FortiSASE SIA Agent-Based Rapid Deployment

Security

SERVICE OVERVIEW

CDW's FortiSASE SIA Agent-Based Rapid Deployment service allows customers to quickly provision and start their FortiSASE journey and begin seeing returns on their security investment sooner.

Secure internet access (SIA) for agent-based remote users is the most typical use case involving the installation and configuration of FortiClient on supported endpoints (including Windows, macOS and Linux endpoints). For this use case, the FortiSASE firewall-as-a-service (FWaaS) comes between the endpoint and the internet by establishing a full-tunnel secure sockets layer VPN (SSL VPN) between the client and the FWaaS. The agent-based SIA secures all internet traffic and protocols using VPN policies by connecting each endpoint to a Fortinet point of presence (PoP).

SERVICE FEATURES

- Remote implementation of the FortiSASE Agent-Based solution
- A designated CDW security professional services consultant for the duration of the project
- Designated CDW project manager for the duration of the project
- Discovery workshop and planning
- FortiSASE SIA Agent-Based Rapid Deployment (refer below)

WHAT WE DO

- Project kick off
- Information gathering, design and architect workshop
- Provision the FortiSASE instance and select the regions where the users will be located and input licences as needed
- Configure remote authentication and onboard users
- Configure authentication sources and access for SSO, LDAP, RADIUS or local (up to five users)
- Configuring security settings and VPN policies in FortiSASE (up to one security setting each and one profile for antivirus/web filter/DNS filter/IPS/file filter/application control)
- Assist the customer in downloading and installing FortiClient on up to five endpoints with an operating system that supports Fortinet

CDW

- Test access to the internet using a remote device (up to five endpoints)
- Status calls - up to two 30-minute calls
- As-built documentation, knowledge transfer and project close-out presentation
- How to onboard more mobile users
- How to update security policies

EXCLUSIONS

- Customized profile for FortiClient
- Remote authentication (LDAP/RADIUS/SAML identity Provider) configuration
- SSL deep inspection configuration
- DLP profile and policies
- FortiClient agent installation

PREREQUISITES

- Required FortiSASE licences have been purchased and received by the customer
- The customer should have a FortiCloud account
- In SAML identity provider (idP) remote authentication, the identity provider needs to be configured and ready
- In LDAP or RADIUS remote authentication, the servers must be reachable from the public internet
- The customer has installed FortiClient on selected users

WHY CDW?

CDW has the experience, experts and services to help organizations craft a combination of the right tools and the right plan that can mitigate security risks, increase visibility, unlock the power of their solutions and be better prepared for the evolving threat landscape.

Our experienced and highly skilled security team will help you align your business and security strategies with each other.

Our 150+ security professionals and 430+ security certifications enable us to bring enterprise-wide security capabilities to our customers. We can architect, integrate and deploy the most advanced security technologies to build a robust security infrastructure. Finally, we can set up systems, processes and controls to ensure you can rapidly remediate security incidents.

The applicable SKU for the service described in this document is 8225451.
Engage your account representative to discuss your desired timeline to start, deadline and the scope.

For more information, contact your CDW account team at 800.972.3922 or visit CDW.ca