Entrust Identity Essentials

Realize a Zero Trust framework

Entrust Identity covers the spectrum of IAM solutions, from best-in-class MFA and VPN protection for Windows-based environments to high assurance credential-based passwordless authentication that can be deployed on-premises or in the cloud.

ENTRUST

IDENTITY
ESSENTIALS

OVERVIEW

Identity Essentials

Identity Essentials is the ideal multi-factor authentication (MFA) solution for companies looking for a fast, cost-efficient option to secure worker identities and enable their remote workforce. With Identity Essentials, you get started with an easy-to-use, easy-to-deploy on-premises MFA solution and can migrate to the cloud with Identity as a Service over time, if and when it makes sense. Seamless integration between Identity Essentials and Identity as a Service ensures a frictionless hybrid set-up while benefitting from three authentication options:

- Device fingerprint authentication
- Mobile push authentication
- Grid card authentication

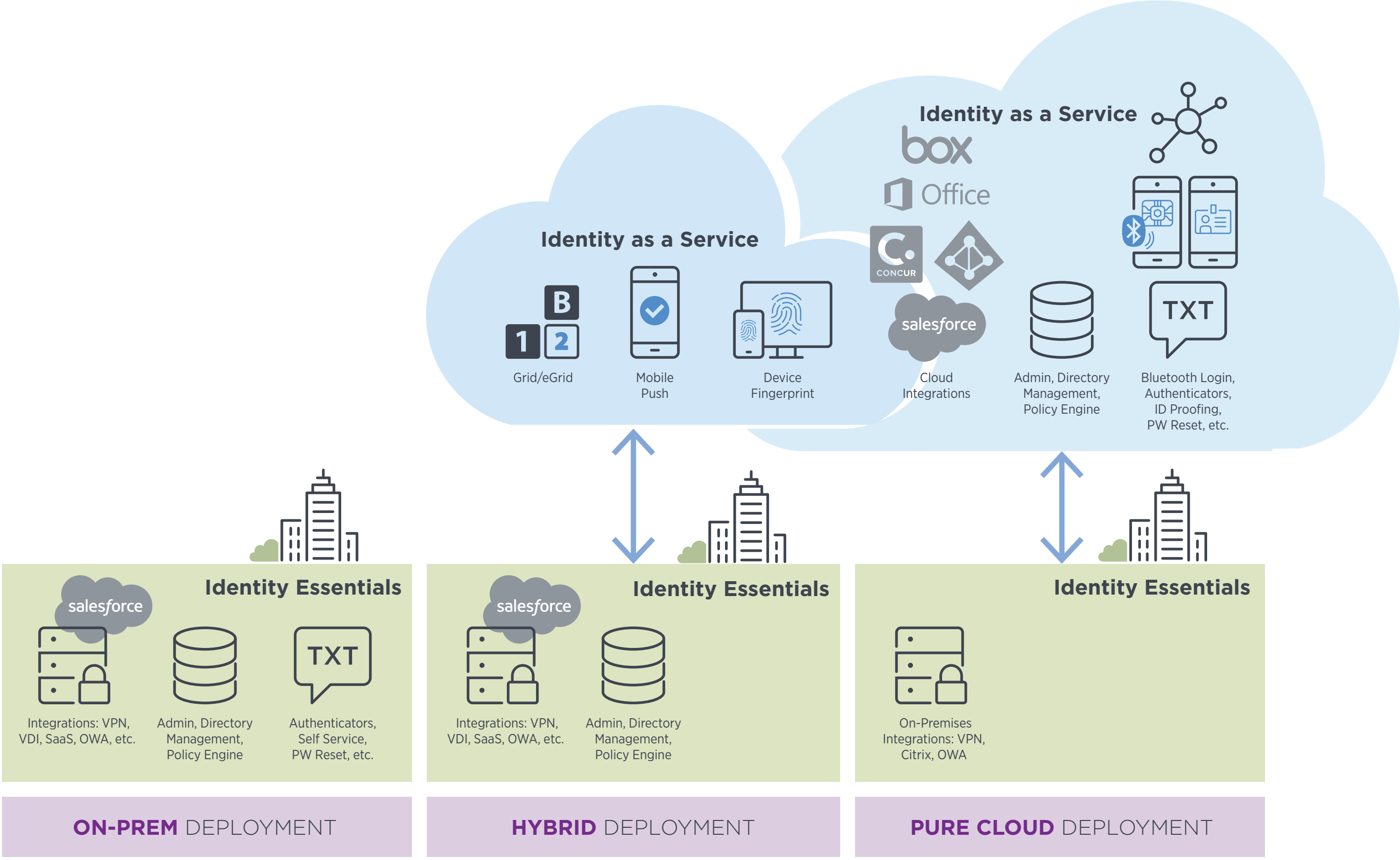
Identity Essentials provides the foundation for Windows-based organizations to realize a Zero Trust approach with Identity as a Service over time.

