

SSH key management and automation

Solution Brief



Security and convenience do not generally go hand in hand. Passwords control access to operating systems, applications, servers, and clouds, but they are largely complex and inefficient. This has led to the creation of password less authentication mechanisms, such as SSH, to enable seamless communication between devices and applications.

Beyond its use as an identification tool, SSH can also move data securely between two endpoints. But this can be a problem if SSH keys fall into the wrong hands because it can open permanent backdoors to sensitive organizational data. Most enterprises do not have a well-documented process for creating, managing, sharing, and removing keys in their infrastructure. Any number of keys can be created and deployed at will, and without a way to track or remove them, they can become a significant security vulnerability. Enterprises with poorly managed keys are not only at risk from breaches but also from becoming non-compliant with mandatory regulations. This makes it necessary for enterprises to secure their SSH keys using advanced tools that can mitigate risks arising from such vulnerabilities.

SSH Key Lifecycle Management and Automation

SSH keys are more secure than passwords. To ensure that it remains that way, the lifecycle of these keys must be efficiently managed. With AppViewX, you can manage and automate your SSH key's lifecycle.

- Create, deploy, rotate, share and delete SSH keys using a single solution
- Terminate outdated keys periodically through automated key rotation
- Create key groups based on their functionality for easier management and policy enforcement

Key	Host	Policy
UbuSvr14_D3_Key9	Default...	RSA
UbuSvr14_D3_Key1	Default...	ECDSA
UbuSvr14_D3_Key2	Default...	RSA
UbuSvr14_D3_Key3	Default...	RSA
RHEL73Server1_D3_Key9	Default...	RSA
RHEL73Server1_D3_Key2	Default...	DSA
RHEL73Server1_D3_Key8	Default...	DSA
RHEL73Server1_D3_Key4	Default...	ECDSA
RHEL73Server1_D3_Key5	Default...	ECDSA
RHEL73Server1_D3_Key6	Default...	DSA
RHEL73Server1_D3_Key7	Default...	DSA
RHEL73Server1_D3_Key8	Default...	RSA
RHEL73Server1_D3_Key1	Default...	DSA
SSHServer4F5SP_D3_Key1	Default...	RSA
SSHServer4F5SP_D3_Key2	Default...	RSA
SSHServer4F5SP_D3_Key3	Default...	RSA
SSHServer4F5SP_D3_Key4	Default...	RSA

Access Control and Policy Management

Multiple teams require access to applications and devices on demand. Managing these sessions manually lacks the necessary auditing and accountability. Role-based access for teams can enable efficient provisioning, ensure policy administration, and help ensure compliance with international standards.

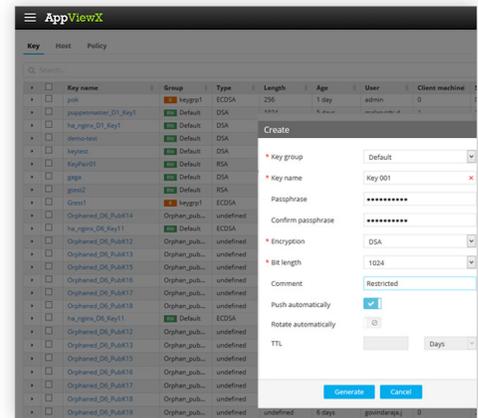
- Provide granular access to hosts and keys to regulate privileged access to important accounts
- Create audit trails for each activity and ensure that every important activity follows an established workflow
- Set policies to ensure that keys are generated using enterprise-defined encryption algorithms and are shared to only authorized users

