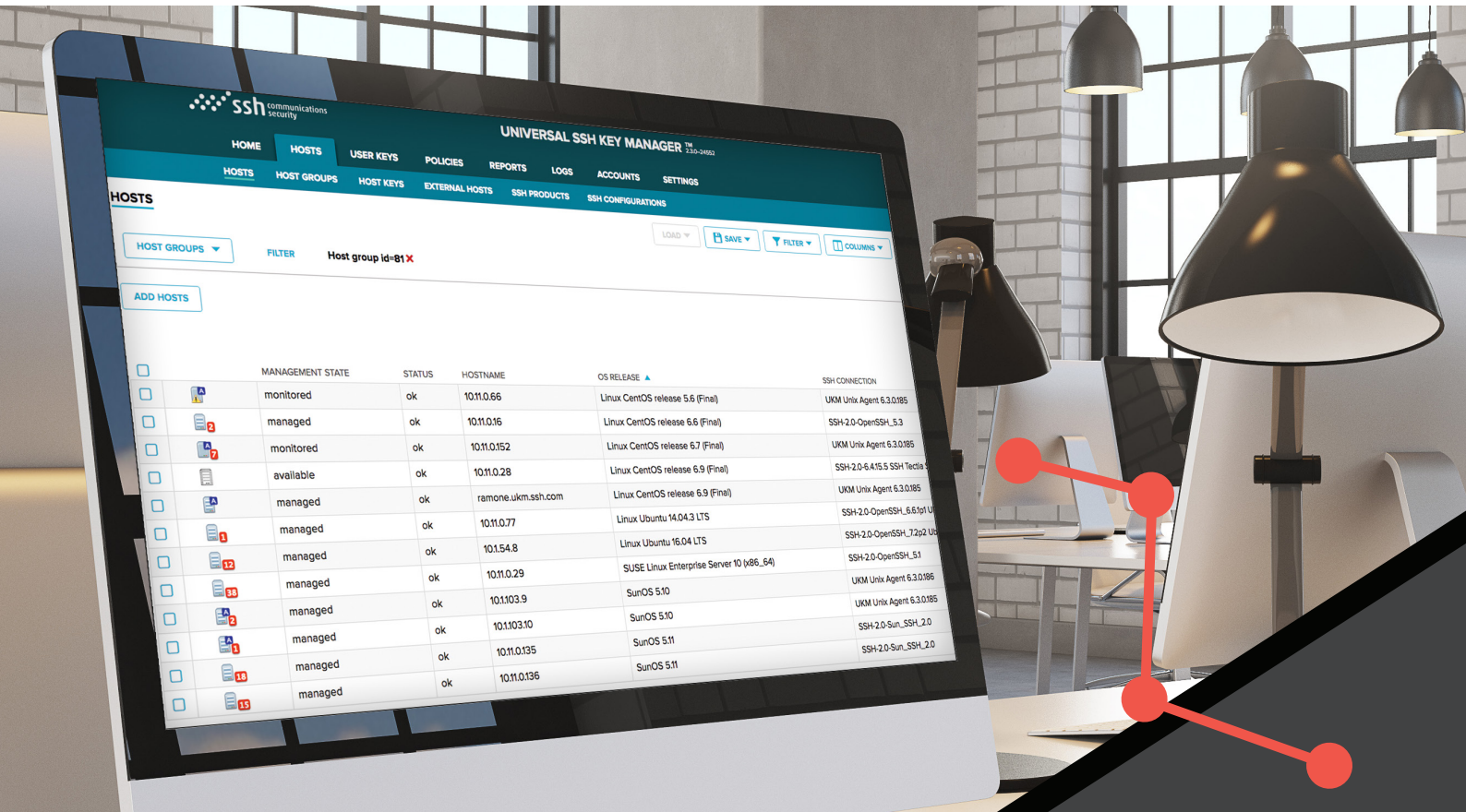
SSH.COM

Universal SSH Key Manager® Datasheet

Discover, manage & automate your entire key environment



What is Universal SSH Key Manager?

The ultimate software solution for major organizations in heavily regulated and audited industries that must have an up-to-date SSH key inventory and full key lifecycle management to pass audits, stay compliant and minimize the risk of data breach cost effectively.