HOW IT WORKS

Fighting bigger threats with better technology

If a hacker obtains an employee's password, they can exploit everything to which the employee has access – cloud and on-premises. And since most organizations are enabling more cloud services for file systems, intranets, collaboration sites, etc., more data is now exposed. Luckily, strong user authentication is now less of a hassle for both users and administrators than it once was. And with the integration of Identity Essentials and Identity as a Service, you can go as deep into the cloud as you want – with passwordless and Smart Login to Windows 7, 8, 10, and MacOS.

Identity Essentials allows you to go as deep into the cloud as you want with seamless integration with Identity as a Service.*


Identity as a Service
Grid/eGrid
Mobile Push
Device Fingerprint
Identity as a Service
box
Office
CONCUR
salesforce
Cloud Integrations
Admin, Directory Management, Policy Engine
TXT
Bluetooth Login, Authenticators, ID Proofing, PW Reset, etc.
Identity Essentials
salesforce
Integrations: VPN, VDI, SaaS, OWA, etc.
Admin, Directory Management, Policy Engine
TXT
Authenticators, Self Service, PW Reset, etc.
ON-PREM DEPLOYMENT
Identity Essentials
salesforce
Integrations: VPN, VDI, SaaS, OWA, etc.
Admin, Directory Management, Policy Engine
HYBRID DEPLOYMENT
Identity Essentials
On-Premises Integrations: VPN, Citrix, OWA
PURE CLOUD DEPLOYMENT

*Only for Identity Essentials customers with a subscription license.

License options: what's included*

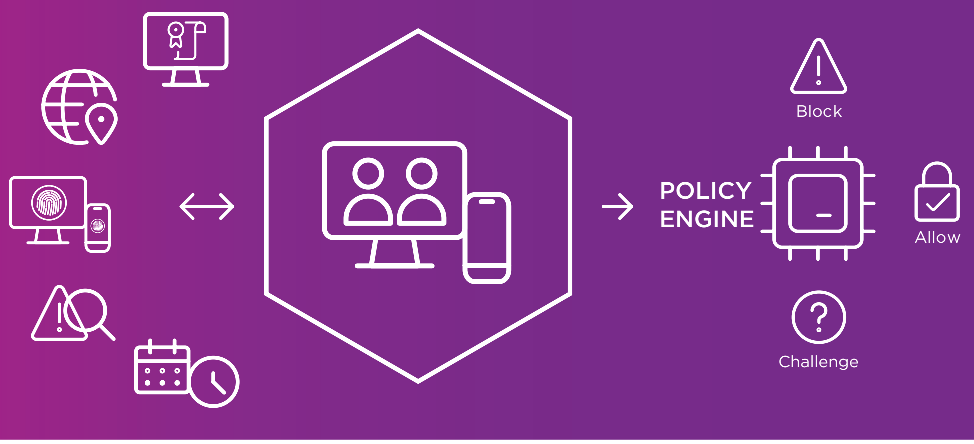
Companies choosing the Subscription bundle get the full benefit of tight integration between Identity Essentials and Identity as a Service.

