SSH

Global Standard Professional Services Offerings

Contents

All Products

Technical Account Management and Consultancy

Standard professional services modules	Description	Typical duration (remote/onsite days)
Technical account management (weekly call) *Note: Customer call cadence can be adjusted as per customer need & cost adjusted pro-rata.*	• Weekly call with product owner and regional professional services solution architect • Helping customers get most value from product • Discuss open support tickets & feature requests • Consultation advice on bespoke customer integrations • Planning for solution upgrades with minimal downtime • Arranging further product training • Quarterly business review reporting on support SLAs & product roadmap sessions	50 hours per year

Standard professional services modules	Description	Typical duration (remote/onsite days)
SSH product consultancy	• Ad-hoc consultancy with regional professional services solution architect • Helping customers get most value from product • Discuss open support tickets & feature requests • Consultation advice on bespoke customer integrations • Planning for solution upgrades with minimal downtime • Arranging further product training • Quarterly business review reporting on support SLAs & product roadmap sessions	Sold in minimum 1 day blocks
OpenSSH consultancy	SSH expertise to help customers optimise SSH use cases: • SSH authentication best practices (ldap, sssd, NIS, AD, PAMD, certificates) • SSH connections between ALL windows, MACoS • System management software • Monitoring tools (Tivoli/Netcool) • Middleware (IBM Websphere / TibCo) • Automation (ansible/chef/puppet) • File transfer • CI-CD tools (Jenkins/Git) • SSH tunnelling (Securely connect legacy client connections) • SSH compliance (key management & access control) • IoT device control • OT access to PLC, HMI, RPA control devices • SSH access to cloud servers and services • Native SSH client support	Sold in minimum 1 day blocks

Deployment and Operations

Standard professional services modules	Description	Typical duration (remote/onsite days)
Tectia install and configuration (C/S)	• Infrastructure requirements • Port configurations • Installation of Tectia on Windows/Linux/AIX • License activation • Starting and stopping server • Adding required permissions for the files and folders • Configuring Tectia Server & Client • Overall settings, services settings • Logging	1
Tectia install and configuration (z/OS)	• Review the customer use cases • Configure and validate z/OS environment is ready to install Tectia • Install Tectia on x amount LPARs • Configure SSHD2 for inbound sftp • Configure SOCKS Proxy for outbound ftp-to-sftp • Configure SFTP client for outbound sftp • Test connections	5
Tectia z/OS FTP to SFTP migration service	• Review the existing FTP jobs • Configure and validate z/OS environment is ready to install Tectia • Install Tectia on x amount LPARs • Configure SOCKS Proxy • Configure FTP client to use SOCKS Proxy • Help configuring target sftp server(s) • Test few outbound ftp-to-sftp jobs • Configure SSHD2 for inbound sftp • Test few inbound sftp jobs	5
Tectia reconfiguration (post validation)	Reconfiguration of Tectia Server to ensure that security best practices are in place and the configuration meets the required	1

Deployment and Operations

Standard professional services modules	Description	Typical duration (remote/onsite days)
Tectia system validation check (required for Premium Support)	• Review of existing installation • Checking installation directory and file permissions • Tectia Server general settings: Load control, login grace time, user configuration directory, domain policy, logging, etc. • Hardening the server configuration • Host key regeneration due to CVE-2021-27891 “Snowflake” • Ensure authentication methods are properly configured • Encryption algorithms • Connection testing and possible troubleshooting	1,5
Tectia upgrade service	• Evaluating the existing install • Backing up the current configurations • Importing the host keys, server configuration from old Tectia • Upgrading Tectia C/S to the latest versions • Checking installation directory and file permissions • Validating the new install and testing connections • Overview of the new features and demo	1

