Universal SSH Key Manager (UKM)

Datasheet

We are SSH, the inventors of SSH

We at SSH invented the Secure Shell protocol, which made it possible to build secure channels over unsecured networks with SSH keys, one of the most popular and ever-expanding access credentials in use. SSH keys are overwhelmingly the preferred authentication method for automation and orchestration tools, CI/CD pipelines, and access to cloud assets.

With the use of SSH keys, a new problem arised - **SSH keys don't expire, don't have identities associated with them, and can be easily shared**.

UKM exists to solve this problem.

Did you know...?

Large enterprises in finance, health care, communications, retail, transportation, or logistics businesses typically have **over 1 million SSH keys within their environment**.

Based on our analysis of customer data, **around 90% of company's SSH keys are untraced, unmanaged, or in the wrong hands**, available to users who should not have these keys or related access.

What can UKM help you with?

Supported platforms:

- HP-UX 11iv1, 11iv2, 11iv3 (PA-RISC)
- HP-UX 11iv2, 11iv3 (IA-64)
- IBM AIX 6.1, 7.1, 7.2, 7.3 (POWER)
- IBM z/OS 1.13, 2.1, 2.2
- Microsoft Windows 10, Server 2016, 2019, 2022
- Oracle Enterprise Linux 5, 6, 7, 8
- Oracle Solaris 10, 11 (x86-64, SPARC)
- Red Hat Enterprise Linux 6, 7, 8, 9 (x86-64)
- CentOS 6, 7, 8 (x86-64)
- Red Hat Enterprise Linux Atomic Host 7
- Amazon Linux 2
- SUSE Linux Enterprise 12, 15
- Ubuntu 18.04, 20.04, and 22.04

Report for full compliance

Get a comprehensive view into all SSH keys in your environment, managed or unmanaged. Gain compliance by demonstrating the real-time state of your key inventory. Generate reports whenever you need. Drill-down into every little detail if required and filter data per your needs.

Control ALL your keys

You probably have many teams located all over the world. Just like your keys. Utilize a jump gate that manages all SSH key access: access per team, key management per team, restricted access to hosts based on location, time of day, or the type of action that can be taken with a key.

Edit, enforce, and validate policies

Enjoy a single pane of glass for key configuration and policy control to reduce manual work and errors. Manage, update, and enforce security policies through central management. Remediate keys as per your company policy. If you need help with sound policies, our experts can help.

Restrict and manage key lifecycle

SSH keys never expire. Each lost, stolen, or obsolete key is a step away from you staying in control of your business. Keys can also be created outside your Privileged Access Management (PAM). Assign the best before date to your keys and catch the ones created outside your PAM.

Delete and replace keys with confidence

Are you worried about deleting an SSH key because you might disrupt a critical connection? Get the confidence to eliminate keys that are unmanaged, duplicated, past their expiration date, should no longer exist, or don't match with your current security standards.

Zero footprint, zero maintenance, Zero Trust

No need to install agents on endpoints. No need to worry about keeping them up-to-date. UKM runs independently of your infrastructure, doesn't slow down any of your day-to-day operations, and requires no maintenance.

Migration to Zero Trust access

And finally, when your organization is ready to take the next step in tightening the security of your access infrastructure, UKM migrates any existing SSH key-based access to utilize Just-In-Time (JIT) access certificates instead via our PrivX module.

SSH

Features and benefits (1/3)