	Software Assurance	Subscription Bundle
Identity Essentials enhancements	●	●
Windows Server 2019 support	●	●
Device Fingerprint with AD FS (Identity as a Service)	●	●
Push Authentication (Identity as a Service)	●	●
ActiveSync device provisioning for Office365 and on-premises Exchange	●	●
Identity as a Service "Plus," including risk engine, cloud-to-cloud auth, etc.		●
Global SMS, app- and voice-based OTP dispatch service		●
Identity as a Service single sign-on portal for all cloud services in one place, protected		●
Identity Essentials support, business hours (can be extended)		●
Grid cards support	●	●
Enhanced functionality on Windows logon console authentication	●	●

*Identity Smart Login is an add-on feature that has extra cost.

Entrust Identity's adaptive risk-based engine provides an added level of security when conditions warrant, like a worker logging in for the first time from a new device, or at an abnormal time of day, or from a different geolocation. Only requiring additional authentication like a mobile push notification when these situations present keeps worker friction to a minimum while also protecting corporate resources.

CUTTING EDGE TECHNOLOGY, ADAPTIVE AUTHENTICATION, NO USER INTERACTION



A large range of supported authenticators

With Identity Essentials, you have choices when it comes to authentication methods. Depending on varying factors such as asset being accessed, the device being used, and the level of technical ability of the user, you may want to choose different authentication methods.

Three modern features (listed below) are all made possible by Identity as a Service integration, allowing employees to access workstations, networks, and applications securely – without the hassle of entering a password or employing traditional two-factor methods with each session. A true passwordless, frictionless, secure login experience.

Identity Essentials Authenticators

- SMS
- Flash SMS
- Secure E-mail
- Voice-Call
- Identity Essentials APP (Encrypted OTP)
- Google Authenticator
- FIDO2 Support
- OATH OTP Token Support

PLUS 3 AUTHENTICATION FEATURES
Powered by Identity as a Service

Device Fingerprint Authentication

When accessing cloud apps through AD FS, a new device fingerprint can be captured, allowing for automatic detection of a previously used device, This provides an extra layer of security and allows you to bypass one-time passcodes (OTPs).

When using the Identity as a Service Risk Engine, this can also be one factor to consider, along with geolocation, IP address, time of login, travel velocity, etc.

Mobile Push Authentication

Add an extra layer of security when employees want to log in at an unusual time or place. The brandable push authentication app provides biometric security using your native mobile biometrics to prevent unauthorized access. The app features Confirm, Deny, and Concern buttons; Concerns are recorded and a report is sent to an administrator.

Grid/eGrid

Grid card authentication provides organizations a simple, yet effective, strong authentication tool for increased security and logical access control. Users are presented an authentication challenge when they log into a restricted network, application, cloud service, or site. Each grid card is unique and carries a serial number, so every user can be uniquely identified and authenticated. Each time a user is asked to authenticate they are presented with a different challenge requiring them to validate via a different set of grid coordinates. The coordinate request changes for each authentication challenge.

