Trantor®

AUTHENTICATION AND MFA · ON-PREMISE

Imago

Centralized identity management, for every access point in your company.

The on-premise authentication and MFA server: passwords verified against your corporate directory or IdP (any LDAP server, Active Directory, OIDC, SAML, RADIUS), second factor with TOTP/FIDO2 and with the Imago BioCard biometric card. Modern SSO and legacy protocols, all under the same policies.

MULTIPLE PROTOCOLS · MULTI-FACTOR AUTHENTICATION · FIDO2 BIOMETRIC CARD · LEGACY APPLICATIONS · COMPUTER BOOT PROTECTION WITH PBA · ANTI-COERCION SYSTEM · ON-PREMISE

TAKE AUTHENTICATION TO THE NEXT LEVEL

Imago exists to unify access and authentication policies, bring MFA to every application, and harden the most vulnerable part of the perimeter, such as the workstations.

trantor.it · info@trantor.it

10 August 2026

WHY IMAGO

What Trantor® Imago solves

01

Passwords everywhere

Users hate memorizing long passwords, let alone changing them every 90 days. With Imago you can bring passwordless authentication to the whole company, using FIDO2 technology or client certificates.

Fragmented policies and audit

Different applications enforce different access rules (maximum number of failed attempts, and so on), and each application keeps its own logs and its own record of successful/failed logins, logouts, password changes (hoping such a record actually exists). To keep everything under control, you need a single place to define all the rules, and a single place to see all the logs.

Inconsistent MFA, not always available

The problem with multi-factor authentication? Some applications support it, others don't. Some let you reuse the same MFA you use elsewhere, others don't. The result: users end up juggling several different 2FA channels, and on some applications they cannot use it at all.

Legacy applications make it hard to modernize access

Applications released years ago, now in maintenance-only mode, will not risk breaking their code to introduce new authentication methods. The result: forget using modern technologies such as biometric cards to log in to those applications. Imago solves the problem in two ways: it integrates natively with every application by exposing protocols such as LDAP and RADIUS, and with Imago 4Legacy users can authenticate on a modern portal before landing on the legacy applications.

Your users' authentication doesn't happen inside your company

Many of the solutions on offer require authentication to pass through the vendor's cloud, causing lock-in (for example, to get FIDO2 authentication at Windows logon you must use the Microsoft Entra ID cloud, and Microsoft offers no alternative), putting the integrity of your infrastructure at risk, and making it impossible to deploy uniform solutions across online and air-gapped/isolated departments.

You want to log in with your fingerprint, without sharing your biometric data

Many biometric authentication systems store this data on a server or on the computer. Letting biometric information such as fingerprints or face scans transit through third-party devices is a privacy and security nightmare. With Imago BioCard biometric cards, your fingerprint stays on the card, always with you, and you can use it to authenticate everywhere.

WHAT TRANTOR IMAGO IS

"A server appliance to manage passwords, second factors, policies and logs in a centralized, uniform way. Imago brings modern authentication to every application, works even fully on-premise, and can plug into a system you already run, such as Active Directory."

Technical overview: part 1

02

Solution components

Central appliance (**Trantor® Imago Appliance**) based on AlmaLinux 10. **Trantor® Imago CP** is the credential provider installed on Windows to bring FIDO2/TOTP authentication to Microsoft workstations. **Trantor® Imago 4Legacy** is a component of the central appliance that adds modern authentication to legacy apps. **Trantor® Imago PBA** is the software that brings pre-boot authentication to Windows computers. There is also native support for **Trantor® Imago BioCard**, FIDO2 biometric cards.

Trantor® Imago Appliance

Central server based on **AlmaLinux 10**, installable on-premise on bare metal or virtual machines, **x86 or ARM**. Two or more appliances unlock **load balancing** and **high availability**.

Protocols exposed for third-party applications

Imago exposes the following authentication protocols to third-party applications: **LDAP/LDAPS** (username with password/password+TOTP), **RADIUS** (username with password/password+TOTP, or username with password and challenge-response, or **802.1X** EAP-TLS / EAP-TTLS-PAP / EAP-TTLS-GTC / EAP-PWD / EAP-PEAP-GTC), **OpenID Connect** (with PKCE, CIBA and device-code), **SAML 2.0**. For user/group enumeration Imago exposes LDAP/LDAPS and **SCIM 2.0**.

