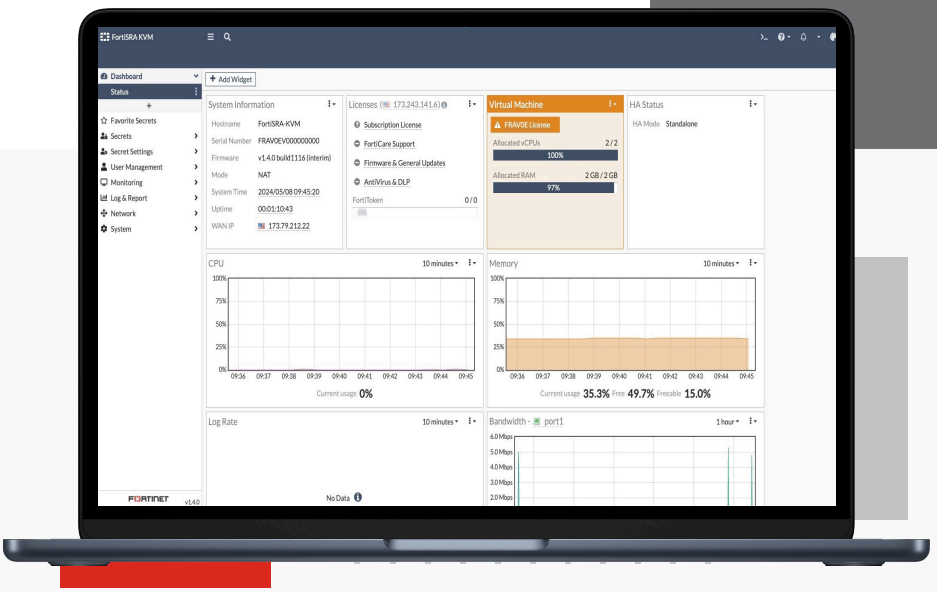
FortiSRA

Fortinet Secure Remote Access

Available in

Virtual Machine



Highlights

Integrates, as part of Fortinet Security Fabric, with FortiAuthenticator, FortiToken, and a FortiSRA web browser extension, as a complete, clientless SRA solution for OT

Includes scheduled credential changing capabilities (LDAPS, Samba, SSH, SSH key)

Enables native program access with PuTTY and RDP along with browser-based access via Chrome, Firefox, and Edge

Deploy secure remote access for critical systems, manage user access and privileges, monitor, log, and record user activity

FortiSRA assists operational technology (OT) organizations in implementing secure remote access (SRA), managing user access and privileges, and monitoring, logging, and recording user activity during remote sessions. Additionally, the solution ensures uptime for SRA services through high availability (HA) and active/standby HA capabilities.

FortiSRA supports privileged access management features that control user accounts with elevated privileges, manage access and permissions for remote users, accounts, processes, systems, and sensitive data across the OT infrastructure.

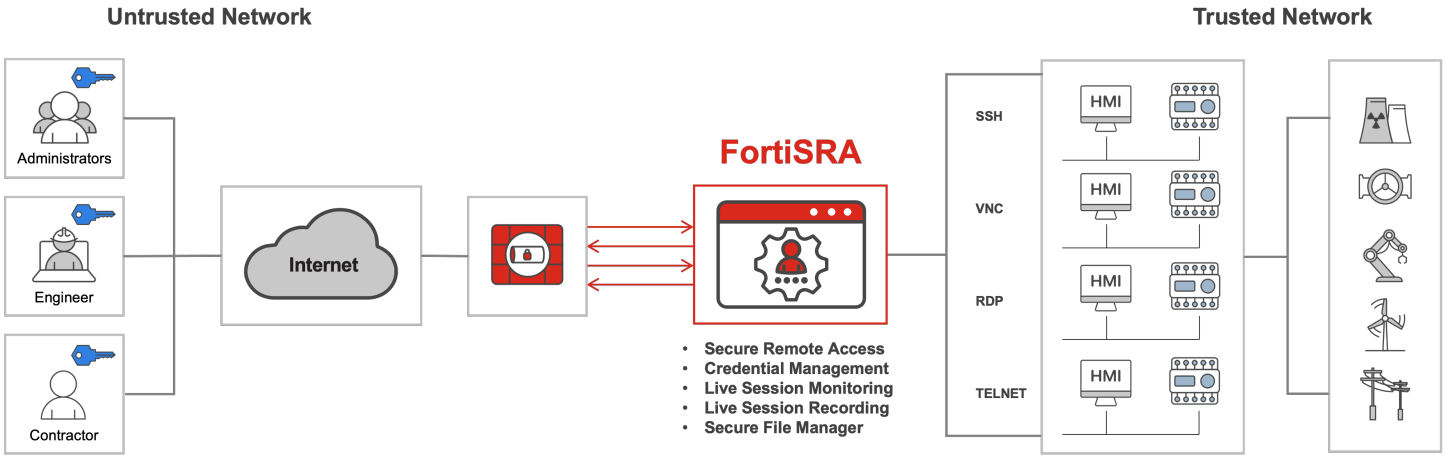
Furthermore, FortiSRA provides gated access to the most sensitive OT resources within an organization. It enables end-to-end management of remote accounts, controls privileged user access, and offers visibility of account usage, including monitoring and audit capabilities. These features allow FortiSRA to mitigate the risk associated with maintaining external access to critical OT resources.