Device fingerprint authentication: a secure, easy login

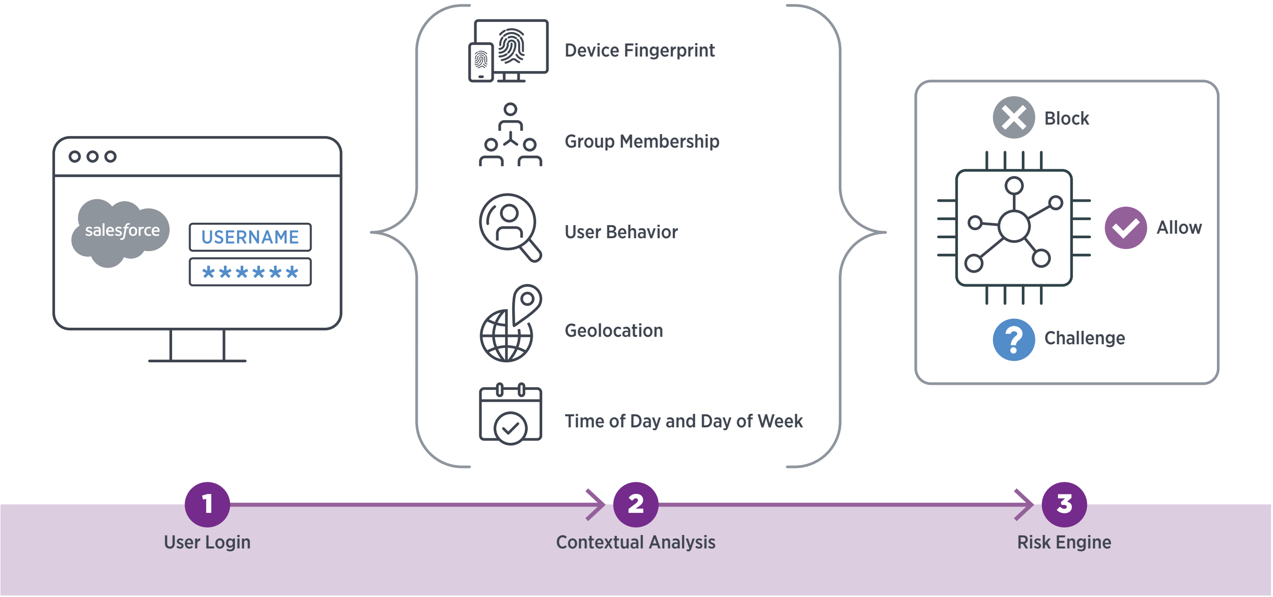
More than 80% of all hacking-related breaches are caused by weak or stolen user credentials. Adding MFA on all services will boost your security dramatically by disarming the hackers of their preferred weapon.

To overcome pushback from your users, look into our adaptive/contextual intelligence capabilities, which have already improved user experience for thousands of organizations.

Identity Essentials pioneered adaptive authentication, where login is granted depending on the context – whether the user is logged in over VPN, Citrix, RDP, or cloud services for example.

Device fingerprint is the latest addition, providing more security than an authentication cookie to validate the machine that has previously been used in a login.

DEVICE FINGERPRINT AUTHENTICATION – Powered by Identity as a Service



Identity Essentials eliminates the need for frustrating, repetitive logins by leveraging Identity as a Service's easy-to-configure engine that detects risk in real-time based on contextual data and user behavior.

ActiveSync protection: No mobile device management required

ActiveSync – the protocol for easy synchronization of email, contacts, etc., imposes an often-overlooked security risk. If a user can easily set up access to important information using only an email address and a password – so can a hacker. And when you protect OWA/Office365 with MFA, ActiveSync should not be forgotten.

THERE ARE **THREE PRIMARY WAYS**
TO ACCESS OFFICE 365/OWA CONTENT

Outlook Client
on PC/Mac
50% of time
spent on email

ActiveSync
via iPhone/Android/Tablet
40% of time spent on email

Browser
Office.com or OWA
10% of time
spent on email

Our solution has helped thousands of organizations over the years by supporting Allow, Block, or Quarantine in Office 365 and Exchange Server 2013/2016/2019. Intuitive, secure device provisioning allows users to quickly and easily onboard new ActiveSync devices by themselves without compromising security – and without having to contact the help desk for assistance.

