. Edit the templates and upload the templates files in **Configuration** → **Print Templates**.
2. Go to policy settings and open the **PKI settings** → **Templates** section.
3. Click **Create certificate Template**.
4. Select the uploaded templates.

Notifications

In the **Configuration** → **Notifications** section, you can configure email notifications for Axidian CertiFlow administrators and operations about the following global events:

- *All licenses consumed*
- *Connection an unregistered card*
- *Running out of available licenses*
- *Software license expired*
- *Software license expires soon*

> **INFO**
> You can specify separate notification settings for administrators and users regarding events related to a specific policy (local events). Configure local notification settings in policy settings (**Notifications**).

To configure notifications:

1. Set up the mail server.
2. Define notification recipient groups.
3. Create event notifications.
4. (Optional) Configure a custom notification template for each event.

Prerequisites

Go to **Configuration** → **Roles** and grant role members the privileges to manage notification settings.

Privileges

- Viewing mail server settings
- Changing mail server settings
- Viewing recipient groups
- Adding recipient groups
- Changing recipient groups
- Removing recipient groups
- Viewing administrator notifications
- Adding administrator notifications
- Changing administrator notifications
- Removing administrator notifications
- Viewing administrator templates
- Changing administrator templates

Mail server

Configure the mail server for sending notifications:

1. Go to **Configuration** → **Notifications** → **Mail Server**.
2. Specify the mail server settings and click **Save**.
3. Click **Send test e-mail** to verify the mail server's operation.
4. Enter the recipient's email address and click **Send**.

If you have not received a test message, check the mail server settings and send the message again.

Recipient groups

Configure notification recipient groups.

To add a recipient group:

1. Click **Create group**.
2. Enter the group name and the recipient email addresses.
3. Click **Create**.

You can edit or delete recipient groups.

> ⚠ **CAUTION**
> You can only delete a recipient group if it is not currently used for sending notifications.

Administrator notifications

Configure email notifications for Axidian CertiFlow administrators:

1. Click **Create notification**.
2. Select an event and specify the **Event type**: Information, Error, or Warning.
3. Select recipients:
   - **Recipient group** – a group created in the **Recipient Groups** section.
   - **Security group** – an Active Directory security group.
4. Click **Create**.

Notification templates

In the **Administrator Templates** section, you can configure email notification templates. Use the default templates or edit them to customize notifications.

A set of objects with parameters is embedded into the default template for each event. Axidian CertiFlow inserts these parameter values into the notification text. You can only use parameters that are built in the template in the notification text; you cannot add new ones. You can remove parameters you do not need.

For example, the *License expired* notification template contains an embedded `licenses` object with the `licenseType`, `licenseCount`, and `validTo` parameters.

To customize a notification, make your edits and click **Save**. To revert to the base template, click **Reset**.

Custom logs

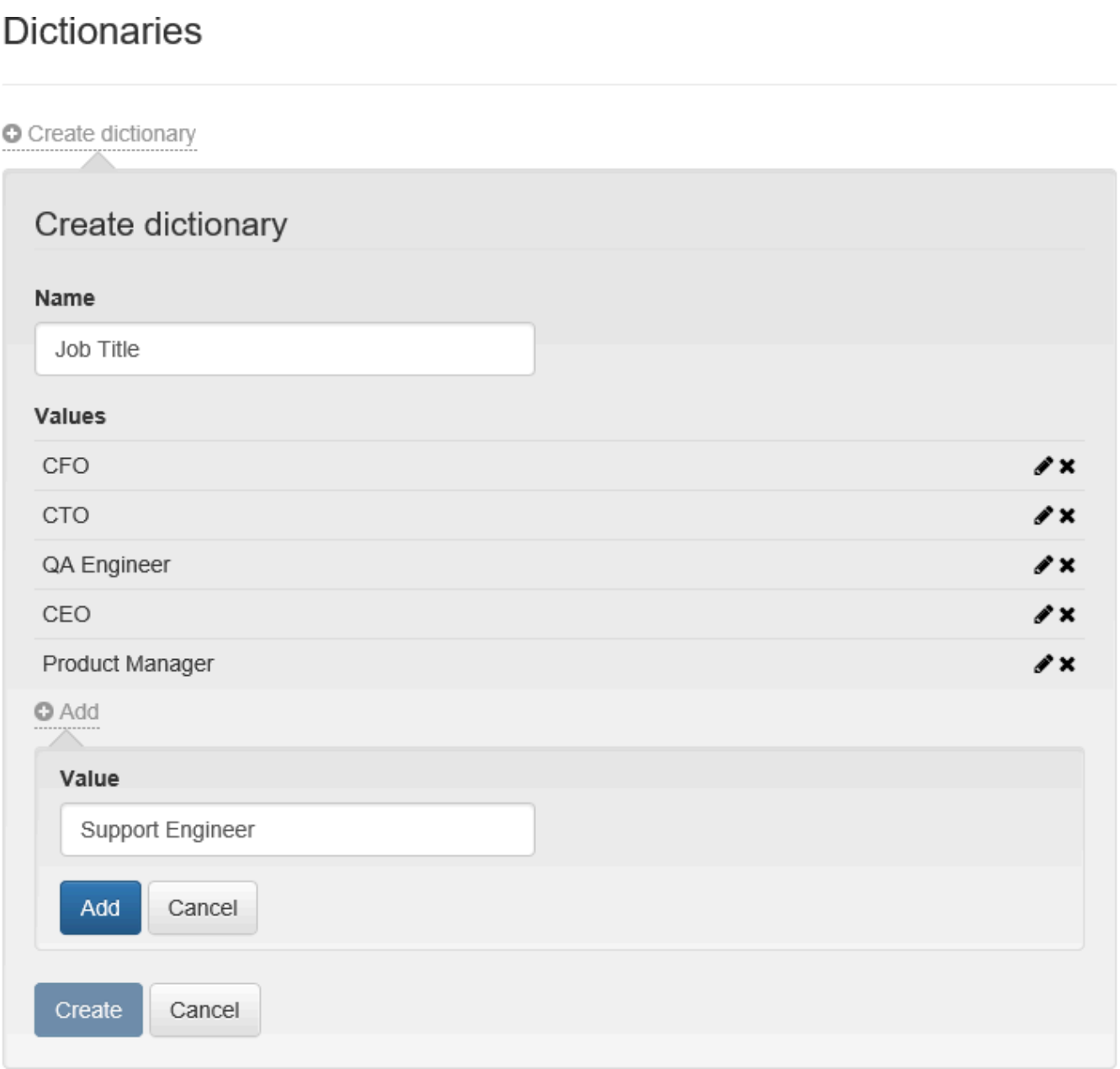
In the **Configuration** → **Custom logs** section, you can configure dictionaries and custom log templates.

Dictionaries

A dictionary is a list of predefined values that you can select when you populate a field in **Custom logs**.

To create a dictionary:

1. Click **Create dictionary**.
2. Specify the dictionary's name, add values, and click **Create**.



To edit a dictionary and its values, select . To delete a dictionary, select .

> **INFO**
> You cannot delete a dictionary or a value that is currently in use.

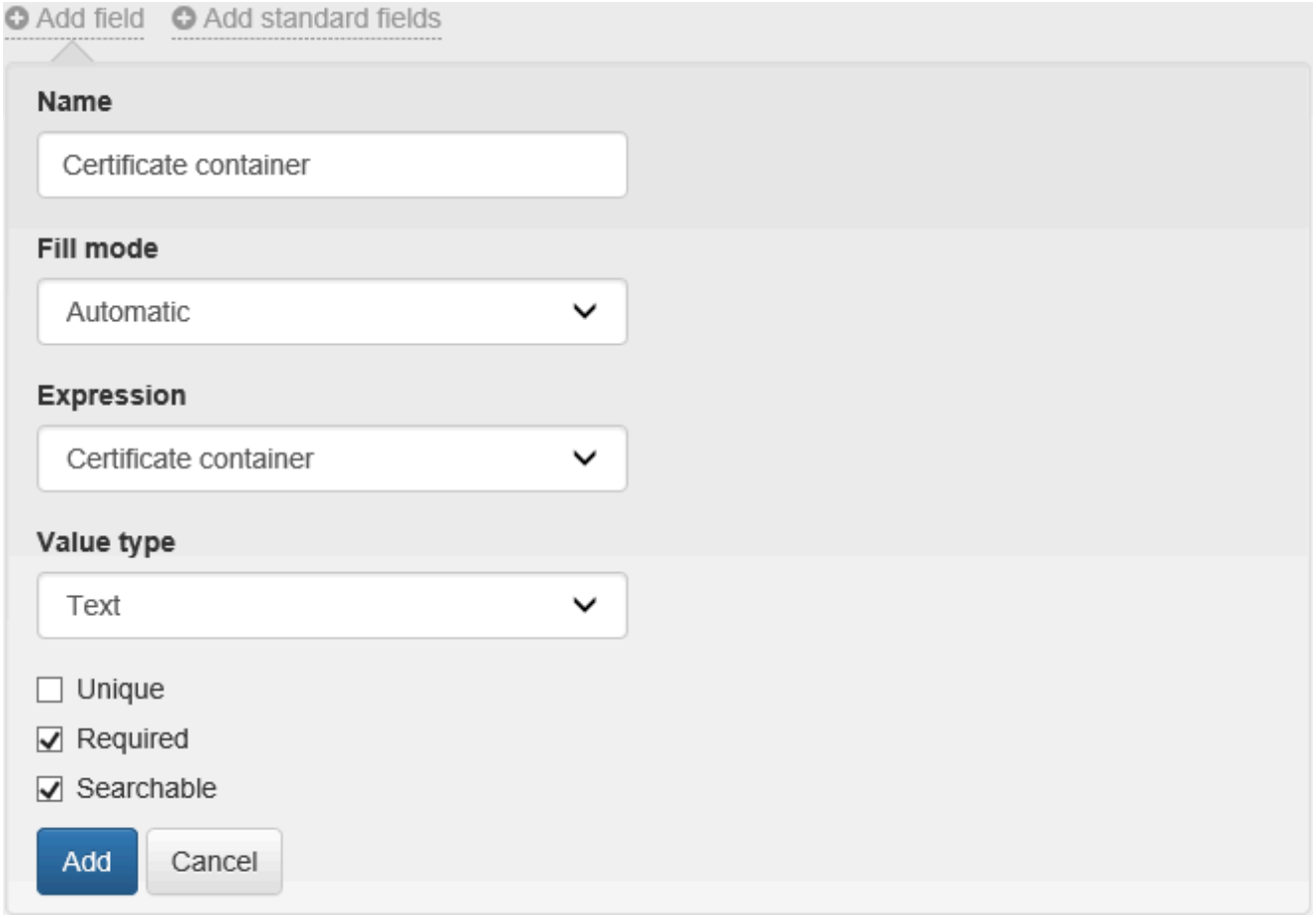
Log templates

A custom log is a set of fields containing data about cards, certificates, and users.

To create an custom log template:

1. Click **Create log template**.
2. Specify the template's name.
3. From the **Objects type** list, select **Card**, **Certificate**, or **Custom**.
4. Select the applicable policies.
5. Select **Add field** or **Add standard fields** for the **Card** and **Certificate** object types. A field is a log column containing information about a card or certificate.
6. Specify the field name.
7. From the **Fill mode** list, select:
   - **Manual**
   - **Automatic**: Select a suitable expression from the **Expression** list for the selected log type.
   - **Dictionary**: Select a dictionary from the list.
8. From the **Value type** list, select **Text** or **Date**.
9. Configure the field parameters:
   - **Unique**: If the field contains unique values.
   - **Required**: This field is required.
   - **Search**: Create a filter in the **Custom logs** section of the Management Console.
10. Click **Add** and **Create** to save the template.

> **INFO**
> - For **Object Type: Card**, the **Card serial number** field is mandatory and unique.
> - For **Object Type: Certificate**, the **Certificate serial number** and **Card serial number** fields are mandatory. These fields are not unique because a single card can store multiple certificates, or a common certificate can be written to different cards.
> - When you edit a field, you can only change its name and the set of parameters: **Unique**, **Required**, **Search**.



To edit a log template, click . To delete a log template, click .

> ⚠ **CAUTION**
> When you delete a field from a template, the field is removed from all records in **Custom logs**.

Management Console

Dashboard

Information about the Axidian CertiFlow services

Users

3 items

Cards

Cards repository

Certificates

Certificates repository

Events

Cards and certificates operations records

Client agent

2 items

Custom Logs

Cards and certificates logs

Documents

Documents repository

Dashboard

This section provides a summary of the Axidian CertiFlow services.

Licenses

- **Type**
- **Quantity** – total number of licenses
- **In use** – number of licenses assigned to users
- **Left** – number of available licenses

> **TIP**
> The warning icon appears in the following cases:
>
> - No licenses were added to Axidian CertiFlow
> - 90 % of licenses is locked
> - All licenses are locked

Agents

Agent information is displayed if the administrator has configured agent settings in the **System features**→Client agent section of the Configuration Wizard.

Number of agents by status:

- **Registered**– agents registered in Axidian CertiFlow
- **Pending** – agents pending registration
- **Denied** – rejected agents

Number of agents connected to the Axidian CertiFlow server:

- **Active** – agents that connected to the server in the last 5 minutes
- **With cards** – agents with at least one card connected during a session

Number of tasks assigned to agents by their status:

- **Pending** – tasks waiting to be done
- **Running** – active tasks

Users

Number of users according to their status in the Axidian CertiFlow database:

- **Locked in system** – users who failed all attempts to answer secret questions when they try to unblock a card in online mode, reset user PIN or access the Remote Self-Service.
- **No answers to security questions** – users who did not set answers to secret questions.

Click the number of users button to go to **Users**.

Cards

Number of cards by status:

- **Issued** – cards issued in Axidian CertiFlow
- **Assigned** – cards assigned to users but not yet issued
- **Pending** – cards awaiting issue or update
- **Disabled** – deactivated cards that can be enabled, replaced or revoked

Number of card with expiring or expired certificates:

- **Managed** – certificates issued in Axidian CertiFlow
- **Common** – certificates added to the card usage policy in .pfx format and written to cards
- **Traced** – certificates issued and written on cards outside Axidian CertiFlow

Cards that need to be updated for the following reasons:

- **Certificates** – the set of mandatory certificate templates has changed in policy settings
- **Switching of policy** – policy settings have changed
- **Connectors data** – current policy has enabled/disabled integration with Axidian Access

Service certificates

Service accounts certificates that are used to integrate with Microsoft CA.

> **TIP**
> The warning icon appears if at least one of the service certificates is expiring (10% of the validity period) or has already expired.

Users

In the **Users** section, you can search for users, create and edit users, create and edit user containers, and import user files.

Search

Simple

To find a user:

1. Select the catalog where the user is located.
2. In the search field, enter the user's **Common Name**, **Last Name**, **Login (sAMAccountName)**, or **Email Address**.
   To find all users in a catalog, enter `*`.
3. Click  or press **Enter**.

Advanced

The advanced search allows you to find users using filters:

- Container
- Common name (CN)
- Container
- Logon name (sAMAccountName)
- First name
- Last name

You can also apply the following filters:

- **Locked in system** – to find users who have exhausted their attempts to answer secret questions and have been blocked.
- **No answers to security questions** – to find users who have not set answers to secret questions.
- **Display disabled accounts** – to find users with both active and disabled catalog accounts.

You can save the user search results to a file. Click  and select the **PDF** or **CSV** format.

Manage internal catalog users

You can create containers and accounts for external users if you have configured a connection to an internal user catalog in the Axidian CertiFlow Configuration Wizard.

Make sure that role members have the privileges to manage users of the internal catalog:

1. Go to **Configuration** → **Roles** and select the required role.
2. Assign the following privileges:
    - Create users
    - Edit users
    - Delete users
    - Create containers
    - Edit containers

To start managing the internal catalog users, go to **Users** and select the internal catalog's root container in the catalog list.

Create a user

You can create users manually or import a file with users.

To create a user:

1. Select **Create user** and select the container where you plan to put the user.
2. Enter the user's details.
3. Click **Create**.

Import users

The supported file formats are TXT (UTF-8) or CSV, with rows structured as follows:

```
Container;CN;FirstName;LastName;LogonName;Email
```

Field	Required/Optional	Description
Container	Optional	Path to the container where the user is created. If not specified, the user is created in the root container.
CN	Optional	The user's name in Common Name format. If not specified, the name is generated from the `LastName` and `FirstName` values.
FirstName	Required	The user's first name
LastName	Required	The user's last name
LogonName	Required	The user's login name in Domain\UserName format
Email	Optional	The user's email address

Additional attributes

You can also use the internal catalog attributes specified in the Axidian CertiFlow Configuration Wizard under **Additional attributes**:

- `telephoneNumber`
- `countryName`
- `stateOrProvinceName`
- `localityName`
- `streetAddress`
- `organizationName`
- `organizationUnitName`
- `title`

You can create additional attributes, if needed. For example, an `ageGroup` attribute to specify an age range.

Import file contents example

```
CN;FirstName;LastName;LogonName;Email
Michael Benson;Michael;Benson;Demo\user1;michael.benson@demo.com
Kevin McCallister;Kevin;McCallister;Demo\user2;kevin.mccallister@demo.com
;John;Smith;Demo\user3
```

To import users:

1. Select **Import Users**.
2. Upload the file.
3. Select an action if the user already exists in Axidian CertiFlow: **Skip** or **Update Data**.
4. (Optional) Enable the **Ignore errors** option to upload a file with import errors.

Create and edit a container

To create a container:

1. Click **Create Container**.
2. Select the parent container.
3. Enter the container name.

4. Click **Create**.

You can move the created container to a different parent container and rename it:

1. Click **Edit Container**.
2. Click **Move** and select the new parent container.
3. Enter the new container name.
4. Click **Save**.

User profile

In the user profile, you can manage the user's data, cards, certificates, and documents.

To navigate to a user profile, find the relevant user in the **Users** section and click on their login.

Upload a photo

A photo appears in the user profile if it is saved in the user's catalog profile.

To add a photo, click **Upload photo**.

Photo upload requirements

- The user photo is written to either the `thumbnailPhoto` or `jpegPhoto` attribute. Select the attribute in the user catalog settings in the Axidian CertiFlow Configuration Wizard.
- The user catalog service account must have write permissions for the selected attribute.
- The photo size must be 100 KB or smaller.

Unlock a user

Axidian CertiFlow features a user account lockout mechanism in addition to card blocking.

Axidian CertiFlow locks a user account if the user exceeds the number of attempts to answer security questions. This occurs either during an online card unlock operation or when a user signs in to the Remote Self-Service.

You can configure the number of attempts to answer security questions in policy settings (**Authentication**).

> ⓘ **INFO**
> A locked user cannot log in to the Remote Self-Service or unlock a card using Axidian CertiFlow Credential Provider.
>
> If both the card and the user account are locked, you can unlock the card without unlocking the user:
>
> 1. Open the **Configuration** section, navigate to the policy settings and go to **Workflow → Administrator permissions**.
> 2. Clear the **Validate answers to security questions** option.

If a user account is locked, Axidian CertiFlow records an event in the Event Log, and the user's profile displays the *User is locked* status.

To unlock a user, open their profile and click **Unlock user**.

Reset answers to security questions

You can reset the user's security questions and their answers. The user must then set new questions and answers in the Self-Service.

To reset a user's security questions, click **Reset answers to security questions** in the user profile.

Reset a user's password

You can reset a domain password if a user needs to log in to the operating system using a password. For example, if they have forgotten their card with an authentication certificate and do not know their domain password.

> **REQUIREMENTS FOR RESETTING A USER'S PASSWORD**
>
> - The **Use LDAPS** option is enabled in the user catalog settings of the Axidian CertiFlow Configuration Wizard
> - The user catalog service account has the *Reset password* and *Write pwdLastSet* permissions

To reset a user's password:

1. In the user profile, click **Reset user password**.
2. Set a new password.
3. (Optionally) Enable the **User must change password at next logon** option.
4. Set the password's expiration period. When this period expires, the password value changes to a random one. The Card Monitor service performs the password change.

How to start the Card Monitor service

The Card Monitor service starts automatically on a daily schedule configured in the **Card Monitor** section of the Axidian CertiFlow Configuration Wizard.

To start Card Monitor manually:

Windows OS
Open PowerShell as an administrator on the Axidian CertiFlow server and run:

```
C:\Program Files\Axidian CertiFlow\CardMonitor\Certiflow.CardMonitor.exe
```

Linux OS
Open a terminal as an administrator on the Axidian CertiFlow server and run:

```
cd /opt/axidian/certiflow/cardmonitor && ./Certiflow.CardMonitor
```

INFO
The new password is not saved in the Axidian CertiFlow database.

View user events

The user profile displays information about the five most recent user events.

To refresh the event list, click . To view detailed information about an event, click ▶. To see the full list of events, click **View all**.

Card operations

You can manage a user's cards in their profile under the **Assigned cards** section.

Card operations

Issue

How to issue certificates

Assign

How to assign cards to users

Reset user PIN

How to reset a user PIN

Unlock

How to unlock a card in online and offline modes

Disable and enable

How to disable and enable a card

Revoke

How to revoke a card

Withdraw

How to withdraw a card from a user

Replace

How to replace a card temporarily or permanently

Update

How to update card contents

Issue and print image or text

How to issue a card with a printed image or text

Card menu

The card menu displays the following information:

- Card status
- Comment
- Policy applied to the card
- Revocation reason, if the card was revoked

- Agent bound to the card
- Administrator PIN
- Tags
- Certificates stored on the card: managed, tracked, and common.

Allow users viewing card contents in the Self-Service

You can allow or prevent users from viewing card contents. If granted access, users can view certificates stored on the card and print certificate documents.

To configure the permission:

1. Open the **Configuration** section, navigate to the policy settings and go to **Workflow → User permissions → Issued card operations**.
2. Enable the **View Contents** option.

Certificate types

Managed certificates

Managed certificates are generated based on the templates configured for integrated Certification Authorities (CAs) and issued by the CAs through Axidian CertiFlow. Certificate templates are configured in policy settings (**PKI Settings**).

You can issue, renew, revoke, and track the validity and status of managed certificates. Axidian CertiFlow retrieves information about the certificate or certificate request status from the CA.

Tracked certificates

Tracked certificates are third-party certificates stored on the card. The information about tracked certificates is imported into Axidian CertiFlow when you issue or update a card. Certificates from the external CAs cannot be issued, renewed, or revoked through Axidian CertiFlow, but you can verify the certificate issuer information and validity period.

Configure certificates tracking

To display information about third-party certificates in the card menu, configure tracking for third-party certificates.

1. Open the **Configuration** section, navigate to the policy settings and go to **Workflow → General permissions**.
2. Enable the **Search for certificates when card is issued or updated to track validity period** option.

Configure tracked certificates expiration alerts

Notify users and administrators when tracked certificates are about to expire.

1. Open the **Configuration** section, navigate to the policy settings and go to **Notifications**.
2. Create a notification for the *Traced certificates are expiring* event.

Print certificate forms

You can print tracked certificates from both the Management Console and the Self-Service using the default certificate print templates.

Common certificates

Common certificates are third-party certificates available to multiple users. You can write a common certificate to a card when you issue or update the card.

To write a common certificate to multiple users' cards:

1. Open the **Configuration** section, navigate to the policy settings and go to **PKI Settings** → **Common certificates**.
2. Click **Add common certificate**, upload a PFX-file, enter the file password and click **Add**.

Configure common certificates expiration alerts

Notify users and administrators when common certificates are about to expire.

1. Open the **Configuration** section, navigate to the policy settings and go to **Notifications**.
2. Create a notification for the *Common certificates are expiring* event.