Agentless and script-based discovery (SSH keys & accounts)	Gain visibility with a quick and non-invasive inventory process for SSH keys as well as different types of accounts.
SSH policies and reports	Quickly report on SSH key configurations and compliance against defined policies.
Automation and integration interface	APIs for easy integration to extend your in-place IAM infrastructure to cover all SSH key deployments. Automation tasks creation via GUI without scripting.
Real-time alerts	Improve and deepen security controls, enhance existing SIEM solutions with violation detection, and fix violations in real time.
Central management of SSH configurations	Policy control, improved situational awareness, and stronger security by using standard configurations. Reduce risk of manual errors.
User portal	Streamline workflows by extending SSH key management to end users in the organization. Allow users to request access and provision keys centrally according to policies.
Compliance support	Compliance with current requirements and planned updates to GDPR, PCI, NIST/FISMA, SOX, HIPAA, Basel III mandates.
Supported platforms for SSH Key Manager Server and SSH User Portal	Red Hat Enterprise Linux 8 and newer / Rocky Linux 8.4 and newer
Supported databases	Oracle 19c, PostgreSQL 12 and 14, Amazon Aurora PostgreSQL
High availability	• Multiple UKM servers support for high availability and scaling • Non-intrusive – no point of failure to production operations
Policy compliance and reporting	• Create policies on OpenSSH configurations, including allowed ciphers and MAC's, host keys and user key properties such as allowed trusts, shared private keys, unused keys, key restrictions and key sign-offs • Validate your SSH key environment against defined policies • Produce PDF reports on policy compliance and application remediation • Schedule automatic sending of reports via email
SSH key discovery	Public and private key discovery by size and type, passphrase existence, rogue keys, key owners and other key attributes (including location, permissions, key comment), trust relationships per host and host groups, and host keys
Transitive trust analysis	Gain visibility into transitive trust relationships that enable potentially unauthorized traversal of the server estate. Address unwanted or excessive access that may be found in the environment.

Features and benefits (2/3)

SSH key monitoring	• Detect unauthorized changes to SSH configurations, unauthorized additions, removals, and changes to user keys • Detect and track SSH key-based logins • Configurable, real-time email alerts & optimized monitoring for network directory (e.g. AD) users having keys on NFS home directories
Key enforcement	• Bring user keys under central admin control (relocation of keys to root-owned directories on host) • Create passphrase-protected keys and enforce passphrase policies • Centralized management of authorization policies • Manage key restrictions (e.g. command or allow-from restrictions)
Configuration enforcement	• Automatically restore local changes of SSH configurations to the last approved version • SSH Key Manager can be set to automatically detect and revert manual changes to SSH configurations
Automation	• Key generation, deployment, renewal, updates, and removal • Centralized SSH software configuration management • Automate processes using command line integration • Provision temporary access (keys automatically removed after expiration)
Admin authentication	• Local authentication, external accounts from Active Directory, password- and certificate-based authentication, SAML 2.0 • Maker/Checker for requiring approvals for SSH Key Manager administrator or operator-initiated key actions
Role-based administration	• Role-Based Access Control (RBAC) for SSH Key Manager admins (local and Active Directory administrator accounts) • Customizable roles to fit the tasks of individual administrators
Logging, alerts, alarms	• Comprehensive audit trails of changes to SSH keys and SSH configurations initiated by SSH Key Manager administrators as well as unauthorized changes done locally on managed hosts • Email and syslog alerts of changes to SSH keys and configurations • Alerts of suspicious key activity per host (keys removed after use) • Export and purge audit events • Track SSH logins using various authentication methods, e.g. passwords or OpenSSH certificates • Trust relationships per host and host groups • Host keys

Features and benefits (3/3)

Management methods	CLI, REST API, Web GUI (recent & stable Firefox, Chrome, Chromium-based Edge)
Management connection types	• Support for agent-based and agentless host management • Support for script-based key discovery - perform scans using existing orchestration tools (e.g. Chef, Puppet, Ansible) and import results • Management actions require agent/agentless connections
Supported key algorithms	RSA, DSA, ECC/ECDSA, Ed25519
Supported Hardware Security Modules (HSM) products	• nCipher nShield Connect HSMs • SafeNet HSM 6.2 and 6.5 • HSMs used for storing keys for agentless connections
Supported SSH versions	• Attachmate RSIT 6.1, 7.1, 8.1 • Centrify SSH 2013 • OpenSSH 4.x-9.x • SunSSH 1.1.5, 2.0 • Tectia SSH 6.4.18+ • Tectia Server for IBM z/OS 6.3+ • IBM ported tools for IBM z/OS: OpenSSH • PuTTY Client • Quest OpenSSH 4.x - 5.2