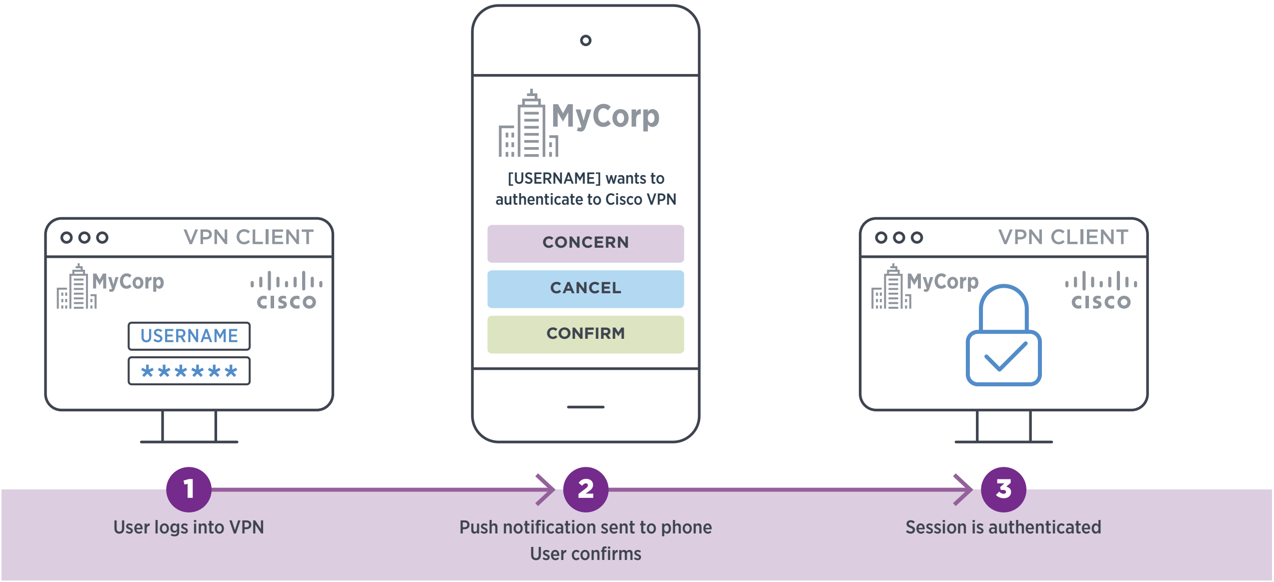
This simple, secure, user-driven device provisioning fits BYOD cultures perfectly. No need for a complete MDM solution. Simplify life for your users by allowing them to onboard their new device and get the access they need in a frictionless, yet very secure way through their email.

Mobile push authentication: perfect for tech-savvy workers

With Identity as a Service integration, Identity Essentials includes push authentication to get access via VPN / Citrix (Radius) and AD FS. When activated, the user is prompted on their mobile screen with “CONCERN”, “CANCEL”, or “CONFIRM.” Pressing the “CONCERN” button blocks access and is also logged in the system to alert the administrator.

Biometric validation (e.g. touch/FaceID) can be added to protect against unauthorized mobile app usage or the user accidentally allowing access to a hacker. Contextual information is also shown in the app (e.g., “Login attempt from Hilton Hotel in Bangkok, Thailand”).

MOBILE PUSH AUTHENTICATION – Powered by Identity as a Service



The app works for both Android and iOS, and comes in two forms: with or without certificate capabilities. Push to authenticate is a great feature for IT-savvy users. Other authentication methods that don’t require installation and setup on the phone (SMS/text, voice call, etc.) are still valid solutions for many frontline workers and a less-techy audience.

