appviewx

SSH+ Guides

Version: 2023.1.0 FP1

Copyright AppViewX, Inc.

Trademarks

External Reference Links

This product includes software developed by the CentOS Project (www.centos.org).

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
2.0	Initial Release of AppViewX_v2023.1.0 FP1 SSH+.	Nov 2023
1.0	Initial Release of AppViewX_v2023.1.0 SSH+.	Sep 2023

About the Documentation

This guide talks about the complete functionality of the AppViewX SSH Key and Host Management solution. With the help of this guide, you can manage:

- SSH Key and Host Group
- Access Group
- Policy
- Request Access
- Devices
- Mapping of a host as a Client Machine

Audience

This guide is intended for CISO, PKI Security, and Application Teams.

All the people belonging to the groups mentioned below should use this guide.

IT Operations	CISO, CIO, CTO, Server & Application Administration
Security	IAM Administration
Risk Management	Risk, Compliance, Audit Administration

Text Conventions

The following text conventions are used in this document:

Convention	Description
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in the text or the glossary.

Convention	Description
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates commands with a paragraph, URLs, codes in examples, text that appears on the screen, or text that you enter.

Chapter 1: SSH+ Administrator Guide

Introduction to SSH+

As application infrastructures grow, so do security threats. Organizations have to find newer ways for protecting their data and granting access to the right users and devices to avoid security threats and breaches. While traditional approach used password authentication, it proved to be insecure. This is where AppViewX SSH+ comes into play.

AppViewX SSH+ is a fully-automated application infra-access management and SSH key lifecycle management solution that allows you to centrally discover, manage, and protect SSH keys with access across hybrid multi-cloud environments. It also helps simplify access management, stay compliant and mitigate risks with SSH+.

AppViewX offers visibility and SSH access management across traditional on-premises data centers and cloud-hosted infrastructures.

Risks of improper SSH Management

Since there is no governing body to regulate the use of SSH keys, there is an element of risk involved. As SSH keys are generated on need basis, several keys may be discarded and left unmanaged when they are no longer of use. Without an inventory, managing these keys and revoking their access pose a security threat to large organizations for potential back-door entry into the network, data theft, or breaches.

Improper SSH key management can lead to unauthorized access, compliance violations, identity and access management issues, data breaches, operational disruption, and reputation damage. To mitigate these risks, organizations should implement proper SSH key management practices, including secure key storage, regular key rotation, and access controls.

What Enterprises Need

AppViewX conducted multiple surveys to identify the core features and functionality needed to address SSH management challenges. SSH and Identity and Access Management (IAM) Administrators highlighted the following requirements:

- Discover keys from standard and non-standard locations
- Identify and report non-standard and non-compliant keys
- Holistic visibility of keys and the users of these keys
- Revoke access to non-compliant and non-standard keys
- Automated rotation and distribution of keys
- Self-service SSH access requests
- Support for cloud and legacy on-premise infrastructure
- Centralized SSH Certificate Authority

How AppViewX Can Help

AppViewX SSH+ key lifecycle management is a fully automated solution that discovers and manages enterprise SSH infrastructure. It can identify and mitigate risks associated with poorly managed passwordless access management.

AppViewX SSH+ features include:

- **Centralized Discovery and Visibility**
  - The solution offers periodic or on-demand scans to discover SSH keys across multi-vendor, hybrid network infrastructures, and map trust relationships to determine access privileges.
  - The consolidated inventory provides a central console to view and manage all SSH keys and hosts.
- **Risk Scorecard and One-Click Remediation**
  - The solution proactively identifies and remediates risks associated with inactive, weak, or suspicious keys using an intuitive SSH scorecard dashboard.
  - The one-click remediation feature enables instant deletion or regeneration of keys.

System Requirements

SSH within the Application Infrastructure

Application infrastructure refers to all the components required to deliver an application and its functions and services to the customer. Although each application is unique, certain common components can be identified that are typically implemented to support application capabilities and service delivery.

Some of the most common components of a typical application infrastructure include:

- **Web server:** Apache, IBM HTTPD, WebSphere, WebLogic, Tomcat, Node.js
- **Application server:** WebSphere, IBM DataPower, WebLogic App server, Iplanet, etc.
- **Database/file storage:** Any on-premise or cloud database or NoSQL document storage
- **Firewalls/NGFW:** Fortinet, Cisco, Checkpoint, F5, etc.
- **Intrusion Detection System (IDS):** Fortinet, Cisco, Checkpoint, F5, etc.

Modern application infrastructure leverages multiple hosting platforms such as on-premise data centers, private clouds, and public clouds offered by third-party hosting providers.

The application infrastructure components communicate with each other to enable service delivery. This can leverage SSH communication. Additionally, administrators of these application infrastructures will need to SSH into these hosts to perform maintenance.

Additionally, security and audit compliance requirements necessitate constant awareness of who has access to what and the maintenance of best security practices for the communications.

Hardware

Ensure that you have, at minimum, the following hardware with the given specifications before proceeding with the installation:

- **Single Node Deployment Requirements**

Node	Bare Minimum		
	CPU	RAM	Hard Disk Space
Single node	8	32GB	500GB

- **Multi-Node Deployment Requirements**

Node	Bare Minimum		
	CPU	RAM	Hard Disk Space
Multi-node (master node)	4	4GB	100GB

Node	Bare Minimum		
	CPU	RAM	Hard Disk Space
Note: One node for a single master installation and a minimum of three nodes for multi-master installation.			
Multi-node (worker node)	8	32GB	500GB

- **Platform Bare Minimum Requirements**

Supported Virtualization Platforms	Versions	vCPU	RAM	HDD
VM Server, VMware ESXi	5.5 or later	8v	32GB	1TB

Operating System

Both single node and multi-node installations of AppViewX are supported on the following operating systems:

- RHEL 8.5
- RHEL 8.6
- RHEL 8.7
- Ubuntu 20.04

Browser

Following is the browser requirements to use the AppViewX SSH+ node:

Browser	Version
Firefox	v74.0.1 (64-bit) or later
Google Chrome	v85.0.4183.83 (64-bit) or later

Installation Instructions

- On-Premise Installation Instructions
- SaaS Installation Instructions

On-Premise Installation Instructions

This chapter provides the step-by-step instruction for on-premise deployment.

Table - Sequence of Installation Steps

Step No	Step Name	Mandatory
1	Working with Prerequisites	Yes
2	Configuring Firewall	Yes
3	Configuring Elevated Access	Yes
4	Running the Prerequisite Tool	Yes
5	Deploying the AppViewX Virtual Appliance	No
6	Performing a Single Node or Standalone Installation	No
7	Performing a Multi-node or High Availability Installation	No
8	Configuring the appviewx.conf file	Yes
9	Configuring POD and Service IP CIDR	No
10	Verifying the Installation	Yes
11	Activating SSH	Yes
12	Accessing the AppViewX Graphical User Interface	Yes
13	Adding Third-party Libraries	No

- Activating SSH+
- Uninstalling AppViewX
- Troubleshooting
- Migrating CentOS to Ubuntu/RHEL

Activating SSH+

License Management Software tracks software installed throughout the enterprise and ensures legal licenses for its usage. The software helps you to obtain the license key, upload the license key, and

troubleshoot the license issues. License management is an essential element of software asset management (SAM).