Do any of these questions apply to your organization?

Are you facing an audit but are unsure about the state of your key environment?

Have you failed an audit and need help with your SSH keys to demonstrate compliance?

Do you have visibility into who has access to what server on the network?

Do you waste valuable admin time manually searching for keys and their attributes?

Can only your trusted SSH provisioning administrators control root access keys?

Can you reliably prevent backdoor access and find the keys created outside your PAM software?

Can you continuously monitor for policy violations, rogue keys, and anomalous activity?

Is your provisioning, recertification,removal, and rotation of SSH keys clumsy and decentralized?

Large enterprises in finance, health, communications, retail, transport or logistics are proven to have over

1 million SSH keys at large.

Based on our analysis, 90% of these keys are untraced, unmanaged or in the hands of people who should not have access.

We invented the Secure Shell protocol.

SSH.COM's expertise in this field is unrivalled. Universal SSH Key Manager is the culmination of years of work with Fortune 500 companies. It is unique and the only software to fully master SSH key management.

Comply with regulations. Answer audit questions instantly. See the big picture. Drill down to every detail. All in a single UI.

Millions of keys. One elegant UI.

VISUALIZE AND REPORT FOR FULL COMPLIANCE

Get a comprehensive view into all the 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 the data per your needs.

EVERY KEY UNDER YOUR CONTROL

Your teams are global and they are many. Just like your keys. Enjoy a jump gate that manages all 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 & VALIDATE POLICIES WITH A FEW CLICKS

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 KEY LIFECYCLE & MANAGE CENTRALLY

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 a best before date on your keys and catch the ones created outside your PAM.

DELETE & REPLACE KEYS WITH CONFIDENCE

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

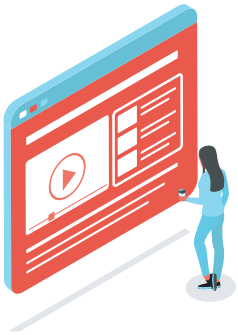
ZERO FOOTPRINT, ZERO MAINTENANCE

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

Universal SSH Key Manager Solution in three parts.

1. Analyze

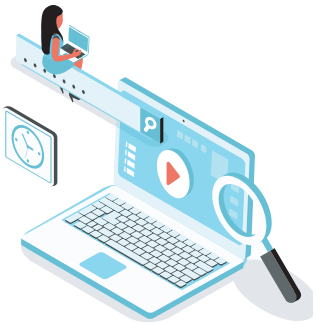
Get your risk and compliance status on the radar.



NON-INVASIVE DISCOVERY WITH MINIMAL MAN-HOURS.

2. Automate

Achieve and prove full compliance.