Certificate status

Certificate Status	Description
Valid	The certificate's validity period has not expired. The certificate is ready for use.

Certificate Status	Description
Revoked	The certificate has been revoked. Revocation can be temporary or permanent. In case of a temporary revocation (for example, after a card has been disabled), the certificate's validity is suspended while the card is off. After the card is enabled, the certificate becomes valid again, provided it did not expire while the card was off. In case of a permanent revocation (for example, after you revoked a certificate or a card), you cannot use the certificate.
Expiring	The certificate's validity period will end soon. Renew the certificate if you intend to continue using it.
Expired	The certificate's validity period has ended. The certificate is not ready for use. You can renew the certificate for a period equal to its original validity period, as defined in the certificate template in the CA. For more information, see Certificate renewal.
Error	Axidian CertiFlow could not determine the certificate's status. The CA might be unavailable. The certificate is not ready for use.
Approved	The administrator has approved the certificate request, but the certificate has not yet been issued to the user.
Rejected	The administrator has rejected the certificate request.
Pending	The certificate request is awaiting approval from the CA operator or the certificate form is awaiting approval from the Axidian CertiFlow administrator.

Export certificate documents

You can save the certificate request form, the certificate form, and the certificate revocation request as PDF files and email them to a user.

To export a certificate document, click  next to the required certificate and select a document. To email a certificate document to a user, click  and select a document.

Issue

When you issue a card, it is personalized for the user: according to policy settings, the card is initialized, key pairs are generated, certificates are issued, and data is written to the card's memory.

The certificate enrollment process includes the following steps:

1. The user creates a certificate request based on a specified template and generates a key pair (public and private) on the card using a Cryptographic Service Provider (CSP).
2. The user forms a certificate request, which includes the public key.
3. The user signs the request with the private key.
4. A Certification Authority (CA) operator signs the request using the key of a service account with the necessary permissions, owned by the Axidian CertiFlow server.
5. The request is sent to the CA.
6. The CA approves or rejects the request. If the request is approved, the issued certificate is written to the card using the Cryptographic Service Provider.

Issue a card

To issue a card for a user:

1. In the Management Console side panel, go to the **Users** section and find the required user.
2. Open the user's profile and click **Issue card**.
3. Select the templates for optional certificates.
4. Connect the card to the workstation and configure the following settings:

> **Initialize card**
>
> The **Initialize card** option allows you to enable or disable initialization for a specific card.
> If the card is initialized when issued, all card contents is deleted.
> You can configure the initialization parameters in policy settings (**Issuance**).

Label

The card name is set automatically if the **Generate card name automatically** option is enabled in policy settings (**Issuance**).

Comment

Enter a comment if the **Require a comment to the card** option is enabled in policy settings (**Issuance**).

Tags

Add tags if you have created them in **Configuration** → **Tags**.
Adding tags is mandatory if the **Require tags to the card** option is enabled in policy settings (**Issuance**).

5. The **Advanced** section is displayed if you have not added the card to Axidian CertiFlow. Enter the PIN according to the initialization settings:

Card is initialized

The card is initialized if you have enabled the **Initialize card** option (Step 5) and configured initialization parameters in the policy settings.

1. Enter the **Administrator PIN**. This field is displayed if you have not added the card to Axidian CertiFlow and the **Add card automatically** option is set in policy settings (**Workflow**).

   > **INFO**
   > If you leave the **Administrator PIN** field empty, the default value specified in **Card Types** is used.

2. If you issue an eToken card with built-in formatting protection, specify the initialization key.
3. Click **Issue**.

Card is not initialized

1. Enter the **User PIN**.

2. Enter the **Administrator PIN**. This field is displayed if you have not added the card to Axidian CertiFlow and the **Add card automatically** option is set in policy settings (**Workflow**).

   > **INFO**
   > If you leave the **User PIN** and **Administrator PIN** fields empty, the default values specified in **Card Types** are used.

3. Click **Issue**.

4. If a card contains third-party certificates, Axidian CertiFlow can detect them and record information about these certificates in the database. Select the certificates and click **OK**.

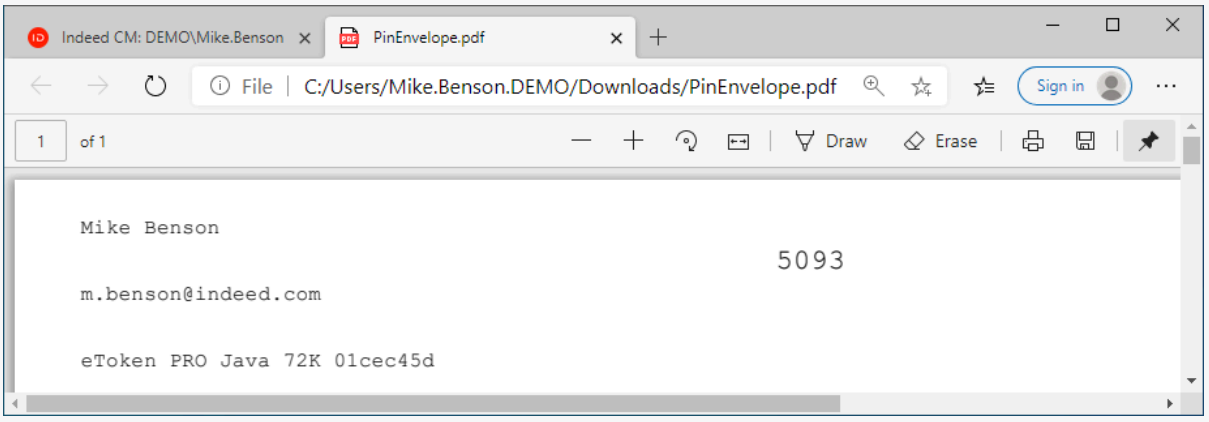
   The certificates window is displayed if you have enabled the **Search for certificates when card is issued or updated to track validity period** option in policy settings (**Workflow → General**).

6. Axidian CertiFlow displays the user PIN after you issue a card if you have enabled the **Set random user PIN** option in policy settings (**Issuance**).

How to send the PIN to the user

To send the PIN to the user's email, configure email notifications in policy settings (**Notifications → User notifications**)

You can also print the PIN and send it in an envelope. Click next to the **User PIN** field. Axidian CertiFlow saves the PIN to the *PinEnvelope.pdf* file.



You can define the print settings in the *C:\inetpub\wwwroot\certiflow\mc\wwwroot\content\pinenvelope.xsl* template.

By default, the file includes user information (name and email) and card information (type, serial number, and user PIN). To modify the print template, edit the *pinenvelope.xsl* file.

7. Click **Close** after the card issue operation completes.

After you issue the card, the user's profile displays the card details in the **Assigned cards** section.

Documents check

A card issue operation can be suspended if your company's regulations require the documents to be verified and approved in the Certification Authority (CA) before you obtain your certificates.

Configure the following settings in Axidian CertiFlow to verify the certificate request in the CA:

1. Open the **Configuration** section and navigate to the policy settings.
2. Go to **PKI settings**, select the required CA and open the **Templates** section.
3. Clear the **Accept certificate request automatically** option.

In the card issue window, you can see this message: *Card issue pending*. The card has *Pending* status. This means that your card issue request is awaiting approval.

If the certificate request is approved in the CA, it gets the *Approved* status and is written on the card. Open the card menu and click **Continue card issue**.

If the request is rejected, revoke and clear the card, then restart the card issue operation.

If you have configured email notifications, you will receive an email with the approval status notification – *Card issue approved* or *Card issue rejected*. If notifications are not configured, wait for the **Continue card issue** option to appear in the card menu.

> ⚠ **CAUTION**
> If several certificates are written to a card at once, the card can be issued only after both certificate requests are approved by the CA.
> If one of the certificates was approved automatically and has a *Valid* status, it is written to the card along with the second certificate.

Assign

Assigning a card to a user associates it with their account and allows them to issue the card through Self-Service.

One card can only belong to one user at a time. A user can have multiple cards assigned to them.

Assign a card

1. Navigate to the user's profile.
2. Select **Assign card**.
3. Depending on whether you have access to the card, select:
   - **Card available**
   - **Card not available**

Card available

Follow the steps below based on whether the card is registered in Axidian CertiFlow.

Card is registered

1. Connect the card to your workstation.
2. Select the card in the **Card** list and click **Assign**.

Card is not registered

You can register a card automatically during the assignment operation. To configure card automatic registration:

1. Open the **Configuration** section, navigate to the policy settings and go to **Workflow** → **General**.
2. Enable the **Add cards automatically when they are issued or assigned** option.

To add and assign a card:

1. Connect the card to your workstation.
2. Select the card in the **Card** list.
3. (Optional) When you add a card, Axidian CertiFlow automatically inserts the administrator PIN defined for this card type in **Configuration** → **Card Types**. If you have previously changed the administrator PIN, enter it in the **Advanced** section.
4. Click **Assign**.

⚠ **CAUTION**

If you enter an incorrect PIN, the PIN may be blocked.

About administrator PIN blocking

Each card has a counter for failed administrator PIN entry attempts. If you add a card which has only one attempt left and you enter an incorrect PIN, the PIN is blocked.

For some cards, a blocked administrator PIN cannot be unblocked. If the administrator PIN is blocked, you can only initialize the card, which erases all data stored on it.

Card not available

You can assign a card to a user remotely if it was previously registered in Axidian CertiFlow.

1. In the Management Console side panel, go to **Cards** and use the search filters to find the card.
2. Select **Assign** in card operations menu.

Allow users assign cards in the Self-Service

You can allow or prevent users from assigning cards in the Self-Service. To configure the permission:

1. Open the **Configuration** section, navigate to the policy settings and go to **Workflow** → **User permissions** → **Card issuing operations**.
2. Enable the **Assign** option.

Unassign a card

You can unassign a card from a user if the card has not yet been issued.

1. Go to the user's profile and open the card menu.
2. Select **Unassign**.

Reset user PIN

If users do not remember their cards PINs and blocked their cards, you can reset the card PIN and set a new one. The PIN changes to the value specified in **Card Types** settings.

> **INFO**
> If you enable the **Initialize card** option in policy settings (**Issuance**), the card PIN changes to the value specified in the card type's initialization parameters.

To reset the card PIN:

1. Navigate to the user's profile.
2. Select **Reset PIN** in the card menu.
3. Connect the card to the workstation and click **Reset**. If you do not have access to the card, enable the Reset PIN on agent option to create a task for the agent installed on the user's workstation.

After you reset the PIN, the user can set a new PIN in the Self-Service.

Allow users reset cards PINs in the Self-Service

You can allow or prevent users from resetting cards PINs in the Self-Service. To configure the permission:

1. Open the **Configuration** section, navigate to the policy settings and go to **Workflow → User permissions → Issued card operations**.
2. Enable the **Reset user PIN** option.

Unlock

The card locks if the user exceeded the number of attempts to enter the card PIN. You can define the maximum number of allowed PIN entry attempts in policy settings (**Issuance** → **Card initialization**).

There are two modes to unlock a user's card: online and offline.

Online mode

The user can unlock a card in the online mode on the Windows OS lock screen. The user answers security questions, sets and confirms a new PIN, and the card unlocks.

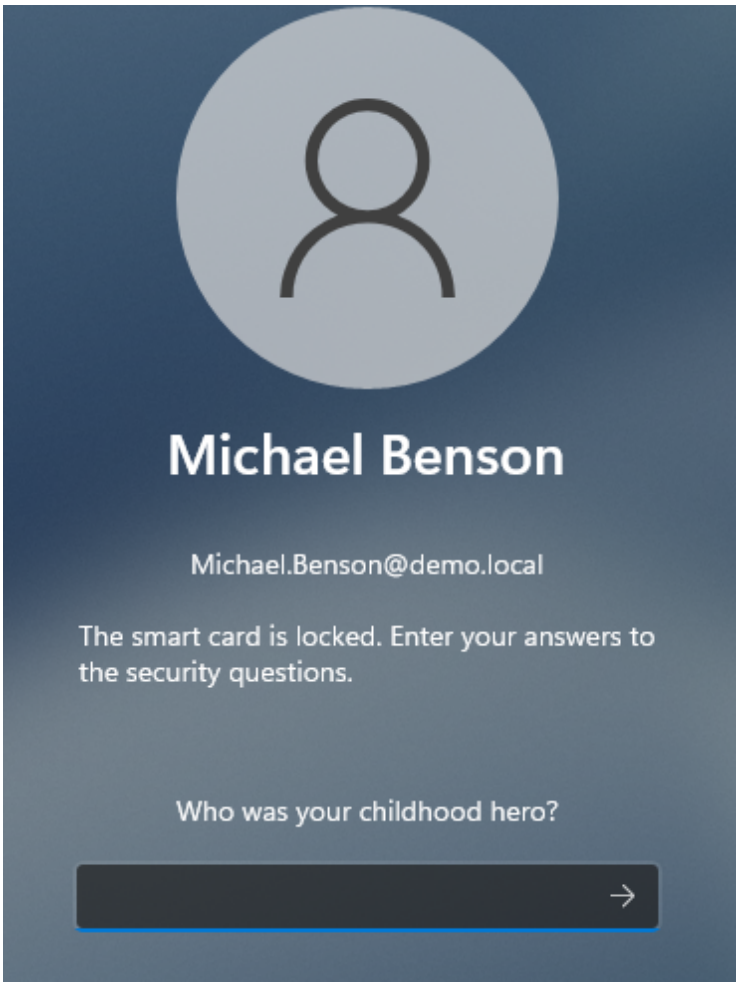
Online unlock requirements:

- The user's workstation is connected to the Axidian CertiFlow server
- The user has set answers to security questions in the Self-Service

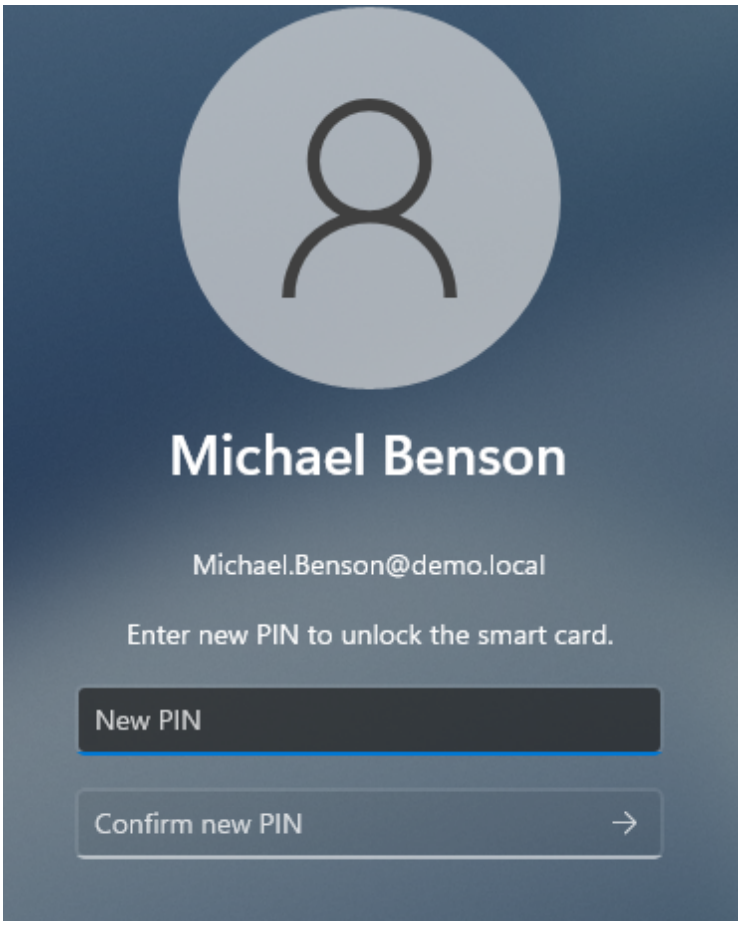
If the user has not set answers security questions, online card unlock is not available. Use the offline mode to unlock the card.

The instruction below describes the online card unlock unlock on the Windows 11 lock screen.

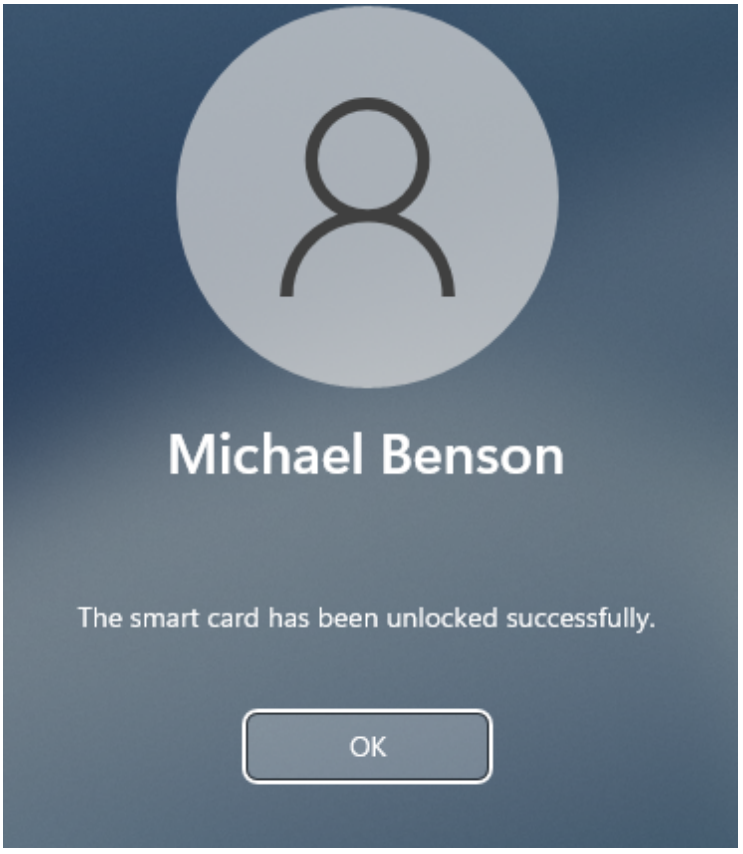
1. Enter the answers to the security questions and click  .



2. Enter the new PIN and confirm it.



3. Once the card is unlocked, you can see the confirmation message. Click **OK**.



Offline mode

You can unlock a card in the offline mode on the Windows lock screen or in a Windows session.

Lock screen

> ⚠ **CAUTION**
> The Windows lock screen does not support card unlock in a Remote Desktop connection.

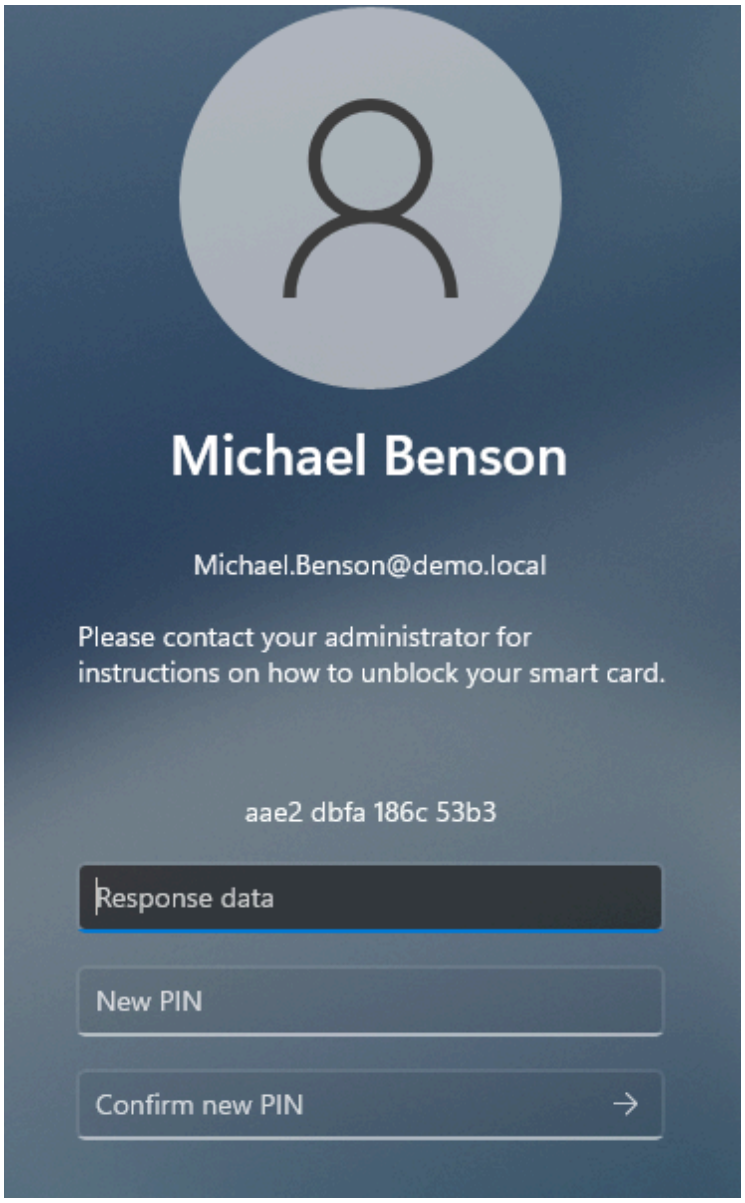
Offline unlock uses a challenge-response authentication mechanism.

Unlock process

1. After the user exceeded the maximum number of allowed PIN entry attempts, Axidian CertiFlow locks the card and displays a message with a unique 16-character challenge code.

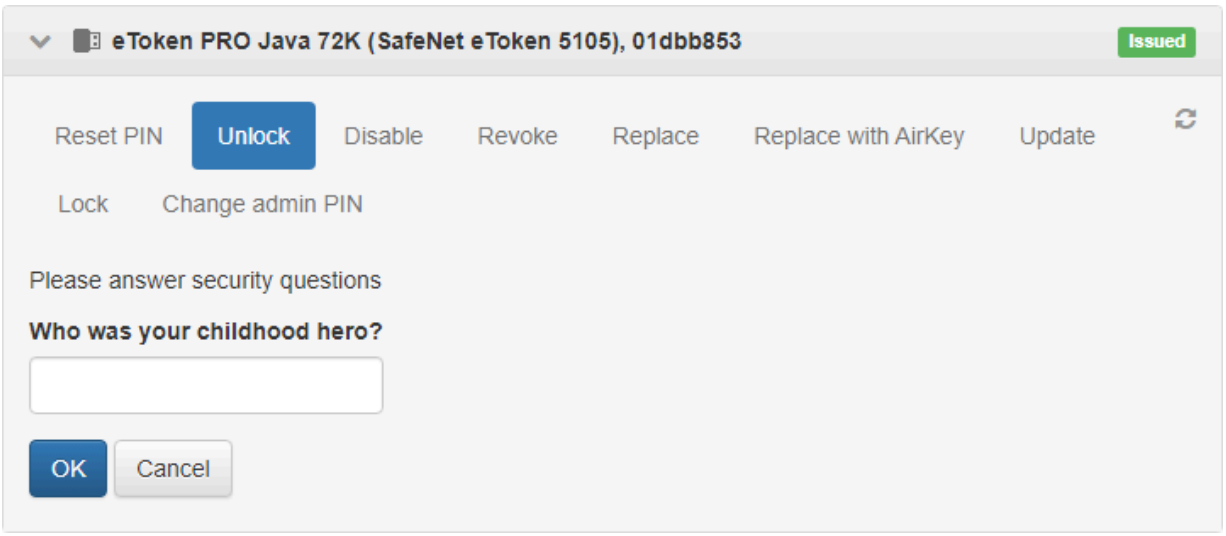
2. The user contacts an operator (for example, by phone), answers the security questions, and provides the challenge code.

