

SECURE ACCESS SERVICE

Service Description

Contents

Introduction	3
Scope of Services	3
Unisys Tasks and Deliverables.....	3
Client Responsibilities and Obligations.....	4
Prerequisites	4
Secure Access Service Technical Support	4
Support Service Requests	4
Response and Repair Times	5
Support Service Hours.....	5
Support Contact Information	5
Software Tools	5
Roles and Responsibilities	6
Key Assumptions and Dependencies	8
Secure Access Service Subscription Fee and Usage Charge	8
Subscription Fee	8
Usage Charge.....	8
Usage Calculation	9
Additional Services	9
Definitions	9

Introduction

This document is incorporated into the Unisys Secure Access Service Order executed between the Client and Unisys. In the event of a conflict between this Service Description and the Order, this Service Description shall govern.

Scope of Services

The Unisys Secure Access Service is a zero trust security solution that provides users with access to required data and applications, based on the concept of least privilege. The Service leverages Unisys technology to enforce zero trust security policies.

Unisys Tasks and Deliverables

Unisys, with the Client's assistance and participation, will deliver the Secure Access Service consisting of:

- **Secure Access Service management plane supervision**
 - Unisys will maintain, monitor, update, and scale, as required, all Secure Access Service management plane software components
- **Compatibility and version tracking**
 - Unisys will track the version of Tools running on all Secure Access Service endpoints
 - Endpoints that require an update to the current production version of Tools will be identified
- **Endpoint software updates**
 - Unisys will create hotfix and software endpoint packages for Tools as required for all Secure Access Service endpoints
 - Note: Client is responsible for distributing software updates to endpoints in the Client's environment
- **Backup and restore**
 - Unisys will create a backup solution for the Secure Access Service management plane
 - Unisys will manage the Secure Access Service management plane infrastructure for service restoration
- **Availability management**
 - Monitoring and alerting
 - Problem management to resolution
 - Coordination with Unisys technical support
 - Troubleshooting the Secure Access Service environment
- **Secure Access Service security policy changes**
 - Changes to the existing delivered configuration, specifically modifications to the two security policy role configurations established in the Secure Access Start-up Service
 - Removal of configurations or roles as necessary to support decommissioning of endpoints
 - Note: Any new configurations or new security policies beyond the initial two roles / configurations included in the standard Service are outside the scope of this Service Description

Deliverables

Unisys will produce the following deliverables:

- On-going delivery of updated Secure Access Service Tools software endpoint packages for Client's deployment
- On-going management and monitoring of the Secure Access Service management plane
- Monthly Usage Report used for billing purposes

Client Responsibilities and Obligations

- Client is responsible to deploy and install all Secure Access Service Tools software endpoint packages in the Client's environment
- Client will maintain user/computer Active Directory® (AD) group membership and notify the Unisys managed service team of changes in the AD group names leveraged by the Service
- Client is responsible for supporting their end users and making reasonable efforts to resolve end user issues; only Client's Support Contacts, not individual end users, may enter requests for support with Unisys
- Client is responsible to identify Client resources, including all Support Contacts, to complete on-demand, online training courses on the software Tools used in the Secure Access Service, to ensure resources complete the training in a timely manner, and stay up-to-date on training as updates or new courses are made available
- The parties acknowledge that cooperation and teamwork by both parties is essential to the success of a project. Client agrees to provide the resources detailed in this section at no charge to Unisys. Client agrees not to unreasonably withhold or delay the provision of any agreement, acceptance, information, assistance or other resource reasonably required or requested by Unisys. If Unisys is delayed or prevented from performing its obligations, to the extent that the delay is caused by factors beyond the reasonable control of Unisys, including, without limitation, the inability of Client to perform its responsibilities in a timely manner, Unisys will be entitled to an equitable adjustment in the timetable and compensation set out in the Order

Prerequisites

The Unisys Secure Access Start-up Service is a prerequisite service to the Secure Access Service. It is required with any Secure Access Service purchase and is charged separately.

Secure Access Service Technical Support

Support Service Requests

Provided that Client is current with payment of fees, in the event of an Issue with the Secure Access Service, a Client Support Contact may engage E-Mail Support or Telephone Support. Unisys will assign one of the following Severity Levels to each reported Issue based on the information provided by the Support Contact:

- Severity Level 1 — The Secure Access Service is not accessible or not functioning.
- Severity Level 2 — The performance of the Secure Access Service is noticeably impaired but continues to be accessible and functional.
- Severity Level 3 — A Support Contact requires information or assistance on the capabilities, configuration, or operation of the Secure Access Service.