To access the application for SSH+, send an email to help@appviewx.com with the hostname of the node in which the application is installed.

Uninstalling AppViewX

Users can uninstall AppViewX when they want to migrate into another environment. They can also uninstall AppViewX when it is no longer required.

To uninstall an application package safely:

1. Open the terminal window.
2. To navigate to the **appviewx_kubernetes** directory, execute the following command:

   ```
   cd /home/appviewx/appviewx_kuberbetes/scripts/uninstall
   ```
3. To start the uninstallation process, execute the following command:

   ```
   /uninstall.sh
   ```
4. Enter the node's credentials when prompted.
5. Reboot all the nodes after completion of the AppViewX uninstallation.

Troubleshooting

Whenever the AppViewX installation fails, you will get an error stating that some script execution failed.

- **Pre requisites not met**

  Please check for all the items below.

  - port not opened
  - insufficient disk/CPU
  - time not in sync
  - packages not found
  - hostname incorrect in configuration
- **Error while installing the docker**

  If a customer brings in a custom OS, the Linux packages that AppViewX includes with the installer may not be compatible with the OS. In such situations, you may need to install the appropriate package to continue. This can be observed from the log messages that indicate an error while installing a package.

- **Error while installing the docker**

  Occasionally, we have observed intermittent errors from the OS during the installation of Docker. If you encounter an error at this stage, please attempt to uninstall the application, reboot all nodes, and then proceed with the installation.

- **Docker gets uninstalled from the CAGateway**

  Root cause: Although we removed the "uninstall docker" commands from our scripts, we discovered that Docker relies on containerd, which is used as a runtime in the product. The scripts also include steps to remove containerd in the install, uninstall, and upgrade scripts, which cannot be avoided. This ultimately results in the removal of Docker as well. Additionally, the containerd version used in the product conflicts with the pre-existing containerd version of Docker on the server.

  Docker and the AppViewX application cannot co-exist in the same server as it is tightly coupled with containerd. The manually installed docker will be removed during every maintenance activity such as install, uninstall and infra upgrade.

- **Context deadline exceeded in consul after the FP3 patching process**

  For setups with high network latency or slow I/O, after the FP3 patch process, the consul may be stuck in 1/2 stage, causing the vault to go in a crash loop back. If you encounter this, check the consul logs using the command

  ```
  kubectl logs consul-consul-server-0 -n avx
  ```

  If the logs specify “context deadline exceeded,” then increase the timeout in consul by the following steps:

  1. Navigate to <installer location>/appviewx_kubernetes/yaml/appviewx_vaut/consul/chart/vaules.yaml
  2. Edit **consulAPITimeout: 5s** (old value) to **consulAPITimeout: 10s** (new value)
  3. Save the changes.

  Note: Increase this timeout only based on the latency.

- **Error while initializing the kube master/worker**

  In certain cases, when uninstallation does not clean up the data properly, we may observer errors while initializing kube master and worker. In such cases, perform an uninstall, reboot all the nodes and then go ahead with the install. Additionally, there are cases where the installation fails due to port connectivity issues. If a failure occurs in this stage, check if ports 6443, 10250, 2379 and 2380 are opened properly.

- **Error while initializing the mongodb chart**

  This specific error occurs after a timeout of 5 minutes to initialize the mongodb charts. This error occurs when the pods are not able to communicate between themselves. Use the following commands to verify that:

  ```
  kubectl describe statefulset -n avx mongo-shareddb
  ```

  For any connectivity issues, the output of this command will display the specific error stating connection timed out.
- **Node is enabled with IPv6 but the application is not.**

  Verify the output of the command:

  ```
  ifconfig | grep -i inet6
  ```

  If an IPv6 address is displayed, it is necessary to enable IPv6 in the appviewx.conf file. Failure to do so may result in communication issues.
- **IP in IP tunnelling is not enabled**

  If the IP in IP traffic is disabled, which means that the IPv4 protocol is not permitted, we will encounter the same problem. The prerequisite check script does not identify this, so we need to verify it separately to confirm.
- **Error while installing the AppViewX plugins**

  If an error occurs during the installation of AppViewX plugins, it is likely due to an error in the configuration file. You may observe and error such as `Upload failed: scp`, in such cases re-trigger plugins_install.sh to install the plugins. Likewise, ensure to review the configuration file carefully and proceed with the execution of plugins_install.sh to install only the plugins.

Migrating CentOS to Ubuntu/RHEL

For detailed instructions, refer to Migrating CentOS to Ubuntu/RHEL.

SaaS Installation Instructions

For detailed instructions, refer to AppViewX SaaS Setup Guides.

- AppViewX Software as a Service
- AppViewX SaaS Onboarding and Getting Started Guide
- Features of the AppViewX Cloud Connector
- System Requirements
- Setting Up the AppViewX Cloud Connector

- Prerequisites for Managing ADC Devices
- Installing the AppViewX Windows Gateway
- Troubleshooting the AppViewX Cloud Connector
- Managing the AppViewX Cloud Connector

AppViewX Software as a Service

For more information, refer to AppViewX Software as a Service and SaaS Architecture Guide.

AppViewX SaaS Onboarding and Getting Started Guide

For more information, refer to AppViewX SaaS Onboarding and Getting Started Guide.

Features of the AppViewX Cloud Connector

For more information, refer to Features of the AppViewX Cloud Connector.

System Requirements

For more information, refer to System Requirements for Setting up the AppViewX Cloud Connector.

Setting Up the AppViewX Cloud Connector

- **Methods to Set up the AppViewX Cloud Connector:** For more details, click here.
- **Setting up the AppViewX Cloud Connector via a Virtual Image:** For more details, click here.

Sequencing of Steps

Step No.	Step Name	Mandatory
1	Deploying the AppViewX OVA	Yes
2	Accessing the Setup Interface	Yes
3	Configuring Basic Cloud Connector Settings	Yes
4	Executing the Prerequisite Check Script	No
5	Assigning a Data Center	Yes
6	Configuring Advanced Cloud Connector Settings	Yes
7	Downloading the License File	Yes

Step No.	Step Name	Mandatory
8	Installing AppViewX Cloud Connector	Yes
9	Reviewing the Installation	Yes

- **Setting up the AppViewX Cloud Connector via the Native OS:** For more details, click here.
- Installing the AppViewX Cloud Connector

Installing the AppViewX Cloud Connector

Note: The following steps assume that:

- All system prerequisites are fulfilled by the host machine.
- The AppViewX Cloud Connector installer (downloaded in the above step) is securely copied via SCP/SFTP to the host machine where the AppViewX Cloud Connector is to be installed.

1. To extract the installer, from the downloaded package, extract the tar.gz file using the command given below: `tar -zxvf <filename>.tar.gz`
   For example: `tar - zxvf pesrv07-test-94-99-appviewx-appviewx-net-cloud-connector.tar.gz`
2. On the node where the AppViewX Cloud Connector agent will be installed, from the extracted installation package, run the **./install.sh** script.
   The script will check if the installation prerequisites for the AppViewX Cloud Connector have been fulfilled.