Offline card unlock screen in Windows 11

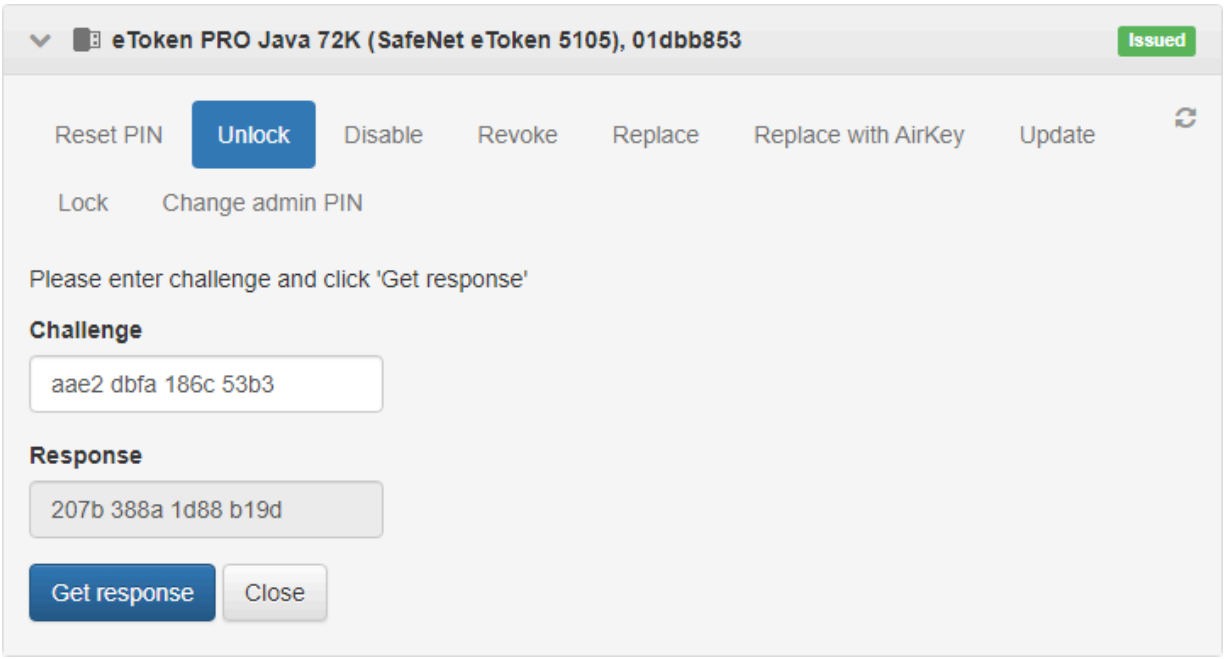


3. The operator opens the user's card menu in Axidian CertiFlow and selects **Unlock** in the card operations list.

4. Before generating the response code for card unlock, the operator asks the security questions.

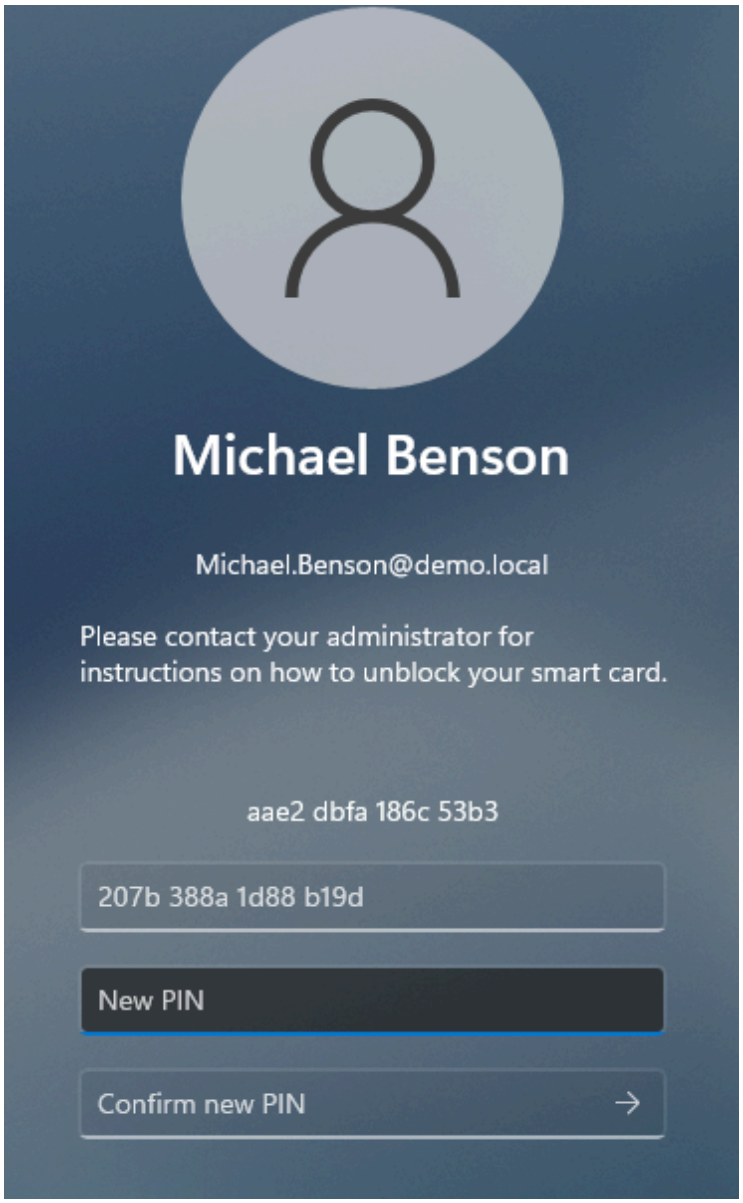


5. The operator enters the user's answers. If the user's answers are correct, the operator enters the challenge code provided by the user. Axidian CertiFlow generates a response code.



6. The operator sends the response code to the user.

7. The user enters the response code on the lock screen and sets a new card PIN.



Session

Use the Axidian CertiFlow Unlock tool to unlock a card that is not used for workstation logon.

1. Connect the card to the workstation and run the Axidian CertiFlow Unlock tool.
2. Select the card from the list.
3. The tool displays the card unlock challenge code in the **Challenge data** field. Send this code to the Axidian CertiFlow operator. The operator will ask the security questions to verify your identity, and will then give you a response code.
4. In the tool, enter the response code in the **Response data** field, set and confirm a new PIN, and select **Unlock**.

The tool unlocks the card and applies the new PIN.

INFO

You can turn off the offline card unlock feature:

1. Open the **Configuration** section, navigate to the policy settings and go to **Workflow** → **Administrator permissions**.
2. Clear the **Unblock card offline** option.

The **Validate answers to security questions** option in **Workflow** determines whether Axidian CertiFlow checks the answers to the security questions during the offline unlock process.

Disable and enable

You can disable a user's card (turn off) for a certain period of time and then enable it again (turn on). To disable or enable a card, you do not need to connect it to a workstation.

Disable a card

To disable a card, click **Temporarily disable card** in the card menu and confirm the operation. The card status changes from *Issued* to *Disabled*.

1. Navigate to the user's profile.
2. Select the required card and then select **Disable** in the card menu.

The card status changes from *Issued* to *Disabled*. If a user tries to authenticate with a disabled card, they receive a message stating that the certificates have been revoked.

Certificate suspension

You can configure Axidian CertiFlow to temporarily suspend the certificates while a card is disabled:

1. Open the **Configuration** section, navigate to the policy settings and go to **PKI Settings**.
2. Select the required CA and go to **Templates**.
3. Click  next to the required certificate template.
4. In the template parameters, enable the **Revoke certificate at card revoking/disabling** option and click **Save**.

The certificates are revoked with *Certificate on hold* status. Enable the card to resume the certificate validity.

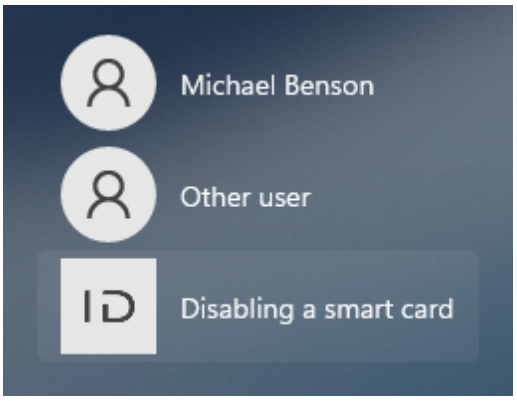
Disable a card without logging into the OS

In an emergency, a user can disable their card without logging into the OS.

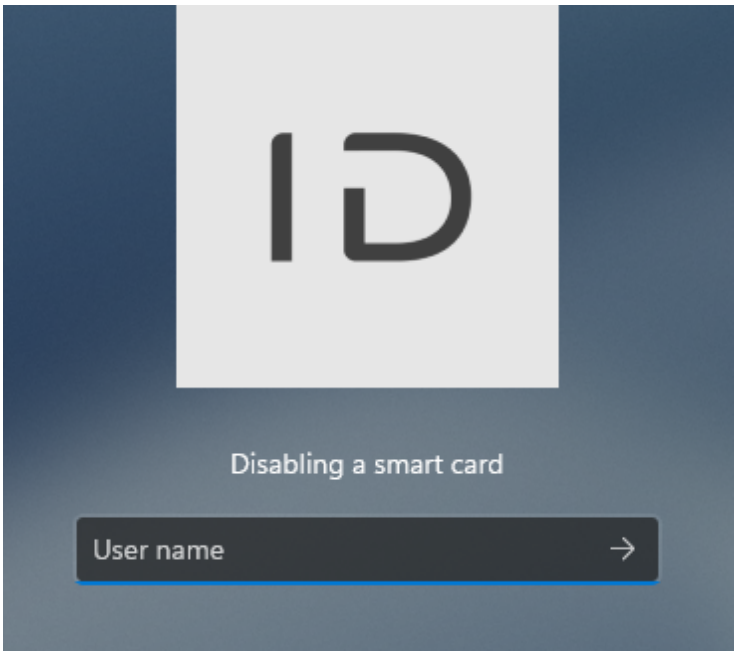
> **INFO**
> The user can only disable a card if the workstation is connected to the Axidian CertiFlow server and the user has configured answers to the security questions.
>
> You can block specific user groups from disabling cards. For more information, see Online card unlock settings.

To disable a user's card:

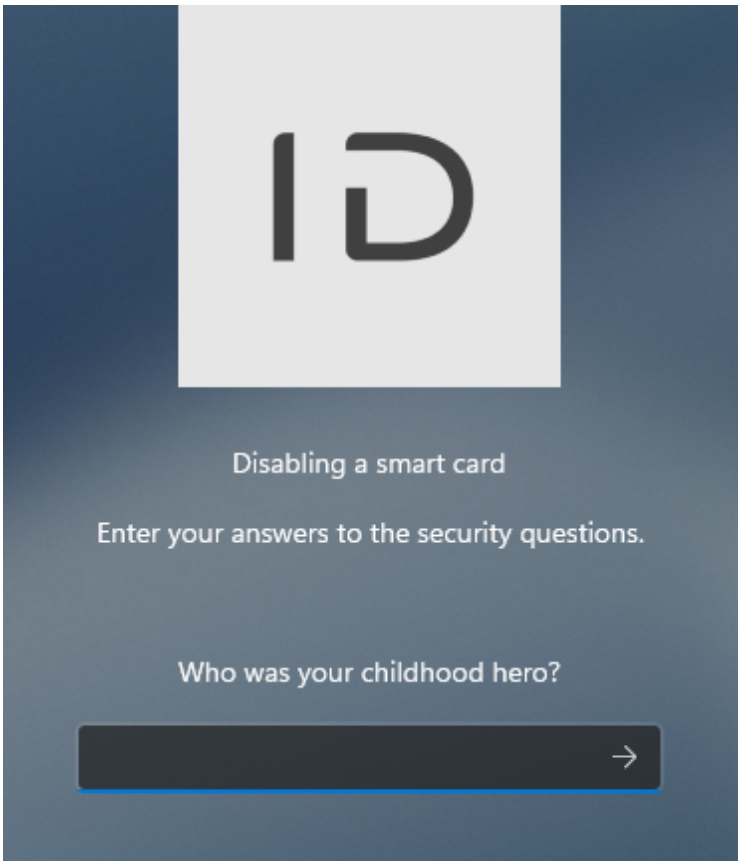
1. On the Windows lock screen, select **Disabling a smart card**.



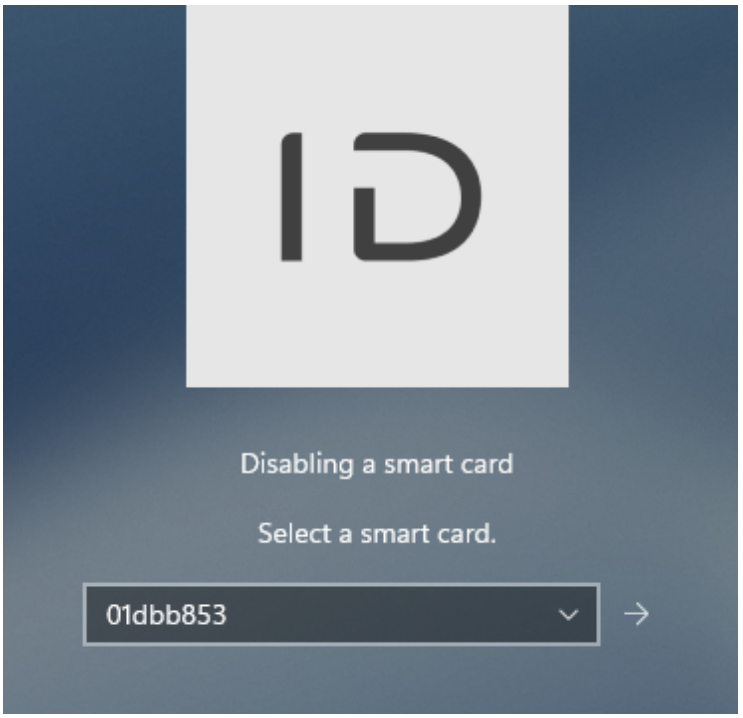
2. Enter the username (Logon Name or UPN).



3. Enter the answers to the security questions.



4. Select the card from the list of issued cards and click  .



Enable a card

1. Navigate to the user's profile.

2. Select the required card and then select **Enable** in the card menu.

Allow users disable and enable cards in the Self-Service

You can allow or prevent users from disabling and enabling their cards in the Self-Service. To configure the permission:

1. Open the **Configuration** section, navigate to the policy settings and go to **Workflow → User permissions → Issued card operations**.
2. Activate the **Disable** and **Enable** options.

Revoke

You can revoke a user's card if it is damaged, lost or compromised.

> ⚠ **CAUTION**
> If you enabled the **Revoke certificate at card revoking/disabling** option in the CA certificate template settings, all certificates stored on a card are removed.

To revoke a card:

1. Navigate to the user's profile.
2. Select the required card and then select **Revoke** in the card menu.
3. Define the revocation reason:
    - **Card broken** – the card is broken or destroyed
    - **Card lost** – the card is lost
    - **Card update** – you need to update the card
    - **Card withdraw** – the card is withdrawn from a deactivated user
    - **Card compromise** – the card key is compromised

    > ⓘ **INFO**
    > If you select **Card lost** or **Card compromise**, Axidian CertiFlow revokes all certificates stored on the card.
4. Connect the card to the workstation and click **Revoke**. If you do not have access to the card, assign a task on the client agent: enable the **Clean card on agent** option.

The card revocation reason is displayed in the user's profile. If a user tries to authenticate with a revoked card, they receive a message stating that the certificates have been revoked.

Allow users revoke cards in the Self-Service

You can allow or prevent users from revoking the card in the Self-Service. To configure the permission:

1. Open the **Configuration** section, navigate to the policy settings and go to **Workflow → User permissions → Issued card operations**.
2. Enable the **Revoke** option.

Withdraw

You can replace or withdraw a revoked card.

To withdraw a card:

1. In the Management Console side panel, go to the **Users** section and find the required user.
2. Open the user's profile, select the required card and click **Withdraw** in the card menu.
3. Depending on whether you have access to the card, select:
   - **Card available**
   - **Card not available**
4. If you do not have access to the card, click **Withdraw**.

   If you have the card, connect it to the workstation and select the following options (optional):

   ▼ **Clean card**

   After you withdraw a card, all certificates written to the card using Axidian CertiFlow are deleted. Certificates, requests, and keys written on the card outside Axidian CertiFlow remain on the card.

   Enter the **User PIN** to be set on the card after it is withdrawn. If you do not specify a user PIN, Axidian CertiFlow applies the PIN defined in the **Card type** settings.

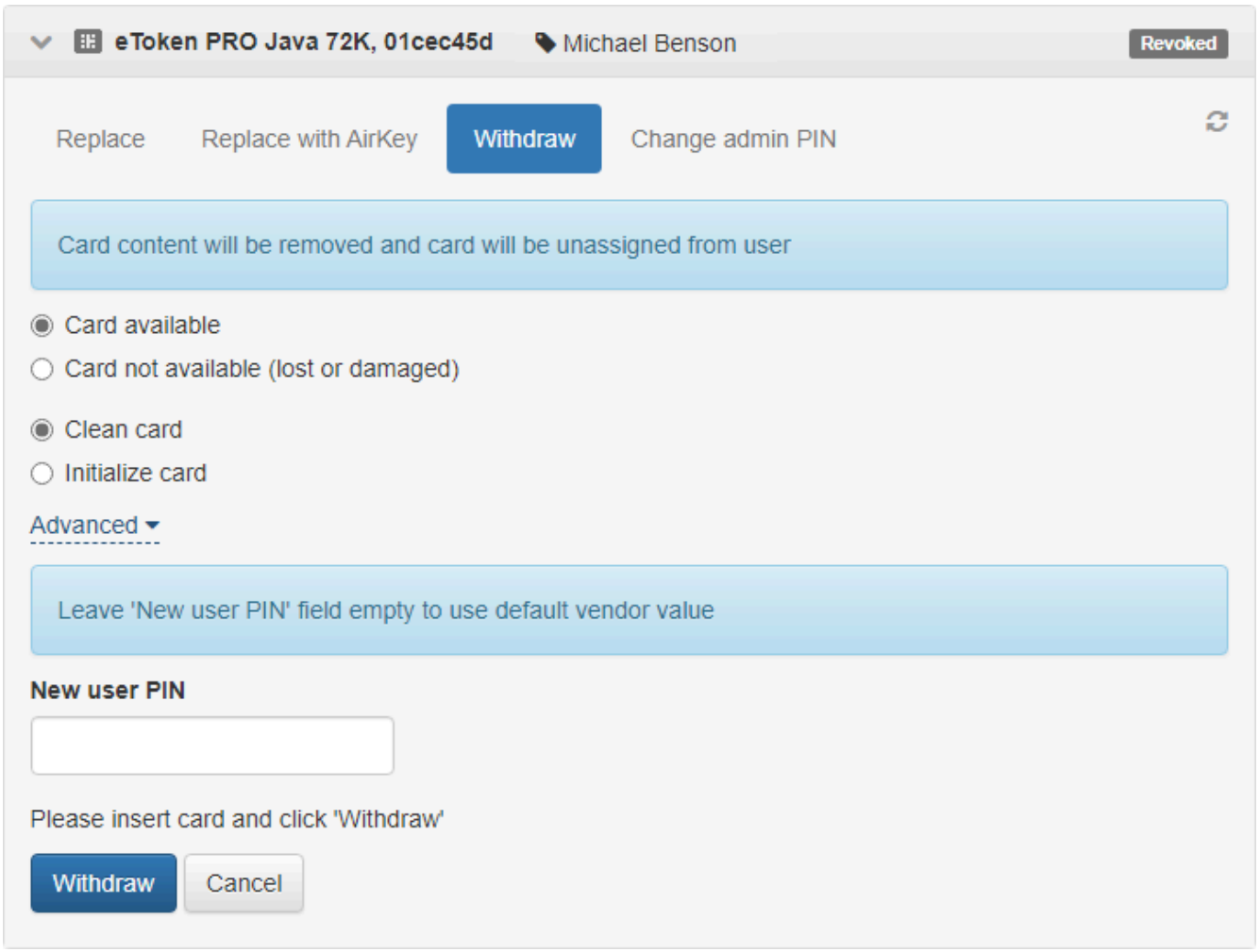
   > ⚠ **CAUTION**
   > Always specify a user PIN when you withdraw and clean the card if the PIN defined in the card type file does not meet the PIN requirements set for that card type in policy settings (**Issuance** → **Card initialization**).

   ▼ **Initialize card**

   After you withdraw a card, Axidian CertiFlow erases all data stored on it.

   Axidian CertiFlow then applies the initialization parameters configured for the **Initialize card while adding** option in **Configuration** → **Card Types**.

5. Click **Withdraw**.


eToken PRO Java 72K, 01cec45d
Michael Benson
Revoked
Replace
Replace with AirKey
Withdraw
Change admin PIN
Card content will be removed and card will be unassigned from user
Card available
Card not available (lost or damaged)
Clean card
Initialize card
Advanced
Leave 'New user PIN' field empty to use default vendor value
New user PIN
Please insert card and click 'Withdraw'
Withdraw
Cancel

Replace

Axidian CertiFlow allows you to replace a user's card. There are two replacement types:

- **Temporary**
  If an employee forgets their card at home, you can issue a new card with a limited validity period. The primary card is disabled, and a temporary card is issued. When the temporary card expires, it is revoked automatically, and the primary card resumes operation.
- **Permanent**
  If a card is broken, lost, or compromised, you can replace it with a new one. The old card is revoked, and the new one becomes the primary card.

Certificates workflow

The certificates status during a card replacement depends on the CA certificate templates settings.

How to configure the CA certificate template parameters

1. Open the **Configuration** section and navigate to policy settings.
2. In the **PKI Settings** section, select the required CA and open **Templates**.
3. Click  next to the required certificate template.

Key pair backup

Whether a key pair backup is stored in Axidian CertiFlow controls the certificate status during a card replacement.

- Key pair backup exists: When you issue a new card (temporary or permanent), the original certificate is transferred to it, preserving the key pair.
- No key pair backup: When you issue a new card, a new certificate with a new key pair is generated.

To save a key pair backup and write it to a new card during replacement, enable the **Backup key** and **Copy backup key to temporary card** options in the CA certificate template parameters.

Revoke a certificate when you revoke or disable a card

The certificates status during card replacement also depends on the **Revoke certificate at card revoking/disabling** option configured in the CA certificate template parameters:

- Option enabled: Certificates are suspended in the CA when the card is revoked or disabled.
- Option disabled: Certificates remain valid.

> **INFO**
> If a key pair backup is saved in Axidian CertiFlow, the certificate remains valid regardless of the **Revoke certificate at card revoking/disabling** setting. The certificate is transferred to the new card.

Temporary replacement

Here is how a temporary replacement works:

1. The primary card is disabled. A temporary card is issued.

Certificate status	
With key pair backup	The certificate remains valid and is transferred to the temporary card, provided the **Copy backup key to temporary card** option is enabled in the certificate template.
Without key pair backup	If the **Revoke certificate at card revoking/disabling** option is enabled in the certificate template, the certificate on the primary card is suspended in the CA. A new certificate with a new key pair is written to the temporary card.

2. The temporary card expires or the employee regains access to their primary card. After the Card Monitor service runs, the temporary card is revoked, and the primary card is enabled.