OT enables factories, power generation and transmission facilities, public transportation networks, oil and gas facilities, and utilities to function. These organizations provide critical products and services through technologies such as industrial automation and control systems (IACS), including distributed control systems and supervisory control and data acquisition systems (DCS/SCADA). Therefore, it's particularly important for them to have a business continuity plan in place. FortiSRA can enable these organizations to securely support remote work and maintain business continuity.

Feature Highlights

Typical FortiSRA Deployment

The components of Fortinet Secure Remote Access Solution.



Manage Account Credentials

In OT environments, effective management of privileged accounts for both users and third-party contractors is paramount to maintaining security and operational resilience. FortiSRA offers a comprehensive solution by automating the entire lifecycle of privileged accounts, which goes beyond mere credential storage. It facilitates automatic password changes based on predefined policies, reducing the risk of unauthorized access and addressing the challenge of orphaned accounts or outdated credential policies for both internal users and external contractors. Moreover, FortiSRA assumes control of the privileged credential vault for specific resources, eliminating the need for users and contractors to directly interact with sensitive credentials, thereby mitigating the potential for credential exposure. Additionally, by ensuring that sensitive privileged account information is not transmitted to end-user devices, FortiSRA strengthens overall security posture, enabling organizations to maintain operational continuity and safeguard critical infrastructure systems effectively.

Control Privileged User Access

Privileged accounts demand careful management due to their access to critical OT resources. FortiSRA addresses this need by ensuring that end users, including third-party contractors, are granted access to essential resources based on assigned roles, such as standard user or administrator, while consistently adhering to the principle of least privilege. It provides administrators with full control over resource secrets through centrally defined policies, including the option for automatic password changes upon check-in. OT organizations can also leverage FortiSRA to implement a hierarchical approval system and regulate potentially risky commands.

Monitor Privileged Access

In addition to managing and controlling privileged accounts, it's equally crucial to provide monitoring capabilities for users, especially third-party contractors, accessing these highly sensitive resources remotely. FortiSRA offers reporting of privileged account usage in the event of a security incident. It also provides full-session video recordings to capture user activity on critical OT systems, including keystrokes and mouse events. When required for audit purposes, FortiSRA offers comprehensive tracking of all privileged account and target system usage.

Specifications

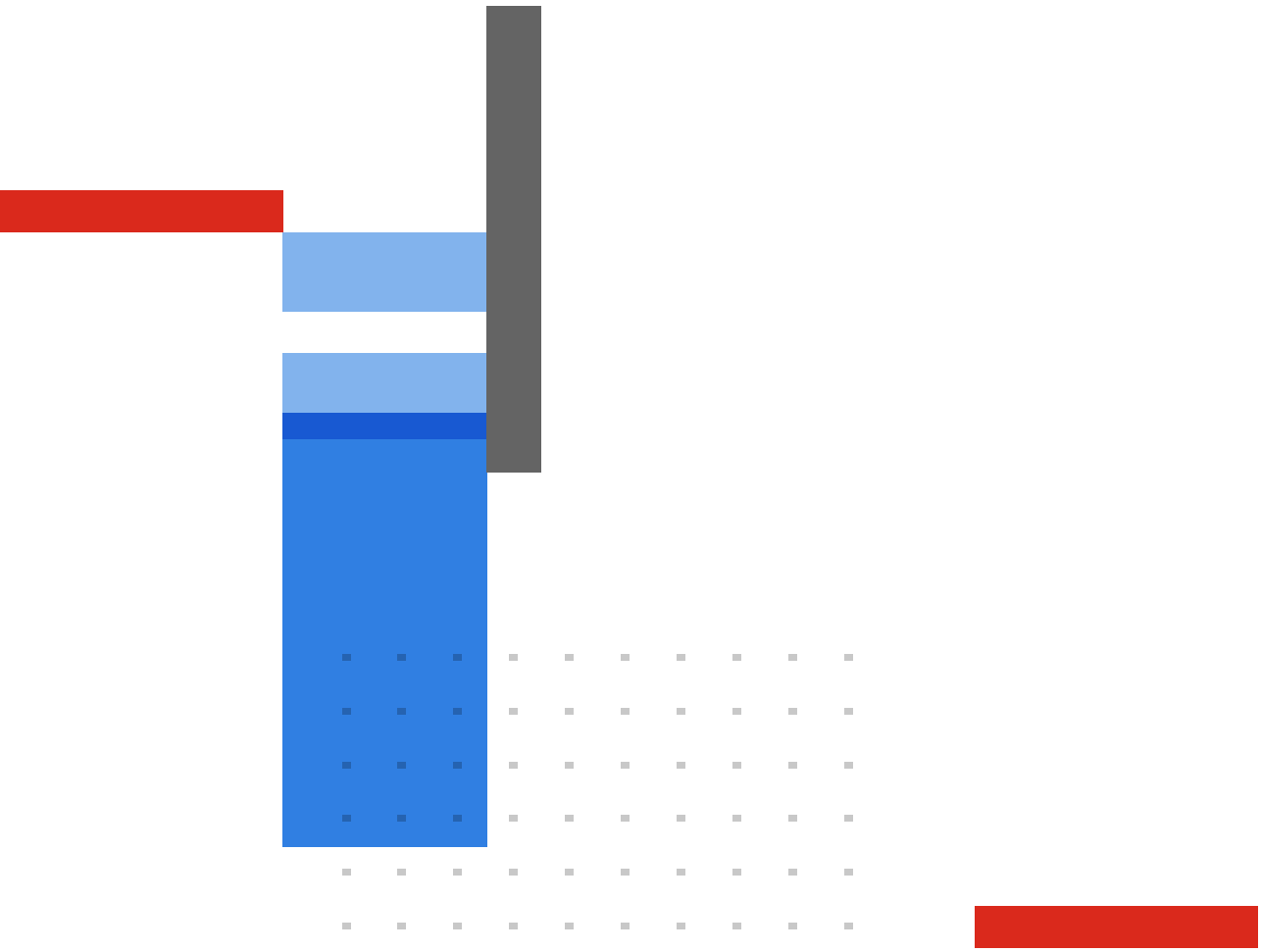
FUNCTION
User Management
Administrator Role Management
API User
FortiToken Cloud
Local User
Multi-factor authentication: FortiToken, Email, SMS
Remote Authentication: LDAP Server
Remote Authentication: RADIUS Server
SAML
User Group
User Trusted Host
Secret Folder
Folder Permission Control
Personal Folder
Public Folder
Secret Policy Management
Secret Template and Access
Custom Template
Template - Cisco Device
Template - FortiGate
Template - Machine
Template - Web Account
Unix SSH (Password or Key)
Windows Domain Account (LDAPS or Samba)
Secret
AD Target Restriction
Approval Request
Associated Secret Launcher
Associated Secret Password Changer
Auto Password Delivery on Native Launcher
Block RDP Clipboard
Cisco Device Auto-Enable on Native Launcher
Favorite Secrets
Move/Clone a Secret
Password Heartbeat
Periodical Password Changer
RDP Security Level
Renew Secret Check-out
Secret Check-out/Check-in
Secret Permission Control
SSH Filter
SSH Keyboard Interactive Authentication on Native Launcher
Verify Password
Video Recording