   Note:
   Ensure that the license file is placed in the same location as the **install.sh** script. If the license file is placed in another location, run the install.sh script using the following command:

   ```
   ./install.sh <complete path of the license file with the filename>
   ```

   On successful verification of the prerequisites, you will be prompted to specify if you want to manage f5 BIG-IP devices and if you need auto-enrollment of the certificates.
3. Enter the required input value:

Important: If you choose to **not enable** any of the following features, you will have to reinstall the AppViewX Cloud Connector to enable them later.

a. If you want manage f5 BIG-IP devices, enter **y**/**n** for yes/no, respectively.

b. If you need auto-enrollment of the certificate using one of the following supported auto-enrollment protocols, enter **y**/**n** for yes/no, respectively.
   - If you choose **y** (yes) here, enter the required protocol(s) name. SSH server is installed.
   - If you choose **n**(no), you will see this prompt:

     Do you want to enable SSH Terminal Server for using SSH terminal usecase (y/n)?

     If you choose y, SSH server is installed.

c. If you want to enable Syslog receiver for a near-real time configuration updates from the devices, enter **y**/**n** for yes/no, respectively. For configuring Syslog reception, refer to Platform User guide section, Syslog Reception.

   In case you have an older version of AppViewX on cloud and want to make use of Syslog capabilities for ADC, you must manually activate the Syslog flag by setting SYSLOG_ENABLED=true in the path ccpath/deps/properties.

4. Enter the sudo password.
   After the relevant details have been entered, the installation proceeds. Installation logs, according to the outcome of the installation, are displayed.

   Given below are sample installation logs:

```
Loaded image: rancher/k3s:v1.23.3-k3s1
Loaded image: rancher/k3d-tools:5.2.2
Loaded image: rancher/mirrored-pause:3.6
[36mINFO[0m[0000] [SimpleConfig] Hostnetwork selected - disabling injection of docker host into the
 cluster, server load balancer and setting the api port to the k3s default
[33mWARN[0m[0000] No node filter specified
[33mWARN[0m[0000] No node filter specified
[33mWARN[0m[0000] No node filter specified
[36mINFO[0m[0000] Prep: Network
[36mINFO[0m[0000] Re-using existing network
 'host' (8bebb4ae61001f74487d0aa6b315396405d0127c938da1206614d113295ae139)
[36mINFO[0m[0000] Created volume 'k3d-cc-images'
```

```
[36mINFO[0m[0000] Starting new tools node...
[36mINFO[0m[0000] Starting Node 'k3d-cc-tools'
[36mINFO[0m[0001] Creating node 'k3d-cc-server-0'
[36mINFO[0m[0001] Using the k3d-tools node to gather environment information
[36mINFO[0m[0001] Starting cluster 'cc'
[36mINFO[0m[0001] Starting servers...
[36mINFO[0m[0001] Starting Node 'k3d-cc-server-0'
[36mINFO[0m[0033] All agents already running.
[36mINFO[0m[0033] All helpers already running.
[36mINFO[0m[0033] Cluster 'cc' created successfully!
[36mINFO[0m[0034] You can now use it like this:
kubectl cluster-info
Cluster setup is completed. Will start the deployment shortly...
Importing the required images...
[36mINFO[0m[0000] Importing image(s) into cluster 'cc'
[36mINFO[0m[0000] Importing images from 1 tarball(s)...
[36mINFO[0m[0000] Importing images
 '[/home/appviewx/CCTEST/deps/tools/mid-server-docker-image/avx-mid-server-base-22.1.0.0.tar]' into
 node 'k3d-cc-server-0'...
[36mINFO[0m[0024] Successfully imported image(s)
[36mINFO[0m[0024] Successfully imported 1 image(s) into 1 cluster(s)
Import in progress...
[36mINFO[0m[0000] Importing image(s) into cluster 'cc'
[36mINFO[0m[0000] Importing images from 1 tarball(s)...
[36mINFO[0m[0000] Importing images
 '[/home/appviewx/CCTEST/deps/tools/mid-server-docker-image/k3d-tools-5.2.2.tar]' into node
 'k3d-cc-server-0'...
[36mINFO[0m[0005] Successfully imported image(s)
[36mINFO[0m[0005] Successfully imported 1 image(s) into 1 cluster(s)
Import in progress...
[36mINFO[0m[0000] Importing image(s) into cluster 'cc'
[36mINFO[0m[0000] Importing images from 1 tarball(s)...
[36mINFO[0m[0000] Importing images
 '[/
home/appviewx/CCTEST/deps/tools/mid-server-docker-image/rancher-mirrored-coredns-coredns-1.8.6.t
ar]' into node 'k3d-cc-server-0'...
[36mINFO[0m[0007] Successfully imported image(s)
```

```
[36mINFO[0m[0007] Successfully imported 1 image(s) into 1 cluster(s)
[36mINFO[0m[0000] Importing image(s) into cluster 'cc'
[36mINFO[0m[0000] Importing images from 1 tarball(s)...
[36mINFO[0m[0000] Importing images
 '[/
home/appviewx/CCTEST/deps/tools/mid-server-docker-image/rancher-local-path-provisioner-v0.0.21.ta
r]' into node 'k3d-cc-server-0'...
[36mINFO[0m[0004] Successfully imported image(s)
[36mINFO[0m[0004] Successfully imported 1 image(s) into 1 cluster(s)
[36mINFO[0m[0000] Importing image(s) into cluster 'cc'
[36mINFO[0m[0000] Importing images from 1 tarball(s)...
[36mINFO[0m[0000] Importing images
 '[/home/appviewx/CCTEST/deps/tools/mid-server-docker-image/rancher-mirrored-pause-3.6.tar]' into
 node 'k3d-cc-server-0'...
[36mINFO[0m[0003] Successfully imported image(s)
[36mINFO[0m[0003] Successfully imported 1 image(s) into 1 cluster(s)
Deploying the Cloud Connector...
NAME: avx-mid-server-starter
LAST DEPLOYED: Mon May 30 15:51:13 2022
NAMESPACE: cc
STATUS: deployed
REVISION: 1
NOTES:
1. It may take a couple of minutes for the Cloud Connector to be up.
  kubectl get pod --namespace cc
**********************************************************************
*    Congratulations!!! The installation completed successfully.   *
*    Please wait till the Cloud Connector is up and running.       *
**********************************************************************
(1%) Cloud Connector status: Running
[32m Cloud Connector is up and running. (B[m
```

Troubleshooting: For installation errors, refer to the Troubleshooting section.

The AppViewX Cloud Connector consists of two important components—the starter plugin and the platform. The starter plugin component is installed along with the AppViewX Cloud Connector, in the same installation process.

When installed, the starter plugin is used to initiate the download of the platform component. The platform component is used to host business use cases related to the AppViewX Cloud Connector.

When the platform component download is in progress, it is indicated by the  symbol prefixed to the platform component version number in the AppViewX Cloud Connector inventory details  . A completed download/upgrade is indicated by the  symbol in the same location  .

Note: Based on the internet bandwidth and the number of cloud connectors being installed, the downloading of the cloud connector may vary between 5 to 15 minutes.

Prerequisites for Managing ADC Devices

For more information, refer to Prerequisites for Managing ADC Devices.

Installing the AppViewX Windows Gateway

For more information, refer to Installing the AppViewX Windows Gateway.