Certificate status	
With key pair backup	The certificate remains valid.
Without key pair backup	The certificate on the temporary card is revoked. The certificate on the primary card is valid again.

How to start the Card Monitor service

The Card Monitor service runs automatically on a daily schedule configured in the Configuration Wizard (**Card Monitor**).

To start Card Monitor manually:

- **Windows OS**
  Open PowerShell as an administrator on the Axidian CertiFlow server and run:

  ```
  C:\Program Files\Axidian CertiFlow\CardMonitor\Certiflow.CardMonitor.exe
  ```

- **Linux OS**
  Open a terminal as an administrator on the Axidian CertiFlow server and run:

  ```
  cd /opt/axidian/certiflow/cardmonitor && ./Certiflow.CardMonitor
  ```

Permanent replacement

The old card is revoked, and a new card is issued to replace it.

	Certificate status
With key pair backup	The certificate remains valid and is transferred to the new card.
Without key pair backup	If the **Revoke certificate at card revoking/disabling** option is enabled in the certificate template, the certificate on the old card is revoked in the CA. A new certificate with a new key pair is written to the new card.

⚠ **CAUTION**
The card PIN is not transferred to the new card. The PIN is set according to the card usage policy settings.

Replace a card in the user profile

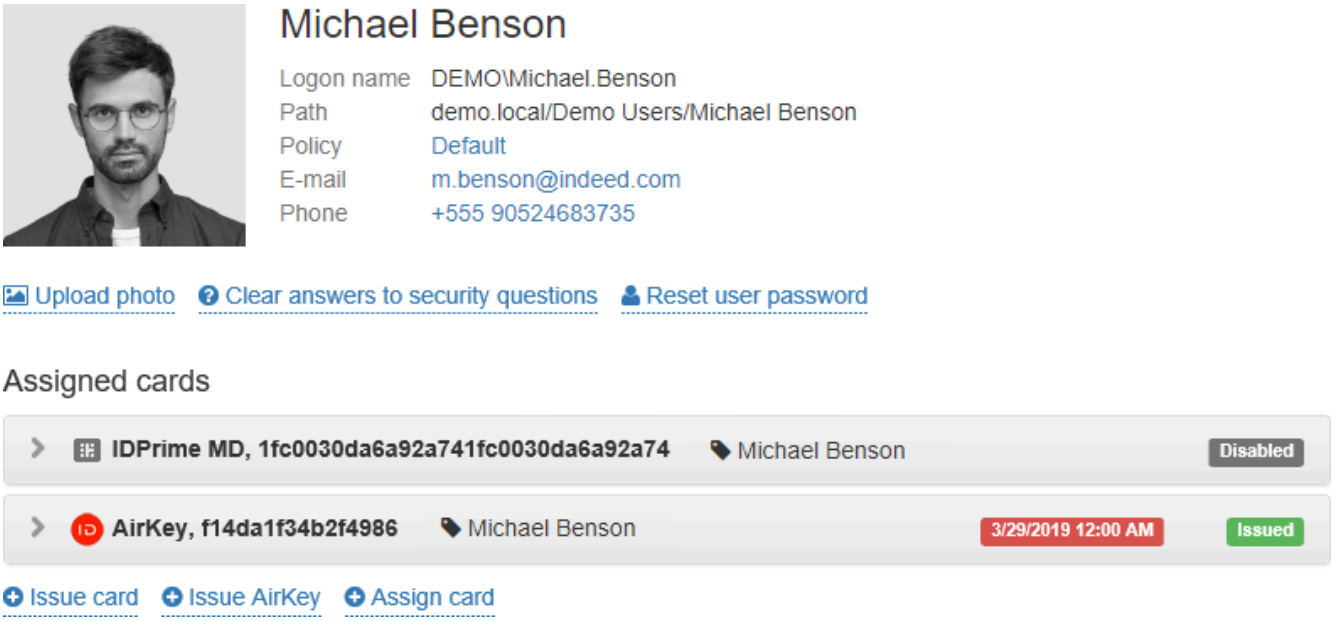
1. In the Management Console side panel, go to the **Users** section and find the required user.
2. Open the user's profile, select the required card and click **Replace** in the card menu.
3. Select the replacement type:

- **Temporary**. Specify the expiration date for the temporary card.
- **Permanent**. Specify the replacement reason.

4. Enter a name of the temporary card.
5. Connect the new card to the workstation.
6. In the **Advanced** section, enter the **Administrator PIN** if you have not previously added the new card to Axidian CertiFlow.
7. Click **Replace**.

> ⚠ **CAUTION**
> If the card usage policy is configured to initialize a card when it is replaced, the new card is initialized. This operation erases all existing data on the card.

During a temporary replacement, the user profile displays two card: the primary card is disabled, and the new card is issued for a limited period.



Replace with AirCard

If Axidian CertiFlow is integrated with Axidian AirCard Enterprise, you can replace a card with an AirCard virtual smart card.

To replace a card with an AirCard, select **Replace with AirCard** in the card menu.

Update

You need to update a card in the following cases:

- The validity period for one or more certificates has expired or is about to expire
- You have assigned a new policy to a user
- You have written certificates to a card outside Axidian CertiFlow
- You have updated policy settings:
  - The number of certificate templates has changed
  - Tracked user attributes in certificate templates have been modified
  - Common certificates have been added or removed
  - At least one optional certificate is configured
  - Integration with Axidian Access has been enabled or disabled

Assigning a user a new policy triggers the following changes during a card update:

1. Axidian CertiFlow removes certificates configured in the current policy but not in the new one.
2. Certificates configured in the new policy but missing from the current one are written to the card.
3. Certificates common to both policies remain unchanged.

Update a card

1. In the Management Console side panel, go to the **Users** section and find the required user.

2. Open the user's profile, select the required card and click **Update** in the card menu.

   > **TIP**
   > If you do not have access to the card, assign a task to the client agent: enable the **Update card on agent** option.

3. Connect the card to the workstation

4. Select the templates for the certificates to be generated and written to the card. Axidian CertiFlow writes mandatory certificates to the card automatically.

5. Enter the user PIN.

6. If a card contains third-party certificates, Axidian CertiFlow can detect them and record information about these certificates in the database. Select the certificates and click **OK**.

The certificates window is displayed if you enable the **Search for certificates when card is issued or updated to track validity period** option in policy settings (**Workflow** → **General**).

7. Click **Update**.

8. Click **Close** after the card update operation completes.

Documents check

A card update operation can be suspended if your company's regulations require the documents to be verified and approved in the Certification Authority (CA) before you obtain your certificates.

Configure the following settings in Axidian CertiFlow to verify the certificate renewal request in the CA:

1. Open the **Configuration** section and navigate to policy settings.
2. Go to **PKI settings**, select the required CA and open the **Templates** section.
3. Clear the **Accept signed certificate renewal request automatically** option.

In the card update window, you can see this message: *Card update pending*. The card has *Pending* status. This means that your card update request is awaiting approval.

If the certificate request is approved in the CA, it gets the *Approved* status and is written on the card. Open the card menu and click **Continue card update**.

If the request is rejected, you can perform the following operations:

- Revoke and clear the card, then restart the card update operation
- Cancel the card update and update the card again

If you have configured email notifications, you will receive an email with the approval status notification – *Card update approved* or *Card update rejected*. If notifications are not configured, wait for the **Continue card update** option to appear in the card menu.

> **INFO**
> The CA settings can restrict automatic certificate renewal and allow renewal only for currently valid certificates. In such cases, the **Accept signed certificate renewal request automatically** option in Axidian CertiFlow does not regulate the automatic certificate renewal process.

Cancel update

You can cancel a card update operation if the **Cancel card update** option is enabled in policy settings (**Workflow** → **Administrator Permissions**).

To cancel a card update:

1. In the card menu, select **Cancel update**.
2. Enter the **User PIN**.
3. Connect the card and click **Cancel update**.

> **TIP**
> If you do not have access to the card, assign a task to the client agent: enable the **Cancel update on agent** option.

Allow users update cards in the Self-Service

You can allow or prevent users from updating their card in the Self-Service. To configure the permission:

1. Open the **Configuration** section and navigate to policy settings.
2. Go to **Workflow** → **User Permissions** → **Issued card operations**.
3. Enable the **Update** option.

Issue and print image or text

You can issue a smart card and print an image or text using Axidian CertiFlow. During the card issue process, Axidian CertiFlow writes certificates on the card and prints an image on it using a print template.

Prerequisites

To configure the issue and print operation:

1. Open the **Configuration** section, navigate to the policy settings and go to **Card printer**.
2. Activate the **Enable card printer support** option.

To print on smart cards, install following components on the workstation:

- EDISecure XID8300 printer drivers
- EDI Secure Connect tool
- The AxidianCertiFlow.EdiSecure.Middleware printer support component
- XID8300 printer connected through USB

The manufacturer supplies the EDISecure XID8300 printer drivers and the EDI Secure Connect tool with the printer. Axidian CertiFlow installation package includes the AxidianCertiFlow.EdiSecure.Middleware component.

Issue a card and print image or text

1. In the Management Console side panel, go to the **Users** section and find the required user.
2. Open the user's profile and select **Issue card**.
3. Enter the card's name.
4. Select **Printer** as the issuance method. Axidian CertiFlow automatically inserts the name of the connected printer.
5. Place the card in the printer's source tray.
6. Click **Issue**.

Axidian CertiFlow allows you to print on a previously issued card.

1. Place the card in the printer's source tray.
2. In the Management Console side panel, go to the **Users** section and find the required user.
3. Open the user's profile and select the required card.
4. Select **Print** in the card menu.

Document operations

The internal document management functionality allows users and administrators to exchange documents for obtaining a signature certificate.

Administrator operations

- Add, edit, and delete documents
- Review user documents
- Sign documents with an electronic signature
- Verify the upload of an original user document

You can manage documents in the user profile and in the document repository under the **Documents** section.

User operations

- Add, edit, and delete documents
- Download documents
- Sign documents with an electronic signature

Prerequisites

To configure document management:

1. Open the Configuration Wizard.
2. Go to **Common features**.
3. Enable the **Internal document management** option.
4. Open the Management Console.
5. Go to **Configuration → Roles**.
6. Grant the required document management privileges to role members.

Document management privileges

- Viewing document repository
- Adding document
- Changing document
- Removing document
- Approving document

To allow users to delete documents in the Self-Service:

1. Open the **Configuration** section and navigate to policy settings.
2. Go to **Workflow** → **User permissions** → **Document operations**.
3. Enable the **Delete** option.
4. Click **Save**.

Documents check

You can review documents submitted for certificates to ensure correct processing and prevent errors.

Once users upload and sign documents in the Self-Service, you can review, approve, or reject these documents in the user's profile.

If you have configured email notifications in policy settings, you will automatically receive an email notification with the attached PDF-document when a user uploads it.

Check signature certificate documents

You can also suspend the card issuance and update operations. In this case, both the Certification Authority (CA) and the Axidian CertiFlow administrator or operator verify the documents.

Users can proceed to issue or update a card only after submitting the required documents for the administrator's review.

Configure documents check

To configure additional verification for certificate documents, prepare the document templates:

1. Open the **Configuration** section and navigate to policy settings.
2. In the **PKI settings** section, select the required CA and open **Templates**.
3. Select the required template and click  .

4. Configure the certificate document verification options according to your intended workflow scenario:

Accept certificate request automatically	Make sure the option is disabled so that you could review the certificate issue request before sending the request to the CA.
Accept signed certificate renewal request automatically	УMake sure the option is disabled so that you could reviewthe certificate renewal request before sending the request to the CA.
Require signed certificate document before continuing card issuing/updating	Enable this option so that the user can write a certificate to the card only after they provide you with a signed certificate form. After the certificate is approved in the CA, the certificate form is available to the user in the Self-Service. The user can download and sign the certificate form and submit it for administrator verification.

Review documents

To review a certificate document:

1. Go to **Users** and search for the required user.
2. Click on the login to open the user profile. The uploaded document appears in the **Documents** section.
3. Download and review the document.
4. Click .
5. In the document approval window, establish the link between the uploaded document, the certificate template, and the card:
    1. In the **Certificate** list, select the template used for issuing the certificate.
    2. In the **Card** list, select the card where the certificate is written.
    3. Click **Approve**.

If the user generated the document from a template on the **Card content** tab, the link between the document, the certificate template, and the card is established automatically. In this case, you do not need to approve the document.

> ⚠ **CAUTION**
> If several certificates are written to a card at once, the card can be issued only after both certificate requests are approved by the CA.
> If one of the certificates was approved automatically and has a *Valid* status, it is written to the card along with the second certificate.

Add and sign documents

You can add documents and sign them with an electronic signature.

> **DOCUMENT SIGNING REQUIREMENTS**
>
> To sign documents with an electronic signature, make sure the following requirements are met:
>
> - You have a card with a signing certificate
> - The signing certificate has any status other than *Revoked*, *Expired* or *Error*
> - The certificate's **Enhanced Key Usage** field contains the **Secure Email** (OID 1.3.6.1.5.5.7.3.4) and **Code Signing** (OID 1.3.6.1.5.5.7.3.3) values

To add and sign a document:

1. In the user profile, go to the **Documents** section and click **Add document**.
2. Select the document type and upload the file.
3. (Optional) Fill in the **Description** field.
4. Click **Sign document**.
5. Connect the card with the signing certificate to the workstation and select it in the **Card** list.
6. Select the appropriate certificate in the **Certificate** list.
7. Enter the user PIN.
8. Click **Add**.

The signed documents automatically appear in the **Documents** list in the user profile. To download the signature file, click .

Original document receipt confirmation

You can confirm the receipt of a document's original copy.

To confirm the receipt of an original when you add a new document:

1. Click **Add document**.
2. Select the document type.
3. Upload the file and enter a description.
4. Enable the **Original received** option.

To confirm the receipt of an original for an existing document:

1. Click next to the required document.

2. Enable the **Original received** option.

Cards

In the **Cards** section, you can perform the following operations:

- Filter cards
- Add cards
- Issue cards
- Delete cards
- Initialize clean cards
- Change card tags
- Import cards

Search

If your card is connected to the workstation, it appears on the **Connected card** tab. If the card is not connected, use the advanced search on the **Advanced** tab.

Search by connected cards

Connect your card to the workstation and click  . To view the card type, hover over the card image.

Advanced search

To find cards, apply the search filters:

- **Serial number**
- **Type**
- **Comment**
- **State** – Clean, Assigned, Pending, Issued, Disabled, Revoked
- **Content status**
- **User**
- **Policy**
- **Tags**

To view all cards list, enter `*` in the **Serial number** field and click  .

> **INFO**
> To filter cards by content status, make sure the Card Monitor service run schedule is set in the Axidian CertiFlow Configuration Wizard.

To export search results, click  and select the PDF or CSV format.

To view the card contents, click  .

To view the administrator PIN, click  . Global administrators have access to the PINs of all cards added to Axidian CertiFlow. Local administrators (local policies administrators) have access to the PINs of cards assigned or issued to users subject to those policies.

Add

1. Connect the card to the workstation and select **Add card** from the cards control panel.
2. Axidian CertiFlow sets the administrator PIN specified for this card type in **Configuration**→**Card types**. If the PIN is different from the value specified in **Configuration**→**Card types**, open the **Advanced** tab and enter the PIN.
3. Click **Add** and **Close**.

To add cards automatically, connecting them consecutively to the same card reader.

> **INFO**
> If the administrator PIN is incorrect, the card can be blocked.
>
> **More about the administrator PIN**
>
> Each card has a counter for failed administrator PIN entry attempts. If you try to add a card which has only one attempt left and you enter an incorrect PIN, the PIN is blocked.
>
> Some cards support the administrator PIN unblock. In this case, you can initialize the card, however, all data stored on it is deleted.

Change the administrator PIN

When you add a card to Axidian CertiFlow, the administrator PIN automatically changes to a random or a non-random value. The administrator PIN settings are configured in **Configuration**→**Card types**.

If the administrator PIN is a random value, you can unblock the user PIN and initialize certain types of cards only with Axidian CertiFlow.

Issue

See User card issue instruction.

Delete

You can delete a card from Axidian CertiFlow when the card is connected to the workstation or when it is not.

> ⚠ **CAUTION**
> When you delete a card which is unavailable (not connected to the workstation), the administrator PIN remains random and unknown if it changed to a random value when the card was added to Axidian CertiFlow.

To delete a card:

1. Find the required card using the search filters and click ✖ .
2. If you have the card, select **Card available** and connect it to the workstation.
   If you do not have the card, select **Card not available (lost or damaged)**.
3. If you have the card and want to delete all data stored on it, enable the **Initialize card** option.
4. Click **Remove**.

Instead of deleting a card, you can withdraw it from a user if it has been issued and then revoked.

Initialize clean cards

You can initialize cards that have been added to Axidian CertiFlow and have the *Clean* status. The *Clean* status means that the card was not assigned to a user.

> ⓘ **INFO**
> The **Initialize card** option is available if the administrator set the permission in **Configuration→Roles**.

1. Find the required card using the search filters and click ✎ to view its contents.
2. Connect the card to the workstation and click **Initialize**. If you do not have access to the card, assign a task on the client agent. To assign the initialization task, enable the **Initialize card on agent** option.

- If the administrator PIN matches the value stored in the Axidian CertiFlow database, click **Initialize**. After the card is initialized, the administrator PIN on the card and in the database does not change. The user PIN is reset to the value defined in **Configuration→Card types**.
- If the administrator PIN does not match the value stored in the Axidian CertiFlow database, open the **Advanced** tab and enter the PIN. Set the **New user PIN** (optional) and click **Initialize**. After the card is initialized, the administrator PIN saved in the database changes to the entered value.

Change tags

You can change tags for multiple cards at once. The administrator creates tags in **Configuration**→**Tags**.

To add or delete tags:

1. Find the required cards using the search filters, select them and click **Change Tags** in the cards control panel.
2. Enter **Tags to add** or **Tags to remove** and click **Change**.

Import

To add multiple cards at once::

1. Click **Import cards**.
2. Upload the prepared **Cards file**.
3. Click **Import**.

You can import cards from a TXT or CSV file. The file must contain lines with a set of fields in the following format:

```
Serial Number;Card Type;Model;Form Factor;Admin PIN;Comment;Tags
```

Где:

- `Serial Number` – a card serial number. Required field.
- `Card Type` – a card type. Required field.
- `Model` – a card model.
- `Form Factor` – a card form factor. Supported form factors: SmartCard (default), UsbToken, MicroSD.
- `Admin PIN` – the administrator PIN value assigned to all cards listed in the import file.
- `Comment` – card notes.
- `Tags` – card tags. Create tags in advance in **Configuration**→**Tags**. If you need to add multiple tags for imported cards, separate them by commas: Tag1,Tag2.

Change card icons

Axidian CertiFlow has a set of images that display the card form factor: USB token or smart card.

To change a card icon:

1. Prepare a PNG image with a maximum size of 20x20 px.
2. To form the file name, use the following template: `<Card type name>_<Card model name>`
    - Card type name – a card type name specified in the card configuration JSON file.

- Card model name - a card model name specified in the card configuration JSON file.

> **INFO**
> The following characters are prohibited in the file name: /, \, :, *, ?, ", <, >, |. All spaces must be replaced with _.
>
> Example: eToken_PRO_Java_72K_eToken_PRO_Java_72K_OS755.png - change an icon for eToken PRO Java 72K card type, eToken PRO Java 72K OS755 cared model.

3. Copy the image to the following folders:
   - *C:\inetpub\wwwroot\mc\Content\images*
   - *C:\inetpub\wwwroot\mcremote\Content\images*
   - *C:\inetpub\wwwroot\mcservice\Content\images*
4. Verify the image. Open the Management Console and go to **Cards**.

Certificates

In the **Certificates** section, you can find all certificates stored on cards registered in Axidian CertiFlow.

Prerequisites

To get access to the certificate repository:

1. Go to **Configuration** → **Roles**.
2. Assign the *Viewing certificate repository* privilege to the members of the *Administrator* or *Operator* role.

Search filters

To find a certificate, set the following filters.

Object	Filter
Certificate	• Certificate type – managed, tracked, common • Serial number • Thumbprint • Subject • Issuer • Template – a list of certificate templates from the integrated CA and an effective policy name • Enhanced Key Usage – enter the numeric OID value. For example, 1.3.6.1.5.5.7.3.4. • Valid from – certificate start date range • Valid to – certificate end date range
User	Common Name
Card	• Card type • Serial number

For example, to get a list of certificates expiring in the current month, select a date range in the **Valid To** filter.

The search results additionally display the certificate status – *Valid, Revoked, Expiring, Expired, Error, Approved, Rejected, Pending*.

More about certificate statuses

Status	Description
Valid	The certificate is valid for use.
Revoked	The certificate is revoked. Revocation can be temporary or permanent. If the revocation is temporary (after the card has been disabled), the certificate's validity is suspended for the period the card is disabled. After the card is enabled, the certificate becomes valid again if its validity period did not expire while the card was disabled. In case of permanent revocation (after card revocation or withdrawal), the certificate is invalid.
Expiring	The certificate will soon expire and needs to be renewed.
Expired	The certificate expired. How to renew a certificate
Error	The certificate status could not be determined. The certification authority might be unavailable. The certificate is invalid.
Approved	The administrator has approved the certificate request, but the certificate has not yet been issued to the user.
Rejected	The administrator has rejected the certificate request.
Pending	The certificate request is awaiting approval from the CA operator or the certificate form is awaiting approval from the Axidian CertiFlow administrator.

Export search results

You can export the search results to an XLSX file. Click and select the XLSX format.

Certificates operations

You can download certificate files or send them by email .

Certificate files include a certificate request form, a certificate form, and a certificate revocation request form.

Events

The **Event Log** section provides you with an overview of all events received by the server from the Axidian CertiFlow services.

By default, event logs are written to the Event Viewer on the Axidian CertiFlow Windows server (*Axidian CertiFlow/Operational*).

To view the list of events, apply the search filters:

- **Level** – Info, Error, Warning
- **Event Id**
- **Service** – Management Console, Self-service, Card monitor, Credential provider, Remote service, API, AirCardCleaner, Migration utility, Agent registration service, Agent service
- **User**
- **Card type**
- **Serial number**
- **Time range**
- **Initiator**

> **USER SEARCH FILTER**
> To define the user catalog attribute for the **User** search filter:
>
> 1. Start the Axidian CertiFlow Configuration Wizard and go **Event Log**.
> 2. Select an attribute from the **Username attribute** list:
>
> - Common name
> - SAM Account Name
> - User Principal Name
> - Custom – enter the attribute name

Export

To generate an event report, click  and select the PDF or CSV format.

Client agent

In the **Agents** section, you can find all agents registered in Axidian CertiFlow.

Prerequisites

To allow access to the agent repository:

1. Open the Configuration Wizard, go to **System features** → **Client Agent** and activate the **Enable client agent** option.
2. Open the Management Console, go to **Configuration** → **Roles** and assign the *Viewing agent repository* privilege to the members of the administrator or operator role.

> **INFO**
> If the **Automatic agent registration** option is disabled in the Configuration Wizard, after the agent is installed and configured on a workstation, it appears in the **Agents** section of the Management Console in *Pending* status.