Passwordless authentication: frictionless access to apps

Entrust Identity

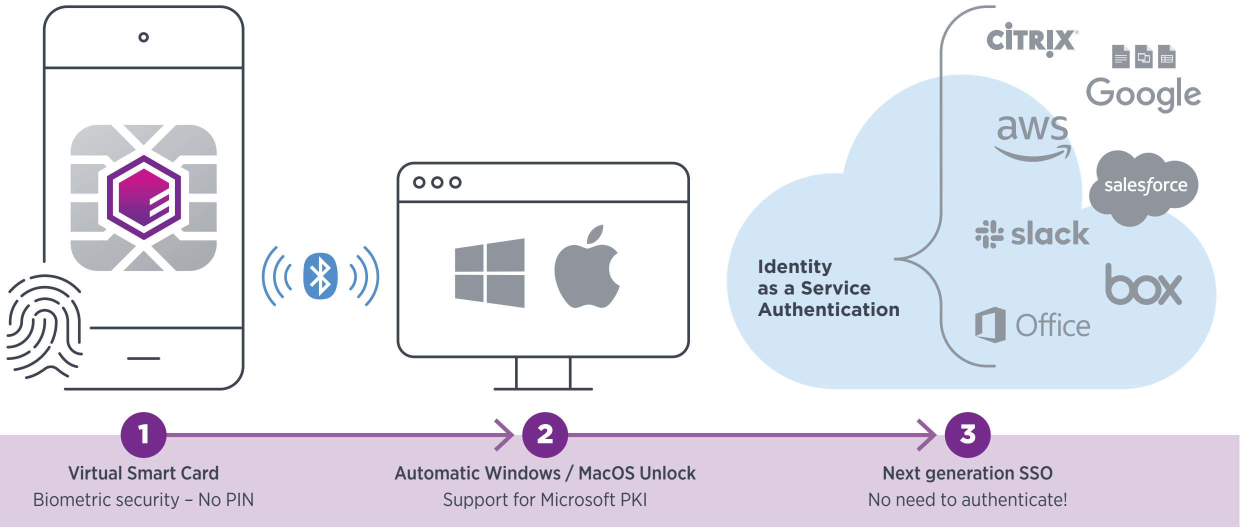
Multi-factor authentication has provided a necessary layer of security on top of passwords for many years. But our world has continued to evolve – from both a technology and a cyber-threat perspective – creating issues with traditional MFA.

Firstly, users expect instant access to data and applications – and MFA has increased the friction and frustration. From typing in one-time passcodes (OTPs) to carrying around USB keys, MFA slows down productivity. Plus, if you lose your USB key or the battery dies on your hardware token, you're locked out. Secondly, hackers are finding ways around certain MFA methods, leading to costly breaches.

Smart Login addresses MFA's key issues by maximizing security and minimizing user friction. Combining the security of digital certificates and the convenience of the mobile phone, we provide advanced solutions that are simple for end-users.

Entrust Identity's Smart Login allows employees to log into their workstation and applications simply by having their phone in their possession. No more passwords and no more 2FA, such as knowledge questions or OTPs. Accessing their computer and applications is quick and easy with fewer security hurdles, allowing them to be more productive. Plus, they no longer have to remember to lock their workstations. Smart Login automatically logs them out when they walk away.

PASSWORDLESS AUTHENTICATION – Powered by Identity as a Service


CITRIX
Google
aws
salesforce
slack
box
Office
Identity as a Service Authentication
1
Virtual Smart Card
Biometric security – No PIN
2
Automatic Windows / MacOS Unlock
Support for Microsoft PKI
3
Next generation SSO
No need to authenticate!

Identity Essentials features

Seamless integration: The Identity Essentials MFA platform integrates seamlessly with login systems and cloud solutions for an intuitive, user-friendly remote access experience.

Adaptive authentication: Automatically adapts the level of authentication based on the user's current circumstances, providing a balance of high security and strong user-friendliness.

Automatic failover: It's possible to establish highly flexible failover mechanisms to ensure that the OTPs always arrive. The solution can even switch between transmissions, depending on the user's current login context.

Broad directory support: Users can be synchronized from Active Directory and general LDAP Directories like OpenLDAP or AD LDS. Users can be imported by selecting a specific user group, or by use of an LDAP filter.

Real-time protection: All OTP codes are generated in real-time at the point of login. There are no pre-issued passcodes or seed files that could be hacked. At the same time, real-time is a prerequisite for delivering session-specific OTPs.

PowerShell: Administrators can use PowerShell scripting to create role-based access, integrate to other systems, or automate daily tasks such as checking license availability or country-specific logins.

Status feedback: Enables the user to follow the login progress; inspires user confidence and reduces the number of help desk calls.

Location and behavior aware: Leverages contextual information such as login behavior patterns and geo-location to grant or deny user access. Geofencing allows administrators to whitelist or blacklist based on systems and locations (e.g., limit access through Citrix NetScaler from certain countries).

