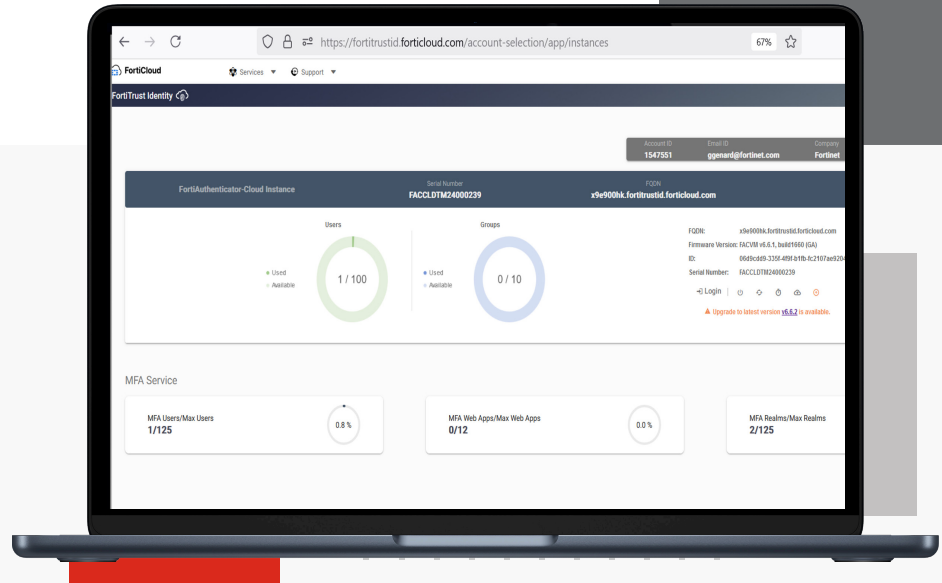**FURTINET**

FortiTrust Identity

Available in

Cloud

Key Features

By integrating with Fortinet Security Fabric, siloed identity stores, and systems across an IT hybrid environment, FortiTrust Identity provides the following:

- User authentication with centralized identity and access management
- Multifactor authentication (MFA) including adaptive authentication and passwordless (FIDO2) methods
- SSO (single sign-on) including identity provider proxy function
- Certificate management

Identity and Access Management Solution

PriConcerns about security, end-user experience, and the overall cost of a unified IAM (Identity and Access Management) solution are rising as enterprises embrace digital business initiatives—including work-from-anywhere for their workforce. FortiTrust Identity is a cloud-delivered IAM solution that uses modern authentication technologies while leveraging existing network infrastructure to enable organizations to secure user access to cloud and on-premises applications and services.
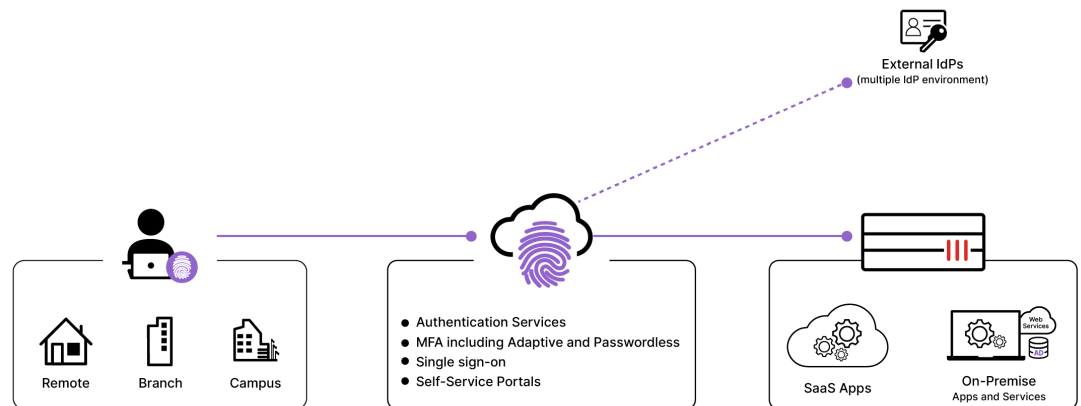
Features and Benefits