Search filters

To find agents, set the following filters:

- **Name** – by default, agent name is the name of the workstation where agent is installed. You can change the name in the agent profile.
- **Status** – agent current state: *Not set*, *Pending*, *Accepted*, *Denied*.
- **Computer name** – DNS name of the workstation where agent is installed.
- **System version** – version of the operating system of the workstation where agent is installed.
- **IP address** – IP address of the workstation (IPv4 or IPv6) where agent is installed.
- **Comment** – comment specified by the administrator in the agent profile.
- **Client version** – version of the Axidian CertiFlow Agent client component installed on the workstation. The following filter values are available:
  - *Not set* to find agents of all versions
  - Version number, for example, 7.1.0.178
  - *Unknown*, to find agents of outdated versions or inactive agents that have no connection with the server

Search templates

- exact match – `Win7x86.domain.loc`

- partial match – `*86.domain.loc` or `*domain*`
- all results – `*`

To go to the agent profile, click on the agent name in the search results. Click **Accept** to confirm the registration request or **Decline** to decline the request.

Agent profile

In the agent profile, you can check information about agent, user sessions, cards bound to the agent and recent events.

- **Agent name** – by default, agent name is the DNS name of the workstation where agent is installed. To edit the agent name, click **Change name**.
- **Comment** – to set or edit a comment, click **Edit comment**.
- **Sessions** – user sessions or service sessions. There are two types of user sessions:
  - Console – the user has logged in to the workstation directly.
  - Terminal – the user has connected to the workstation remotely (for example, using RDP).
- **Bound cards** – list of cards bound to the agent.
- **Recent events** – the last five events related to the agent's operation.

Bind agents to cards

The agent automatically detects cards connected to the workstation and requests a list of tasks from the Axidian CertiFlow server. In this case, it is not necessary to bind the user's card to the workstation.

Associating cards with agents allows you to manage cards remotely. For more information, see Manage cards usage

To bind a card to an agent:

1. In the agent profile, go to **Bound cards** and click **Bind card**.
2. If the card is available, connect it to the workstation or select it from the list of connected cards and click **Bind**. If the card is not available, specify its serial number and card type, and click **Bind**.

The card appears in the **Bound cards** section of the agent profile.

To unbind a card, click ✖ and then **Unbind**.

Manage cards usage

You can configure the bound cards usage parameters in policy settings (**Agents** → **Control**).

When you connect a card to your workstation, the agent detects the following events:

- The card is not bound to the agent. This may happen when a user has connected another user's card to his workstation.
- The card is not assigned to the user. This may happen when a user authenticated with a smart card bound to the agent and then changed account in the operating system.

Axidian CertiFlow can take the following actions when an agent detects a suspicious event:

- **Write event**
- **Lock user session, write event**
- **Lock card, write event**
- **Lock user session and card, write event**

In the **Timeout before locking the user session (sec.)** field, enter a value from 1 to 5 to define the number of seconds that pass before a user session is locked.

To configure the agent to check binding between a user session and the connected card, activate the **Enable user card binding** option.

If you plan to install agents on workstations outside your company's domain, enable the **Consider user card binding on PC that is not joined to domain** option.

Set the user notification and agent action for binding violations.

You can use the following attributes in user messages:

- {sn} – a card serial number
- {atr} – a card ATR (Answer to Reset) value
- {model} – a card model
- {label} – a card label

> ⓘ **EXAMPLE MESSAGE**
> The connected card {model}: {sn} does not match the user session.

Check connected cards

The agent scans all cards connected to a user workstation and logs the following events:

- If there is a card with a blocked user PIN or administrator PIN
- If there were any attempts to enter an incorrect user PIN or administrator PIN
- If an unregistered card was connected to a workstation

The Card Monitor service logs an event when the agent fails to communicate with the Axidian CertiFlow server beyond the defined timeout. Configure this timeout in the **Card Monitor** section of the Axidian CertiFlow Configuration Wizard.

You can get notifications about the following events:

- Administrator PIN lock detected on the card
- User PIN lock detected on the card
- Attempt to enter an invalid administrator PIN on the card
- Attempt to enter an invalid user PIN on the card

Axidian CertiFlow sends notifications about cards in *Issued, Pending, Revoked, Disabled* and *Assigned* status.

You can configure global or local policy notifications.

Card manufacturers with events detection support

Card manufacturer	Supported events
ACS	User PIN block detection Invalid user PIN entry detection
Axidian	User/administrator PIN block detection
Avest	User/administrator PIN block detection
Bit4id	User/administrator PIN block detection
CRYPTAS	User/administrator PIN block detection Invalid user/administrator PIN entry detection
Cryptovision	User/administrator PIN block detection
Feitian	User/administrator PIN block detection
HID	Events detection is not supported
ISBC	User/administrator PIN block detection
Microsoft VSC (TPM) **Microsoft Windows Hello for Business (WHfB)**	Events detection is not supported
Registry	Events detection is not supported
RSA	User/administrator PIN block detection
Thales Group (Ex Gemalto and SafeNet)	User/administrator PIN block detection Invalid user/administrator PIN entry detection
Yubico	Events detection is not supported

Event log

Agent activity logs are stored in both server and client logs.

To view agent events in the Management Console, go to **Events**.

The agent on a user workstation writes events to the local Axidian CertiFlow event log and sends them to the server. If the workstation cannot connect to the Axidian CertiFlow server, it stores the events locally and sends them once it establishes the connection.

Assign tasks manually

You can manage cards and certificates remotely using agent tasks.

Task execution workflow

- Any active agent can execute a task that does not require user interaction.
- Only the agent bound to the card can execute a task that requires user interaction, such as entering answers to secret questions for unlocking the card.

Task execution process

Initial connection: When a card connects to a workstation, the agent requests its assigned tasks from the Axidian CertiFlow server.

Established connection: For a card that is already connected, the agent requests new tasks from the Axidian CertiFlow server every 30 seconds by default.

> ⓘ **INFO**
> An agent can execute operations that require user interaction only within an active user session in the operating system.
> If card-to-agent binding is not configured and user session card binding control is disabled, an agent can execute user-interactive tasks in any user session on the workstation.

Assign a task

1. Find the card:
    - In the **Cards** section
    - In the user's profile
2. Open the card menu and select a task.

The assigned task appears in the **Assigned tasks** section of the card menu.

Cancel a task if it is pending for too long or is taking excessive time to complete. Click ✖ next to the task.

Task status

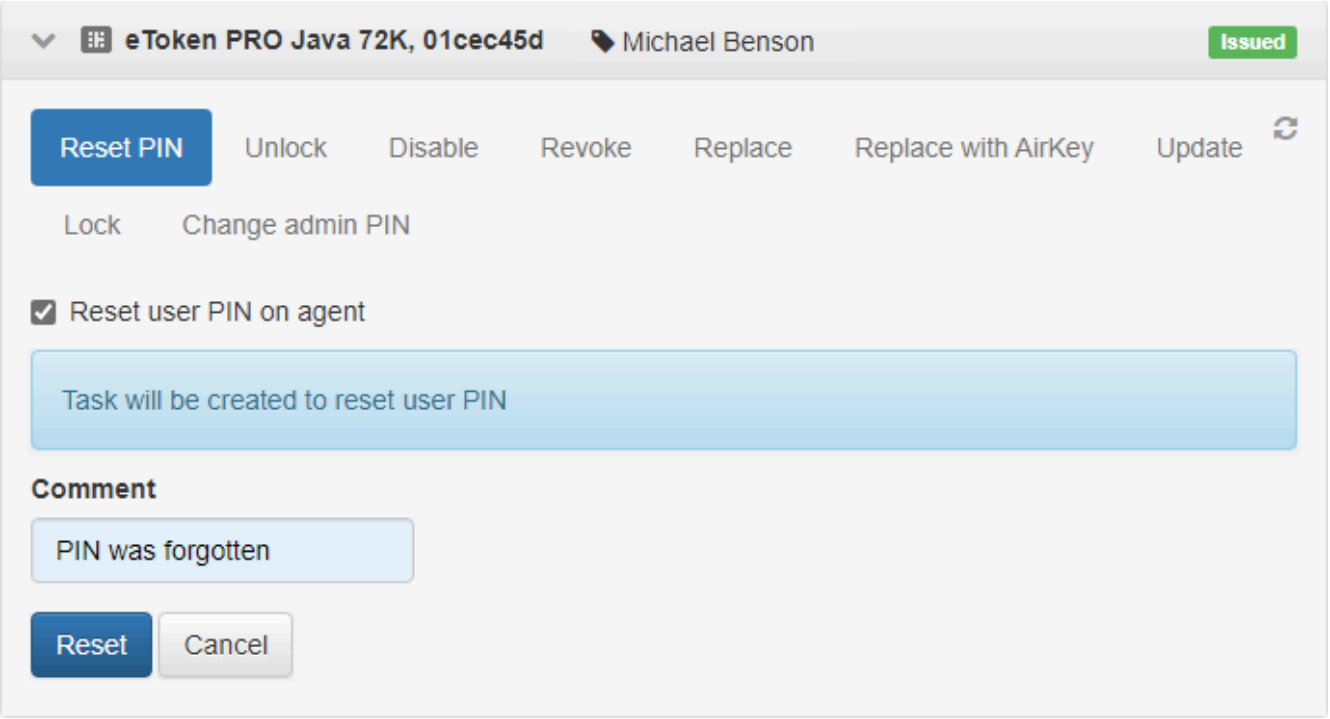
Idle – The task is queued and will execute when its conditions are met (for example, the target workstation with the agent is powered on, the required card is connected, or a preceding task is complete).
Running (blue) – The agent has started executing the task.
Running (orange) – The task exceeds 10 minutes.
Completed – The task is executed.
Error – An error occurred during task execution.

Reset user PIN

You can reset a user PIN if it is forgotten or blocked. To reset the PIN, the user must answer their secret questions correctly. Make sure that the user has configured secret questions and answers in the Self-Service.

To unlock a card through an agent:

1. Select **Reset PIN** in the card menu.
2. Enable the **Reset user PIN on agent** option.
3. (Optional) Enter a comment. The comment logs in the Axidian CertiFlow Event Log.
4. Click **Reset**.

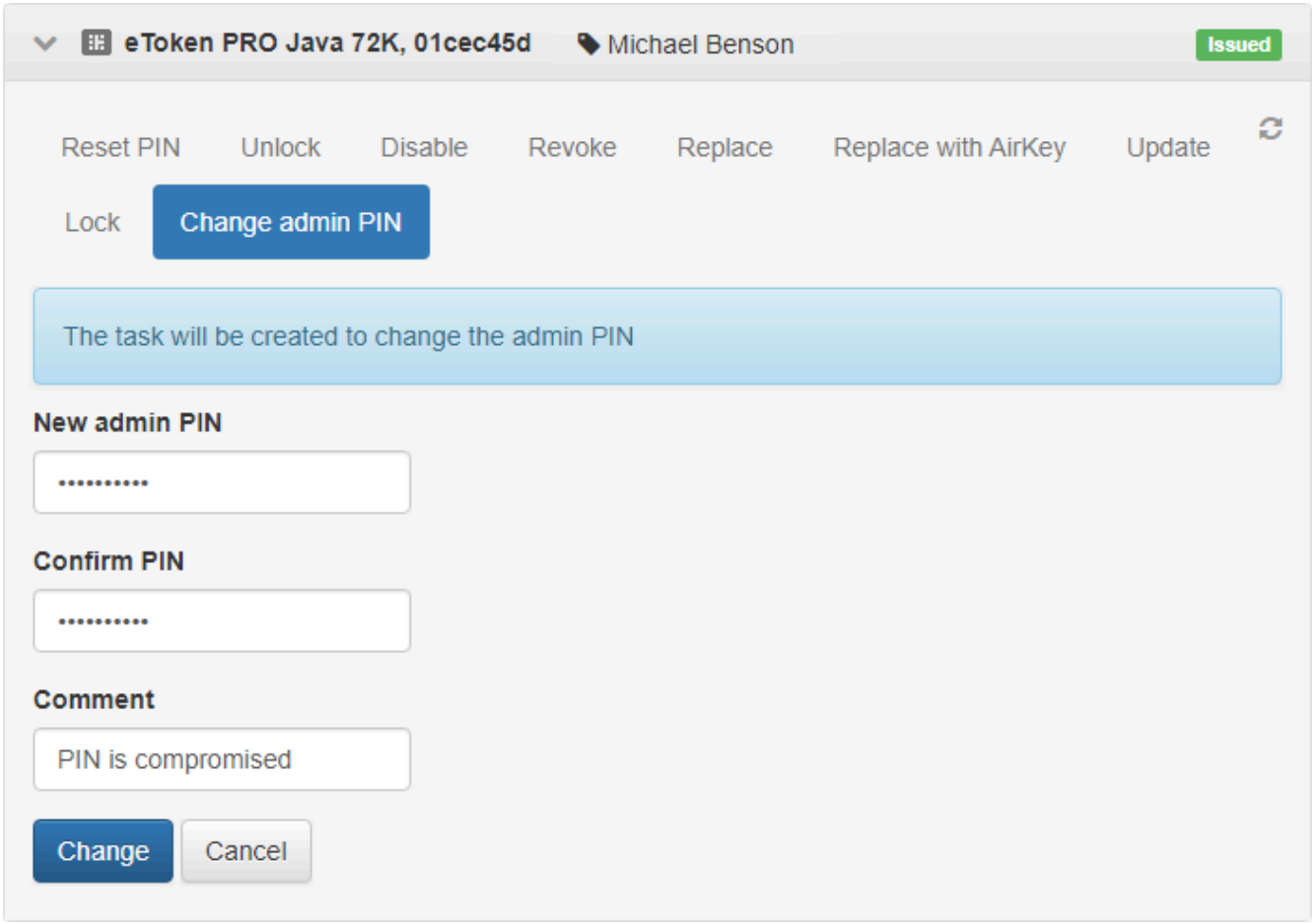


When the task runs, the agent launches the unlock utility on the user workstation. The user must answer the secret questions correctly, enter a new PIN and click **Reset**.

If the user selects **Cancel**, the task status reverts to *Pending*. The Axidian CertiFlow Event Log records that the user cancelled the task. The prompt to answer secret questions reappears in the user's session after 60 seconds.

Change administrator PIN

1. Select **Change admin PIN** in the card menu.
2. Fill in the **New admin PIN** and **Confirm PIN** fields.
3. (Optional) Enter a comment. The comment logs in the Axidian CertiFlow Event Log.
4. Click **Change**.



The administrator PIN changes automatically when the card is connected to a workstation where agent is installed.

If you have specified a message for the **Change card admin PIN operation** in the card usage policy, the user receives a notification when the task is completed.

Revoke a card

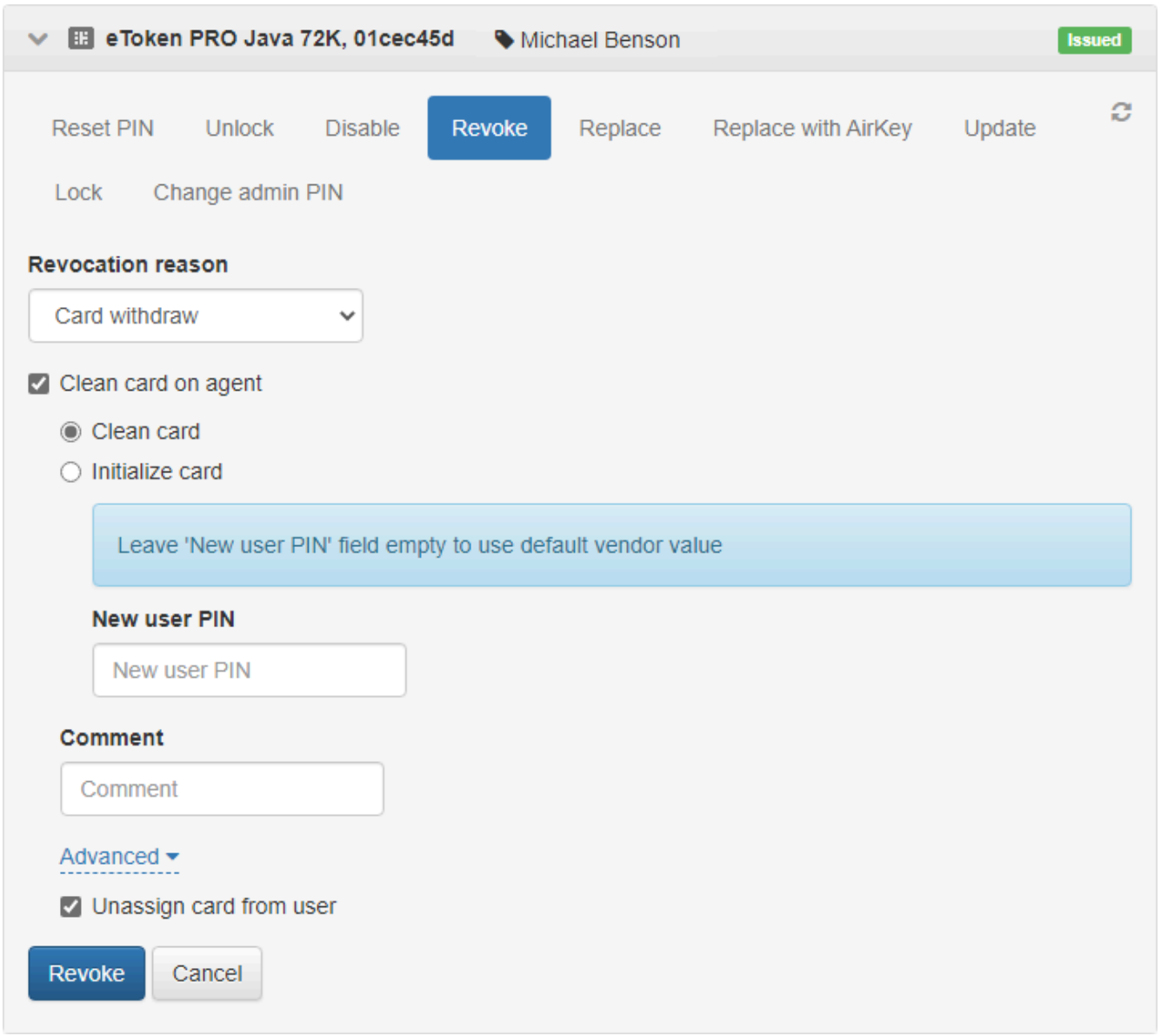
1. Select **Revoke** in the card menu.
2. Specify the revocation reason.
3. Enable the **Clean card on agent** option.
4. Select a data removal level:

- **Clean card**: Deletes all certificates written to the card by Axidian CertiFlow. Pre-existing certificates and keys stored on the card before enrollment are not removed.
- **Initialize card**: Removes all content, deletes the password policy (if configured), and changes the card's name.

5. Enter the new user PIN to be set on the card after it is revoked. If you do not set a PIN, Axidian CertiFlow applies the default PIN from the **Card Types** configuration.

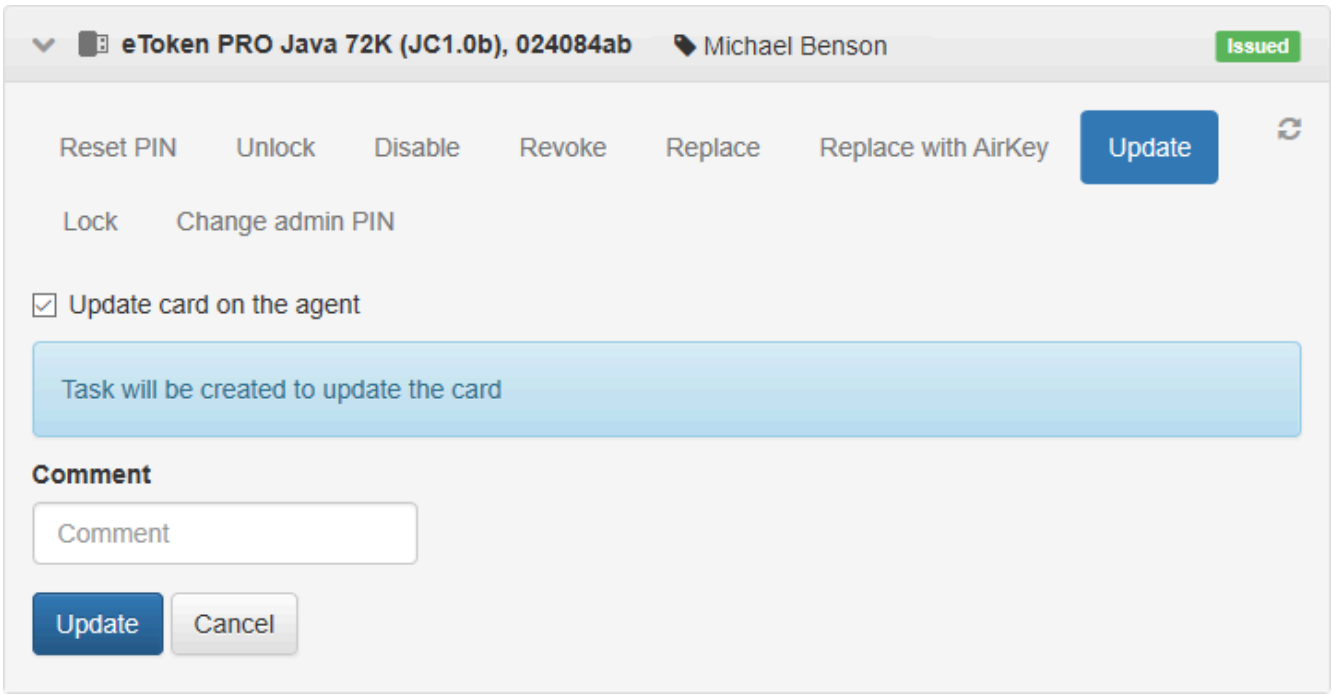
> **WHEN TO SET A USER PIN**
> Define a user PIN if the default user PIN in the card type file does not meet the security requirements configured for this card type after the card was initialized when issued.

6. (Optional) Enter a comment. The comment logs in the Axidian CertiFlow Event Log.
7. To unassign the card from the user, click **Advanced** and enable the **Unassign card from user** option. If this option is disabled, the card remains assigned to the user.
8. Click **Revoke**.



Update a card

1. Select **Update** in the card menu.
2. Enable the **Update card on agent** option.
3. (Optional) Enter a comment. The comment logs in the Axidian CertiFlow Event Log.
4. Click **Update**.



Configure third-party certificates tracking

If a card contains third-party certificates, Axidian CertiFlow can detect them and record information about these certificates in the database. During a card update operation, the user can select which certificates should be tracked.

To configure third-party certificates tracking:

1. Open the **Configuration** section and navigate to the policy settings.
2. Go to **Workflow** → **General**.
3. Enable the following options:
   - **Search for certificates when card is issued or updated to track validity period**
   - **Allow user to select tracked certificates**

When the user connects the card to the workstation, the update operation starts.

The update operation may be paused if your company's policy requires document verification for digital certificate renewals. In this case, the card update window displays the following message: *Card update pending approval*. The card's status changes to *Pending*.

For more information, see Card update documents check.

Cancel a card update operation

You can cancel a card update operation through the agent if you enabled the **Cancel card update** option in policy settings (**Workflow** → **Administrator Permissions**).