Tectia®
SSH Client/Server

Product Admin
Training

Standard professional services modules	Description	Typical duration (remote/onsite days)
Tectia product training for admins (max 5 trainees)	• Pre-requisites: SSH protocol architecture, understanding SSH, key features, SFTP, SCP • SSHG3 Client & Server architecture • Overview of Tectia • Installation of Tectia C/S • Authentication methods: password, public key, certificate, 2FA, Smart Card, Tokens, host-based authentication • Enable/disable Tectia Server functionality: Enabling FIPS mode, SFTP, chrooting, X11 tunnelling, allowing/restricting connections • Logging & troubleshooting • Example use cases for Tectia CLIENT ONLY: • Adding profiles and testing connections for File Transfers • Command line tools • Tectia Broker	1,5
Tectia product training for Lab Env (available for 30 days)	Tectia training lab is hosted in AWS and access is provided via PrivX. It includes below servers: 1. Linux Server: t2-medium 2. Windows Server: t2-medium *Note: Training lab servers are available for 4 weeks from start of training on weekdays (Mon-Fri) during day time (12 hours based on customer timezone). Lab servers can be made available on weekend on request.*	5 trainee access for 30 days

Universal SSH Key Manager® (UKM)

Deployment and Operations

Standard professional services modules	Description	Typical duration (remote/onsite days)
UKM install and configuration (small < 1000 hosts)	• Solution deployment planning, installation, and basic UKM configuration • Discovery of target servers, example batch • Discuss about CMDB integration for automatic server on- and off-boarding • Examples of environment lockdown, authorized key relocation • Example key ownership configuration & User Portal application on-boarding • Create UKM policies and perform example key remediation against selected policies and policy-violating keys	5
UKM install and configuration (medium 1000 - 5000 hosts)	• Solution deployment planning, installation, and basic UKM configuration • Discovery of target servers, example batch • Discuss about CMDB integration for automatic server on- and offboarding • Examples of environment lockdown, authorized key relocation • Example key ownership configuration & User Portal application on-boarding • Create UKM policies, and perform example key remediation against selected policies and keys violating policies	10
UKM install and configuration (large > 5000 hosts)	• Solution deployment planning, installation, and basic UKM configuration • Discovery of target servers, example batch • Discuss about CMDB integration for automatic server on- and offboarding • Examples of environment lockdown, authorized key relocation • Example key ownership configuration & User Portal application on-boarding • Create UKM policies, and perform example key remediation against selected policies and keys violating policies	20
UKM annual upgrade service (2 days per upgrade)	• Annual service providing upgrade to latest versions of UKM software • Overview of latest features provided to UKM onsite team • Completion of basic functional tests to ensure existing and new functionality is working • Verification that integration scripts in place for reporting/on-boarding are still working	6 days per year (per UKM system)
UKM HA and DR testing service	• High Availability review • Disaster Recovery review • Fault tolerance testing completed on UKM components to ensure no single points of failure DR test completed to ensure UKM service is still operational when running from DR datacenter & also on failback to production data centre	2 days per year (per UKM system)

Standard professional services modules	Description	Typical duration (remote/onsite days)
UKM automated CMDB host on-boarding	Integration script provided to interact with CMDB database (eg. ServiceNow), automatic on-boarding of target servers into UKM, assigning of correct metadata for host grouping, etc.	3

Universal SSH Key Manager® (UKM)

Product Admin Training

Standard professional services modules	Description	Typical duration (remote/onsite days)
UKM product training for admins (max 5 trainees)	• SSH key management problem & project phases • SSH Secure Shell basics • UKM architecture (basic) • UKM installation (RPM) • UKM basic configuration • Target host preparation • UKM host discovery • UKM tasks and processes • User Portal installation • User Portal configuration • Policy configuration & reporting • Auditing, monitoring, alerting & data archive • UKM CLI & data management (basic) • UKM troubleshooting (basic) • Target host lockdown	3
UKM product training for Lab Env (available for 30 days)	UKM training lab is hosted in AWS, and access is provided via PrivX. It includes below servers: 1. UKM frontend and backend: t2-medium 2. UKM user portal server and CLI: t2-medium 3. Linux target node 1: t2-small 4. Linux target node 2: t2-small *Note: Training lab serves is available for 4 weeks from start of training on weekdays (Mon-Fri) during day time (12 hours based on customer timezone). Lab servers can be made available on weekend on request.*	5 trainee access for 30 days

Universal SSH Key Manager® (UKM)

Product Architect Training

Standard professional services modules	Description	Typical duration (remote/onsite days)
UKM product training for architects (max 5 trainees)	• SSH key management problem & project phases • SSH Secure Shell basics • SSH Secure Shell advanced • UKM architecture (basic) • UKM architecture (advanced) • UKM installation (RPM) • UKM basic configuration • UKM advanced configuration • Target host prepration • UKM host discovery • UKM tasks and processes • User Portal installation • User Portal configuration • Policy configuration & reporting • Auditing, monitoring, alerting & data archive • UKM CLI & data management (basic) • API v3, UKM CLI & data management (advanced) • UKM troubleshooting (basic) • UKM troubleshooting (advanced) • Target host lockdown • Script-based host scan • UKM upgrade	5