Protocols supported to connect to existing directories/IdPs

Imago can use the following backends as authentication sources: **LDAP/LDAPS** (username+password), **RADIUS** (username+password, username+password+challenge, **802.1X** EAP-TLS / EAP-TTLS-PAP / EAP-TTLS-GTC / EAP-PWD / EAP-PEAP-GTC), **OpenID Connect** (with device-code, PKCE, CIBA), **SAML 2.0**. For user/group enumeration, Imago can use LDAP/LDAPS, **SCIM 2.0**, or file import.

Multi-factor and passwordless authentication

Imago supports both local 2FA management (via **TOTP** or **FIDO2**) and management through an external **MFA server** (via the Imago API plus a connector plugin). You can also allow selected users to use FIDO2 as their only authentication factor, enabling **passwordless access** (especially useful with Imago BioCard biometric cards, which unlock with the user's fingerprint). Imago brings multi-factor authentication to **legacy applications** that use LDAP or RADIUS, too.

Trantor® Imago CP

Imago CP is the **Credential Provider** for **Windows** x64/ARM64, compatible with Windows 10/11 and Windows Server 2019/2022/2025. It brings the Imago login features to Windows workstations, supporting **passwords, TOTP, FIDO2, OIDC device-code, passwordless authentication, anti-coercion**, and integrating with Imago PBA for **SSO**. Imago CP also supports temporary **offline authentication** and can be used over **RDP** as well.

Trantor® Imago 4Legacy

Imago's **identity-aware proxy** puts **FIDO2/TOTP in front of legacy apps**: the portal authenticates, the proxy lets users in with ephemeral one-time credentials. The legacy application never comes into contact with the user's real password.

Technical overview: part 2

Trantor® Imago PBA

Imago PBA is software for **pre-boot authentication**: it is essentially a small operating system based on **AlmaLinux 10**, installed on the Windows computer alongside Windows itself, and **executed at boot** to authenticate through Imago. If authentication succeeds, Imago PBA unlocks the BitLocker of the Windows partition and starts it. The Imago PBA Linux partition is protected with **digitally signed immutable images** (whose certificate is enrolled in the computer's firmware) and all data is encrypted with **LUKS2+TPM**. Installation/update/removal of Imago PBA all happen through the **Imago PBA Manager** program installed on the computer's Windows, so there is no need for ISO boots or pre-imaging. Imago PBA can be used together with Imago CP to obtain **SSO** (that is: the user logs in on Imago PBA and is already logged in when Windows boots). Imago PBA can also optionally expose an **RDP** server so users can unlock the PC remotely, particularly useful for servers, but not only. Imago PBA, like the CP, also supports temporary **offline authentication**. When Imago PBA is used together with Intel Boot Guard or AMD Platform Secure Boot (PSB), it provides high levels of protection even in case of **tampering with the motherboard firmware**.

Trantor® Imago BioCard

Imago BioCards are **FIDO2 cards** that use on-board biometrics to authenticate the user. Their defining traits are the native integration with Imago, and the fact that the **fingerprint** stays on the card and is never transmitted to computers or servers. Details follow in the next pages.

Authentication for WiFi networks too, with Trantor® SecureWiFi

If you also run **Trantor® SecureWiFi**, you can use Imago as the authentication backend for the WiFi network: SecureWiFi autonomously configures Imago's **RADIUS/802.1X connector** so that devices (phones/tablets/computers/etc.) can **authenticate to the WiFi network through Imago**. SecureWiFi also automatically generates WiFi profiles importable on Windows/macOS/Linux/Android/iOS **so that users never have to configure WiFi by hand**.

Anti-coercion system

Imago includes an **anti-coercion** system that lets a user discreetly signal that, for whatever reason, they are logging in **under duress**. When an anti-coercion login is performed (**from any access point connected to Imago**), Imago immediately sends **an alert** to all configured administrators. Moreover, if the anti-coercion login happens on Windows (with Imago PBA or Imago CP), an administrator-defined **script can run automatically on Windows** to prepare an environment that looks realistic but holds no truly confidential data (for example, the script can unmount confidential network drives and mount network drives with decoy data).