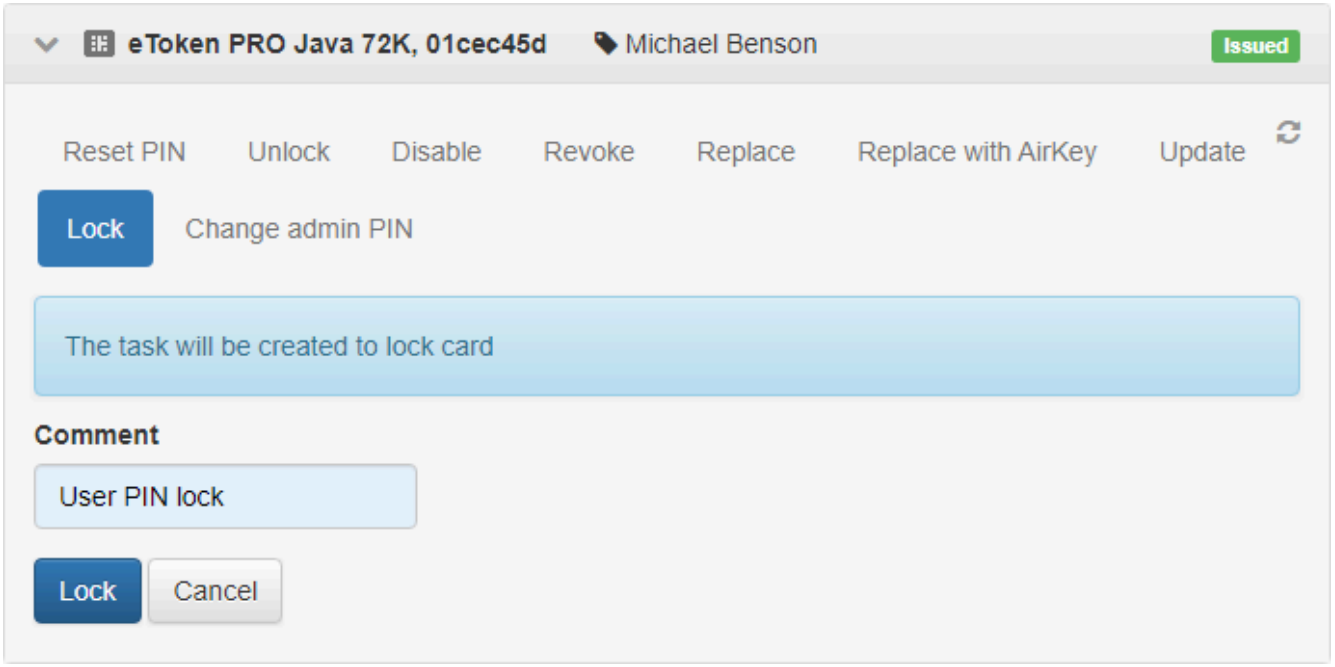
To cancel a card update operation:

1. Select **Cancel update** in the card menu.
2. Enter the user PIN.
3. Enable the **Cancel update on agent** option.
4. Click **Cancel**.

Lock a card

Locking a card locks its user PIN.

1. Select **Lock** in the card menu.
2. (Optional) Enter a comment. The comment logs in the Axidian CertiFlow Event Log.
3. Click **Lock**.



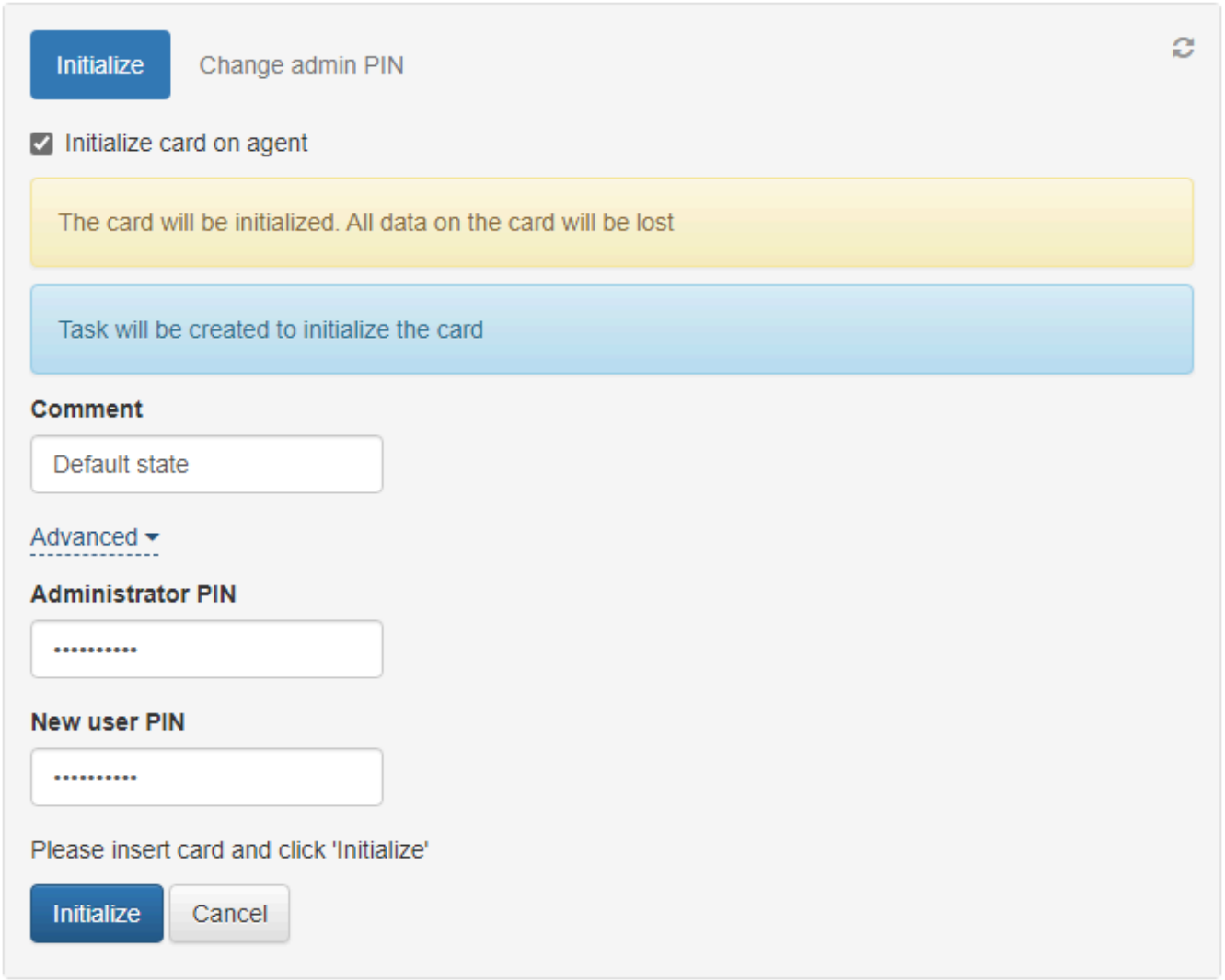
Initialize a card

Agent can initialize cards in *Clean* status.

1. Select **Initialize** in the card menu.
2. Enable the **Initialize card on agent** option:
   - If the administrator PIN set on the card matches the one stored in the Axidian CertiFlow database, click **Initialize**. The administrator PIN on the card and in the database remain unchanged, and the user PIN is reset to the value specified in the card type file.
   - If the administrator PIN on the card does not match the one stored in the sAxidian CertiFlow database, enter the correct PIN in the **Advanced** section. Optionally, set a **New user PIN** and then

click **Initialize**. The administrator PIN in the database is updated to the value you provided.

3. (Optional) Enter a comment. The comment logs in the Axidian CertiFlow Event Log.



Bulk tasks

Bulk tasks are operations you can assign to multiple cards at once. Axidian CertiFlow assigns these tasks to selected cards, and the agent executes the tasks when users connect the cards to their workstations.

Task list

- **Lock user PIN**: Locks the user PIN. Assign this task to cards in *Issued* or *Pending* status.
- **Change user PIN**: Notifies the user that they must change their PIN. Assign this task to cards with the *Issued* or *Pending* status.
- **Change admin PIN**: Changes the administrator PIN. You can assign this task to card in any status.
- **Update card**: Updates the card contents. Assign this task to card in *Issued* status.
- **Clean card**: Clears or initializes the card. You can also unassign the card from the user. Assign this task to cards in *Revoked* status.

Create a bulk task

1. In the Management Console, go to the **Cards** section.
2. Select the target cards and click **Create agent tasks**.
3. Select a task, set the required parameters, and click **Create**.

The task appears in the selected cards menus. Axidian CertiFlow records the task execution results for each agent.

Send a user message

The agent can notify users when it completes the following operations:

- Locking a card
- Changing the administrator PIN
- Cleaning a card

Axidian CertiFlow does not send the notifications by default. To enable a notification, enter the message text.

Automatic operations

The Axidian CertiFlow Client Agent can automatically perform the following operations:

- Add cards to Axidian CertiFlow and assign them to users
- Issue empty or assigned cards
- Resume cards issue or update operations
- Prompt a user PIN change according to the configured schedule

These operations are executed remotely on user workstations where agents are installed.

To control which operations agents can perform, configure the agent policy settings in **Configuration** → **Agents** → **Workflow**.

Add cards

When an unregistered card connects to a workstation, the agent can automatically add this card to Axidian CertiFlow. The card then binds to the agent installed on the workstation.

To configure agent to add cards automatically, enable the following options:

- **Add card**
- **Add card without administrator PIN if provided PIN is incorrect**

During card registration, the agent authenticates to access the card. It automatically applies the administrator PIN defined for the specific card type in policy settings (**Agents** → **Workflow** → **Administrator PINs**).

> **INFO**
> If you have not set a policy for the administrator PIN, the agent uses the default value from the card type settings.

The agent supports two methods for adding a card:

- Add a card and change the administrator PIN
- Add a card without the administrator PIN (PIN is left empty)

How to add a card and change the administrator PIN

Correct PIN scenario: If you enter a correct administrator PIN, the agent adds the card and sets a new administrator PIN. The new PIN is either random or matches the value specified in the **Set non-random administrator PIN** option in **Configuration** > **Card Types**.

Incorrect PIN scenario: If you enter an incorrect PIN, the PIN may be blocked. To prevent this, ensure the **Add card without administrator PIN if provided PIN is incorrect** option is enabled. In this case, the agent adds the card without storing or setting an administrator PIN.

About administrator PIN blocking

Each card has a counter for failed administrator PIN entry attempts. If you add a card which has only one attempt left and you enter an incorrect PIN, the PIN is blocked.

For some cards, a blocked administrator PIN cannot be unblocked. If the administrator PIN is blocked, you can only initialize the card, which erases all data stored on it.

How to add a card without the administrator PIN

Incorrect PIN scenario: If you enter an incorrect administrator PIN, the agent can add the card without an administrator PIN. To use this scenario, make sure the **Add card without administrator PIN if provided PIN is incorrect** option is enabled.

If agent added a card without the administrator PIN, you can set the PIN later:

- Manually in the card menu, if you have the *Setting administrator PIN* privilege (**Configuration** → **Roles**).
- Automatically during card issuance with initialization.
- Assigning a **Change Administrator PIN** task to the agent on the user workstation.

Correct PIN scenario: If you enter a correct administrator PIN, the agent adds the card and sets a new administrator PIN. The PIN is either random or matches the value configured in the **Set non-random administrator PIN** option in **Configuration** → **Card Types**.

Assign cards to users

The agent can automatically assign a card to a user when a card is added to Axidian CertiFlow. The card is assigned to the user logged in to the session.

To configure automatic card assignment, enable the following options:

- **Add card**
- **Assign card**

To automatically issue assigned cards, enable the **Issue assigned card** option.

Issue empty cards

The agent can automatically issue cards in *Clean* status (not assigned to a user). The card issuance settings are determined by the policy that applies to the user logged in to the session.

Use case: You need to issue a large number of new cards that you have distributed to users. The cards are not assigned to users. To prevent users from having to issue the cards manually in the Self-Service, you can configure automatic issuance using agents installed on user workstations.

To configure automatic issuance of empty cards, enable the **Issue clean card** option.

Once all cards have been issued, disable the **Issue clean card** option. This prevents a card from being reissued later in its lifecycle. For example, after the card has been revoked.

> **TIP**
> We recommend configuring the agent workflow so that only pre-assigned cards can be issued automatically.

Issue assigned cards

The agent can automatically issue cards in *Assigned* status. The card issuance settings are determined by the policy that applies to the user logged in to the session.

To configure automatic issuance of assigned cards, enable the **Issue assigned card** option.

When the agent issues an assigned card, it verifies that the user logged in to the session is bound to the card. The agent cannot issue a card assigned to another user.

Resume cards issuance or update operations

The agent can automatically resume issuing and updating cards in *Pending* status. To automatically resume card issue or update operations, enable the following options:

- **Resume card issuing**

- **Resume card updating**

Card issue or update operations are paused if your company's policy requires document verification for obtaining digital certificates. The agent resumes issuance or updating once you have approved the user's documents.

For more information, see Card issue documents check and Card update documents check.

Change user PIN

You can configure the validity period for a user PIN on a card.

To set the user PIN validity period:

1. Enable the **Request user PIN changing after (days)** option.
2. Specify the number of days a user PIN remains valid.

Once this period expires, the Card Monitor service creates a **User PIN change** task on the agent. When the user connects the card to the workstation, the agent opens a PIN change window.

Change the user PIN on first login

IDPrime and eToken cards support a hardware requirement to change the user PIN the first time the card is connected to a workstation.

To configure the PIN change requirement for IDPrime and eToken cards:

1. Open the **Configuration** section, navigate to the policy settings and go to **Issuance**.
2. Enable the **User PIN must be changed on first logon** option.

> **TIP**
> You can also configure the PIN change requirement outside Axidian CertiFlow. For example, in a PKI software.

When the user connects the card to a workstation for the first time, the agent opens a PIN change window.

Custom Logs

In the Log section, you can select the created log and request the necessary information using the filters configured for a specific log.

Custom logs store data about cards and certificates, their owners and the systems where they are used.

Log entries are automatically logged when you issue, replace, withdraw or update cards in the Axidian CertiFlow Management Console or Self-Service.

Prerequisites

To allow access to custom logs:

1. Open the Configuration Wizard, go to **Common features** and enable the **Enable custom log** option.
2. Open the Management Console, go to **Configuration→Roles** and assign the *Viewing custom logs* privilege to the administrator or operator role members.
3. Configure the log fields in **Configuration→Custom logs→**Log Templates.

Add and view logs

Log records are entered automatically when you issue, replace or remove cards in the Management Console and in the Self-Service. Log records are entered in the certificate logs when you update cards.

To add a record manually:

1. Click **Add record**.
2. Fill in the required fields and click **Add**.

Export

To upload a custom log to a file, click  and select .xlsx or .csv format.

Documents

The **Documents** section displays a list of documents uploaded to Axidian CertiFlow.

Prerequisites

To allow access to the documents repository:

1. Open the Configuration Wizard, go to **Common features** and enable the **Internal document management** option.
2. Open the Management Console, go to **Configuration→Roles** and assign the *Viewing document repository* privilege to the administrator or operator role members.

Search filters

To find documents, set the following filters:

- **Type**
- **File name**
- **Description**
- **User**
- **Signature status**
- **Original document**
- **Time range**

For example, to find all users who have not uploaded the original documents, set the following filters: **Type→Certificate** and **Original document→Not provided**.

Export search results

You can export the search results to an XLSX file. Click  and select the XLSX format.

Documents operations

You can download  , delete  and edit  documents.

If the user provided the original document, you can record its receipt in Axidian CertiFlow. Click  next to the required document and select **Original received**.

INFO

The internal document management functionality allows users and administrators to exchange documents for obtaining a signature certificate.

Administrators can manage documents in the Management Console and users – in Self-Service.

User guide

You can manage your cards and certificates in Self-Service and in Remote Self-Service.

Self-Service

Self-Service is available at *https://<Server FQDN>/certiflow/ss*.

The administrator defines the service authentication settings in **Configuration→Policies→**Authentication.

The following information is available in a user profile:

- **User information** – a user's name, Logon name, e-mail, phone number and photo. This information is added automatically from the user catalog profile.
- **Your cards** – a list of cards assigned to the user and a list of certificates stored on cards.
- **Your documents** – a list of user documents.

> **INFO**
> The administrator assigns user permissions for operations with cards in **Configuration→Policies→**Workflow.

Remote Self-Service

Remote Self-Service allows you to manage your cards without connecting them to your workstation (except for card unblock operation).

Log in

Remote Self-Service is available at *https://<Server FQDN>/certiflow/rss*.

To log in to Remote Self-Service:

1. Enter your login and the text from the CAPTCHA image.
2. To authenticate, enter answers to secret questions.

Unblock cards

To unblock a card:

1. Launch the Axidian CertiFlow Unblock tool from the Axidian CertiFlow installation package.
2. Select a card from the **Available cards** list.
3. Copy the unblock code from the **Request** field.
4. Open the Remote Self-Service at *https://<Server FQDN>/certiflow/rss*.
5. Select a card and click **Unblock**.
6. Enter the unblock code and click **Get results**.
7. Enter the confirmation code in the **Answer** field.
8. Enter the new PIN, confirm it and click **Unblock**.

Card operations

Issue

How to issue a card

Update

How to update card contents

Disable and enable

How to disable and enable a card

Revoke and clear

How to revoke and clear a card

Reset and change PIN

How to reset your PIN

View contents

How to view and print card contents

Issue

You can get a ready-to-use card or issue a card yourself if you have an empty card. If you have a ready-to-use card, all information about this card is displayed when you log in to Self-Service.

Issue a card

The administrator defines the list of issuance options in policy settings. The following instruction describes how to issue a card with the maximum available options.

1. Connect a card to the workstation.
2. Click **Issue card**.
3. Select certificate templates.

   Administrator settings

   The user can select certificates if you enable the **Select optional certificates when card is issued** option in policy settings (**Workflow→User permissions→Card issuing operations**).

4. Depending on the administrator settings, the card is either initialized or not initialized when issued.

   Not initialized

   1. Enter **User PIN**.
   2. Enter **Admin PIN**.

      Administrator settings

      The **Admin PIN** field is displayed if the card was not added to Axidian CertiFlow and you enabled the **Allow user to add cards when they are issued** option in policy settings (**Workflow→General**).

      INFO

      If you do not set **Admin PIN** and **User PIN**, Axidian CertiFlow uses the PIN values specified by the administrator in **Configuration→Card types**.

   3. Click **Issue**.

4. If your card stores third-party certificates, select the certificates to register them in Axidian CertiFlow.

Administrator settings

The user can select certificates if you enable the **Search for certificates when card is issued or updated to track validity period** and **Allow user to select tracked certificates** options in policy settings (**Workflow→General**).

Initialized

Administrator settings

Enable the **Initialize card** option in policy settings (**Issuance**) and configure initialization settings in **Issuance→Card initialization**.

⚠ **CAUTION**
If the card is initialized when issued, all card contents is deleted.

1. Enter **Admin PIN**. If you do not set **Admin PIN**, Axidian CertiFlow uses the PIN value specified by the administrator in **Configuration→Card types**.

Administrator settings

The **Admin PIN** field is displayed if the card was not added to Axidian CertiFlow and you enabled the **Allow user to add cards when they are issued** option in policy settings (**Workflow→General**).

2. Click **Issue**.

5. If a random PIN was set during the card issue, it is displayed on your screen. If necessary, save your PIN and email it to yourself or your manager.

Administrator settings

A random PIN is set if you enable the **Set random user PIN** option in policy settings (**Issuance**).

The PIN value can be sent by email if you configure email notifications.

6. Click **Close**.

After you issue a card, it is displayed in **Your cards**.

If you have not set the answers to secret questions, proceed to the secret questions settings.

Documents check

Card issue can be suspended if your company's regulations require the documents check and approval before you obtain your certificates.

In the card issue window, you can see this message: *Card issue pending*. The card has *Pending* status. This means that your card issue request is awaiting approval.

You can send the documents in the following ways:

- Using Axidian CertiFlow if the administrator configured the internal electronic document management functionality.
- By any other means authorized in your company. For example, via email.

Send documents using Axidian CertiFlow

If the administrator configured the internal electronic document management functionality, send your documents to the administrator in Self-Service.

> ⓘ **INFO**
> The administrator defines the document approval settings. For more information, see Administrator guide.

Sign and upload the following documents to Axidian CertiFlow.

Certificate request

Submit a signed certificate request form for it to be approved in the certification authority (CA). The administrator can precheck the certificate request before it is sent to the CA.

1. Upload the signed certificate request to Axidian CertiFlow:
    1. Print out the certificate request. Open the **Contents** tab in your card menu and click ! .
    2. Sign the certificate request and upload it to Axidian CertiFlow. **How to sign and upload a document to Axidian CertiFlow**
2. Wait for the certificate request to be approved in the CA. On the **Contents** tab in your card menu you can check the certificate status – *Pending*.
3. If the certificate request is approved in the CA, it gets the *Approved* status and is written on the card. Open the card menu and click **Continue card issue**.
   If the request is rejected, revoke and clear the card or contact the administrator, then restart the card issue operation.

> **INFO**
> If the administrator configured user email notifications, you will receive an email with the approval status notification – *Card issue approved* or *Card issue rejected*.
>
> If user notifications are not configured, wait for the **Continue card issue** option to appear in the card menu.

Certificate form

If your company's e-signature verification certificate policy requires additional approval of the certificate form, the administrator must approve the document before writing the certificate to the card.

In this case, the CA approves the certificate automatically. On the **Contents** tab in the card menu, you can check the status of the certificate – *Valid*. This means that the certificate has been issued in the CA, but not yet written to the card.

1. Upload the signed certificate form to Axidian CertiFlow:
    1. Print the certificate form. Open the **Contents** tab in the card menu, click ! next to the certificate template and select **Certificate**.
    2. Sign the certificate form and upload it to Axidian CertiFlow. **How to sign and upload a document to Axidian CertiFlow**
2. Wait for the administrator to approve the document.
3. If the administrator has approved the document, the certificate is written to the card. Open the card menu and click **Continue card issue**.
   If the administrator has rejected a document, edit and sign the document again and upload it back to Axidian CertiFlow.

> **INFO**
> If the administrator configured user email notifications, you will receive an email with the approval status notification– *Document approved*.
>
> If user notifications are not configured, wait for the **Continue card issue** option to appear in the card menu.

Certificate request and certificate form

To continue the card issue operation and write a certificate to the card:

1. Submit a signed certificate request form and wait for the request to be approved in the CA.
2. Submit a signed certificate form and wait for the administrator to approve the document.

Use the following procedure:

1. Upload the signed certificate request to Axidian CertiFlow:
    1. Print out the certificate request. Open the **Contents** tab in your card menu and click ! .
    2. Sign the certificate request and upload it to Axidian CertiFlow. **How to sign and upload a document to Axidian CertiFlow**
2. Wait for the certificate request to be approved in the CA.
3. If the certificate request is approved in the CA, the certificate status is *Valid*. This means that the certificate has been issued in the CA, but not yet written to the card. Upload the signed certificate form to Axidian CertiFlow for admininstrator's check:
    1. Print the certificate form. Open the **Contents** tab in the card menu, click ! next to the certificate template and select **Certificate**.
    2. Sign the certificate form and upload it to Axidian CertiFlow.

    If the request is rejected in the CA, revoke and clear the card or contact the administrator, then restart the card issue operation.
4. If the administrator has approved the document, the certificate is written to the card. Open the card menu and click **Continue card issue**.
    If the administrator has rejected a document, edit and sign the document again and upload it back to Axidian CertiFlow.

> **INFO**
> If the administrator configured user email notifications, you will receive an email with the approval status notification – *Document approved*, *Card issue approved* or *Card issue rejected*.

Other

Provide documents to the administrator in accordance with your company's e-signature verification certificate policy.

Use the following procedure:

1. Provide the administrator with a signed certificate request form for it to be approved in the CA.
2. Wait for the certificate request to be approved in the CA. On the **Contents** tab in your card menu you can check the certificate status – *Pending*.
3. 3. If the certificate request is approved in the CA, it gets the *Approved* status and is written on the card. Open the card menu and click **Continue card issue**.
   If the request is rejected, revoke and clear the card or contact the administrator, then restart the card issue operation.