Troubleshooting the AppViewX Cloud Connector

For more information, refer to Troubleshooting the AppViewX Cloud Connector.

Managing the AppViewX Cloud Connector

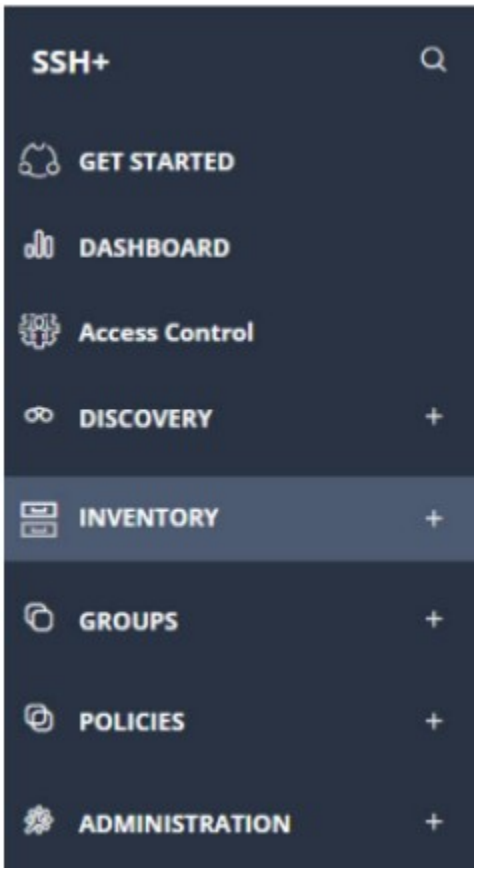
For more information, refer to Managing the AppViewX Cloud Connector.

Accessing SSH+ Features

You have to access the SSH+ node to access the various functions provided by it.

To access SSH+:

1. Log into AppViewX with valid credentials.
2. Hover the mouse pointer over  (**Menu**) icon on the top-left corner of the screen.
3. From the left pane, click **SSH+**. You can now see the different menus of **SSH+** on the left hand side of the page.



4. From the left pane, expand any of the nodes to see that page.

Getting Started

This section explains the SSH+ management workflow:

Onboarding Users

AppViewX offers comprehensive support for Role and Resource-Based Access Control (RBAC). RBAC is a method of restricting AppViewX functions, and managing and monitoring network resources in AppViewX based on the roles of individual users within an enterprise. It allows you to integrate with the existing identity stores such as Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) to enforce authorization policies. Roles and resources can be customized to suit any organizational structure and user requirements.

For more information on configuring role and RBAC, refer to the Section, Configuring Role and Resource-Based Access Control (RBAC) in the Platform Guide.

Discovery and Visibility

You can gain full visibility of SSH user and host keys by discovering them within your network infrastructure.

- **Discover Hosts and Keys from IP network:** You can discover user or/and host keys configured on your server by creating and running scans on your network using IP address or subnet. The Discovery sensor scans your network (on the default SSH enabled port 22) for SSH keys configured on your server. You can map the discovered keys to the selected key compliance groups and manage/monitor them.

  Clicking this link takes you to the **Discovery** page. See Using IP Range Option.

- **Risk Report Dashboard:** You can generate reports on user and host activity, key usage, and access requests. This information can help identify potential security risks, compliance issues, or other areas for improvement.

  Clicking this link takes you to the **Dashboard** page. See Reports.

- **User Key Inventory:** You can see the total number of weak, shared, orphan, and suspicious keys in the key discovery status. Click the number hyperlink to drill down on the metrics. This helps you track the progress of the key discovery efforts, identify any potential security risks, and prioritize the remediation actions.

  Clicking this link takes you to the **Key Inventory** page. See Viewing User/Host Key Inventory.

- **Host Key Inventory:** You can see the total number of weak, shared, orphan, and suspicious keys in the key discovery status. Click the number hyperlink to drill down on the metrics. This helps you track the progress of the key discovery efforts, identify any potential security risks, and prioritize the remediation actions.

  Clicking this link takes you to the **Key Inventory** page. See Viewing User/Host Key Inventory.

Access Management

You can ensure secure access control and authorization within your network infrastructure.

- **Onboard AWS Hosts:** Clicking this link takes you to the **Device Management > Device :: Cloud** page. See Adding Cloud.
- **Host onboarding settings:** Clicking this link takes you to the **Host Inventory** page. See Adding Host.

- **Manage Host Access Groups:** Clicking this link takes you to the **Infra Access Groups** page. See Adding Infra Access Group.
- **Request Access:** Clicking this link takes you to the **Access Control** page. See Viewing Terminal Access Control Page.

Compliance

You can establish and enforce key compliance and rotation policies to ensure secure and standardized key management practices.

- **Configure Key Compliance Policy:** Clicking this link takes you to the **Key Policy** page. See Key Policy.
- **Configure Host Configuration Policy:** Clicking this link takes you to the **Host Policy** page.

Additional Settings

- **Onboard Network Hosts:** Clicking this link takes you to the **Device Management > Device :: Server** page. See Adding Server.

Adding Access to Users

Overview

With access control, you can control and manage users and user groups who have access to the infra access groups and the actions they perform on the hosts. This helps to keep the infra access hosts secure.

You can view all the access requests from users on the **Get Started** page in the **Approvals** section. You can approve/reject the requests efficiently and effectively based on the business justification and for the time duration requested in the access request form. On approving an access request, the user is granted access to the specified infra access group and hosts for the requested duration. The users will be able to perform authorized tasks such as running scripts, executing commands, and troubleshooting issues on those resources for that duration. On rejecting an access request, the user is denied access to the requested resources and will not be able to perform any actions.

Approving Access Requests

All requests for terminal access are displayed on the **Access Inventory** page.

To approve or reject access request:

1. Go to (**Menu**) **> SSH+ > Access Request > Access Inventory**.
   The **Access Inventory** page is displayed.
2. Click the **Application Infra name** hyperlink to open the access request. Alternatively, you can select the checkboxes against the application infra names and click **Actions** from the command bar to do a bulk approval or rejection.
3. Based on the requestors and their access rights, you can approve or reject the request.
   On approving the request, the **Access Status** column on the **Terminal Access Control** page turns to *Accessible*.

   On approving an access request, the user is granted access to the specified infra access group and hosts for the requested duration. The users will be able to perform authorized tasks on those resources. On rejecting an access request, the user is denied access to the requested resources.

Viewing Terminal Access Control Page

To request access to terminal:

Go to (**Menu**) **> SSH+ > Access Control**.
The **Terminal Access Control** page is displayed.

Field description for Terminal Access Control page

Field	Description
Name	Displays the name of the infra access group.
Host(s) Count	Displays the count of the hosts associated with the infra access group.
Access Status	Displays the access status of the infra access group: • **N/A:** Initial status when you do not have access to the group. • **Pending Approval:** Status when you have sent the access request and are awaiting approval form the administrator. • **Accessible:** Status when the administrator grants access to the group. • **Access Denied:** Status when the administrator rejects access to the group.