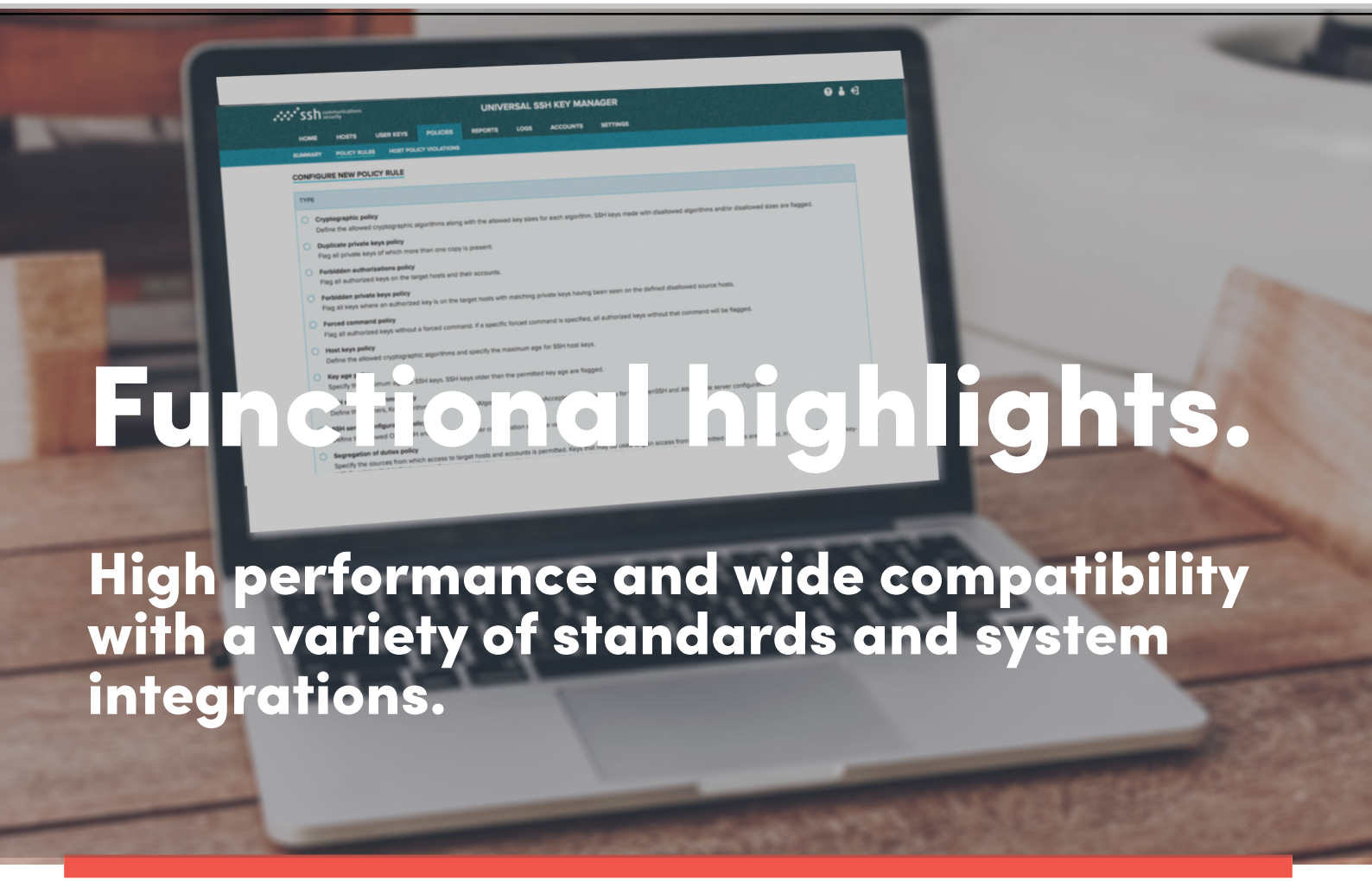


TAKE CONTROL OF UNMANAGED KEYS AND PASS YOUR AUDIT.

3. Comply

Proactively reduce risk and gain operational efficiency.

PERMANENTLY SOLVE YOUR KEY PROBLEMS AND CUT OPEX.



Functional highlights.

High performance and wide compatibility with a variety of standards and system integrations.

- Patented automatic SSH key discovery and tracking for existing authorizations, usage, configurations, and unused and policy-violating keys.
- Universal solution for open source SSH keys,Centrify, Attachmate, Bitwise etc.
- Non-intrusive deployment with no the need to install agents on endpoints.
- Centralized management via a single pane of glass for key configuration and policy control to reduce manual work and errors.
- Hardware Security Module (HSM) support.
- Easy API integration to existing ticketing systems and e.g. your IAM infrastructure.
- Policy-based reports on the compliance of your SSH configurations and key environment.
- Compliance with current requirements and planned updates to e.g. GDPR, PCI, NIST/FISMA, SOX, HIPAA and BASEL III.
- Alerts to SIEM or IPS/IDS systems for enhanced control, and rapid situational responses and violation fixes.

