

SafeNet Authentication Client

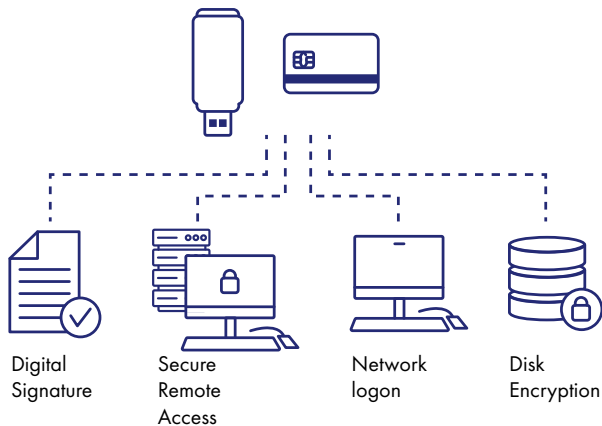
The power to easily manage Thales's PKI-based authentication

SafeNet Authentication Client is a unified middleware client that manages Thales's extensive SafeNet portfolio of Identity and Access Management Solutions, including certificate-based authenticators such as eToken, IDPrime smart cards, USB and software-based devices. Offering full backward compatibility and incorporating features from previous middleware versions, SafeNet Authentication Client ensures complete support for all currently deployed eToken devices, as well as IDPrime smart cards.

SafeNet Authentication Client links applications to Thales's PKI authenticators, providing full local administration and support for multiple advanced security applications such as digital signing, pre-boot authentication and disk encryption. With SafeNet Authentication Client, private keys can be generated and stored on-board highly secure smart card-based authenticators, allowing users to securely carry all their digital credentials wherever they go.

Leverage your PKI solution for multiple use cases

- Transparently operates with any standard certificate-based security application
- Consolidated & simplified management tools allow users to manage their own cards/tokens and certificates
- Supports secure access, data encryption and digital signing— all with a single authenticator
- Streamlines security operations by allowing organizations to deploy multiple security applications on a single platform
- Allows organizations to use certificate-enabled security capabilities from any client or server thanks to multi-platform support

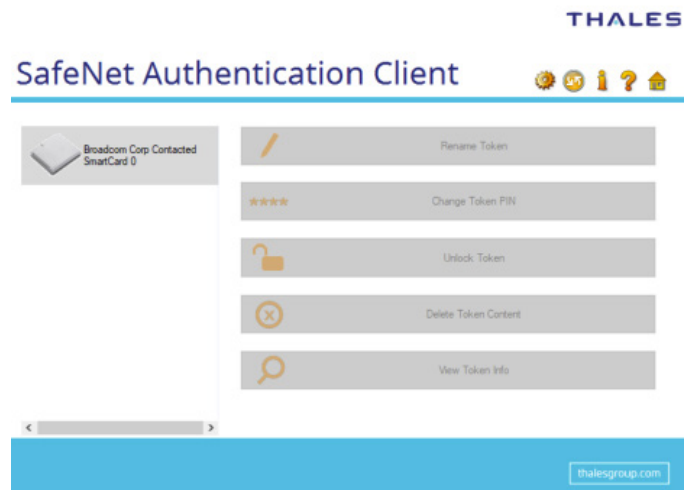


Features

- Strong two-factor authentication for network logon. Smart card logon on Windows machines
- Files and Disk Encryption
- Support for Common Criteria and FIPS certified devices
- Full support for SafeNet eTokens, IDPrime smart cards(with FIDO or not), IDPrime virtual smart cards, including multi-slots support and PIN Quality modifications
- Support for PIN Pad Readers
- Support for See What You Sign (SWYS) PIN Pad readers
- Enables local administration and usage of devices
- Support for full client customization, including security configuration, policies and user interface
- Seamless integration with any certificate-enabled application based on industry standard APIs
- Support for Virtual Keyboard enables you to enter passwords without using a physical keyboard, providing protection against kernel level keyloggers
- Key logger and PIN protection
- Common look and feel across all platforms
- Multi-language support

A unified solution for all users

SafeNet Authentication Client is available for Windows, Mac, and Linux, so your organization can take full advantage of SafeNet's solutions ranging from identity and access management, certificate-based security, strong authentication, encryption and digital signing, from virtually any device.



Technical specifications

Supported operating systems

Windows Servers:

- Windows Server 2016 (64-bit)
- Windows Server 2019 (64-bit)
- Windows Server 2022 (64-bit)
- Windows Server 2025 (64-bit)

Windows OS:

- Windows 10 (64-bit)
- Windows 11 (64-bit)

MacOS:

- macOS 26.2 (Tahoe)
- macOS 15.7.3 (Sequoia)
- macOS 14 (Sonoma)

Linux Distributions:

- Red Hat 9.x and 10.x (latest versions)
- CentOS 9.x and 10.x (latest versions)
- Fedora latest version
- Debian 12.x and 13.x
- Ubuntu 22, 24.04.3 LTS

Supported SafeNet Authenticators

Please refer to the this link for all supported [SafeNet Authenticators](#) and refer to the [Product Support Policy](#) for the latest software version.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.