Identity and Access Management

Synoptek

Table of Contents

Introduction

This Service Definition is subject to all terms and conditions of the Service Order to which it was attached. This Service Definition describes and contains additional terms that apply to Synoptek's Identity & Access Management services

The service definitions found herein reflect Synoptek standards at the time the Service Order(s) was issued. Synoptek reserves the right to change any particular standard herein to reflect Synoptek's best practices or industry standards at its sole discretion with or without notice.

Service Offering

Synoptek's Identity & Access Management services provide customers a comprehensive IAM solution complete with SSO, MFA, and User Directory integration. When implemented and managed properly, organizations can efficiently and securely provision access to company resources and tools to their workforce.

Upon signing of a Service Order, Synoptek will assess the customer's business needs and implement a best-fit identity access & management accompanied with best practice end-user security.

Unless otherwise specified, this service is priced per user.

STANDARD COMPONENTS

This service provides customers with an agent-less* identity access & management solution to streamline user provisioning and provide access to corporate resources and tools as per business needs and objectives.

** Agent-less solutions do not require a desktop client to use. However, mobile devices may still be involved with features such as Multi-Factor Authentication.*

Feature and Description	Additional Information	Included
SINGLE-SIGN ON	Synoptek will implement an end-user web portal to provide access to specific company resources and tools as per the Customer's policies and needs. This portal will be accessible via desktop and mobile browser.	Yes
MULTI-FACTOR AUTHENTICATION	Synoptek will secure access to the Customer's SSO portal using a policy-based multi-factor authentication solution. Available authentication factors include: one-time passwords, email, SMS, voice, biometrics, and supported third-party options.	Yes
USER DIRECTORY INTEGRATION	Synoptek will integrate the Customer's user directory (e.g. Traditional Active Directory, LDAP), to federate users' authorization between the implemented IAM solution and the Customer's current employee roster.	Yes

SELF-SERVICE PASSWORD RESET	Synoptek will provide end-users with a means of self-service password reset. This process will be backed by security questions and/or multi-factor authentication.	Yes
USER PROVISIONING	Synoptek will provision users with approved access policies appropriate access to corporate resources and tools. Synoptek recommends an access policy of "Least Privileged" but will discuss with the Customer to ensure policies are in line according to the organization's needs and objectives.	Yes

ADD-ON COMPONENTS

This service can be customized with the following add-ons to support the adoption and/or benefits of the solution to the Customer.

Feature and Description	Additional Information	Included
ADAPTIAVE MULTI-FACTOR AUTHENTICATION	Synoptek will implement an adaptive multi-factor authentication solution to secure the Customer's SSO portal. This add-on enhances the Customer's experience by enforcing a dynamic set of authentication requirement(s) based on the level of risk determined from the location and device an end-user access from.	Optional
APP CONNECTORS	Synoptek can manage non pre-built ("custom") application connectors for the solution's SSO dashboard. These applications must support SAML, form-based, or API-based authentication protocols. Each application will be subject to billable hours to deploy and an additional monthly cost to support its ongoing management.	Optional
VIRTUAL CISO	Synoptek will provide the Customer a virtual Chief Information Security Officer whose goal will be to help plan, define, and execute best practice security with respect to the Customer's needs (e.g. this managed IAM service).	Optional

	Based on engagements between the Customer and Synoptek's vCISO, the vCISCO will propose and implement agreed upon adjustments to the Customer's IAM solution's policies to align with business objectives and need. This may include, but is not necessarily limited to, the adjustment of MFA policies and the adjustment of apps provisioned to specific groups of users,	
SECURITY TESTING AND TRAINING	Synoptek will enroll the Customer's end-users in an online security training program to educate and encourage best practice security. Synoptek will also regularly run automated phishing tests on the Customer's workforce and report back how phish-prone the organization currently is.	Optional
RADIUS AUTHENTICATION	Synoptek will manage authentication protocol for networks supporting RADIUS.	Optional

Service Deployment

Synoptek's Service Deployment team is responsible for the onboarding and offboarding of Identity Access & Management.

EXPECTATIONS DURING ONBOARDING

The initial onboarding of this service includes up to 5 non-custom application connectors. Additional non-custom connectors may result in additional fees. Non-custom connectors requested post-deployment will be deployed via billable change order.

Custom application connectors will result in additional fees to account for time developing and testing.

Synoptek Requirements

- New Flex Asset in SynopDocs for IAM.
- MSP Tenant setup
    - Permissions and roles defined
    - "Access" form updated
    - Deployment and Operations teams defined and assigned
        - Deployment team should be setup by default with necessary access to create and manage tenants
    - Named Management User access should be setup for Synoptek Staff via 'Access' form.
- Deployment process defined:
    - Customer tenant setup process defined and documented
    - Default rules and policies assigned
    - "How to integrate with AD/Azure AD" documentation standardized for Deployment practice
- Documentation to link to 'Native' integration processes
- SynopDocs per-customer documentation completed for internal support reference.
- Security Assessment completed and advisement logged
- "Assumed Identity" risk analyzed and approved
- Customer distributable (brief/digestible) documentation regarding setup of OTP app, "How To," etc,

Other Requirements

- Customer end users must have a compatible MFA token/device.
- To preserve current end-user passwords during deployment, Synoptek requires integration with a traditional Active Directory. Lack of such will require an organization-wide password reset during deployment.

Synoptek Deliverables

- Integration with user directory (e.g. Active Directory, LDAP)
    - Or establishment of new OneLogin accounts and passwords for all users
- Integration into all scoped natively supported applications completed and tested
    - Roles defined for automatic app assignments (AD group, OU, Department, Job Title, etc.)
- MFA requirements defined and implemented
    - Customers MFA enrolled
- Internal documentation completed
- Notifications setup as necessary
- Simple Customer Logo Branding

Service Support

REQUIREMENTS FOR THIS SERVICE

SYNOPTEK RESPONSIBILITIES

- Synoptek will deliver a secure identity access & management solution to:
    - Securely provide Customer's end-users with access to resources and tools pertinent to their responsibilities and needs
    - Support the Customer's overall business strategy and objectives

CUSTOMER RESPONSIBILITIES

- The Customer will provide access to their user directory and adhere to the provided solution's best practices during deployment and on.
- The Customer will provide up-to-date criteria regarding which applications and resources are to be accessible to which end-users.
- Provide or confirm that all employees have an MFA token/device. Device provision is not in scope.