Secure device provisioning: Allows users to quickly and easily self-enroll new ActiveSync devices without compromising security and without having to contact the help desk for assistance.

OTP delivery methods: Plug-ins and standard OTP delivery methods – like apps, SMS, voice-call, secure email, cloud keys, and hard/soft tokens – support your business requirements now and in the future.

Advanced database auditing: Helps customers comply with strict industry regulations and meet audit control requirements.

Additional features via Identity as a Service integration

Mobile push authentication app (with your own branding): Adds a user-friendly level of security when employees want to log in at an unusual time or place. A notification message pops up on their mobile phone to confirm that they are the one requesting access.

Device fingerprint authentication: After a successful login to a cloud service through AD FS, a device fingerprint can be captured and used for future login security assessments, allowing for easier login.

Passwordless authentication: Provisions a credential on the worker's phone, enabling passwordless workstation login (Macs and PCs) and application SSO (cloud and on-premises) via Bluetooth when the phone is in close proximity and unlocked with the user's fingerprint or facial match.

Single sign-on (SSO): Identity as a Service delivers SSO to all apps – cloud and on-premises – including legacy apps. Federates with cloud apps via standards like SAML and OIDC.

Azure AD Integration: Integrates with Azure AD for user synchronization, etc.

Email and file encryption: Integration with the major MDM vendors – including Microsoft, IBM, and VMware – ensures workplace communications are secure with email and file encryption.

Document signing: MDM vendor integration supports secure workplace transactions and non-repudiation with document signing.

Identity proofing: Securely verifies identities of employees, contractors, partners, and others.

Consumer authentication: Identity as a Service goes beyond workforce authentication. It can be used to address all of your consumer authentication needs as well.

Entrust Identity Portfolio: Identity Essentials is part of our unified Entrust Identity portfolio that also includes Identity as a Service and Identity Enterprise. Entrust Identity offers workforce identity and access management (IAM) solutions to support a range of organization sizes, from 50 to 1 million plus users.

Supported systems

Identity Essentials supports a variety of login systems used for remote access. The platform is designed to integrate seamlessly into hundreds of VPNs, providing a secure and intuitive login process. Below is a list of examples of supported remote access systems.

RADIUS VPN/SSL VPN Clients

- Check Point
- Cisco ASA
- Citrix Netscaler (Citrix ADC)
- Juniper
- Pulse Secure
- Barracuda NG firewalls
- VMware Horizon View
- Netop Remote Control
- Palo Alto
- F5 BIG-IP
- NCP VPN
- Other RADIUS clients

Internet Information Services (IIS) Websites

Support for the following types of websites:

- Outlook Web Access 2010 / 2013 / 2016 / 2019
- Remote Desktop Web Access (Windows Server 2012 R2 / 2016 / 2019)
- IIS Websites using Basic, Integrated Windows Authentication, and ASP.Net Form Based Authentication

Windows Logon, Remote Desktop Services

Support for the following servers and services:

- Remote Desktop Services (RDP Connections)
- Windows Servers / 2012 / 2012 R2 / 2016 / 2019
- Windows 8, Windows 8.1, and Windows 10
- VMware Virtual Desktop Portal & Client Access

Secure Device Provisioning

Protection for ActiveSync devices on the following systems:

- Exchange 2010 SP3
- Exchange 2013
- Exchange 2016
- Exchange 2019
- Exchange Online

Microsoft AD FS Protection

- AD FS 3.0/4.0/5.0 adapter for multi-factor authentication

Multi-factor authentication support for:

- Access to cloud applications such as Salesforce.com, Microsoft Office 365, Google Apps, etc. (AD FS 3.0/4.0/5.0)
- Access to websites published through Microsoft Web Application Proxy (AD FS 3.0/4.0/5.0), such as Outlook Web Access
- Approval of devices in connection with workplace joins (AD FS 3.0/4.0/5.0)

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust secures a rapidly changing world by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com