> **INFO**
> If the administrator configured user email notifications, you will receive an email with the approval status notification – *Card issue approved* or *Card issue rejected*.
>
> If user notifications are not configured, wait for the **Continue card issue** option to appear in the card menu.

Issue virtual cards

You can issue the following types of virtual cards in Axidian CertiFlow:

- Registry
- TPM Virtual Smart Card (VSC)
- Windows Hello for Business
- AirCard

Registry

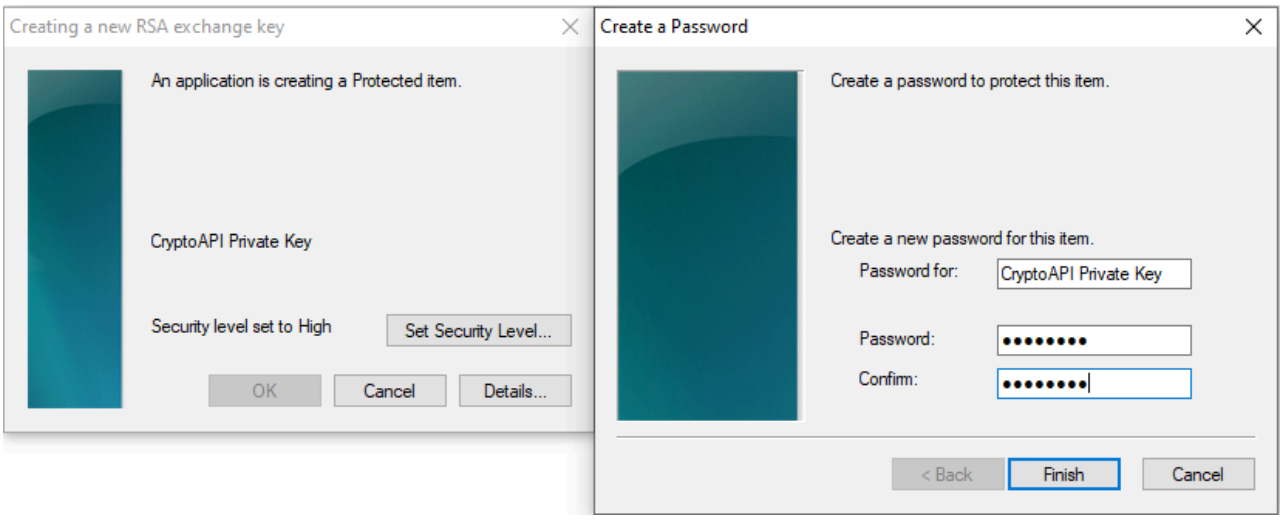
Administrator settings

1. Configure Registry cards support.
2. Add the **Registry.xml** card type in Axidian CertiFlow.
3. Install the CertiFlow.Registry.Middleware component on user workstations.

> **REGISTRY CARDS ISSUE PROPERTIES**
>
> - Only RSA certificates are supported
> - PIN management is not supported
> - Card initialization is not supported

To issue a Registry card:

1. Click **Issue card**.
2. Enter the card name.
3. In the **Card** field, select the following:
   - **Registry - Machine: Registry**, to issue a certificate in the local computer certificate store.
   - **Registry - User: Registry**, to issue the certificate in the current user's certificate store.
4. Click **Issue**. Axidian CertiFlow sends the certificate request to the CA.
5. Create a password for the private key container in the RSA private key creation window.
   This is required if the administrator has enabled the **Prompt the user during enrollment and require user input when the private key is used** option on the **Request Handling** tab in the Microsoft CA Certificate Template settings.
   1. Click **Select security level** and enter a password that meets your company's security requirements.
   2. Click **Finish** and **OK**.



> ⚠ **CAUTION**
> It is not possible to reset the key container password. If you do not remember the key container password, issue the certificate again.

TPM Virtual Smart Card

Administrator settings

1. Open the Axidian CertiFlow Configuration Wizard, go to **Common features** and enable the **Create TPM Virtual Smart Card (VSC)** option.
2. Add the **Tpm.xml** card type to Axidian CertiFlow.

> ⚠ **UNLOCK TPM CARDS**
> To be able to unlock the TPM card, when you add a card type in Axidian CertiFlow, the administrator PIN must change to random or any non-random Triple DES.

3. Install the Trusted Platform Module (2.0) on user workstations.
4. Install the Certiflow.TPM.Middleware component on user workstations.

> ⓘ **TPM VSC CARDS ISSUE PROPERTIES**
> - Only RSA certificates are supported
> - Card initialization is not supported

To issue a TPM VSC card:

1. Click **Issue card**.

2. Enter the card name.
3. Select **Create a TPM** or select a card created before.
4. Click **Issue**.

Axidian CertiFlow creates a virtual card. The TPM virtual card can be used as a hardware card on user workstations. For example, for domain authentication.

Windows Hello for Business

Administrator settings

1. Deploy the Windows Hello for Business infrastructure according to Microsoft instructions.
2. Open the Axidian CertiFlow Configuration Wizard, go to **Common features** and enable the **Create Windows Hello for Business**.
3. Add the **Whfb.xml** card type to Axidian CertiFlow.
4. Install the Trusted Platform Module (2.0) on user workstations.
5. Install the AxidianCertiflow.WHfB.Middleware component on user workstations.

> **WINDOWS HELLO FOR BUSINESS CARDS PROPERTIES**
>
> - Only RSA 2048 certificates are supported
> - Maximum number of WHfB cards on a Windows 10 computer is 10
> - Only one WHfB card can be created for one user on one workstation
> - Card initialization is not supported

To issue a Windows Hello for Business card:

1. Click **Issue card**.
2. Enter the card name.
3. Click **Create WHfB**.
4. Click **Issue**.
5. Configure card PIN settings:
    1. Click **Set up PIN**.
    2. Enter the credentials for the main authentication and user authentication (using the Axidian CertiFlow MFA adapter) and click **Submit**.
    3. Enter PIN and click **OK**.

Axidian CertiFlow creates a virtual card. The Windows Hello for Business virtual card can be used as a hardware card on user workstations. For example, for domain authentication.

AirCard

Administrator settings

1. 1. Open the **Configuration** section, navigate to the policy settings and go to **Workflow**. enable the **Issue AirCard** option in **User permissions**→ **General**.
2. Add the **AirCard.xml** card type to Axidian CertiFlow.
3. Install the AxidianCertiflow.AirCard.Middleware and AxidianCertiflow.AirCard.Runtime components on user workstations.
4. Configure the Axidian AirCard Enterprise server network availability for user workstations.

> **INFO**
> You can issue only RSA certificates on AirCards.

After you install the Axidian AirCard Runtime, an AirCard indicator appears in Windows Taskbar.

To issue an AirCard:

1. Click **Issue AirCard**.
2. Enter the card name.
3. Select **Create a new AirCard** or select a card created before.
4. Click **Issue**.

After AirCard is issued, it binds with a workstation automatically. The list of allowed computers is displayed in the card menu.

Connect AirCard to a workstation

You can connect an AirCard to a workstation:

- Automatically in Axidian CertiFlow
  After an AirCard is issued, it automatically connects to the authorized computers if they belong to the company's corporate network.
- Manually in the Axidian AirCard Enterprise control panel
  Use this method if you cannot connect the card automatically (for example, if the computer is outside the company's network). In this case, only the administrator can issue an AirCard.

How to connect an AirCard manually

Add an AirCard manually in Axidian AirCard Enterprise control panel and connect it to the workstation:

1. Open the Axidian AirCard Enterprise control panel.
2. Click  and  .
3. In the **Code** field, enter the code sent by the administrator. The code is valid for an hour and can only be used once. The Axidian AirCard Enterprise server address is set automatically.
4. Click **Add**.

You can view AirCards connected to your workstation in the **Active smart cards** section of the Axidian AirCard Enterprise control panel. Each card has an ID (serial number) which is displayed in the Axidian CertiFlow services.

You can see the connected cards indicator in Windows taskbar. If no cards are connected to the workstation, or there is no connection to the Axidian AirCard Enterprise server, the indicator is grey, if at least one card is connected, the indicator is blue.

Update

If one or more certificates on your card expire, or you want to issue a new certificate, perform the update operation.

> **INFO**
> The administrator configures user permissions for card update operation. For more information, see Administrator guide.

Update a card

The administrator defines the list of update options in policy settings. The instruction below describes how to update a card with the maximum available options.

1. Connect a card to the workstation.
2. Click **Update card contents**.
3. Select certificate templates.

   > **Administrator settings**
   >
   > The user can select certificate templates if you enable the **Select optional certificates when card is updated** option in policy settings (**Workflow → User permissions → Issued card operations**).

4. Enter **User PIN**.
5. If your card stores third-party certificates, select the certificates to register them in Axidian CertiFlow.

   > **Administrator settings**
   >
   > The user can select certificates if you enable the **Search for certificates when card is issued or updated to track validity period** and **Allow user to select tracked certificates** options in policy settings (**Workflow→General**).

6. Click **Update**.

Documents check

The card update operation can be suspended if your company's regulations require the documents check and approval before you obtain your certificates.

In the card update window, you can see this message: *Card update operation pending*. The card has the *Pending* status. This means that your card update request is waiting for approval.

You can send the documents in the following ways:

- Using Axidian CertiFlow if the administrator configured the internal electronic document management functionality.
- By any other means authorized in your company. For example, via email.

Send documents using Axidian CertiFlow

If the administrator configured the internal electronic document management functionality, send your documents to the administrator in Self-Service.

> **INFO**
> The administrator defines the document approval settings. For more information, see Administrator guide.

Sign and upload the following documents to Axidian CertiFlow:

Certificate request

Submit a signed certificate request form for it to be approved in the certification authority (CA). The administrator can precheck the certificate request before it is sent to the CA.

1. Upload the signed certificate request to Axidian CertiFlow:
    1. Print out the certificate request. Open the **Contents** tab in your card menu and click ! .
    2. Sign the certificate request and upload it to Axidian CertiFlow. **How to sign and upload a document to Axidian CertiFlow**
2. Wait for the certificate request to be approved in the CA. On the **Contents** tab in your card menu you can check the certificate status – *Pending*.
3. If the certificate request is approved in the CA, it gets the *Approved* status and is written on the card. Open the card menu and click **Continue card update operation**.
   If the request is rejected, revoke and clear the card or contact the administrator, then restart the card update operation.

> **INFO**
> If the administrator configured user email notifications, you will receive an email with the approval status notification – *Card update operation approved* or *Card update operation rejected*.
>
> If user notifications are not configured, wait for the **Continue card update operation** button to appear in the card menu.

Certificate form

If your company's e-signature verification certificate policy requires additional approval of the certificate form, the administrator must approve the document before writing the certificate to the card.

In this case, the CA approves the certificate automatically. On the **Contents** tab in the card menu, you can check the status of the certificate - *Valid*. This means that the certificate has been issued in the CA, but not yet written to the card.

1. Upload the signed certificate form to Axidian CertiFlow:
    1. Print the certificate form. Open the **Contents** tab in the card menu, click ! next to the certificate template and select **Certificate**.
    2. Sign the certificate form and upload it to Axidian CertiFlow. **How to sign and upload a document to Axidian CertiFlow**
2. Wait for the administrator to approve the document.
3. If the administrator has approved the document, the certificate is written to the card. Open the card menu and click **Continue card update operation**.
   If the administrator has rejected a document, edit and sign the document again and upload it back to Axidian CertiFlow.

> **INFO**
> If the administrator configured user email notifications, you will receive an email with the approval status notification– *Document approved*.
>
> If user notifications are not configured, wait for the **Continue card update operation** button to appear in the card menu.

Certificate request and certificate form

To continue the card update operation and write a certificate to the card:

1. Submit a signed certificate request form and wait for the request to be approved in the CA.
2. Submit a signed certificate form and wait for the administrator to approve the document.

Use the following procedure:

1. Upload the signed certificate request to Axidian CertiFlow:
    1. Print out the certificate request. Open the **Contents** tab in your card menu and click ! .
    2. Sign the certificate request and upload it to Axidian CertiFlow. **How to sign and upload a document to Axidian CertiFlow**
2. Wait for the certificate request to be approved in the CA.
3. If the certificate request is approved in the CA, the certificate status is *Valid*. This means that the certificate has been issued in the CA, but not yet written to the card. Upload the signed certificate form to Axidian CertiFlow for admininstrator's check:
    1. Print the certificate form. Open the **Contents** tab in the card menu, click ! next to the certificate template and select **Certificate**.
    2. Sign the certificate form and upload it to Axidian CertiFlow.

    If the request is rejected in the CA, revoke and clear the card or contact the administrator, then restart the card issue process.
4. If the administrator has approved the document, the certificate is written to the card. Open the card menu and click **Continue card update operation**.
    If the administrator has rejected a document, edit and sign the document again and upload it back to Axidian CertiFlow.

> **INFO**
> If the administrator configured user email notifications, you will receive an email with the approval status notification – *Document approved*, *Card update operation approved* or *Card update operation rejected*.

Other

Provide documents to the administrator in accordance with your company's e-signature verification certificate policy.

Use the following procedure:

1. Provide the administrator with a signed certificate request form for it to be approved in the CA.
2. Wait for the certificate request to be approved in the CA. On the **Contents** tab in your card menu you can check the certificate status – *Pending*.
3. 3. If the certificate request is approved in the CA, it gets the *Approved* status and is written on the card. Open the card menu and click **Continue card update operation**.
   If the request is rejected, revoke and clear the card or contact the administrator, then restart the card issue process.

> **INFO**
> If the administrator configured user email notifications, you will receive an email with the approval status notification – *Card update operation approved* or *Card update operation rejected*.
>
> If user notifications are not configured, wait for the **Continue card update operation** button to appear in the card menu.

Disable and enable

You can disable your card for a certain period of time and then enable it again. To disable or enable a card, you do not need to connect it to a workstation.

> **INFO**
> The administrator configures user permissions for card disable and enable operations. For more information, see Administrator guide.
>
> If the administrator enabled the **Revoke certificate at card revoking/disabling** option in the CA certificate template settings, all certificates stored on a card are removed.

To disable a card, click **Temporarily disable card** in the card menu and confirm the operation. The card status changes from *Issued* to *Disabled*.

To enable a card, click **Enable card** in the card menu and confirm the operation. The card status changes from *Disabled* to *Issued*.

Disable a card without logging in to the OS

You can disable a card without logging in to the operating system if the administrator configured this permission.

Your workstation must have a connection to the Axidian CertiFlow server and the secret questions must be set in Self-Service.

To disable a card:

1. Select **Disable card** on the OS login screen.
2. Enter your login and select a card that you want to disable.
3. Enter answers to secret questions.
4. Select your card from the list and click **Next**.

Revoke and clear

You can revoke your card if it is damaged, lost or compromised.

> ⓘ **INFO**
> The administrator configures user permissions for card revoke and clear operations. For more information, see Administrator guide.
>
> If the administrator enabled the **Revoke certificate at card revoking/disabling** option in the CA certificate template settings, all certificates stored on a card are removed.

Revoke

To revoke a card:

1. Select **Report card as lost, damaged or compromised** in the card menu.
2. Specify the reason of card revocation:
3. Click **Revoke**.

Card status changes from *Issued* на *Revoked*.

Clear

You can only clear a card with the *Revoked* status. To clear your card, connect it to your workstation and click **Clear card**.

> ⓘ **INFO**
> To clear TPM, Registry, Windows Hello for Business cards, click **Delete card**.

> ⚠ **CAUTION**
> When you clear your card, all data written to it using Axidian CertiFlow is deleted.

User PIN

You can change the user PIN when you clear the card. Axidian CertiFlow changes it to the default value or a value consistent with your company's security policy (password length and complexity requirements).

Set **New user PIN** or leave the field blank to set the default PIN. Click **Clear**.

After a card is cleared, it remains assigned to you in Axidian CertiFlow and can be issued again.

Reset and change PIN

If you do not remember your card PIN and blocked your card, you can reset the PIN and set a new one.

> **INFO**
> The administrator configures user permissions for card PIN reset operation. For more information, see Administrator guide.

To reset the card PIN:

1. Select **Reset card PIN** in the card menu.
2. Connect the card to the workstation.
3. Enter a new PIN and confirm it.
4. Click **Reset** and **Close**.

To change the card PIN:

1. Select **Change card PIN** in the card menu.
2. Connect the card to the workstation.
3. Enter your current PIN, enter a new PIN and confirm it.
4. Click **Change** and **Close**.

View contents

You can view the certificates stored on the card and print the certificate documents on the **Contents** tab in the card menu.

> **INFO**
> The administrator configures access to the card contents. For more information, see Administrator guide.

Change answers to secret questions

To change answers to secret questions:

1. Click **Change answers to secret questions** under user information list.
2. Select the question and enter the answer to the question.
3. Click **OK**.

> **INFO**
> The administrator configures user permissions for changing answers to secret questions. For more information, see Administrator guide.

Michael Benson

Logon name	DEMO\Michael.Benson
E-mail	m.benson@indeed.com
Phone	+555 90524683735

Change answers to security questions

Security questions

Security questions are required to confirm operations with your cards

Security question

Who was your childhood hero?

Answer

OK Cancel

Documents

The internal document management functionality allows users and administrators to exchange documents for obtaining a signature certificate.

Document types

- **Personal** – ID copies
- **Certificate request** – a signed copy of an application for obtaining a signature certificate
- **Certificate** – a signed copy of the certificate form
- **Certificate revocation request** – a signed copy of an application for terminating a signature certificate
- **User documents** – other types of documents

You can manage documents in **Your documents** in Self-Service. The following operations are available: add, sign, download, edit and delete.

Administrator settings

To allow users to manage documents in Self-Service:

1. Open the Configuration Wizard.
2. Go to **Common features**.
3. Enable the **Internal Document Management** option.

To allow users to delete documents:

1. Open the Management Console and go to policy settings.
2. Go to **Workflow→User Permissions→Documents**.
3. Enable the **Delete** option.

Sign documents

The following operations are available:

- Add documents signed on paper
- Add documents and sign with digital signature
- Sign documents generated from ready-made templates

Add paper-signed documents

To add a paper-signed document^

1. Click **Add Document** in **Your Documents**.
2. Select the document type.
3. Upload the file.
4. (Optional) Fill in the **Description** field.
5. Click **Add**.

Add and sign documents with a digital signature

> **REQUIREMENTS FOR SIGNING DOCUMENTS**
>
> - You have a card with a signature certificate.
> - The signature certificate has any status except *Revoked*, *Expired*, *Key Expired*, and *Error*.
> - the **Enhanced Key Usage** field contains the Secure Email (Secure Email, OID 1.3.6.1.5.5.7.3.4) and Code Signing (codeSigning, OID 1.3.6.1.5.5.7.3.3) values according to digital signature requirements (RFC 5280).

To add and sign a document:

1. Click **Add document** in **Your documents**.
2. Select the document type and upload the file.
3. Fill in the **Description** field (optional).
4. Enable the **Sign document** option.
5. Connect your card with a signature certificate to the workstation and select it in the **Card list**.
6. In the **Certificate** list, select the appropriate signature certificate.
7. Enter the user PIN.
8. Click **Add**.

Sign documents generated from ready-made templates

You can sign documents that are already available in Axidian CertiFlow. Documents are generated from templates configured by the administrator in **Configuration**→Print Templates.

Signed documents automatically appear in the **Your Documents** list.

To sign a document:

1. In **Your Cards**, select the card that contains the required certificate and go to the **Contents** tab.

2. Click next to the required certificate and select a document template: certificate, certificate request, or certificate revocation request. The document opens.
3. Click **Sign document**. To download and print the document without a signature, click **Save document**.
4. Connect the card with the signature certificate to the workstation and select it in the **Card list**.
5. In the **Certificate** list, select the appropriate signature certificate.
6. Enter the user PIN.
7. Click **Sign**.

Client agent

The administrator can install a client agent on a user workstation to assign card tasks on the agent. For more information, see Administrator guide.

The agent starts automatically.

The following tasks involve user operations:

- Change the card PIN
- Reset the card PIN
- Update card contents

Change PIN

The administrator can set an expiration date for your card PIN.

If your PIN has expired, you can change it when you connect the card to the workstation.

> ⓘ **IDPRIME AND ETOKEN 72K CARDS**
> If the administrator has configured the requirement to change the PIN for IDPrime and eToken 72K cards, you must set a new PIN when you connect an IDPrime or a eToken 72K card to the workstation for the first time.

Reset PIN

If you do not remember the card PIN, contact the administrator. The administrator assigns a card PIN reset task on the agent installed on your workstation. Connect the card to the workstation and wait for the PIN reset form to appear.

> ⚠ **CAUTION**
> To reset your PIN, you must have configured answers to security questions. If you do not remember the answers, change them in Self-Service.

To reset the PIN:

1. Connect the card to the workstation. A PIN reset form appears.
2. Enter answers to secret questions.
3. Set a new PIN and confirm it.

4. Click **Reset**.

When the PIN is reset, you can see the following message: *User PIN reset successfully*.

Update card contents

If one or more certificates on your card expire, or you want to issue a new certificate, the card must be updated.

The administrator assigns a card update task on the agent installed on your workstation.

To update your card:

1. Connect the card to the workstation.
2. Enter PIN and click **Update**.
3. If your card stores third-party certificates, select the certificates to register them in Axidian CertiFlow.

   ▼ **Administrator settings**

   Enable the **Select optional certificates when card is updated** option in policy settings (**Workflow→User permissions→Issued card operations**).

4. Click **OK**.

The update may take several minutes. When the card is updated, you can see the following message: *Card updated successfully*. IIf the update task ends with an error, it appears on your screen.

The card update operation can be suspended if your company's regulations require the documents check and approval before you obtain your certificates. In the card update window, you can see this message: *Card update operation pending*. The card has the *Pending* status.
More about documents check

View files and links

The administrator can add files and links for to users in Self-Service.

The uploaded files and links are available at *https://<Server FQDN>/certiflow/ss/Downloads*.

> **TIP**
> Files and links upload is available if the administrator activated the **Enable downloads** option in the **Common features** setion of the Axidian CertiFlow Configuration Wizard.

API

A set of API functions allows you to manage cards by means of client applications. You can access API functions through the web-API application.

Authentication

How to authenticate in API services

Cards

How to manage cards using API

Authentication

You can use any API tools to manage cards with Axidian CertiFlow API. This article describes how to configure API authentication in Swagger, Postman, Windows Powershell and Linux Bash.

Select the instruction depending on the authentication type configured in the Axidian CertiFlow Configuration Wizard.

Windows

Check authentication settings

1. Launch the IIS Manager and select **Default Web Site** in the left menu.
2. Expand the **CertiFlow** applications list and select the **api** application.
3. In the application control panel, select the **Authentication** property and make sure that **Windows Authentication** is set.
4. Close the IIS Manager.
5. Open the *C:\inetpub\wwwroot\certiflow\api\appsettings.json* configuration file and make sure that the `authentication` parameter is set to `Windows`.

Swagger

To use Swagger, set up the API configuration file:

1. Navigate to the *C:\inetpub\wwwroot\certiflow\api* catalog and open the *appsettings.json* file.
2. In the `webApiSettings` section, set the `enableSwagger` parameter to `true` and save the changes.
3. Apply changes to the Axidian CertiFlow Server.

Swagger is available at `https://<Server FQDN>/certiflow/api/swagger`.

Postman

Postman is available as a desktop or a web application. The instruction below describes how to configure authentication in the Postman desktop application.