FEATURES AND BENEFITS	
Agentless and script-based discovery	Gain visibility with a quick and non-invasive inventory process for SSH keys.
SSH policies and reports	Quickly report 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..
Real-time alerts	Improves and deepens security controls and enhances 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. Reduced risk of manual errors.
User Portal	Streamlines 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	Enables compliance to 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	• Virtual appliance for VMWare ESX 5.5 and other hypervisors • Red Hat Enterprise Linux / CentOS 6.5 and newer
Supported Databases	Oracle 11.2, 12, PostgreSQL 9.6, 10.
High Availability	• Multiple UKM server support for high availability and scaling • Non-intrusive – no point of failure to production operations
Policy compliance and reporting	• Create policies on Open SSH 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 the SSH key environment against defined policies • Produce PDF reports on policy compliance and application remediation • Schedule automatic sending of reports by email
Discovery	• Public & private key discovery by size and type • Passphrase existence • Rogue keys • Key owner and other key attributes (including location, permissions, key comment) • Trust relationships per host & host groups • Host keys.
Monitoring	• Detects unauthorized changes to SSH configurations • Detects unauthorized additions, removals and changes to user keys • Detection and tracking of 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	• Brings user keys under central admin control (Relocate keys to root owned directories on host) • Creation of passphrase-protected keys and enforcement of passphrase policies • Centralized management of authorization policies • Managing key restrictions (such as command and allow-from restrictions)
Configuration Enforcement	• Automatically restore local changes to SSH configurations to the last approved version • Key Manager can be set to automatically detect and revert manual changes to SSH configurations per host scans.
Automation	• Key generation, deployment, renewal, update and removal • Centralized SSH software configuration management • Automate processes using command line integration • Provision temporary access (keys automatically removed after expiration)

FEATURES AND BENEFITS

Admin Authentication	• Local authentication • External accounts from Active Directory • Password and certificate based authentication • Maker/Checker for requiring approvals for Key Manager administrator or operator-initiated key actions
Role Based Administration	• RBAC for Key Manager admins (for both local & Active Directory administrator accounts) • Customizable roles to fit the tasks of individual administrators
Logging, Alerts, Alarms	• Comprehensive audit trail for changes to SSH keys and SSH configurations both initiated by Key Manager administrators as well as unauthorized changes done locally on the managed hosts • Email and syslog alerts for changes to SSH keys and configurations • Alerts of suspicious key activity per host (keys removed after use) • Exporting and purging audit events • Track SSH logins using various authentication methods such as password, and OpenSSH certificates
Management Methods	• CLI, REST API, Web GUI (Recent & stable Firefox, Chrome, Internet Explorer 10, 11)
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 Luna SA 5.4, SafeNet HSM 6.2 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 - 7.x • SunSSH 1.1.5, 2.0 • Tectia SSH 6.4 • Tectia Server for IBM z/OS 6.3, 6.4 • IBM ported tools for IBM z/OS: OpenSSH • PuTTY Client • Quest OpenSSH 4.x - 5.2 • Bitvise SSH Server 6.24, 6.45

Supported platforms for managed hosts	Agentless	Agent-based	Offline scan
HP-UX 11iv1, 11iv2, 11iv3 (PA-RISC)	o	o	o
HP-UX 11iv2, 11iv3 (IA-64)	o	o	o
IBM AIX 5.3, 6.1, 7.1 (POWER)	o	o	o
IBM z/OS 1.13, 2.1, 2.2	o		
Microsoft Windows Vista, 7, 10, Server 2003, Server 2008, Server 2008 R2, Server 2012, Server 2012 R2, Server 2016		o	o
Oracle Enterprise Linux 5 , 6, 7	o	o	o
Oracle Solaris 9, 10, 11 (SPARC)	o	o	o
Oracle Solaris 10, 11 (x86-64)	o	o	o
Red Hat Enterprise Linux 4, 5, 6, 7 (x86, x86-64)	o	o	o
CentOS 4, 5, 6, 7 (x86, x86-64)	o	o	o
Red Hat Enterprise Linux Atomic Host 7	o		
SUSE Linux Enterprise Desktop 10, 11 (x86, x86-64)	o	o	o
SUSE Linux Enterprise Server 10, 11 (x86, x86-64)	o	o	o
Ubuntu Desktop 12.04, 14.04, 16.04, 18.04 (x86, x86-64)	o		o
Ubuntu Server 12.04, 14.04, 16.04, 18.04 (x86, x86-64)	o		o

SSH Communications Security Oyj

Kornetintie 3, 00380 Helsinki

www.ssh.com

+358 20 500 7000

info.fi@ssh.com