- Subscription service, no capital expense
- Strengthen enterprise security and reduce IT operations complexity by simplifying and centralizing the management of user identity information
- Scalable architecture with an admin portal for easy operations, administration, and maintenance
- Multi-protocol support with cloud-based broker/proxy capability enables organizations with a multiple identity providers (IdPs) strategy to achieve their zero-trust access initiatives (Figure 1 shows challenges, and Figure 2 illustrates a solution with broker/proxy capability)
- Variety of MFA offerings, such as OTP and FIDO2 (aka passwordless) methods to increase the confidence of the identity-claimed
- Simplify and provide a consistent digital experience for end-users with adaptive authentication and single sign-on (SSO)
- Native integration with Fortinet Security Fabric provides IT with more security controls
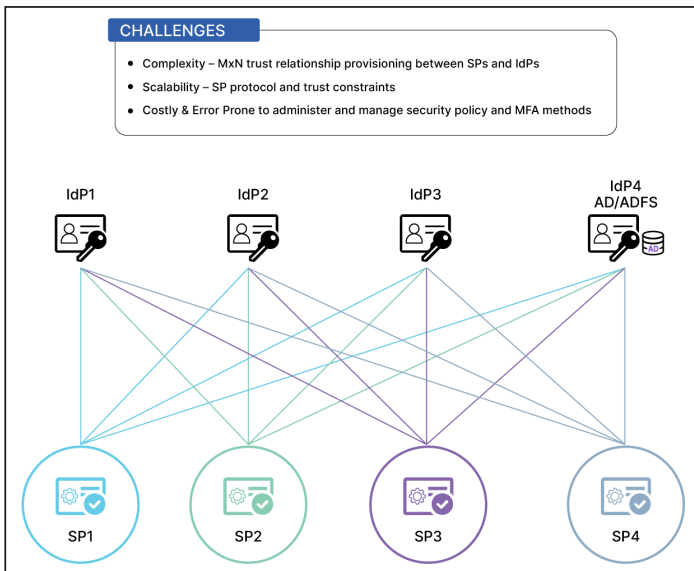- Rest API available for integrations

CHALLENGES
- Complexity – MxN trust relationship provisioning between SPs and IdPs
- Scalability – SP protocol and trust constraints
- Costly & Error Prone to administer and manage security policy and MFA methods

IdP1   IdP2   IdP3   IdP4 AD/ADFS

SP1   SP2   SP3   SP4

Figure 1 - Organizations with Multiple IdPs

BENEFITS
- Simplify authentication services
- Scalability – Remove SP constraints
- Reduce Cost and Risks – Integrated solution from One Vendor with OneView to manage

