Services Offering Description

ONE IDENTITY SAFEGUARD PREPAID EXPERT SERVICE ADVANCED PACKAGE

AAC-SFG-PP

ONE IDENTITY SAFEGUARD PREPAID EXPERT SERVICE ADVANCED PACKAGE

One Identity utilizes a phased approach to implementation, which is completely flexible and designed to achieve the most efficient/effective delivery schedule, whilst optimising the transfer of knowledge to customer resources.

One Identity Expert Services have a well-defined project management methodology for deploying Identity and Access Management solutions. The methodology provides governance around our engagement approach which is based on the stages described below.

The following sections provide an overview of each stage, Activities, Project Deliverables and resources provided with this service package.

In the Activities below, where Configuration Items such as Assets or Users are added, "up to nn" is used to denote the guaranteed amount that One Identity will commit to creating/onboarding as part of the engagement. Customer's admin teams will be able to complete the remainder (and manage in BAU) using the knowledge they have gained from One Identity's consultant during the engagement.

Core Feature Project Deliverables:

Project Deliverable	Description
Discovery phase	One Identity will run discovery workshops not to exceed six hours total with key stakeholders to include the following: • Review Privileged Access concepts and problems that can be solved by Safeguard • Decide on architecture • Review any existing PAM config (e.g. TPAM) • Identify use cases • Review volumetrics (number of servers, users etc.) • Validate a set of functional and non-functional requirements that the solution must meet • Identify out of scope items • Agree project plan Project Deliverables: Project plan, requirements matrix
Design phase	One Identity will create design documentation to capture both the high-level architecture and detailed design in order to meet the requirements agreed at the Discovery phase.

	This is a living document and will be updated over the course of the project. Project Deliverables: Detailed Design document.
Develop phase	• Build virtual single-node SPP and single-node SPS clusters to latest SPP/SPS product versions • Add archive servers and configure backups • Develop custom powershell scripting for automation use cases • Configure A2A and test A2A use cases Project Deliverables: Fully built non-prod cluster, backups configured and password/session/A2A functionality verified.

Deploy phase	In this phase One Identity will build and configure the production instance according to the design, completing the detailed steps below.
	
	• Build SPP cluster (1x 3-node or 1x 5-node cluster of virtual or physical appliances)
	  ○ Build cluster nodes to latest SPP product version
	  ○ Add to cluster
	  ○ Add archive servers and configure backups
	  ○ Add list of managed IP networks
	• Build SPS cluster (1x 2-node cluster of virtual or physical appliances)
	  ○ Build 2 nodes to latest SPS product version
	  ○ Create cluster
	  ○ Add archive servers and configure backups
	  ○ Join to SPP cluster
	• Configure HA and DR.
	• Configure archive storage
	• Configure monitoring and management
	• Configure MFA
	• Configure Ticketing System (if supported)
	• Configure Safeguard to be a subordinate issuing CA in Customer's PKI hierarchy
	• Create and sign CRL
	• Configure RDP to use this CA for TLS
	• Configure network discovery, if required.
	• Create reason codes and other workflow items.
	• Create customer's dedicated Starling instance and configure Approval Anywhere
	• Deliver automation to create discovery jobs based on business services or other similar input data
	• Configure one Active directory forest as an authentication provider
	• Create up to five partitions
	• Create password profiles (up to 15)
	• Create SSH key profiles (up to 15)
	• Create discovery rules (up to 15)

	• Add assets via discovery rules (and/or up to 150 manually/via CSV) • Add users (up to 80) • Create entitlements and access request policies for SSH, RDP and Password release, modeled on RBAC roles (up to 60 policies) • Configure Safeguard for Privileged Analytics • Configure Application to Application (A2A) access (up to 5 applications) • Configure MSSQL sessions in SPS (up to 8 servers) • Implement Personal Password Vault • Create Remote Desktop Gateway policy on SPS • Run full DR test Project Deliverables: Fully configured Production Safeguard instance in accordance with the configurations specified above, DR Test
Deliver Phase	This phase will commission the new production instance. • Add the first teams/roles (up to 60 users) to Safeguard on a team-by-team basis • Support Customer with user acceptance testing as per the One Identity UAT plan which confirms a user can logon, request a password, and request a session. Project Deliverables: Fully commissioned system with key user subset using Safeguard in accordance with the configurations specified above.

PREREQUISITES AND ASSUMPTIONS

The Activities are based on the following specific assumptions. Any changes to these assumptions may result in the need to mutually negotiate a change in scope or fees:

1. That all VPN access, VDI/desktop access, standard and privileged accounts and all other required connectivity is in place to ensure One Identity's activities can be completed remotely.
2. The effort (and associated fees) for this service offering is based on preliminary discussions with the customer to establish the scope and assumes a typical level of complexity for the existing PAM solution. For a number of reasons it may be necessary to agree to changes in this effort (and associated fees) based on the outcomes from the discovery workshop, including but not limited to:
   2.1. Extensive custom API scripting is required for particular use cases.
   2.2. Individual teams are not able to complete their migration at the allotted time.
3. If a PAM solution already exists the migration model is in-parallel where live users will be migrated across to Safeguard on team-by-team basis
4. Discovery phase:
   4.1. The customer will ensure key stakeholders identified and available
5. Design phase:

5.1. The customer will ensure relevant technical resources are in place to review the design and answer questions on specific points.

6. Development phase, that the following prerequisites will be in place:
   6.1. SPP and SPS VMs added to VMware and console access granted in vCenter
   6.2. Certificates provided (exact certs required will be identified by One Identity during Discover phase)
   6.3. Maintenance windows approved
   6.4. Change control procedures agreed
   6.5. Service accounts created with appropriate rights to target systems
   6.6. Archive storage areas provisioned
   6.7. All users have access to MFA tokens where necessary
   6.8. Load Balancer VIPs configured and ready
   6.9. Appropriate firewall rules created (One Identity will supply requirements ahead of the engagement, customer to indicate minimum lead time for firewall requests)
   6.10. Details of the following integrations (if required):
      6.10.1. Syslog
      6.10.2. Email
      6.10.3. SNMP
7. Deployment phase:
   7.1. The customer will ensure relevant testing resources are available
8. Deliver phase:
   8.1. The customer will ensure relevant testing resources are available
   8.2. The customer will ensure end user teams are available at their scheduled time to complete migration.
9. Decommissioning of any legacy PAM infrastructure is out of scope and the customer will address this separately.