Response and Repair Times

In the event that an immediate resolution is not available upon the report of an Issue, Unisys will respond within four (4) hours of a Telephone Support or E-mail Support request to the Support Contact who reported the Issue for all Severity Level 1 Issues, and within one (1) Business Day for all Severity Level 2 Issues. Unisys will respond to all Severity Level 3 Issues within two (2) Business Days of the Issue report. Response times are available for Telephone Support and E-mail Support requests received during the hours for Secure Access Service Technical Support identified below. For all Severity Level 1 Issues, Unisys will begin troubleshooting and diagnosis of the Issue immediately upon Unisys's response to the Issue report, and provide a workaround, fix, or correction as soon as commercially practical thereafter. For Severity Level 2 Issues and Severity Level 3 Issues, Unisys shall begin troubleshooting and diagnosis of the Issue promptly but not to exceed two (2) Business Days from Unisys's receipt of the Issue report, and provide a workaround, fix, or correction as soon as commercially practical thereafter.

Support Service Hours

Unisys provides Secure Access Service support on the following days and during the following hours:

24 hours a day, 7 days a week, 365 days a year.

Support Contact Information

All support Issues must be submitted via the contact methods prescribed by Unisys. Secure Access Service support contact information will be provided to the Client in writing prior to the completion of the required Secure Access Start-up Service.

Software Tools

Unisys may install, or may require Client to install, Tools in your environment so Unisys can provide the Services and you can receive the Services. Any Tools provided are only for the period of the Unisys Services and for Unisys use and your use to the extent necessary for Unisys to provide services and for you to receive the Unisys Services. You must destroy or return any Tools to Unisys when Unisys Services end.

Unisys may from time to time provide substitute Tools or Updates to the Tools. Updates may also modify or delete in their entirety certain features and functionality. Updates are deemed Tools subject to these terms. Upon receiving an Update from Unisys, you agree to stop using the earlier copies and replace the earlier copies with the Updates provided by Unisys and hold Unisys harmless for any delays or damages resulting from your failure to do so. Unisys has no obligation to provide any Updates for the Tools or to continue to provide or enable any particular features or functionality.

Certain third party software may be provided with or embedded in Tools as described in the applicable License and Attribution Documents described in the documentation that accompany the Tool or in the table, below. This Service Description and the Agreement shall not add additional conditions or restrictions, or affect any rights or duties you may have under an open source license.

Tools		
A. Unisys brand Solutions		
Unisys solution name(s)	Version	License and Attribution
Stealth(core) Unisys Stealth® Solution	5.2	See applicable <u>License and Attribution Documents at this url: www.unisys.com/client-contract-terms/</u> .

If an open source license for any Tool(s) provided by Unisys gives you the right to receive the source code from Unisys, you can obtain a copy of the applicable source code by sending a request to thirdpartysoftwareapproval@unisys.com. Your request should include: •The name of the component or binary file(s) •The name and version number of the software •Date you received the software •Your name •Your company name (if applicable) •Your return mailing address and email •A telephone number.

Your request must be sent within three (3) years of the date you received the software from Unisys. Please note that we may charge you for the cost of the physical media and processing.

Roles and Responsibilities

The following RACI (Responsible/Accountable/Consulted/Informed) matrix describes the participation required by Unisys and the Client during the engagement to complete various tasks and/or deliverables.

- Responsible (R) – The party responsible for the execution of the task
- Accountable (A) – The party accountable for the task and signs off the work
- Consulted (C) – The party who acts as subject matter expert(s) to be consulted
- Informed (I) – The party who receives progress updates

Activities	Unisys	Client
Service transition from the Secure Access Start-up Service		
Unisys managed services team will engage to ensure the Secure Access Service environment is manageable, by reviewing and approving the infrastructure and configuration as implemented in the Secure Access -Start-up Service.	R	C
Administration		
Administration of Active Directory integration for the following: <ul style="list-style-type: none"> • Users move-add-change • Users added or removed from a group(s) 		R
Administration of Active Directory integration for the following: <ul style="list-style-type: none"> • Add - delete - rename Secure Access Service referenced groups • Any changes to Active Directory structure 	I	R
Administration of the Secure Access Service management plane including: <ul style="list-style-type: none"> • Users or computer object move-add-change • Users added or removed from a group(s) • Computer objects added or removed from a groups(s) 	R	C