FUNCTION
Launcher
Custom Launcher
PuTTY
Remote Desktop - Windows
Tight VNC
VNC Viewer
Web Launcher
Web RDP
Web SFTP
Web SMB
Web SSH
Web VNC
WinSCP
Secret Request Approval
Approval Profile (up to 3 Tiers)
Multiple Approvals Requirement
Request Notification
Request Review and Approve
Script
Password Changer
Custom Password Changer
Password Policy
Monitor and Record
Active Sessions Monitor
Session Recording
User Monitor
Log and Audit
Events - HA
Events - System
Events - User
Logs - Secrets
Logs - Video (Record and Replay)
System
Automatic Configuration Backup
Disaster Recovery support
Glass Breaking
HA
High Availability
Maintenance Mode
Max Duration for the Launcher Session
vTPM: KVM
vTPM: VMWare

FUNCTION
Authentication
Address (Used in AD Target Restriction)
Scheme and Rules
Stability
Long Session
Stress Test (Overload, CPU 70%)
Installation
Installation Doc/ Administration Guide
Upgrade
Security
Advanced RDP authentication protocol including CredSSP, TLS
Anti-Virus scanning for web-based file transfer (Web SFTP, Web Samba) and SCP-based file transfer
Automatic blocking of privileged commands with SSH filtering profile
Auto password changing after check-in
Data Leak Prevention based on file types, size, or watermarks
High-strength SSH encryption algorithm
Policy-based access profile enforcement
Role-based access control
Scheduled password change
Secret access request/approval
Secret check-out/check-in protection
Support for Trusted Platform Module to protect user private keys
Two Factor Authentication for local users or remote SAML, RADIUS, LDAP users
User access control based on IP and/or schedule

Ordering Information

PRODUCT	SKU	DESCRIPTION
Virtual Machine		
FortiSRA-VM	FC1-10-RAVUL-687-02-DD	One year subscription for FortiSRA Virtual Machine, supports 5 to 9 user seats. Includes 24/7 FortiCare support. Centralized management requires additional software and separate license. HA requires additional license.
	FC2-10-RAVUL-687-02-DD	One year subscription for FortiSRA Virtual Machine, supports 10 to 24 user seats. Includes 24/7 FortiCare support. Centralized Management requires additional software and separate license. HA requires additional license.
	FC3-10-RAVUL-687-02-DD	One year subscription for FortiSRA Virtual Machine, supports 25 to 49 user seats. Includes 24/7 FortiCare support. Centralized Management requires additional software and separate license. HA requires additional license.



www.fortinet.com

June 26, 2024

FSRA-DAT-R02-20240626