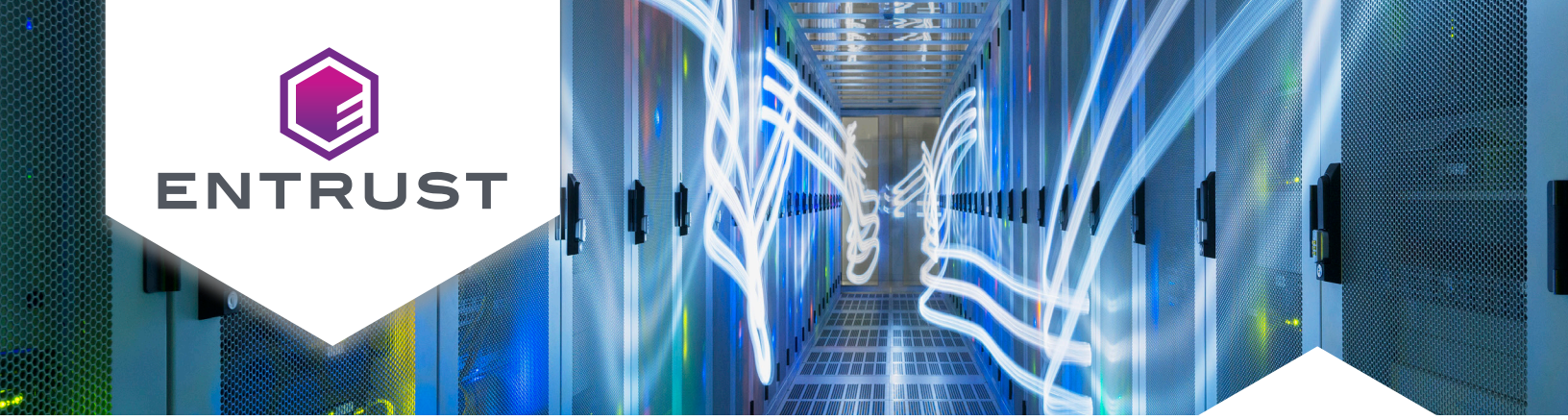

Entrust Security Manager

HIGHLIGHTS

A proven solution for hosted or on-premises PKI

Entrust Security Manager, the world's leading public key infrastructure (PKI), allows organizations to easily manage digital keys and certificates that secure user, device, and application identities. In addition, Security Manager includes industry-leading certificate authority (CA) and administrative services registration authority, forming a robust infrastructure that allows API, command line, or Web Console based administration, Public Trusted CAB/Forum compliant PKI, National ID and ePassport.

Digital certificates allow organizations to leverage encryption and digital signatures to support security services such as:

- User and device authentication
- Transaction integrity
- Verification
- Data security

KEY FEATURES & BENEFITS

- Manages digital identities within an organization for company-wide security, without burdening administration
- Simplifies the user experience; agents, toolkits, and self-service portals allow for frictionless enrollment and renewal
- Enforces corporate-wide security policies relating to private key protection, administration, and digital certificate settings
- Offers high levels of interoperability, including integration with Microsoft key storage (CAPI/CNG), Active Directory, Apple Keychain, and Java
- Identifies, manages, and authenticates mobile device access to networks

HOW IT WORKS

Simplified certificate management

Entrust Security Manager software enables valuable security capabilities – including authentication, digital signature, digital verification, and encryption – to be applied across a variety of applications, mobile devices, LTE, and IoT endpoints.

Mobile security

Entrust Security Manager is fully integrated with industry-leading enterprise mobility management (EMM) and mobile device management (MDM) platforms from VMware, Microsoft, IBM, and more. Out-of-the-box MDM/EMM integrations ensure that laptops, mobile phones, and tablets are equipped with policy-enforced encryption and data protection.

Learn more about Security Manager at entrust.com

Entrust Security Manager

Government and citizen credentials

From border crossings and driver's licenses to national ID cards, Entrust Security Manager provides critical system components for credential issuance, management, and validation. The ePassport suite may be configured as a CSCA, CVCA, or DV CA to issue certificates used to secure global travel systems.

Easy and transparent

Automatic and transparent key and certificate management means users do not need to be security experts to maintain high assurance environments. The platform provides key history, backup, and recovery features so encrypted information will not get lost if users misplace their keys.

Compliant and accredited

Security Manager runs in the world's highest assurance environments and enables organizations to operate under stringent audits and controls. The Security Manager CA is certified under Federal Information Processing Standards (FIPS) 140-3, Common Criteria, CAB/Forum, and other globally recognized standards.

Highly available, horizontally scaling, no downtime upgrades

Security Manager supports high availability configurations with multi-node certificate authority deployments sharing a central database repository. Multi-node deployments provide improved HA setups, zero-downtime upgrades and patches, and increased token processing system when managing certificates.