Activities	Unisys	Client
Testing and troubleshooting of endpoint packages		
Preparation of Tools endpoint packages for endpoints in the Client's environment (i.e., workstations, servers)	R	C
Test and validate operation and impact of Tools endpoint packages on test endpoints	R	C
Provide test endpoints for the operating systems and platforms to be rolled out	C	R
Approve Tools endpoint updates	C	R
Deployment of Tools endpoint packages	C	R
Efforts to diagnose and respond to issues arising with the deployment of Tools endpoint packages	R	A
Ongoing endpoint package deployment		
As new endpoints are added to existing configurations, Secure Access Service Tools will be installed in the build	A	R
Work with Client desktop and server provisioning teams to ensure endpoint packages are included in the build process	R	C
Provision Tools agents in the build process for new endpoints	C	R
Policy maintenance and back-up		
Create and manage Secure Access Service application-level backups of various Secure Access Service components and their configurations and restore them in case a recovery is necessary.	R	I
Participate in Client's disaster recovery exercises when required.	C	R
Support		
Problem management and resolution: coordination of diagnosis, root cause analysis, and remediation efforts for issues that arise in the Secure Access Service	R	A
New endpoint packages		
Prepare updated Tools endpoint packages for distribution to the client	R	C
Conduct system tests of all such updates in a lab environment before being applied to the Client's production infrastructure.	R	I
Service delivery management		
Unisys will provide service delivery / project management for coordination of the Services under the Agreement to include: <ul style="list-style-type: none"> ▪ Resource planning, leading meetings/workshops, communications planning ▪ Serving as single point of contact to all Unisys Service under this Service Description ▪ Leading monthly operational review meetings ▪ Holding service level requirements reviews and continuous improvement meetings 	R	C
Designation of a Client resource to be recognized as Primary Contact.	I	R

Key Assumptions and Dependencies

- The Secure Access Service will be provided remotely using a mix of on and off shore resources as deemed appropriate by Unisys
- Unisys may change the Cloud Hosting Provider utilized at any time, at Unisys discretion
- Client and Unisys shall attend regularly scheduled review calls and status meetings
- Client and Unisys shall promptly escalate issues within their respective organizations as appropriate

Unisys's provision of the Service is dependent on Client's compliance with its responsibilities as listed in this Service Description. If Client fails to perform its responsibilities or if an exclusion applies, Unisys will be excused from performing the Service to the extent, and for the duration that Client's failure to meet its responsibilities reasonably prevents Unisys from performing its responsibilities. In addition, Unisys reserves the right to charge Client for expenses, costs, or time incurred, caused by Client's failure to perform its responsibilities. In addition to the Client Responsibilities listed above, Client is also responsible to:

- promptly supply Unisys with reasonably requested and necessary technical data (e.g., host names, IP addresses,) and other similar information to allow Unisys to provide the Services
- provide prompt, reasonable cooperation and assistance to Unisys in performance of the Service
- promptly provide any agreement, acceptance, information, assistance, or other resource reasonably required or requested by Unisys (without unreasonable withholding or delay) and elevate required decisions to the appropriate level in Client's organization to facilitate prompt and timely decision-making. Client will respond within five (5) Business Days to any Unisys request for direction, information, approvals, or decisions that are reasonably necessary for Unisys to perform the Services
- notify Unisys in advance of any updates or changes planned in Client's environment
- comply with all legal and regulatory requirements governing the Client's operations, to include notification to Unisys of relevant requirements
- formally identify a project sponsor as the professional liaison with the Unisys team

Secure Access Service Subscription Fee and Usage Charge

Subscription Fee

The Secure Access Service Monthly Subscription Fee is determined by the Per User Monthly Fee multiplied by the Minimum User Commitment. The Client's Per User Monthly Fee and Minimum User Commitment is documented in the Order for the Service. Unisys shall invoice Client the Monthly Subscription Fee for the Secure Access Service quarterly, based on calendar quarters, in advance. For the avoidance of doubt, if the number of Service Users in a given month is less than the Minimum User Commitment, the Monthly Subscription Fee for the month will be based on the Minimum User Commitment.

Usage Charge

The Secure Access Service Monthly Usage Charge is a charge incurred when the number of Service Users in a given month exceeds the Minimum User Commitment. The Monthly Usage Charge is determined by the number of Service Users in excess of the Minimum User Commitment, multiplied by the Per User Monthly Fee. Unisys shall invoice Client the Monthly Usage Charge quarterly, based on calendar quarters, in arrears.

If the Service is active for any portion of a calendar month, the full Monthly Subscription Fee is incurred, as well as any Monthly Usage Charge (if applicable).

All stated charges are exclusive of applicable taxes, which shall be invoiced by Unisys and paid by Client.

Usage Calculation

A Monthly Usage Report will be retrieved by Unisys from the Secure Access Service management plane within 10 Business Days of the end of each calendar month that the Service is in effect. The Monthly Usage Report will be used to determine the applicable Monthly Usage Charge, if any, for the month. The Monthly Usage Report for each month will be posted in the Client Portal within 15 Business Days of the end of a calendar month.