1. Click **Add** in the workbench to open a new tab.
2. Go to the **Auth** tab and select **NTLM Authentication**.
3. Enter the username and password.
4. Select the request type and specify the request URL.
5. Click **Send**.

OpenID Connect

Check authentication settings

To check API authentication settings on the Axidian CertiFlow Windows server:

1. Launch the IIS Manager and select **Default Web Site** in the left menu.
2. Expand the **CertiFlow** applications list and select the **api** application.
3. In the application control panel, select the **Authentication** property and make sure that **Anonymous Authentication** is set.
4. Close the IIS Manager.
5. Navigate to the *C:\inetpub\wwwroot\certiflow\api* catalog and open the *appsettings.json* file.
6. Make sure the `authentication` parameter is set to `OAuth2Introspection`.

To check API authentication settings on the Axidian CertiFlow Linux server:

1. Navigate to the */opt/axidian/certiflow/api* catalog and open the *appsettings.json* file.
2. Make sure the `authentication` parameter is set to `OAuth2Introspection`.

Swagger

To use Swagger, set up the API configuration file:

1. Navigate to the *C:\inetpub\wwwroot\certiflow\api* catalog in Windows OS or */opt/axidian/certiflow/api* in Linux OS and open the *appsettings.json* file.
2. In the `webApiSettings` section, set the `enableSwagger` parameter to `true`.
3. Save the changes.
4. Apply changes to the Axidian CertiFlow Server.

To authenticate in Swagger:

1. Open your browser and go to `https://<Server FQDN>/certiflow/api/swagger`.
2. Click **Authorize**.
3. In the **Scopes** string, click **Select all**.
4. Click **Authorize**.

Postman

Postman is available as a desktop or a web application. The instruction below describes how to configure authentication in the Postman desktop application.

To configure authentication in Postman:

1. Click **Add** in the workbench to open a new tab.

2. Navigate to the **Auth** tab and select **OAuth 2.0**.
3. Leave the **Add auth data to** field value as default.
4. In the **Current Token** section, leave the **Header Prefix** field value as default.
5. In the **Configure New Token** section, specify the data to obtain an access token:
   - **Token Name** – specify the token name.
   - **Grant Type** – select **Password Credentials**.
   - **Access Token URL** – specify the link to obtain an access token: `https://<Server FQDN>/oidc/connect/token`.
   - **Client ID** – specify the `WebApiClient` service identifier.
   - **Username** – specify the username in the `Domain\Username` format.
   - **Password** – specify the user password.
   - **Client Authentication** – select **Send as Basic Auth header**.
6. Click **Get New Access Token**.
7. Click **Use Token**.

To make an API request:

1. Select the request type.
2. Specify the request URL.
3. Click **Send**.

Windows Powershell

To work with the API through Powershell, use Powershell scripts.

Obtain an access token and make a request:

1. Open the terminal or a Powershell script file and prepare the following parameters.

```
$body = @{grant_type='password'; username='Domain\Username';
password='P@ssw0rd'; scope='openid webapi';client_id='WebApiClient' }
$url="https://<Server FQDN>/oidc/connect/token"
```

2. Extract the access token from the response.

```
$resp = Invoke-RestMethod -Method Post -Uri $url -Body $body -
UseDefaultCredentials
$token = $resp.access_token
```

3. Add the token to the request header.

```
$headers = @{Authorization="Bearer $token"}
```

4. Make a request.

```
Invoke-RestMethod -Method Get -Uri $url -Headers $headers -UseDefaultCredentials
```

Linux Bash

To work with the API through Linux Bash, use Bash scripts.

Obtain an access token and make a request:

1. In the terminal or in a Bash script file, prepare the following parameters.

```
username="DOMAIN\\username"
password="P@ssw0rd"
base_url="https://<Server FQDN>"
body="grant_type=password&username=$username&password=$password&scope=openid%20web
token_url="$base_url/certiflow/oidc/connect/token"
```

```
2. Extract the access token from the response.

 ```bash
 resp=$(curl -s -X POST $token_url -H "Content-Type: application/x-www-form-
urlencoded" --data $body)
 token=$(echo $resp | grep -o '"access_token": "[^"]*' | cut -d'"' -f4)
```

3. Add the token to the request header.

```
headers="Authorization: Bearer $token"
```

4. Make a request.

GET request example

```
curl -X GET "$base_url/certiflow/api/Cards?state=Issued&offset=0&count=0" -H
"$headers" -d ''
```

POST request example
```

```
curl -X POST "$base_url/certiflow/api/Cards/123/Enable" -H "$headers" -d ''
```

Bash script example

```
#!/bin/sh
#User input
username="DEMO\\admin"
password="P@ssw0rd"
base_url="https://certiflow-test.local"
body="grant_type=password&username=$username&password=$password&scope=openid%20we
token_url="$base_url/certiflow/oidc/connect/token"
# Get token
resp=$(curl -s -X POST $token_url -H "Content-Type: application/x-www-form-urlenc
# Parse token
token=$(echo $resp | grep -o '"access_token": "[^"]*' | cut -d'"' -f4)
# Combine header
headers="Authorization: Bearer $token"
# Test enable card (POST)
curl -X POST "https://certiflow-test.local/certiflow/api/Cards/123/Enable" -H "ac
# Test Get enabled card (GET)
curl -X GET "https://certiflow-test.local/certiflow/api/Cards?state=Issued&offset
text/plain"
```

Cards

Cards API allows you to perform the following operations:

- Get a list of cards added to Axidian CertiFlow
- Find a card by ID
- Revoke a card
- Withdraw a revoked card
- Disable a card
- Enable a card
- Preupdate a user certificate

`GET /Cards`

`GET /Cards` request returns a list of cards according to the specified filters.

Request parameteres

Parameter	Description
`userName`	User logon name in down-level logon name format (DOMAIN\LogonName) or in User principal name (UPN) format
`policyName`	Card policy name
`serialNumber`	c
`cardTypeName`	Card type name
`cardModelName`	Card model name. The value is only displayed for eToken PRO Java 72K and IDPrime MD cards if card model settings are installed in **Configuration→Card types**
`comment`	Card notes
`tags`	Card tags
`state`	Card status: `Clean`, `Assigned`, `Pending`, `Issued`, `Disabled`, `Revoked`
`contentExpirationStatus`	Information about the expiration date of certificates that are associated with a card: `None`: No expiring or expired certificates `ManagedCertificatesExpiring`: Managed certificates are about to expire `ManagedCertificatesExpired`: Managed certificates expired `CommonCertificatesExpiring`: Common certificates are about to expire `CommonCertificatesExpired`: Common certificates expired `TracedCertificatesExpiring`: Traced certificates are about to expire `TracedCertificatesExpired`: Traced certificates expired
`timeIssued`	Card issue date in ISO 8601 format. Example: 2024-12-03T11:22:20.1824104Z, 2024-12-03
`timeUpdated`	Card update date in ISO 8601 format
`timeRevoked`	Card revocation date in ISO 8601 format
`offset`	Shift by the specified number of cards

Parameter	Description
`count`	Number of cards stated in the response

Response parameteres

Parameter	Description
`id`	Card ID
`serialNumber`	Card serial number
`cardTypeName`	Card type name
`cardModelName`	Card model name. The value is only displayed for eToken PRO Java 72K and IDPrime MD cards if card model settings are installed in **Configuration→Card types**
`atr`	Answer To Reset
`label`	Card label
`comment`	Card notes
`tags`	Tags
`state`	Card status
`formFactor`	Card form factor
`pacNumber`	Card PAC number
`expirationDate`	Card expiration date in ISO 8601 format
`timeIssued`	Card issue date in ISO 8601 format
`timeDisabled`	Card disabling date in ISO 8601 format
`timeUpdated`	Card update date in ISO 8601 format
`timeRevoked`	Card revocation date in ISO 8601 format
`userId`	Card owner user ID
`userName`	User logon name in down-level logon name format (DOMAIN\LogonName) or in User principal name (UPN) format
`policyId`	Card policy ID

Parameter	Description
`policyName`	Card policy name
`certificates`	`type`: Certificate type `serialNumber`: Certificate serial number `thumbprint`: Certificate Thumbprint `subject`: Common name of the Certificate Subject `issuer`: Common name of the Certificate Issuer `validFrom`: Certificate issue date in ISO 8601 format `validTo`: Certificate expiration date in ISO 8601 format

Request example

```
http://localhost/certiflow/api/Cards – show all cards
http://localhost/certiflow/api/Cards?offset=0&count=50 – show 50 cards without a shift
```

`GET /Cards/{id}`

`GET /Cards/{id}` request returns data filtered by card ID.

Request parameters

`id`: Card ID

Request example

```
http://localhost/certiflow/api/Cards/1
```

`POST /Cards/{id}/Revoke`

`POST /Cards/{id}/Revoke` request allows you to revoke a card.

Request parameteres

Parameter	Required/Optional	Description
`id`	Required	Card ID
`reason`	Optional	Card revocation reason 0 `--`: Reason is not stated 1: `CardBroken` 2: `CardLost` 3: `CardUpgrade` 4: CardExpired 5: `CardWithdraw` 6: `UserRemoved` 7: `CardCompromised`

Request example

```
http://localhost/certiflow/api/cards/1/revoke
```

`POST /Cards/{id}/Withdraw`

`POST /Cards/{id}/Withdraw` allows you to withdraw a revoked card from a user. Card contents is preserved when you withdraw the card.

You can only withdraw a card with *Revoked* status.

Request parameters

`id`: Card ID

Request example

```
http://localhost/certiflow/api/cards/1/withdraw
```

`POST /Cards/{id}/Disable`

`POST /Cards/{id}/Disable` allows you to temporarily deactivate a card.

Request parameters

`id`: Card ID

Request example
`http://localhost/certiflow/api/cards/1/disable`

`POST /Cards/{id}/Enable`

`POST /Cards/{id}/Enable` allows you to enable a card.

Request parameteres

`id`: Card ID

Request example
`http://localhost/certiflow/api/cards/1/enable`

`POST /Cards/{id}/Preupdate`

`POST /Cards/{id}/Preupdate` allows you to revoke an invalid user certificate.

Request parameteres

`id`: Card ID

Request example
`http://localhost/certiflow/api/cards/1/preupdate`

INFO

You can use `POST /Cards/{id}/Preupdate` method when you assign a new policy on a card user. The certificate is revoked automatically if it is not supported in the new policy and the **Revoke certificate when card is revoked/disabled** option is enabled in the certificate template in the old policy.

`POST /Cards/{id}/Preupdate` method cannot be performed on a card that is disabled, assigned, revoked, or pending.

Troubleshooting

Collect logs

How to collect the Axidian CertiFlow logs

Technical support

How to contact Axidian technical support

Collect logs

Server

Follow these steps to retrieve troubleshooting data and log files of the Axidian CertiFlow server components.

1. Open the required service's catalog.

Service files locations

Windows

Service name	Location
Card Monitor	*%ProgramFiles%\Axidian CertiFlow\CardMonitor*
Agentregistrationapi	*%SystemDrive%\inetpub\wwwroot\certiflow\agent\agentregistrationapi*
Agentserviceapi	*%SystemDrive%\inetpub\wwwroot\certiflow\agent\agentserviceapi*
API	*%SystemDrive%\inetpub\wwwroot\certiflow\api*
Credprovapi	*%SystemDrive%\inetpub\wwwroot\certiflow\credprovapi*
Management Console	*%SystemDrive%\inetpub\wwwroot\certiflow\mc*
OpenID Connect Server	*%SystemDrive%\inetpub\wwwroot\certiflow\oidc*
Remote Self-Service	*%SystemDrive%\inetpub\wwwroot\certiflow\rss*
Self-Service	*%SystemDrive%\inetpub\wwwroot\certiflow\ss*
Configuration Wizard	*%SystemDrive%\inetpub\wwwroot\certiflow\wizard*
AirCard Enterprise server	*%SystemDrive%\inetpub\wwwroot\Axidian.AirCard.EntServer*

Linux

Service name	Location
Card Monitor	*/opt/axidian/certiflow/cardmonitor*
Agentregistrationapi	*/opt/axidian/certiflow/agentregistrationapi*
Agentserviceapi	*/opt/axidian/certiflow/agent/agentserviceapi*
API	*/opt/axidian/certiflow/api*
Credprovapi	*/opt/axidian/certiflow/credprovapi*

Service name	Location
Management Console	*/opt/axidian/certiflow/certiflow\mc*
OpenID Connect Server	*/opt/axidian/certiflow/oidc*
Remote Self-Service	*/opt/axidian/certiflow/rss*
Self-Service	*/opt/axidian/certiflow/ss*
Configuration Wizard	*/opt/axidian/certiflow/wizard*

2. Open the *nlog.config* file in a text editor, such as Notepad, launched with administrator privileges, and change the value of the `minlevel` parameter from `Off` to `Trace`.

```
<logger name="*" minlevel="Trace" writeTo="file" />
```

3. Save the changes and close the file.

4. Open the *logs* catalog in the service's main catalog and delete the existing log files.

5. Reproduce the issue.

6. Return to the *logs* catalog and make sure that new subcatalogs with debug information files have been created.

7. Send the entire *logs* catalog with all its contents to Axidian technical support. Include the issue description.

8. To disable logging, change the `minlevel` parameter value from `Trace` to `Off` and save the changes.

Client

Windows

To collect client logs, use the CertiFlow GetLog tool.

1. Open the *CertiFlow.GetLog* catalog in the Axidian CertiFlow installation package and run *CertiFlow.GetLog.exe* as administrator.

2. To connect to the local machine, enter ***localhost*** in the **Computer** field. To connect to a remote machine, enter its name or IP. Click **Connect**.

> **INFO**
> To establish a connection to a remote computer running Windows Vista or higher, make sure that the Windows Management Instrumentation (WMI) service is running on the remote computer.

3. Click **Enable Log** to start logging.

4. Reproduce the issue.

5. Click **Disable Log** to stop logging.

6. Click **Get Log...** to collect the logs.

7. Specify the catalog to save the logs and click **Save**.

8. Click **Disconnect** to disconnect from the computer.

9. Send the logs to Axidian technical support. Include the issue description.

> **INFO**
> By default, logs are stored locally in *C:\Windows\System32\LogFiles\certiflow*. For remote log collection, the default network path is *ADMIN$\System32\LogFiles\certiflow*. To select another storage, go to **Advanced Settings** and specify an alternative logging catalog in the **Use alternative location** option.

Advanced Settings

Setting	Description
Max. log size (bytes)	The maximum size, in bytes, for all files in the log catalog. Default value: 1 GB. When the maximum size is reached, the contents of the catalog are automatically deleted, except for log files modified within the **Max. log file age** period.
Max. log file age (s)	The maximum age of a log file in seconds. If the total size of logs in the catalog exceeds the **Max. log size** value, all files modified within the **Max. log file age** period are deleted from the catalog. Example: The maximum size of all logs in the *LogFiles\certiflow* catalog is 1 GB (Max. log size (bytes) = 1000000000), and the maximum log file age is 24 hours (Max. log file age (s) = 86400). When the size of the log folder exceeds 1 GB, all files except those written in the last 24 hours are deleted.
Cleaner interval (s)	The interval, in seconds, at which the size of the log catalog is checked. Default value: 1 hour (3600 seconds).
Activity checking period (ms)	The interval, in milliseconds, at which logging activity is checked. Before starting to write logs, the client component verifies whether logging is enabled on the workstation. Default checking interval: 1 minute (60,000 milliseconds).
Enable log cycling	Enables log file cycling mode. If this option is enabled, logs for service are written according to the specified settings for the number of files and file size. - **Max. size of a log file (bytes)**: The maximum size of a single log file in bytes. Default: 10 MB (10,000,000 bytes). When the specified size is reached, the file's contents are overwritten with new data. - **Max. number of saved log files**: The maximum number of log files to keep. Default: 5, excluding the currently active log file. If the set number of files is exceeded, the oldest file is deleted, and logs continue to be written to a new file.
Use alternative location	Specifies an alternative catalog for writing logs. If this option is disabled, logs are written to the default catalogs: - Local path: *%WINDIR%\System32\LogFiles\certiflow* - Network path: *ADMIN$\System32\LogFiles\certiflow*

Linux

Logs for Axidian CertiFlow Middleware installed on Linux are written to the */tmp/certiflow/logs* catalog.

To manage logs:

1. Open the */etc/cm/logging.cfg* file as administrator.
2. Change the value of the `enabled` parameter:
   - Set `1` to enable logging.
   - Set `0` to disable logging.
3. Save the file.

To collect logs:

1. Clear the existing logs in the */tmp/certiflow/logs* catalog.
2. Reproduce the issue.
3. Send the logs to Axidian technical support. Include the issue description.

Installer packages

All Axidian CertiFlow installers for Windows are distributed as MSI (Windows Installer) packages. To get debug logs for MSI packages, run the installer in the command line with specific parameters.

Here is the command syntax for launching an MSI package with logging enabled:

```
msiexec /i <path_to_installer> /lv <path_to_log_file>
```

After the installer completes, send the log file to Axidian technical support. Include the issue description.

```
msiexec /i AxidianCertiFlow.Client.Tools-<version_number>.x64.en-us.msi /lv log.txt
This command launches the Axidian CertiFlow Client Tools installer from the current
folder. Installation logs are written to the log.txt file, located in the same folder.

msiexec /i D:\CertiFlow.Client\AxidianCertiFlow.Client.Tools-<version_number>.x64.en-
us.msi /lv C:\install_log.txt
This command launches the Axidian CertiFlow Client Tools installer from the
D:\CertiFlow.Client folder. Installation logs are written to the install_log.txt file,
located in the C: drive root.
```

To collect installer logs when you deploy component using Group Policy and cannot specify command-line parameters, enable Windows Installer logging by setting a registry key:

- To enable logging, create a *REG_SZ* key named **Logging** with the value ***voicewarmupx*** in the *HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer* registry branch.
- To disable logging, set an empty value for the **Logging** key.

You can also enable and disable debug logs for Axidian CertiFlow installers using the REG files included in the Axidian CertiFlow installation package, located in the *\GetLog\Regfiles* folder (files: *MSI logs On.reg* and *MSI logs Off.reg*).

- To enable debug logging for installers on a workstation, run the *MSI logs On.reg* file.
- To disable debug logging for installers on a workstation, run the *MSI logs Off.reg* file.

The log file is saved to the *Temp* folder. Each new log file name is generated randomly but starts with the letters *Msi* and has the LOG extension. To locate the *Temp* folder, execute the following command:

```
cd %temp%
```

Log collection errors and troubleshooting

- Connecting to a remote computer

Error	Cause	Solution
`0x800706BA The RPC server is unavailable`	Windows Management Instrumentation (WMI) service is stopped or blocked on the remote computer running Windows Vista or higher.	Start the WMI service: 1. In **Control Panel**, select **Windows Firewall → Allow an app or feature through Windows Firewall**. 2. Click **Change settings** and enable the **Windows Management Instrumentation (WMI)** option.
`0x000004B3 No network provider accepted the given network path`	The remote computer is not accessible over the network.	Check the network connection settings.

- Connecting to a local computer

Error	Cause	Solution
`0x80070005 Access is denied` or `The network path is not accessible. Access is denied`	The user account running the CertiFlow GetLog tool does not have permission to read and/or edit the Windows registry key containing the logging parameters.	Grant the user account the required permissions: 1. In Windows Registry Editor, navigate to the key *HKEY_LOCAL_MACHINE\SOFTWARE\CertiFlow*. 2. Right-click the **Logging** node and select **Permissions**. 3. In the **Permissions for Logging** window, click **Add** and select the required user account. 4. Grant the selected account **Full Control** and **Read** permissions. 5. Click **Apply**. For the permission changes to take effect, the user must log off and then log back on.
	The user does not have write permissions for the log save catalog.	Grant the user account the required permissions for the specified catalog.

- Saving logs

Error	Cause	Solution
`0x80070035 The network path was not found`	The network catalog used to access log files is unavailable (the default catalog is *ADMIN$\System32\LogFiles*).	Check the access settings for the network catalog.
`0x80070003 The system cannot find the file specified`	An incorrect network path for saving files was specified.	Specify the correct network path.

Technical support

If you have questions regarding the product documentation or you are experiencing an issue with the functionality of your Axidian CertiFlow solution, you can contact Axidian technical support.

Follow these steps to submit a support request.

1. Open Technical Support Portal.
2. Enter your email address and password and click **Login**.
3. Click **Submit a Ticket**.
4. Select department and click **Next**.
5. Fill in the required fields and click **Submit**.

Release notes

This section covers updates and improvements in Axidian CertiFlow.

7.2

- Added support for Samba AD DC user catalog.
- Added support for Windows Server 2025 for Axidian CertiFlow server components.
- Optimized the Axidian CertiFlow operation settings in the Axidian CertiFlow Configuration Wizard.
- Optimized administration in the Management Console.
- Fixed an error that prevented importing Microsoft CA root certificates to the card.
- Fixed an issue with installing the AirCard virtual smart card on the allowed computers.
- Fixed an encryption key access permission error when running Log Server on Linux OS.

7.1

- Added support for FreeIPA user catalog.
- Integrated with Axidian Access 8.2 and higher.
- Implemented the Axidian CertiFlow event log on Linux OS using the Log Server application.
- Added a user PIN change feature to agent bulk tasks.
- Automated the process of issuing cards using the agent.
- Added the functionality to configure a time period for forcing user PIN changes to agent settings.
- Added a notification about an unregistered card connecting to a workstation with agent.
- Added filtering by version to the agent search section.
- Added a document search section and a certificate search section to the Management Console.
- Implemented verification of original documents and tracking the unsigned documents.
- Added a service certificate monitoring functionality.
- Added support for new card models: SafeNet eToken Fusion Series, SafeNet eToken 5300, SafeNet eToken 5110CC (940), IDPrime 940 and IDPrime 940B, IDPrime 3940 and IDPrime 3940 FIDO.
- Added notifications for license expiration.
- Implemented the global mail server configuration settings.
- Optimized the message settings in notification templates.
- Expanded card management capabilities using API.
- Added automatic revocation of cards from removed users to the Card Monitor service functionality to free up licenses.
- Added new settings for generating random PINs.

- Enhanced the role-based model functionality.

7.0

- Added support for Linux OS for Axidian CertiFlow server components.
- Added authentication using the OpenID Connect protocol in the Management Console, Self-Service, API Service, and the Configuration Wizard.
- Introduced the internal document management service to control the certificate lifecycle from issuance to expiration and to exchange documents between users and administrators.
- Added the functionality to upload and sign documents to obtain a signature verification key certificate in the Self-Service.
- Implemented the functionality to suspend card issuance and renewal for additional verification of user documents in the Management Console.
- Added a remote card clear operation to agent bulk tasks.
- Implemented automatic cancellation of all agent tasks when a card is revoked and withdrawn.
- Added support for hardware PIN change on eToken PRO Java 72K cards.
- Added the functionality to delete inactive agents on a scheduled basis.
- Added logs about tracked certificates.
- Added the functionality to control the selection of optional certificates during card issuance and renewal in the Self-Service.
- Added the functionality to assign a policy to multiple Microsoft Active Directory user groups.
- Added the functionality to specify which characters to exclude when generating a random PIN in card issuance settings.
- Implemented validation for filling fields in the Configuration Wizard parameters.
- Added information about the user assigned to the card, the policy active on the card, and certificates on the card to the API return values.
- Added the user attributes `sAMAccountName` (Logon name) and `userPrincipalName` (Principal Name) to the executable file.
- Fixed an error when attempting to register an agent with an outdated root certificate in the store.
- Fixed the display of OS names in the agents section.