Technical features

- Automated digital ID management – updates, revocation, and recovery
- Active/active high availability native to Security Manager cluster
- Performance scales linear as more CA nodes added
- Support for unlimited administrators and up to 10 million users per CA node
- Web-based administration for delegated and distributed administration
- Centrally managed policies and controls
- Certified for FIPS 140-3 Level 2
- Common Criteria EAL4+
- Comprehensive and customizable auditing and reporting
- Support for peer-to-peer and hierarchical cross-certification of CAs
- Provides compliant certificate revocation lists (CRLs) and integrates seamlessly into Entrust Validation Authority and other leading OCSP vendors
- Admin Services features an ICAO compliant ePassport system for enrollment and certificate management including Country Verifying CA (CVCA), Document Verifying CA (DVCA), and National Public Key Directory (NPKD)
- Flexible enrollment options, including PKIX-CMP, PKIX-CMPv2, ACME, PKCS#7/10, CSR, SCEP, EST, MDMWS, REST

Learn more about Security Manager at entrust.com

Entrust Security Manager

- Interoperability with PKI-aware applications such as virtual private networks, browsers, mobile devices, email, and business applications
- Interoperability with many LDAP directories (including Microsoft Active Directory), smart cards, derived credentials, TPMs, and HSMs (including nShield HSMs)
- Platforms supported: Microsoft Windows Server 2016, 2019, 2022; Red Hat Enterprise Linux 7, 8; CentOS 7, 8

HOW IT WORKS CONTINUED

Easy Certificate Issuance

Issue certificates for users, applications, or devices, including tablets and smartphones, which support the X.509 certificate standard.

Perfected Automation

Take advantage of the solution's automated key and certificate lifecycle management capabilities. Some of the automation Certificate Management protocols supported include: REST, ACME, PKIX-CMPv2, EST, SCEP, PKCS#7/PKCS#10, CSR, MDM Web Services, API, IoT Endpoint Agent, Entelligence Windows, and MacOS clients.

Tight Integration

Generate certificates for devices as requested by Entrust Administration Services, Certificate Enrollment Gateway, Entrust Certificate Hub, Entrust Identity as a Service, or Entrust Identity Enterprise. These solutions provide interfaces for enrolling and managing certificates issued to a variety of endpoints.

Secure Storage of Encryption Key History

Security Manager maintains an auditable database of users' private key histories for recovery purposes. Secure Access, Audit, and Policy controls allow organizations to recover encrypted data with confidence.

Flexible Revocation Technology: CRL and OCSP Support

Publish CRLs that are used to verify whether a user or application's certificate is still trusted by the CA that issued it.

End-User Convenience

Leverage an advanced security infrastructure that accommodates users who log in from different workstations, work offline or from mobile devices, or use various methods of authentication (e.g., smart cards, tokens, or biometric devices).

Optional Enhancements

Leverage Entrust Security Manager's optional components. Organizations have the option to add further security management capabilities – including automated enrollment, self-registration, and self-recovery of digital identities and secure roaming.

Learn more about Security Manager at entrust.com

Entrust Security Manager

OUR OFFERINGS

Complementary Entrust products

Entrust Entelligence Security Provider

This thin agent allows organizations to use a single digital identity seamlessly to add security capabilities beyond authentication to applications such as email or file encryption on either Windows or Apple MacOS.

Entrust Administration Services

This component provides web-based applications and services that interact with Security Manager to manage digital IDs and certificates. It includes administration interfaces allowing administrators to manage users and certificates, and enrollment services that allow users and non-human entities (e.g., computers and mobile devices) to enroll for certificates. Entrust Administration Services also enables auto-enrollment of users and machines via MDM vendor partnerships, Microsoft gateway, Entrust IoT Security, and other components.

Entrust Certificate Hub

Certificate Hub provides active certificate lifecycle management across multiple certificate authorities (CAs). With its intuitive "single pane of glass" view, you can find, control, and automate the management of certificates.

Certificate Enrollment Gateway

Entrust's next-generation microservice framework that provides automated user and device enrollment.

Entrust Validation Authority

Reliably and efficiently verifies the status of digital certificates from one or multiple CAs.

Entrust Roaming Server

The server provides users with secure access to digital content from any location without the need for users to carry the digital IDs required to establish secure connections.

Entrust Security Manager Proxy

Security Manager Proxy allows communication with Security Manager over the internet using standard internet protocols without making changes to existing firewall settings.

Entrust Toolkits

Entrust Toolkits provide a common set of services that permit developers to deploy applications that solve business problems without having to spend valuable development cycles creating these common services.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223