ADISTEC PROFESSIONAL SERVICES

Rapid Deploy for One Identity® Safeguard

DESCRIPTION

Our implementation package assists our customers in the implementation of One Identity Safeguard for the management of privileged access to credentials (passwords and/or keys). This package is designed for both customers with advanced requirements and companies with an already defined policy of protection and access management.

SCOPE OF OUR SERVICE

- → Assessment
  - Kick Off.
  - Discovery Workshop.
    - Definition of success factors, up to two (2) use cases.
    - Analysis of the current infrastructure.
      - Survey of domain and forest of AD.
      - Determine users and functional groups.
    - Survey of privileged credential release flow.
  - Presentation of the report.
    - Finds.
    - Recommendations and best practices deployment options.
- → Design
  - Scenario and conditions analysis.
  - Architecture
    - Stand Alone
      - Up to one (01) physical or virtual appliance for credential management (passwords and/or keys).
      - Up to one (01) physical or virtual appliance for session recording and behavioral analysis.
      - Configuration of networking parameters.
    - High Availability
      - Up to three (03) Physical or virtual appliance for credential management (passwords and/or keys).
      - Up to two (02) Physical or virtual appliance for session recording and behavioral analysis.
      - Configuration of networking parameters.
  - High Level Design (HLD)
    - High-level design based on the results of the workshop
      - Ports.
      - Name of machines.
      - Networks.
      - Interaction with Firewall & Antivirus.

SCOPE OF OUR SERVICE (*continued*)

- Low Level Design (LLD)
  - Low-level design based on workshop results
    - Configuration of the one (01) domain.
    - Define privileged account groups.
    - Create up to one (01) new group or monitor up to three (03) current groups.
    - Credential Management Flow Design
      - Definition of up to two (02) rules.
      - Definition of up to two (02) policies.
- Disaster Recovery Plan (DRP) Design.
- Presentation of HLD and LLD.

→ Development

- Installation of up to one (01) development or test environment
  - Install devices (One Identity Safeguard) in environment development or Test.
  - Basic configuration of Privileged Access Management (PAM).
  - Integration with the user repository
    - Up to one (01) Active Directory (belonging to a [01] Forest).
  - Integration with systems or devices
    - Up to one (01) Windows system.
    - Up to one (01) Linux.
    - Configure PPM settings against the permissions policy.
    - Configure Privileged Passwords Management (PPM) settings against the permissions policy.
    - Configure Privileged Sessions Management (PSM) settings against the permissions policy.
  - Integration (01) network device into the Privileged Access Management system (*optional* PAM).
    - Test using Telnet or SSH protocol.
    - Configure Privileged Passwords Management (PPM) settings against the permissions policy.
    - Stable privileged sessions Management (PSM) settings against permission policy.
  - Creation of Installation Guide.
  - Testing
    - Acceptance tests, up to two (2) use cases.

SCOPE OF OUR SERVICE (*continued*)

→ Implementation
- Installation of PAM in one (01) Production environment.
  - Move Safeguard devices to production.
  - Import settings from Development or Test environment.
  - Integration with up to twenty (20) systems.
    - Devices that support Telnet or SSH access.
    - Systems with Microsoft Windows or Linux.
  - Global settings
    - High Disponibility (*according to architecture*).
    - Recuperation plan in the event of disasters (*according to architecture*).

→ Testing y QA
- Use case testing, up to two (2) use cases.
- Administration Account Request Process
  - Up to one (01) Microsoft Windows system.
  - Up to one (01) Linux system.
  - Up to one (01) device via Telnet or SSH.
- Acceptance test.
- Skill Transfer
  - Remote Mode.
  - Up to (04) four attendees.
  - Duration: 6 hours.

SERVICE DETAILS

Mode: On-Line
Duration Estimated: 220 hours

PART NUMBER

P/N	Description
APS-QST-OISFRD	Rapid Deploy for One Identity Safeguard®

LIMITATIONS AND OUT OF REACH

The physical installation of the appliance(s) is not included in this service, the client must perform the rack & stack of the appliance(s). For virtual appliances, the import process must be executed by the client. The configuration of networking (either physical or virtual) and network load balance for the correct operation of the appliances is out of reach. Adistec does not guarantee or guarantee the compatibility of devices, systems or applications that are not on the public list of platforms approved by Quest (Here). If the system, application, or device is not on the Quest compatibility list, Adistec undertakes to make all commercially reasonable efforts (if they do not put the work plan and the scheduled deadlines at risk) to work on a workaround that allows its integration, but without ensuring or guaranteeing it. A System is defined as an application, operating system, database, or compatible network device based on the solution's compatibility matrix that has a unique account management structure to be managed by the Software.