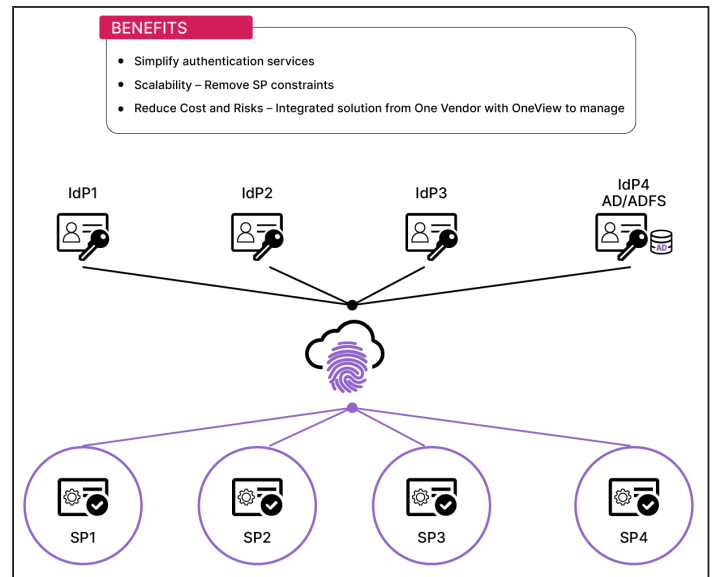IdP1   IdP2   IdP3   IdP4 AD/ADFS

SP1   SP2   SP3   SP4

Figure 2 - IdP Broker/Proxy with Multiple External IdPs

Capabilities

Highly Available Identity-as-a-Service

- Hosted in Fortinet Data Center
- 24/7 Monitoring

Authentication Service

The authentication service built into FortiTrust Identity provides authentication for employees, partners, and contractors via our access identification and verification methods, including our IdP broker/proxy capability that works seamlessly with external IdPs. With FortiTrust Identity, organizations can consolidate several methods into one experience with a single view of managing identity. FortiTrust Identity supports industry authentication and authorization standards:

- Cloud/web types: SSO; SAML IdP/IdP Proxy, OAuth2/OIDC provider
- RADSec/802.1x
- MFA or strong authentication: OTP, email, SMS (OTP), and FIDO2 security with a variety of hardware form factors and mobile apps. Organizations can choose a factor (or factors) that best fits their environment. Specifically, organizations can secure cross-platform token transfer with the mobile apps for their iOS and Android devices
- Adaptive authentication uses the information gathered at a login attempt to evaluate the circumstantial risks of a given login attempt. This information includes time of day, geo-location, historical usage pattern, etc. The second authentication factor is only requested when that risk is higher than a predetermined threshold. Furthermore, the login attempt can be blocked if the circumstantial risk is high enough

SSO

- SSO simplifies the end-user experience and reduces the need for repeated authentications to gain secure access across enterprise applications and services

Interoperability

- FortiTrust Identity provides IdP broker/proxy capability out-of-the-box for organizations that have identities managed across multiple external IdPs. This capability provides a centralized authentication service across these external IdPs, enabling organizations to have a uniform policy and MFA method independent from external IdPs

Integration

- Integration natively with Fortinet Security Fabric, specifically with FortiGate, extends authentication services for secure user access to on-premises resources. No additional gateway or software agents are required to purchase, install, and maintain

Certificate Management

- Streamlined certificate management enables rapid, cost-effective deployment of certificates

Specifications - Standards Supported

- Identity Federation: SAML2.0, OAuth2, OIDC
- RADSec/802.1x authentication
- MFA: One-Time-Password (OTP) tokens, email, SMS (OTP), FIDO2 (roaming authenticators and FIDO server)
- Others: Certificate revocation (RFC3280), PKCS#12 certificate import, PKCS#10 CSR import (RFC2986), online certificate status protocol (RFC2560), SCEP (simple certificate enrollment protocol)

Specifications - Identity

	IDENTITY
MFA	
Mobile Token with Mobile Push	✓
Email/SMS OTP, Hardware Tokens	✓
SMS Credits	✓
FIDO2 Authentication/ Registration Server	✓
Third-party Application Integration	✓
Adaptive Authentication	
Integrated with Dynamic Policies and Fabric Connectors	✓
Enforce based on Authorized Networks	✓
Enforced based on User Location	✓
Enforce based on Time of Day/ Day of Week	✓
Enforce Device Trust Policies based on Device Posture*	✓
Cloud-hosted IAM	
Secure Application Access	✓
Fortinet Single Sign On (FSSO)	✓
Identity and Role-based Security Policies	✓
Central User Identity Management	✓
Certificate Management-VPN	✓
SAML Service Provider/ Identity Provider Web SSO	✓
Open ID Connect SSO	✓
RadSec, 802.1x Authentication Server	✓
Additional Information	
FortiCare Premium Support	✓