Based on the Minimum User Commitment, a predetermined number of Servers are included in the Secure Access Service at no additional charge. The Monthly Usage Report will report the total number of unique Servers that participated in the Service at any time during the calendar month, including the Servers being used to host the Secure Access Service management plane. The number of Servers included in the Secure Access Service is documented in the Client's Order for the Service. If the number of Servers reported exceeds the number included at no charge in the Minimum User Commitment, this will constitute a change request and trigger a change control process.

For reporting purposes, the reporting period for a Monthly Usage Report starts on the first calendar day of a month and ends on the last calendar day of a month, each month.

In the event of a system issue preventing retrieval of the Monthly Usage Report for a given month, usage information for each of the previous three months shall be averaged together to determine the number of Service Users and Servers for that month.

Additional Services

Additional services are available at the standard Unisys consulting rate.

Definitions

"Agreement" means the Order accepted by Unisys and incorporates Unisys standard terms published at www.unisys.com/client-contract-terms/.

"Business Days" means any day from Monday to Friday except government and bank holidays in the location where the Order for the Services is accepted by Unisys.

"Client" means the client referred to in the relevant Order.

"Client Portal" means an electronic portal hosted by Unisys and accessible by Client management personnel designated by the Client. The portal is used to publish Client-specific information related to the Service such as Usage Reports. The Client Portal is not part of the technical support process and is not to be used by Client Support Contacts to report an Issue.

"Cloud Hosting Provider" means the public cloud provider from whom Unisys procures the cloud computing resources on which the Service is instantiated.

"E-Mail Support" means electronically generated Issue (defined below) identification and correction as set forth herein, and other technical and support services provided in response to electronically transmitted inquiries by the Support Contacts.

"Issue" means an error, question, accessibility problem or other issue related to the Secure Access Service.

“**Maintenance Services**” consist of the provision of any enhancements, modifications, updates, corrections or a subsequent release or version of the Unisys provided Software Service Tools.

“**Minimum User Commitment**” means the contractually committed minimum number of Service Users per month that will be charged for the Service.

“**Monthly Subscription Fee**” means a fixed monthly fee for use of the Service, based on the Per User Monthly Fee and a Minimum User Commitment.

“**Monthly Usage Charge**” means a monthly charge incurred when the number Service Users in a given month exceeds the Minimum User Commitment.

“**Monthly Usage Report**” means a report identifying the total number of Service Users, and total number of Servers participating in the Service, each month.

“**Order**” means a written order from Client for the Services of which this Service Description is a part (A) directly with Unisys that is accepted by Unisys, or (B) with a Unisys reseller, subject to Unisys acceptance of an order for the Services from its reseller.

“**Per User Monthly Fee**” means the monthly charge for each Service User.

“**Primary Contact**” means the individual within the Client’s organization identified as the focal point for all Unisys communications relative to this Service, with the authority to make binding decisions and act on behalf of Client in matters regarding and related to this Service.

“**Secure Access Service**” or “**Service**” means the offering as defined in this Secure Access Service Description under the heading “Scope of Services – Unisys Tasks and Deliverables.”

“**Secure Access Service Technical Support**” means E-Mail Support, Maintenance Services, Web Site Support and Telephone Support.

“**Secure Access Start-up Service**” means a predetermined set of planning, installation, configuration and knowledge-transfer services.

“**Servers**” means an endpoint running a server operating system as defined in Tools documentation.

“**Services**” means work, products, or services provided under an Order, including any SaaS provided on a recurring basis or a subscription basis.

“**Service User**” means a unique user accessing the service at any time during the calendar month.

“**Severity Level**” means the severity levels referred to under the heading “Secure Access Service Technical Support, Support Service Requests.”

“**Support Contacts**” means Client’s designated technical support contact(s). Client may designate up to five (5) Support Contacts.

“**Telephone Support**” means support services provided to the Support Contacts in response to telephone requests for assistance.

“**Tools**” means Unisys-provided software service tools.

“**Unisys**” means the Unisys legal entity on whom Client placed the Order for the Services, or if Client placed the Order for the Services through a Unisys’ reseller, the Unisys legal entity that accepted the reseller’s corresponding order for the Services. The Unisys entity through which the Services are available in the United States is Unisys Corporation, 801 Lakeview Drive, Suite 100, Blue Bell, Pennsylvania 19422.

“**Updates**” means updates to the Tools, which may include replacement Tools, upgrades, bug fixes, patches, other error corrections, and/or new features, including related documentation.

“**Web Site Support**” means generic, not specific to Client, support information available through Unisys’s Internet web site located at www.unisys.com.