Deployment and Operations

Standard professional services modules	Description	Typical duration (remote/onsite days)
PrivX install and configuration (single instance ssh/rdp only)	• Hardware requirements and configuring firewalls • Installation of PrivX server - for cloud/on-prem • Licensing • Using PrivX dashboard • Checking the service status • New SSH connection: from UI + file transfers + settings • New RDP connection: from UI + file transfers + settings • SSH native client connections (using PuTTY) • RDP native client connections (using Windows RDP client)	3
PrivX install and configuration (single instance ssh/rdp/web)	• Installation of PrivX server + PrivX components (web carrier & web proxy) • Hardware requirements and configuring firewalls • Licensing • Using the PrivX dashboard • Checking the service status of PrivX and the components • New SSH connection: from UI + file transfers + settings • New RDP connection: from UI + file transfers + settings • SSH native client connections (using PuTTY) • RDP native client connection (using Windows RDP client) • Configuring the components in PrivX GUI • Adding access to web service via HTTPs using carrier/proxy • Configuring required ports • New web connection: from UI + file transfers + settings	5
PrivX install and configuration (HA/ DR multi instance ssh/rdp/web)	• Workshop to gather information about customer environment • Preparation of PrivX solution design • Infrastructure provisioning, load balancer and firewall configuration • External PostgreSQL database installation and configuration • PrivX HA installation • PrivX carrier and web proxy installation • User and host directories configuration/host onboarding for SSH and RDP targets • Web target configuration • Updating of PrivX solution design documentation covering following aspect: a) PrivX system components and specifications b) Network/firewall details c) PrivX upgrade process d) High availability e) Disaster recovery	15

Deployment and Operations

Standard professional services modules	Description	Typical duration (remote/onsite days)
PrivX install and configuration (HA/DR multi network ssh/rdp/web + extender)	• Workshop to gather information about customer enviroment • Preparation of PrivX solution design • Infrastructure provisioning, load balancer and firewall configuration • External PostgreSQL database installation and configuration • PrivX HA installation • PrivX Extender installation and configuration • PrivX carrier and web proxy installation and configuration • User and host directories configuration/host onboarding for SSH and RDP targets • Web target configuration • Updating of PrivX solution design documentation covering following aspect: a) PrivX system components and specifications b) Network/firewall details c) PrivX upgrade process d) High availability e) Disaster recovery	20
PrivX account discovery service	• Scan environment (UKM offline scan scripts) • Upload scan output files to PrivX server • Process output files to create a CSV output showing • Accounts and SSH keys present across estate • Scripted process to create accounts and associate roles in PrivX	3
PrivX CMDB host on-boarding	Integration script provided to interact with CMDB database (e.g. ServiceNow) and automatic on-boarding of target servers into PrivX and assigning of correct roles to known target accounts	3

Deployment and Operations

Standard professional services modules	Description	Typical duration (remote/onsite days)
PrivX system validation check & testing (required for Premium Support)	Produce PrivX design validation document covering following aspects: • Architectural diagram • IAC: Cloud formation templates, auto scalling group, launch configurations, etc. • User directories & roles • User authentication (inc. 2FA) to PrivX • Host on-boarding (Windows) + PrivX authentication to target • Host on-boarding (Linux) + PrivX authentication to target • Host on-boarding (web) + PrivX authentication to target • Role to target user mapping • Functional capacity review (CPU, Memory, IO, Storage, Network) • Scalability • High availability review • Disaster recovery review • Joiner-mover-leaver process • Host lifecycle management • Target host user lifecycle management • Session recording • Integration with SIEM system (alerts & processes) • Review Linux SSHD server configurations on target hosts and changes required	6 days per year (per PrivX system)
PrivX annual upgrade service (2 days per upgrade)	• Evaluating the existing installation • Pre-upgrade discussion with the customer • Number of upgrades/year based on customer requirement • Upgrading from non-supported version to the latest » Incremental upgrades • Backups of PrivX configuration and external DB • System backup (Vmware Snapshots/EMI) • Version upgrade • Post upgrade validation • Restoration of previous settings • Overview of the new features and demo	6 days per year (per PrivX system)
PrivX HA and DR testing service	Produce PrivX HA and DR test document covering following aspects: • High availability review • Disaster recover review • Fault tolerance overview • Actual HA test by simulating one or more componenet failure • Actual DR test by simulating one data centre or regioin failure	2 days per year (per PrivX system)