Field	Description
	• **Expired:** Status once your access to the group is expired for the requested duration. You can request access for the same group again by raising an access request. • **Failed:** Status when the access request fails for some reason. You can try raising the access request once more.
Access Mode	Displays the access mode for the terminal: • AppViewX Terminal • Client • Unmanaged Clients
Logs	Click **View** to open the log. The log displays details about the user who has access to the infra access group, access mode (whether SSH if it was accessed after granting approval or Credential if password was used to access the terminal), status (whether access is active or expired), when the access request was initiated, when the access was terminated, and for how long the access was granted. You can export the logs in .CSV or PDF format.
Actions	If you have a password, you can click the **Ellipses (…)** button, which in turn will open the **Open with Password** popup window. On providing the password, you can access the terminal.

Glossary

Term definition

Term	Definition
SSH	Secure Socket Shell (SSH), also known as simply Secure Shell, is a cryptographic protocol used to enable secure access to remote servers and devices over the internet using SSH keys.
Host key	A host key is a key that is used to identify the server. It is generated by the server and shared with the client during the initial connection setup. The client uses this key to verify the identity of the server before establishing a connection.

Term definition (continued)

Term	Definition
Public key	A public key is used to encrypt data and verify digital signatures. It can be freely distributed, and anyone can use it to encrypt data or verify digital signatures. It is also used to establish a secure connection between the client and the server.
Private key	A private key is a secret key that is used to decrypt data and create digital signatures. It must be kept secret and never shared with anyone. The private key is used to authenticate the user and establish a secure connection with the server.
Suspicious key	A key that is found in non-standard location without a server side. Suspicious keys are discovered only when the **Scan Type** is selected as **Full**.
Shared key	A key found on more than one client machine.
Orphan key	A key found on server without a client side.
SSH key	SSH keys are used to encrypt communicate with a remote system. SSH keys usually come in pairs comprising a public and a private key and are used to grant access to authorized personnel to critical systems such as cloud, on-premise servers, and network devices.
SSH key rotation	The process of changing the cryptographic keys used for secure communication between two devices, such as a client and a server.
User key	A user key is a public key that is associated with a particular user account on the server. It is used to authenticate the user and establish a secure connection with the server.
Weak user key	A key that is weakened over a period of time or because of inferior key algorithm or size.
Weak host key	A key that is weakened over a period of time or because of inferior key algorithm or size.

Chapter 2: SSH+ User Guide

Introduction to SSH+

As application infrastructures grow, so do security threats. Organizations have to find newer ways for protecting their data and granting access to the right users and devices to avoid security threats and breaches. While traditional approach used password authentication, it proved to be insecure. This is where AppViewX SSH+ comes into play.

AppViewX SSH+ is a fully-automated application infra-access management and SSH key lifecycle management solution that allows you to centrally discover, manage, and protect SSH keys with access across hybrid multi-cloud environments. It also helps simplify access management, stay compliant and mitigate risks with SSH+.

AppViewX offers visibility and SSH access management across traditional on-premises data centers and cloud-hosted infrastructures.

Risks of improper SSH Management

Since there is no governing body to regulate the use of SSH keys, there is an element of risk involved. As SSH keys are generated on need basis, several keys may be discarded and left unmanaged when they are no longer of use. Without an inventory, managing these keys and revoking their access pose a security threat to large organizations for potential back-door entry into the network, data theft, or breaches.

Improper SSH key management can lead to unauthorized access, compliance violations, identity and access management issues, data breaches, operational disruption, and reputation damage. To mitigate these risks, organizations should implement proper SSH key management practices, including secure key storage, regular key rotation, and access controls.

What Enterprises Need

AppViewX conducted multiple surveys to identify the core features and functionality needed to address SSH management challenges. SSH and Identity and Access Management (IAM) Administrators highlighted the following requirements:

- Discover keys from standard and non-standard locations
- Identify and report non-standard and non-compliant keys
- Holistic visibility of keys and the users of these keys
- Revoke access to non-compliant and non-standard keys
- Automated rotation and distribution of keys
- Self-service SSH access requests
- Support for cloud and legacy on-premise infrastructure
- Centralized SSH Certificate Authority

How AppViewX Can Help

AppViewX SSH+ key lifecycle management is a fully automated solution that discovers and manages enterprise SSH infrastructure. It can identify and mitigate risks associated with poorly managed passwordless access management.

AppViewX SSH+ features include:

- **Centralized Discovery and Visibility**
  - The solution offers periodic or on-demand scans to discover SSH keys across multi-vendor, hybrid network infrastructures, and map trust relationships to determine access privileges.
  - The consolidated inventory provides a central console to view and manage all SSH keys and hosts.
- **Risk Scorecard and One-Click Remediation**
  - The solution proactively identifies and remediates risks associated with inactive, weak, or suspicious keys using an intuitive SSH scorecard dashboard.
  - The one-click remediation feature enables instant deletion or regeneration of keys.

System Requirements

SSH within the Application Infrastructure

Application infrastructure refers to all the components required to deliver an application and its functions and services to the customer. Although each application is unique, certain common components can be identified that are typically implemented to support application capabilities and service delivery.

Some of the most common components of a typical application infrastructure include:

- **Web server:** Apache, IBM HTTPD, WebSphere, WebLogic, Tomcat, Node.js
- **Application server:** WebSphere, IBM DataPower, WebLogic App server, Iplanet, etc.
- **Database/file storage:** Any on-premise or cloud database or NoSQL document storage
- **Firewalls/NGFW:** Fortinet, Cisco, Checkpoint, F5, etc.
- **Intrusion Detection System (IDS):** Fortinet, Cisco, Checkpoint, F5, etc.

Modern application infrastructure leverages multiple hosting platforms such as on-premise data centers, private clouds, and public clouds offered by third-party hosting providers.

The application infrastructure components communicate with each other to enable service delivery. This can leverage SSH communication. Additionally, administrators of these application infrastructures will need to SSH into these hosts to perform maintenance.

Additionally, security and audit compliance requirements necessitate constant awareness of who has access to what and the maintenance of best security practices for the communications.

Hardware

Ensure that you have, at minimum, the following hardware with the given specifications before proceeding with the installation:

- **Single Node Deployment Requirements**

Node	Bare Minimum		
	CPU	RAM	Hard Disk Space
Single node	8	32GB	500GB

- **Multi-Node Deployment Requirements**

Node	Bare Minimum		
	CPU	RAM	Hard Disk Space
Multi-node (master node)	4	4GB	100GB
Note: One node for a single master installation and a minimum of three nodes for multi-master installation.			
Multi-node (worker node)	8	32GB	500GB

- **Platform Bare Minimum Requirements**

Supported Virtualization Platforms	Versions	vCPU	RAM	HDD
VM Server, VMware ESXi	5.5 or later	8v	32GB	1TB

Operating System

Both single node and multi-node installations of AppViewX are supported on the following operating systems:

- RHEL 8.5
- RHEL 8.6
- RHEL 8.7
- Ubuntu 20.04

Browser

Following is the browser requirements to use the AppViewX SSH+ node:

`Sample codeph`

```
Sampel codeblock
```

Browser	Version
Firefox	v74.0.1 (64-bit) or later
Google Chrome	v85.0.4183.83 (64-bit) or later

Getting Started

This section explains the SSH+ management workflow:

Discovery and Visibility

You can gain full visibility of SSH user and host keys by discovering them within your network infrastructure.