* Requires FortiClient EMS

Order Information

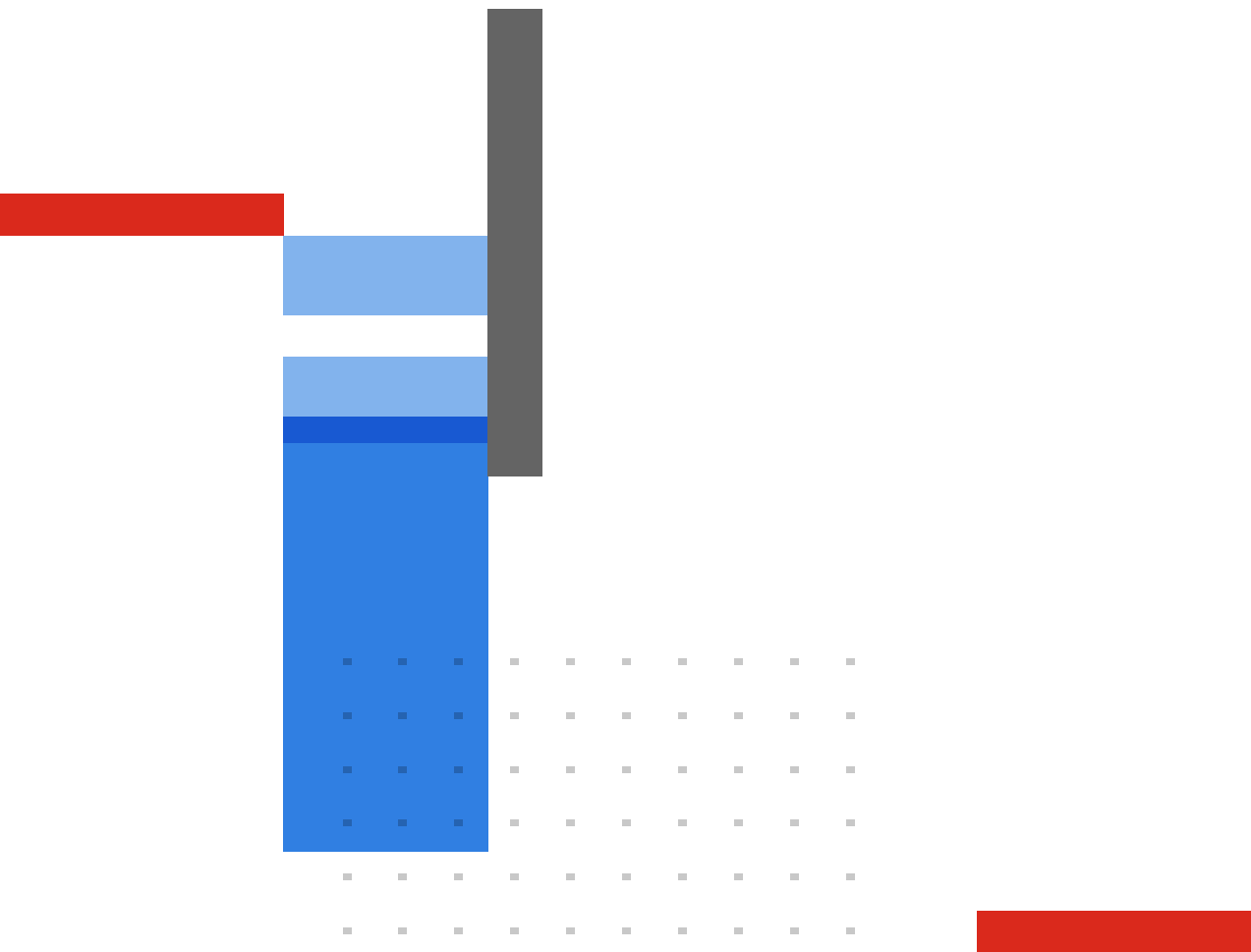| User Licenses	SKU	Description
100-499	FC2-10-ACCLD-511-02-DD	Cloud-managed Identity User Subscription including 24×7 FortiCare and SMS credits for 100-499 Users.
500-1999	FC3-10-ACCLD-511-02-DD	Cloud-managed Identity User Subscription including 24×7 FortiCare and SMS credits for 500-1999 Users.
2000-9999	FC4-10-ACCLD-511-02-DD	Cloud-managed Identity User Subscription including 24×7 FortiCare and SMS credits for 2000-9999 Users.
10 000+	FC5-10-ACCLD-511-02-DD	Cloud-managed Identity User Subscription including 24×7 FortiCare and SMS credits for 10 000+ Users.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

F⊡RTINET

www.fortinet.com

December 12, 2024

FTID-DAT-R02-20241212