Time	User	Device name	Log message
08/28/2017 03:58:20 PM	ec2-user		Connector connector sshuff is added to the SSH key sshuff
08/28/2017 03:58:20 PM	ec2-user		Server device null added to the connector sshuff for the SSH
08/28/2017 03:58:19 PM	ec2-user		Connector connector sshuff is added to the SSH key sshuff
08/28/2017 03:58:19 PM	ec2-user		Server device null added to the connector sshuff for the SSH
08/28/2017 03:58:40 PM	user2	192.168.112.205	SSH key push "sshuff" for device 192.168.112.205 for user use
08/28/2017 03:58:40 PM	senoah.k	172.16.28.127	SSH key push "sshuff" for device 172.16.28.127 for user seno
08/28/2017 03:58:30 PM	mohafuzul.a	fdfdfff	SSH key "sshuff" has been successfully pushed to fdfdfff for th
08/28/2017 03:58:18 PM	ec2-user	172.16.28.127	WID initiated: SSH key push request with workbook 8143 WID
08/28/2017 03:58:16 PM	ec2-user	192.168.112.205	WID initiated: SSH key push request with workbook 8147 WID
08/28/2017 03:58:11 PM	ec2-user	fdfdfff	WID initiated: SSH key push request with workbook 8142 WID
08/28/2017 03:58:11 PM	senoah.k	172.16.28.127	SSH key push "sshuff" for device 172.16.28.127 for user seno
08/28/2017 03:58:10 PM	user2	192.168.112.205	SSH key push "sshuff" for device 192.168.112.205 for user use
08/28/2017 03:58:02 PM	ec2-user	192.168.112.205	Server device 192.168.112.205 added to the connector sshuff
08/28/2017 03:58:05 PM	ec2-user		Connector connector sshuff is added to the SSH key sshuff
08/28/2017 03:58:05 PM	ec2-user		Server device null added to the connector sshuff for the
08/28/2017 03:58:05 PM	ec2-user		Connector connector sshuff is added to the SSH key sshuff
08/28/2017 03:58:05 PM	ec2-user		Server device null added to the connector sshuff for the
08/28/2017 03:58:05 PM	ec2-user		Connector connector sshuff is added to the SSH key sshuff
08/28/2017 03:58:05 PM	ec2-user		Server device pg3444 added to the connector sshuff for th
08/28/2017 03:58:05 PM	ec2-user		Connector connector sshuff is added to the SSH key sshuff
08/28/2017 03:58:05 PM	ec2-user		Server device null added to the connector sshuff for the
08/28/2017 03:58:05 PM	ec2-user		Connector connector sshuff is added to the SSH key sshuff
08/28/2017 03:58:05 PM	ec2-user		Server device 172.16.28.127 added to the connector sshuff
08/28/2017 03:58:05 PM	ec2-user		Connector connector sshuff is added to the SSH key sshuff
08/28/2017 03:58:05 PM	ec2-user		Server device fdfdfff added to the connector sshuff for the

Private Key Management

Private keys are the backbone of your SSH network. These cryptographic keys must be industry-standard and protected against unauthorized users. AppViewX can help you ensure that your private keys remain private.

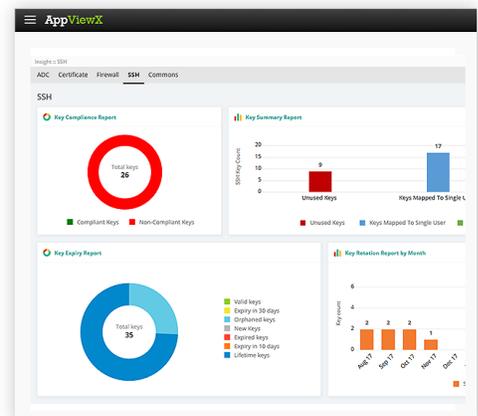
- Generate keys with advanced encryption techniques and bit lengths
- Secure private keys in an AES-256 encrypted environment
- Download private keys with passphrase protection to manually push keys to hosts



Comprehensive Visibility

A lot of SSH keys in an environment are unaccounted for because anyone can create an SSH key pair, push it to a device, and eventually forget about it. With AppViewX, you can gain visibility into your rogue and unused keys before they compromise your sensitive data.

- Discover keys in your environment through different modes, such as IP, subnet, and managed devices, and build an inventory automatically
- Gain a holistic view of SSH keys and their respective host connections with intuitive single-click actions for key management and automation



About AppViewX

AppViewX is a global leader in the management, automation and orchestration of network services in brownfield and greenfield data centers. The AppViewX Platform helps network operations (NetOps) adapt to technology and process demands, such as agile, DevOps, IoT, cloud, and software-defined infrastructure. AppViewX delivers greater business agility and efficiency at a lower cost. For more information, visit www.appviewx.com.

AppViewX, Inc.

500 Yale Avenue North, Suite 100, Seattle, WA 98109

✉ info@appviewx.com

🌐 www.appviewx.com

📞 +1 (206) 207-7541

📞 +44 (0) 203-514-2226