PrivX®

Product Admin Training

Standard professional services modules	Description	Typical duration (remote/onsite days)
PrivX product training for admins (max 5 trainees)	• Infrastructure requirements and security configurations • PrivX server installation for cloud/on-prem • PrivX carrier and proxy installation • Managing the dashboard • Creating user, roles & configuring workflows • Directories (Local, AD, LDAP, OIDC) and user groups • Adding access to Linux hosts via SSH • Adding access to Windows hosts via RDP • Adding access to web service via HTTPs using carrier/proxy • Integrating PrivX using API clients • Importing data via API/CLI • Secret vault management • Authentication types • Auditing and reporting • Backup and restore • Troubleshooting • Typical use cases	3
PrivX product training for Lab Env (available for 30 days)	PrivX training lab is hosted in AWS, and it includes below servers: 1. PrivX server: t2-medium 2. PrivX carrier and web proxy: t2-medium 3. PrivX Extender: t2-small 4. 3 Linux target servers: t2-small 5. 1 Windows target node: t2-medium *Note: Training lab servers are available for 4 weeks from start of training on weekdays (Mon-Fri) during day time (12 hours based on customer timezone). Lab servers can be made available on weekend on request.*	5 trainee access for 30 days
PostgresDB training	Not applicable at present	2

PrivX®

Product Architect Training

Standard professional services modules	Description	Typical duration (remote/onsite days)
PrivX product training for architects (max 5 trainees)	• What is PrivX • PrivX architecture design for cloud (Azure, AWS and Google cloud) and on-prem • PrivX microservices architecture • Network configurations • IAM, authentication & authorizations • Role-based access: Defining and designing roles and users • Rest APIs • Automation using Chef, Puppet, Ansible • Additional security features: HSM, WAF, MFA, SSO, ephemeral certificates • Designing break-glass scenario	4
PrivX product training for end users (max 5 trainees)	• Managing the dashboard • Principles of users, roles & workflows • Authentication directories (Local, AD, LDAP, OIDC) and user groups • Access to Linux hosts via SSH • Access to Windows hosts via RDP • Access to Web Service via HTTPs using carrier/proxy • Requesting access to role using workflow • Using PrivX Secret Vault	0,5

Deployment and Operations

Standard professional services modules	Description	Typical duration (remote/onsite days)
NQX central management system installation	• Installation environment review • CM installation • Database installation • Certifications import/creation • Creating admin user and logging with GUI • Set default values (CM Settings) » Create backup scheduler » Using the dashboard • CM Introduction	2
NQX central management system Hot stand-by installation	• Installation environment review • Scope of hot stand-by installation: Two systems/database • System environment (CM, NTP, DNS, DHCP) • IP addresses for systems (see above) • PKI-plan, customer plan to utilize certifications (installation and configuration of NQX CM - import from external system or use own, NQX specific)	2
NQX telemetry	• Installing Grafana and Influx DB • Providing templates for easy view of data • Configuring NQX to send data to the telemetry systems • Connecting to external SIEM system (Future step) • Deploy basic templates to monitor NQX telemetry data	2

Product Training

Standard professional services modules	Description	Typical duration (remote/onsite days)
NQX end users training (hands-on training with test environment)	• NQX introduction – Encryptor • NQX CM management tool introduction • Tasks to manage network » Create a node » Add interfaces » Create policy rules » Using PKIs and certifications » Create L2 and L3 VPN tunnels » Node software upgrades » Tools for maintenance	3
NQX CM-training for admins	• CM users and profile settings • Trust policy • CM installation • Critical system processes • Back-up and restore • Node HA configuration • CM Hot Standby configuration	2

Finland / Global Headquarters: Karvaamokuja 2b - 00380 Helsinki, Finland
Telephone: +358 20 500 7000, Email: info.fi@ssh.com, Website: www.ssh.com