

Semperis Directory Services Protection Deployment

Project Description:

This statement of work is to support Customer in the deployment of Semperis Directory Services Protector (DSP) software on a single Active Directory Forest.

Project Scope

Semperis will engage with designated Customer technical resources and project manager (if required and assigned) to plan, design and support the deployment of Semperis DSP solution. To ensure the success of the deployment, Semperis has developed a deployment methodology and all parties will collaborate to conduct the following phases.

Detailed DSP Deployment Phases

Discovery and Planning Phase:

- a. DSP Planning Workshop**
 - Organize a collaborative workshop to align our understanding of your deployment objectives and requirements.
 - Define key project milestones, timelines, and success criteria.
 - Establish clear communication channels and roles within the deployment team.
- b. Server and Storage Sizing**
 - Perform an assessment of your organization's size and projected workload to determine optimal server and storage requirements.
 - Develop recommendations for hardware provisioning to ensure scalability and performance.
- c. Network, Security, and Firewall Requirements**
 - Collaborate with your IT team to establish network, security, and firewall requirements for seamless DSP integration.
 - Provide guidance on implementing security measures to protect your Active Directory environment.
- d. SQL Database Requirements**
 - Assess SQL database requirements for DSP and ensure proper configuration and capacity planning.
- e. AV/EDR Exclusions**
 - Define necessary exclusions in your Anti-Virus (AV) and/or Endpoint Detection and Response (EDR) solutions to accommodate DSP services.
- f. Entra and Tenant Connection Requirements**
 - Review requirements related to configuring Microsoft Entra, creating and configuring the DSP Application, creating and configuring an Event Hub, and configuring Entra tenant connection.

Installation and Configuration Phase:

- a. DSP Pre-check**
 - Perform environment checks, including running any readiness script(s)
 - Discuss ports, registry keys, and other deployment requirements, including LSASS protection, audit GPO & SACL, service accounts & universal security groups, SQL DB & service account access, firewall ports, AV exclusions, Entra and Tenant Connection, and change control.
 - Download DSP software and ensure proper licensing.
- b. DSP Install Part 1**
 - Deploy and configure DSP IAS (Identity Analytics Server)
 - Install the DSP management server.
 - Push out Protector agent in each target domain.
 - Initiate directory synchronization.



- Install the DSP PowerShell module
- c. DSP Install Part 2**
 - Deploy remaining Protector agents
 - Deploy Audit agents.
 - Connect IAS to the Management Server.
 - Configure DSP settings, including SMTP, DSP retention, DSP health alerts, RBAC (Role-Based Access Control), config backup, and more.
 - Provide an overview and walkthrough of DSP features, including changes & undo, reports & filtering, compliance report bundle, DSP audit log, notifications, and security indicators.
- d. DSP Install Part 3**
 - Review and provide Knowledge Transfer of security indicators and audit notifications
 - Allow an open forum for customers to ask questions.
 - Describe the RAT (Reporting and Analysis Tool) if additional reporting beyond default templates is needed.

Deployment Completion

- a.** Semperis will provide a recap of the deployment and objectives from the kickoff and ensure goals of the ADFR deployment project have been met.

General Responsibilities & Assumptions

- Customer will assign technical point of contact for the duration of engagement stated in this Statement of Work
- Customer will provide all necessary information required to plan, design, and deploy DSP solution
- Customer is responsible to oversee and approve all required changes that are reasonable and necessary to assist with and to accommodate Semperis Customer success manager and solutions architect during the deployment of the DSP solution
- Customer is responsible for change management requirements and change control requirements during the provisioning and configuration of Active Directory Forest Recovery Solution
- Customer is responsible to provide and upload all discovery documentation
- Semperis is responsible to review all provided documentation to prepare for design recommendations and recommend any changes required to current customer environment prior to installation of software
- All services will be delivered to customer remotely

Change to Statement of Work

This statement of work may be modified or amended only in writing after signature of both customer and Semperis designated representative. Change order form will be provided to customer by the Semperis representative. Services that are not specified in this Statement of Work are considered out of scope and will be addressed with a change order request or new Statement of Work.

Project Scheduling

Customer and Semperis will jointly prepare and manage the schedule for this project. Parties will develop the deployment timeline together and report on any anticipated schedule estimates, timelines, or deadlines. Any dates, timelines, or schedules contained in this Statement of Work or otherwise during the planning and deployment of the product are only estimates.