- **Discover Hosts and Keys from IP network:** You can discover user or/and host keys configured on your server by creating and running scans on your network using IP address or subnet. The Discovery sensor scans your network (on the default SSH enabled port 22) for SSH keys configured on your server. You can map the discovered keys to the selected key compliance groups and manage/monitor them.

  Clicking this link takes you to the **Discovery** page. See Using IP Range Option.

- **Risk Report Dashboard:** You can generate reports on user and host activity, key usage, and access requests. This information can help identify potential security risks, compliance issues, or other areas for improvement.

  Clicking this link takes you to the **Dashboard** page. See Risk Dashboard.

- **User Key Inventory:** You can see the total number of weak, shared, orphan, and suspicious keys in the key discovery status. Click the number hyperlink to drill down on the metrics. This helps you track the progress of the key discovery efforts, identify any potential security risks, and prioritize the remediation actions.

  Clicking this link takes you to the **Key Inventory** page. See Viewing User/Host Key Inventory.

- **Host Key Inventory:** You can see the total number of weak, shared, orphan, and suspicious keys in the key discovery status. Click the number hyperlink to drill down on the metrics. This helps you track the progress of the key discovery efforts, identify any potential security risks, and prioritize the remediation actions.

  Clicking this link takes you to the **Key Inventory** page. See Viewing User/Host Key Inventory.

Access Management

You can ensure secure access control and authorization within your network infrastructure.

- **Onboard AWS Hosts:** Clicking this link takes you to the **Device Management > Device :: Cloud** page. See Adding Cloud.
- **Host onboarding settings:** Clicking this link takes you to the **Host Inventory** page. See Adding Host.
- **Manage Host Access Groups:** Clicking this link takes you to the **Infra Access Groups** page. See Adding Infra Access Group.
- **Request Access:** Clicking this link takes you to the **Access Control** page. See Viewing Terminal Access Control Page.

Compliance

You can establish and enforce key compliance and rotation policies to ensure secure and standardized key management practices.

- **Configure Key Compliance Policy:** Clicking this link takes you to the **Key Policy** page. See Key Policy.
- **Configure Host Configuration Policy:** Clicking this link takes you to the **Host Policy** page.

Additional Settings

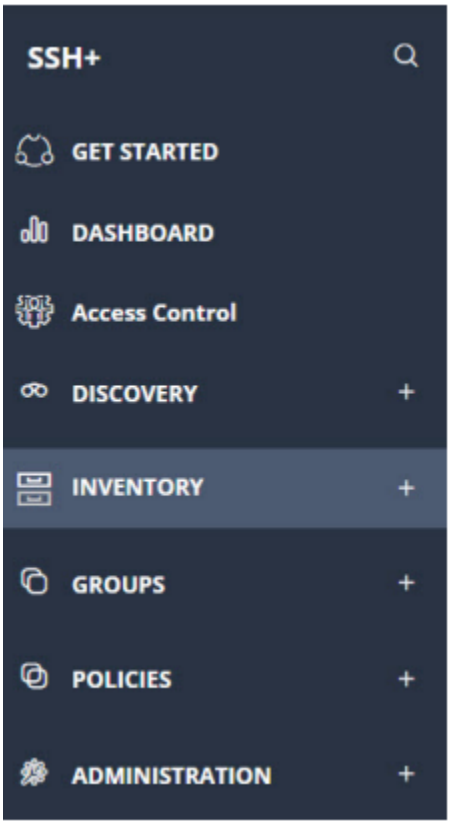
- **Onboard Network Hosts:** Clicking this link takes you to the **Device Management > Device :: Server** page. See Adding Server.

Accessing SSH+ Features

You have to access the SSH+ node to access the various functions provided by it.

To access SSH+:

1. Log into AppViewX with valid credentials.
2. Hover the mouse pointer over (**Menu**) icon on the top-left corner of the screen.
3. From the left pane, click **SSH+**. You can now see the different menus of **SSH+** on the left hand side of the page.



4. From the left pane, expand any of the nodes to see that page.

Discovering Keys

- Overview
- Network Scan
- Managed Devices
- Discovery Status
- Scheduler

Overview

Before you begin: To access this functionality, ensure that you have enabled the right ACF permissions under SSH+ by going to **Platform > Identity > Role > Authorized functions.**

SSH keys are installed to grant and protect access to privileged accounts. When initially deployed on a device, the device is configured to change privileged account passwords; however, if the devices are deployed after the SSH keys are installed, changing the passwords does not stop SSH keys from working

thus rendering the privileged account insecure. To make it secure, these keys must be found so you can remove them and make the accounts secure again.

From the **Discovery** page, you can:

- Discover keys configured by creating and running scans on your network using IP range or subnet option. You can map the discovered keys to the selected key compliance groups and manage/monitor them. See Network Scan.
- Discover keys on the devices you configured by creating and running scans on your devices. You can map the discovered keys to the selected key compliance groups and manage/monitor them. See Managed Devices.
- Fetch the details and the status of the discovery such as the discovery method, action, recurrence, status along with the start and end time. See Discovery Status.
- Create, customize, or delete scheduler to run the discoveries. See Scheduler.
- Fetch the key discovery status of the user and host keys, risk report, details of the user and host keys and the hosts. See Viewing Discovery Summary.

Network Scan

You can discover user or/and host keys configured on your server by creating and running scans on your network using IP address or subnet. The Discovery sensor scans your network (on the default SSH enabled port 22) for SSH keys configured on your server. You can map the discovered keys to the selected key compliance groups and manage/monitor them.

- Using IP Range Option
- Using Subnet Option

Using IP Range Option

To discover keys using the IP Range option:

1. Go to (**Menu**) **> SSH+ > Discovery > Network Scan > IP Range**.
   The **Discover** page is displayed.
2. Enter the following details:

Field description for Discover IP Range section

Field	Description
Discover By	

Field	Description
***Select**	Select one of the options: • **Instant:** To discover the keys immediately. By default, **Instant** option is selected. • **Scheduled:** To schedule the discovery of keys on a specific date and time.
Scheduler (This section appears only if you have selected the **Discovery** option as *Scheduled*)	
***Schedule Name**	Enter a unique name. This helps you identify it easily.
Description	Enter details pertaining to the scheduling discovery purpose.
***Starts On**	Under the **Starts On**, set the time to start the run. You can customize the date, month, year, and time by clicking the Calendar icon.
***Repeat Every**	Schedule discovery can be set to repeat discovery after every 1 hour or can be customized per your requirement.
***End Date**	Select one of the options to end the scheduled discovery: • **Never:** To keep the scheduled discovery going. • **On:** To select the end date when the scheduled discovery has to stop. • **After:** To stop the scheduled discovery after a certain number of occurrences.
Discover SSH Keys	
***Discovery Name**	This field appears on selecting the **Instant** discovery option. Enter a unique name. This helps you identify it easily.
Description	This field appears on selecting the **Instant** discovery option. Enter details pertaining to the discovery stating the purpose.
***Start IP**	Enter start range of the IP address for discovery.
***End IP**	Enter end range of IP address for discovery.
***Ip(S) Per Batch**	Select a value from the dropdown list. Based on this value, the subnet provided is split into multiple batches for the discovery process.
***Ports**	By default, the port is 22. You can enter a port number from where the keys have to be discovered.