Trantor® Imago as a protocol/SSO proxy

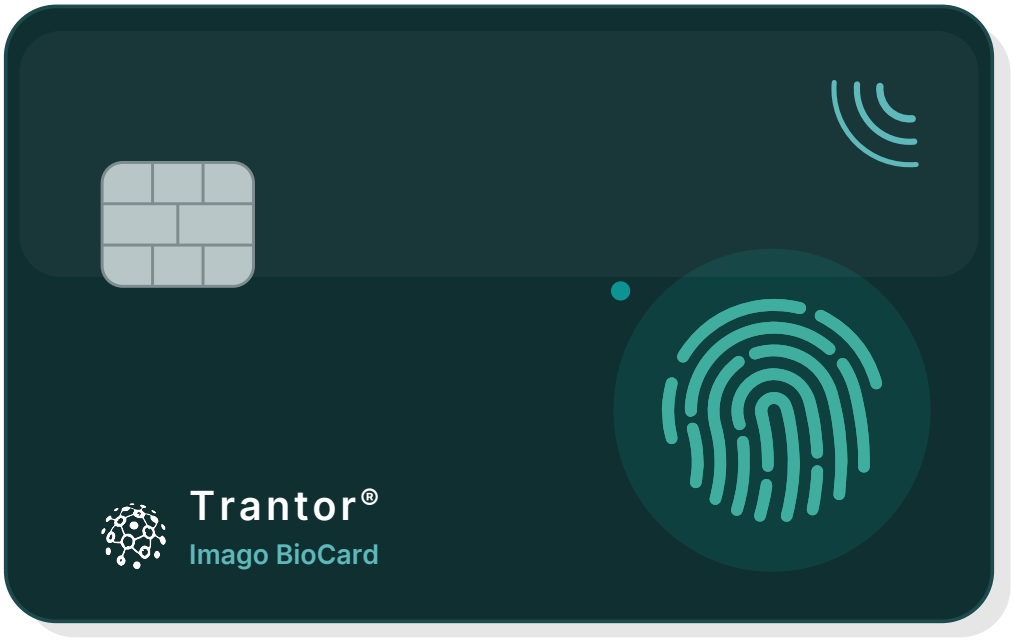
Imago allows many **combinations of protocols, both externally exposed and internally used by underlying realms**: in doing so, it acts as a proxy that **converts between protocols**. Some examples: an application connects to Imago with RADIUS+challenge, and Imago converts it into OIDC+device-code towards the realm; an application connects to Imago with OIDC+SCIM, while Imago talks RADIUS+LDAP to the realm; an application connects to Imago with passwordless FIDO2, and Imago talks to Active Directory to obtain the access token.

THE CARD

Imago BioCard

04

Full product name: **Trantor® Imago BioCard**. The biometric FIDO2 card of the range: NFC and smartcard readers, the credential is released at the touch of a fingerprint.



	Card specifications
Form factor	Standard-size card, perfect to carry with you at all times
Technology	FIDO2 / WebAuthn: public-key credential, phishing-resistant
Biometrics	On-board fingerprint sensor: the card unlocks at a touch and the biometric data never leaves the card
Interfaces	Contactless NFC and smartcard readers
Where it works	Web applications with native WebAuthn support, Windows/Linux/macOS workstation logon, and even legacy applications thanks to Trantor® Imago 4Legacy
Enrollment	From the Imago self-service portal, independently
If lost	The card is revoked centrally; TOTP remains as a fallback on the channels that use it

THE FINGERPRINT STAYS ON THE CARD

The sensor verifies the fingerprint on board: no biometric data travels over the network or ends up on a server. The card unlocks itself; Imago verifies the credential.

POSITIONING

Trantor® Imago and the alternatives

05

Every alternative below is a serious product with real strengths. The useful comparison is not the feature list: it is where identities live, whether legacy is included or left out, and what happens when the link to the cloud goes down.

