Universal SSH Key Manager®

Centralize, Simplify, and Automate SSH Key Management

Secure Shell (SSH) technology reliably provides critical data authentication and security for much of the business world. Daily activities such as file transfers, backups, and user access depend on it to keep workflow humming. System administrators and security managers depend on it to minimize risk.

However, the public and private authentication keys that allow access to that data can proliferate over time. Employees, contractors, and even vendors are not only granted access, they also may be able to generate keys.

It becomes impossible to track who has access to which systems, or if access should be modified or terminated. Left unattended, no one knows how many keys were created according to policies, if they are currently being used, or if their connections to outside systems are trustworthy.

A large company may have hundreds or even thousands of active or unused keys, leaving the door ajar to unauthorized entry to business systems.

Universal SSH Key Manager from SDS is a business-wide key administration system that can solve those problems. UKM is a comprehensive runtime solution that automatically traces and authenticates keys without disrupting operations.

A typical Fortune 1000 company may realize an average of $1 to $3 million in savings on overhead costs per year by employing UKM to automate processes and standardize authorization.

If your business uses OpenSSH, Tectia, or another SSH implementation, UKM provides the control you need for today's security challenges.

UKM reduces the risk of a serious security breach by finding, authorizing, and even eliminating access keys.

Identity and Access Management for Secure Shell Infrastructure

Universal SSH Key Manager (UKM) from SDS gains and retains control of SSH user keys without interrupting critical business systems or impeding workflow.

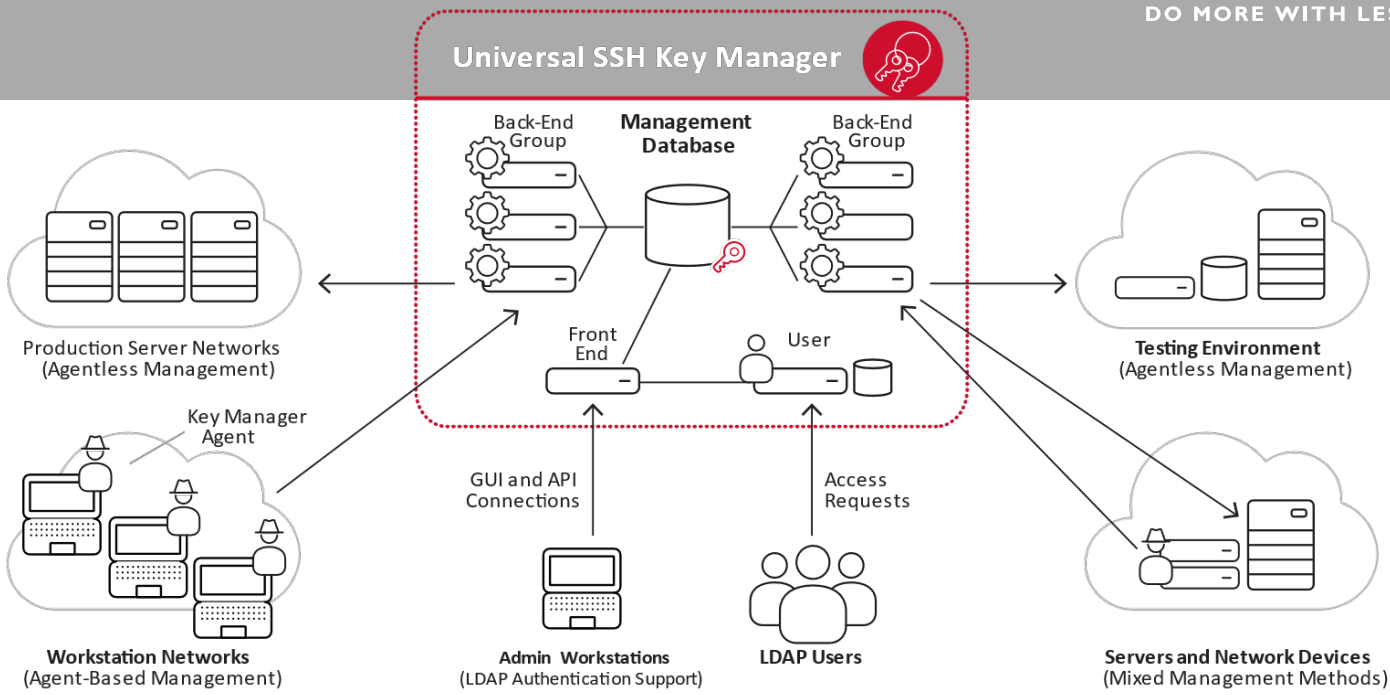
- Finds and tracks existing keys
- Verifies trusted connections
- Renews authorizations
- Removes inactive keys

No changes to vital processes.
No guessing about compliance.
And UKM cuts costs along the way.

UKM is the solution for any size business that is concerned about managing and safeguarding access to the Secure Shell environment.

DATASHEET

SDS
DO MORE WITH LESS



FINDS

- Performs an inventory of existing SSH keys
- Maps trust relationships to outside systems
- Identifies unused or unneeded keys
- Identifies unneeded authorizations

TRACKS

- Traces when and where keys are used
- Alerts when keys are added, removed, or modified
- Alerts when unauthorized changes are made to SSH configurations

RECONCILES

- Removes unused keys
- Relocates keys to root-owned directories
- Updates authorizations
- Renews old, non-compliant keys
- Centralizes oversight

CONTROLS

- Connects authorization process to existing ticketing systems
- Centrally manages and enforces SSH configurations
- Automates key removal
- Detects and alerts on policy violations

Most businesses consider dealing with SSH keys a difficult function. There's no ownership of the process, nobody really knows all of the procedures, and the management systems are fragmented or inefficient.①

UKM resolves those issues, centralizing oversight of the SSH environment and automating processes to minimize operator involvement.

With the optional UKM user portal, key renewal and authorization can even be delegated to the users and key owners while maintaining security policies and providing an audit trail.

About SDS

Founded in 1982, SDS supports over 25 products for z/OS, MVS, VSE, VM, AIX, Linux, and Windows. SDS has licensed more than 1,000 enterprise clients worldwide with quality mainframe software and offers award-winning technical support. Comprehensive solutions focus on security, encryption, data compression, and network monitoring. To learn more, please visit our web site.

① Global Encryption Trends Study, Ponemon Institute© LLC, February 2016.