

Identity and Access Management for Secure Shell Infrastructure

As the inventors of the Secure Shell protocol, SSH Communications Security is focused on helping IT organizations secure the path to their information assets. Our Universal SSH Key Manager is a multiplatform, scalable solution that brings compliance and control to Secure Shell environments. Universal SSH Key Manager reduces risk of unauthorized access from both internal and external actors, solves thorny compliance issues and reduces costs.

The Problem

The vast majority of large enterprises rely on Secure Shell (SSH) to provide secure authentication and confidentiality (encryption) for many business critical functions such as automated backups, day to day file transfers and interactive user access for systems administration. Many mission critical IT functions are enabled through SSH. However, most enterprises use manual processes for generating, configuring and deploying the SSH public and private keys that enable these functions.

Over time, this results in the uncontrolled proliferation of authentication keys. Security managers lose visibility and control over who has access to what servers and whether access rights previously granted should be revoked. It becomes nearly impossible to map the trust relationships between individual users, system accounts and application IDs with their respective destination servers.

Standard identity and access management solutions that govern end user access typically do not encompass SSH key based access to systems and accounts. Lack of governance and control is exposing enterprises to elevated risk, compliance failures and the excess overhead of manual processes.

The Challenge

Traditional approaches to managing SSH user keys are time consuming and expensive, and there is little if any automation or auditability. Because so many business critical functions - many of them automated - rely on SSH, it is very difficult to bring SSH Key management under control without disrupting those functions. The problem is highlighted when there is need to revoke access when there are organizational changes, employee departures, mergers and acquisitions.

Enterprises generate significant overhead in the day to day activity of SSH user key setups, have increased risk from the lack of key renewals and removals, and face pressure from compliance initiatives.

Automated Access Control



Return on Security Investment

Lower Costs: Eliminate inefficient and error prone manual administration processes.

Reduce Risk: Protect against catastrophic loss - gain control and visibility over all privileged access.

Gain Compliance: A centralized, auditable solution ensures compliance to mandates.

A non-disruptive solution is needed to eliminate inefficient and error prone manual processes, dramatically reduce risk and address compliance exposures. Finally, processes and controls are needed to take care of the issues now and ensure they don't re-emerge in the future.

The Solution

SSH Communications Security's Universal SSH Key Manager (UKM) is an enterprise grade SSH user key management solution. UKM takes a non-disruptive approach that enables enterprises to gain and retain control of the SSH infrastructure without interfering with production systems. No need to rip and replace how users get their work done or change the hundreds of automated processes that are the lifeblood of ongoing business. UKM's non-disruptive approach is based on three principles:

Discover: Discover all SSH keys, map trust relationships and identify policy violations.

Remediate: Remove keys that should be revoked and bring valid keys under correct policy compliance.

Manage: Eliminate manual processes, centralize control, enforce compliance, audit all activity.

UKM on average saves a typical Fortune 1000 organization \$1 to \$3 million per year in overhead costs while reducing the risk of serious security breach and resolving open compliance issues. Whether your environment uses OpenSSH, Tectia, or other common SSH implementations, UKM brings this complex problem under control.

Discover	Remediate	Manage
<ul style="list-style-type: none"> • Take inventory of SSH keys • Map trust relationships • Track key activity • Identify unused/unneded keys • Identify unneded authorizations 	<ul style="list-style-type: none"> • Remove unused keys • Relocate keys to root owned directories • Update authorizations • Renew old, non-compliant keys • Centralize control 	<ul style="list-style-type: none"> • Connect authorization process to existing ticketing systems • Centrally manage and enforce SSH configurations • Automate key removal • Detect and alert on policy violations

Features	Benefits
Agentless discovery	Non-disruptive deployment
Support for multiple management instances	High scale, high availability
Multiplatform support – Unix, Linux, Windows, IBM z/OS	Deployable in vast majority of enterprises
Automation interface	Link to existing IAM infrastructure
Automated key creation, update, removal	Lower costs, fewer errors, faster turnaround
Central management and enforcement of SSH client and server configurations	Policy control, stronger security, fewer errors
Real time alerts	Fix violations in real time
Audit trail	Easier compliance reporting
Compliance support	Enables compliance to current requirements and planned updates to PCI, NIST/FISMA, SOX, HIPAA, Basel III mandates

Universal SSH Key Manager Technical Specifications

Supported Platforms for SSH Key Manager Server	<ul style="list-style-type: none">• CentOS 6.5 or later (x86--64)• Red Hat Enterprise Linux 6.5 or later (x86--64)• SUSE Linux Enterprise Server 11 sp2 (x86--64)
Supported Databases	<ul style="list-style-type: none">• Oracle 11.2• PostgreSQL 9.2
High Availability	<ul style="list-style-type: none">• Multiple UKM server support for high availability and scaling• Non-intrusive – no point of failure to production operations
Discovery	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Detects unauthorized changes to SSH configurations• Detects unauthorized adds, deletes, changes to user keys• Detection and tracking of SSH key-based logins• Configurable, real-time email alerts
Key Enforcement	<ul style="list-style-type: none">• Brings user keys under central admin control (Relocate keys to root owned directories on host)• Centralized management of authorization policies• Managing key restrictions (such as command and allow-from restrictions)
Automation	<ul style="list-style-type: none">• Key generation, deployment, renewal, update and removal• Centralized SSH software configuration management• Automate processes using command line integration
Admin Authentication	<ul style="list-style-type: none">• Local authentication• External accounts from Active Directory• Password and certificate based authentication
Role Based Administration	<ul style="list-style-type: none">• RBAC for Key Manager admins (for both local & Active Directory administrator accounts)• Customizable roles to fit the tasks of individual administrators
Logging, Alerts, Alarms	<ul style="list-style-type: none">• 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)
Management Methods	<ul style="list-style-type: none">• Web GUI<ul style="list-style-type: none">- Recent & stable Firefox- Recent & stable Chrome- Internet Explorer 8, 9, 10 & 11• CLI
Management Connection Types	<ul style="list-style-type: none">• Support for agent-based and agentless host management
Supported Key Algorithms	<ul style="list-style-type: none">• ECC/ECDSA• Ed25519• DSA• RSA
Supported SSH versions	<ul style="list-style-type: none">• Attachmate RSIT 6.1, 7.1, 8.1• Centrifly SSH 2013• OpenSSH 4.0 or newer• SunSSH 1.1 or newer• Tectia SSH 6.0 or newer• Tectia Server for IBM z/OS 6.3, 6.4• Quest OpenSSH 5.2

Supported Platforms for Managed Hosts	Platform	Agentless	Agent-Based
	HP-UX 11iv1, 11iv2, 11iv3 (PA-RISC)	•	•
	HP-UX 11iv2, 11iv3 (IA-64)	•	•
	IBM AIX 5.3, 6.1, 7.1 (POWER)	•	•
	IBM z/OS 1.12	•	
	Microsoft Windows XP, Vista, 7		•
	Microsoft Windows Server 2003, Server 2008, Server 2008 R2		•
	Oracle Enterprise Linux 5	•	•
	Oracle Solaris 9, 10, 11 (SPARC)	•	•
	Oracle Solaris 10, 11 (x86-64)	•	•
	Red Hat Enterprise Linux 4, 5, 6 (x86, x86-64)	•	•
	SUSE Linux Enterprise Desktop 10, 11 (x86, x86-64)	•	•
	SUSE Linux Enterprise Server 10, 11 (x86, x86-64)	•	•
	Ubuntu Desktop 12.04 (x86, x86-64)	•	
	Ubuntu Server 12.04 (x86, x86-64)	•	

Universal SSH Key Manager Architecture