Field	Description
Access Type	You can choose between **Key** and **Certificate** access modes during host addition. By default, **Certificate** option is selected
***DataCenter**	Select a datacenter to connect to the host(s).
***Credential Type**	Select one of the options: • **Manual entry:** Enter the username and password. • **Credential List:** Select the credential details that are already stored in the credential inventory page.
***Credential Name**	This field appears only if you have selected **Credential Type** as *Credential List*.
***Login Type**	Select one of the options: • **Password:** Enter username and password. • **Identity Key:** Click **Upload** and the **Upload SSH Private Key** window opens. Browse for the key file and fill out all the fields. Enter passphrase.
Sudoer User	Enable this checkbox if you want to do a full scan on the entire location. This checkbox is disabled for the **Identity Key** login type. **CAUTION:** Incorrect selection of sudoer access might result in work order failure.
***Access Elevation**	This field appears only on selection of **Sudoer User**.
***Discover**	Select one or both of the options: • **User Keys:** To discover user keys. • **Host Keys:** To discover host keys.
***Application Infra Access Group**	Select the Application Infra Access Group(s) to which you want to map the onboarded host. To add new group name, type the name in above text box and press Enter.
Key Compliance Group	Select the required Key Compliance Group to which you want to map the discovered user keys. The discovered keys are associated with the selected **Key Compliance Group**.

Field	Description
	Note: The key group selection simplifies the grouping of the discovered keys and checks the discovered keys for key compliance. The keys are checked for compliance based on the policy of the key group it is associated with.
***Scan Type**	Select one of the options: • **Default:** The system scans the default ssh folders. • **Full:** The system scans the entire location. You can enter the files name/path that you want to exclude from the discovery for non-standard location. Make sure to select the **Sudoer User** checkbox. • **Directory:** The system starts scan in the defined directory. Enter the file name/path you want to exclude/include for non-standard location. **Note:** Changing the scan type clears the File Path table.
File Path	This field is enabled only if you select **Full** or **Directory** as your **Scan Type**. Enter the file/s name/path that you want to exclude/include scan (only for directory scan) from the discovery for non-standard location. File path should always starts with /.
Operation	This field is enabled only if you select **Full** or **Directory** as your **Scan Type**. Select one of the options: • **Exclude:** Disables the scan in the file/s name/path location entered in **File Path**. • **Include:** Enables the scan only in the file/s name/path location entered in **File Path**.

Field	Description
	Note: Multiple folder/path entries can be entered for scan, which are displayed in the consecutive table with respect to **File Path** and **Operation**.
Note: Fields indicated with red asterisk (*) symbol are mandatory.	

3. Click **Add.**
   The **File Path** table is populated with the operation.
4. In **Inventory Action,** select one of the options:
   - **Do Not Move:** To avoid the movement of newly discovered keys in the inventory.
   - **Manage:** To allow the system to manage the newly discovered keys, which are moved to the inventory with **Managed** status.
   - **Monitor:** To allow the system to monitor the newly discovered keys, which are moved to the inventory with **Monitored** status.
5. Click **Discover.**
   The discovery runs per the settings and the key scan instance is added to the discovery inventory with the **Status** as *In Progress* until the discovery is completed. The **Status** in the discovery inventory changes to *Completed* or *Failed* depending on the outcome of the scan.

Using Subnet Option

To discover keys with the subnet option:

1. Go to (**Menu**) **> SSH+ > Discovery > Network Scan > Subnet**.
   The **Discover** page is displayed.
2. Enter the following details:

Field description for Discover Subnet section

Field	Description
Discover By	
***Select**	Select one of the options:

Field	Description
	• **Instant:** To discover the keys immediately. By default, **Instant** option is selected. • **Scheduled:** To schedule the discovery of keys on a specific date and time.
Scheduler (This section appears only if you have selected the **Discovery** option as *Scheduled*)	
***Schedule Name**	Enter a unique name. This helps you identify it easily.
Description	Enter details pertaining to the scheduling discovery purpose.
***Starts On**	Under the **Starts On**, set the time to start the run. You can customize the date, month, year, and time by clicking the Calendar icon.
***Repeat Every**	Schedule discovery can be set to repeat discovery after every 5 minutes or can be customized per your requirement.
***End Date**	Select one of the options to end the scheduled discovery: • **Never:** To keep the scheduled discovery going. • **On:** To select the end date when the scheduled discovery has to stop. • **After:** To stop the scheduled discovery after a certain number of occurrences.
Discover SSH Keys	
***Discovery Name**	This field appears on selecting the **Instant** discovery option. Enter a unique name.
Description	This field appears on selecting the **Instant** discovery option. Enter details pertaining to the discovery stating the purpose.
***Network**	Enter the IP address of the network. For example, 192.168.1.1/24
***Subnets Per Batch Of Discovery**	Select a value from the dropdown list. Based on this value, the subnet provided is split into multiple batches for the discovery process.
***Ports**	By default, the port is 22. You can enter a port number from where the keys have to be discovered.
Access Type	You can choose between **Key** and **Certificate** access modes during host addition. By default, **Certificate** option is selected

Field	Description
***DataCenter**	Select a datacenter to connect to the host(s).
***Credential Type**	Select one of the options: • **Manual entry:** Enter the username and password. • **Credential List:** Select the credential details that are already stored in the credential inventory page.
***Credential Name**	This field appears only if you have selected **Credential Type** as *Credential List*.
***Login Type**	Select one of the options: • **Password:** Enter username and password. • **Identity Key:** Click **Upload** and the **Upload SSH Private Key** window opens. Browse for the key file and fill out all the fields. Enter passphrase.
Sudoer User	Enable this checkbox if you want to do a full scan on the entire location. This checkbox is disabled for the **Identity Key** login type. **CAUTION:** Incorrect selection of sudoer access might result in work order failure.
***Access Elevation**	This field appears only on selection of **Sudoer User**.
***Discover**	Select one or both of the options: • **User Keys:** To discover user keys. • **Host Keys:** To discover host keys.
***Application Infra Access Group**	Select the Application Infra Access Group(s) to which you want to map the onboarded host. To add new group name, type the name in above text box and press Enter.
Key Compliance Group	Select the required Key Compliance Group to which you want to map the discovered user keys. The discovered keys are associated with the selected **Key Compliance Group**. **Note:** The key group selection simplifies the grouping of the discovered keys and checks the discovered keys for user

Field	Description
	compliance. The keys are checked for compliance based on the policy of the key group it is associated with.
***Scan Type**	Select one of the options: • **Default:** The system scans the default ssh folders. • **Full:** The system scans the entire location. You can enter the files name/path that you want to exclude from the discovery for non-standard location. Make sure to select the **Sudoer User** checkbox. • **Directory:** The system starts scan in the defined directory. Enter the file name/path you want to exclude/include for non-standard location. **Note:** Changing the scan type clears the File Path table.
File Path	This field is enabled only if you select **Full** or **Directory** as your **Scan Type**. Enter the file/s name/path that you want to exclude/include scan (only for directory scan) from the discovery for non-standard location. File path should always starts with /.
Operation	This field is enabled only if you select **Full** or **Directory** as your **Scan Type**. Select one of the options: • **Exclude:** Disables the scan in the file/s name/path location entered in **File Path**. • **Include:** Enables the scan only in the file/s name/path location entered in **File Path**. **Note:** Multiple folder/path entries can be entered for scan, which are displayed in the consecutive table with respect to **File Path** and **Operation**.