Solution	Where control lives	MFA and protocols	Considerations
Trantor® Imago Trantor® · Italy	On-premise server, in your network: no mandatory cloud, works even in isolated environments	TOTP and biometric FIDO2 card; passwords on your directory (any LDAP, Active Directory included) or via OIDC/SAML; modern SSO, proxy for legacy and secure boot with Imago PBA	One policy engine and one audit trail for every access point; credentials never leave the company; direct support from the development team
Microsoft Entra ID Microsoft · non-EU	Microsoft cloud, not optional: even hybrid goes through Microsoft's servers	MFA with Authenticator, FIDO2 and Windows Hello; OIDC/SAML SSO; legacy stays on the on-premise AD	The default choice in Microsoft shops, with MFA in the per-user P1/P2 plans; management, policies and identities live in the vendor's cloud; no PBA; no proxy for legacy apps
Okta Workforce Identity Okta · non-EU	Vendor cloud, not optional	Broad MFA catalog (push, FIDO2, TOTP); SSO across thousands of catalog apps; agents for AD and LDAP	The reference cloud IdP, with the widest ecosystem; per-user, per-module pricing; no PBA; no proxy for legacy apps
Cisco Duo Cisco · non-EU	Cisco cloud, not optional	One of the easiest push MFAs to adopt; SSO in the higher editions; directories, RADIUS and LDAP require the Authentication Proxy	Fast adoption and a good user experience; per-user monthly fee, and the service depends on cloud reachability; no PBA; no proxy for legacy apps
Keycloak open source · Red Hat	On-premise or in the cloud	Full OIDC and SAML, TOTP and WebAuthn/FIDO2 included; federation with LDAP and Active Directory	Maximum freedom and a huge community; hardening, updates and high availability remain the customer's job, with commercial support only via Red Hat; no PBA; no Windows Credential Provider; no proxy for legacy apps
privacyIDEA NetKnights · Germany	On-premise	Multi-token MFA server (TOTP, WebAuthn, smartcards); for SSO and access it relies on an IdP or on the PAM/RADIUS modules	The other European alternative, open source; a somewhat dated and clunky management UI; covers the second factor more than the whole: SSO, self-service and legacy must be assembled piece by piece; no PBA; limited legacy app support (e.g. TOTP as a password suffix)

MODEL

Trantor® Imago at a glance

06

What Trantor® Imago offers your company

- **Modern SSO:** OIDC and SAML for modern web applications and for legacy applications.
- **Extended MFA:** offline TOTP, FIDO2 cards and tokens, and integration with external MFA services (for example, for SMS push).
- **Workstation access with MFA:** Windows, Linux and macOS; TOTP or FIDO2, even on-premise and without any cloud.
- **Self-service portal:** FIDO2/TOTP enrollment, password change and reset, second-factor reset.
- **Proxy for legacy:** FIDO2 in front of apps that only speak LDAP or RADIUS.
- **Unified, centralized policies and audit:** every application, every authentication method, all with centralized policies and audit.
- **The card you unlock with your fingerprint:** Imago BioCard is a FIDO2 card for biometric authentication, usable to access applications and workstations, even without passwords.

How Trantor® Imago ensures high security standards

- **Hardened appliance:** the central server uses digitally signed immutable Linux images, LUKS2+TPM disk encryption, and root access disabled and allowed only through an emergency key kept in a safe.
- **FIDO2/WebAuthn authentication:** a phishing-proof system with strong cryptographic properties.
- **Biometric cards:** Imago BioCards keep the fingerprint on the card itself, and they protect FIDO2 authentication using biometry in place of a PIN.
- **Modern protocols everywhere:** Imago 4Legacy and Imago's proxy features allow you to adopt modern technologies (like OpenID Connect with PKCE, SCIM 2.0, and FIDO2) everywhere.
- **Anti-coercion system:** because cybersecurity is strictly linked to physical security.

Open standards, no ransom

Imago speaks OIDC, SAML, RADIUS, LDAP, SCIM and WebAuthn: open standards at every level. Your authentication stays readable and verifiable, even without us.

Detailed scope and terms are declared before signing, with the same rule as the whole Trantor® range.

THE NEXT MOVE

Let's give your access a face.

Book a consultation now to map your company's access: modern apps, legacy, VPN and workstations. And we'll tell you what Imago can do for you.

trantor.it
info@trantor.it