Field	Description
	Note: Fields indicated with red asterisk (*) symbol are mandatory.

3. Click **Add.**
   The **File Path** table is populated with the operation.
4. In **Inventory Action,** select one of the options:
   - **Do Not Move:** To avoid the movement of newly discovered keys in the inventory.
   - **Manage:** To allow the system to manage the newly discovered keys, which are moved to the inventory with **Managed** status.
   - **Monitor:** To allow the system to monitor the newly discovered keys, which are moved to the inventory with **Monitored** status.
5. Click **Discover.**

   The discovery runs per the settings and the key scan instance is added to the discovery inventory with the **Status** as *In Progress* until the discovery is completed. The **Status** in the discovery inventory changes to *Completed* or *Failed* depending on the outcome of the scan.

Managed Devices

You can discover keys by creating and running scans on your configured devices. The Discovery sensor scans these devices for SSH keys configured on your server. You can map the discovered keys to the selected key compliance groups and manage/monitor them.

To discover keys using managed devices option:

1. Go to (**Menu**) **> SSH+ > Discovery > Managed Devices**.
   The **Managed Devices > Discover** page is displayed.
2. Enter the following details:

Field description for Discover Managed Devices section

Field	Description
Discover By	
***Select**	Select one of the options:

Field	Description
	• **Instant:** To discover the keys immediately. By default, **Instant** option is selected. • **Scheduled:** To schedule the discovery of keys on a specific date and time.
Scheduler (This section appears only if you have selected the **Discovery** option as *Scheduled*)	
***Schedule Name**	Enter a unique name. This helps you identify it easily.
Description	Enter details pertaining to the scheduling discovery purpose.
***Starts On**	Under the **Starts On**, set the time to start the run. You can customize the date, month, year, and time by clicking the Calendar icon.
***Repeat Every**	Schedule discovery can be set to repeat discovery after every 5 minutes or can be customized per your requirement.
***End Date**	Select one of the options to end the scheduled discovery: • **Never:** To keep the scheduled discovery going. • **On:** To select the end date when the scheduled discovery has to stop. • **After:** To stop the scheduled discovery after a certain number of occurrences.
Discover SSH Keys	
***Discovery Name**	This field appears only on selecting the **Instant** discovery option. Enter a unique name. This helps you identify it easily.
Description	This field appears only on selecting the **Instant** discovery option. Enter details pertaining to the discovery stating the purpose.
A list of added and managed devices is displayed. Only devices with status as *Managed* are displayed in the list. From the list of managed device(s), select the **Managed Device(s)**. The selected device(s) is the source of discovery. To select all the managed devices, select **Select all**. All the managed devices are the source of discovery. To understand the functionality of Regex, see Using Regex Feature.	

Field	Description
***Ip(S) Per Batch**	Select a value from the dropdown list. Based on this value, the subnet provided is split into multiple batches for the discovery process
***Discover**	Select one or both of the options: • **User Keys:** To discover user keys. • **Host Keys:** To discover host keys.
Key Compliance Group	Select the required **Key Compliance Group** to which you want to map the discovered keys. The discovered keys are associated with the selected **Key Compliance Group**. **Note:** The key group selection simplifies the grouping of the discovered keys and checks the discovered keys for key compliance. The keys are checked for compliance based on the policy of the key group it is associated with.
***Scan Type**	Select one of the options: • **Default:** The system scans the default ssh folders. • **Full:** The system scans the entire location. You can enter the files name/path that you want to exclude from the discovery for non-standard location. • **Directory:** The system starts scan in the defined directory. Enter the file name/path you want to exclude/include for non-standard location. **Note:** Changing the scan type clears the File Path table.
File Path	This field is enabled only if you select **Full or Directory** as your **Scan Type**. Enter the file/s name/path that you want to exclude/include scan (only for directory scan) from the discovery for non-standard location. File path should always starts with '/'.
Operation	This field is enabled only if you select **Full** or **Directory** as your **Scan Type**.

Field	Description
	Select from the following options: • **Exclude:** Disables the scan in the file/s name/path location entered in **File Path**. • **Include:** Enables the scan only in the file/s name/path location entered in **File Path**. **Note:** Multiple folder/path entries can be entered for scan, which are displayed in the consecutive table with respect to **File Path** and **Operation**.
Note: Fields indicated with red asterisk (*) symbol are mandatory.	

3. Click **Add.**

   The **File Path** table is populated with the operation.
4. In **Inventory Action,** select one of the options:
   - **Do Not Move:** To avoid the movement of newly discovered keys in the inventory.
   - **Manage:** To allow the system to manage the newly discovered keys, which are moved to the inventory with **Managed** status.
   - **Monitor:** To allow the system to monitor the newly discovered keys, which are moved to the inventory with **Monitored** status.
5. Click **Discover.**

   The discovery runs per the settings and the key scan instance is added to the discovery inventory with the **Status** as *In Progress* until the discovery is completed. The **Status** in the discovery inventory changes to *Completed* or *Failed* depending on the outcome of the scan.

• Using Regex Feature

Using Regex Feature

Regex stands for regular expression; it is a string used to define filters. The string can contain a part of the device name or a key scan instance. These expressions are stored in the registry and can be used to select the devices/key scan instances in future. This feature is available for discovering keys using the managed devices.

It enables you to filter your records on the strings mentioned in **Regex**.

1. Go to **Managed Devices > Discover** page.
   The **Discover Managed Devices** page is displayed.
2. On the left side is the list of the devices/key scan instances.
3. In the search bar, enter an expression.
4. Click **Add as regex >>**.

   The expression is added in the list on the right hand side.

   Note: These expressions are stored in the registry and can be used to select the devices/key scan instances in future.

   You can use this register of expressions (**Regex**) for all future managed devices.

Discovery Status

To discover keys using the discovery status option:

1. Go to (**Menu**) **> SSH+ > Discovery > Discovery Status**.
   The **Discovery Status** page is displayed.
2. Displays the following details:

Field description for Discovery Status section

Field	Description
Discovery Name	Displays unique discovery name. This helps you identify it easily.
Discovery Mode	Displays the mode of discovery as **Managed** or **Monitored**.
Discover action	Displays the discovery action as **Instant** or **Scheduled**.
Recurrence Type	Displays the frequency of the run of the discovery key instance.
Status	Displays the discovery status which are **Completed**, **In Progress**, or **Failed**.
Start Time	Displays the **Start Time**, set the time to start the discovery run. You can customize it if the **Recurrence Type** is one of these: • Daily • Weekly

Field	Description
	• Monthly • Yearly
End Time	Displays the date and time when the discovery ends.
Description	Displays the details pertaining to the discovery stating the purpose.

What to do next:

- To schedule a discovery using the same input parameters, click **Actions > Rediscover**.
- To delete a discovery, select the checkbox against the **Discovery Name**(s) that has to be deleted and click **Actions > Delete**.

  The selected discovery is deleted from the AppViewX database.

- Viewing Discovery Summary

Viewing Discovery Summary

To view the discovery summary:

1. Go to (**Menu**) **> SSH+ > Discovery > Discovery Status**.

   The **Discovery Status** page is displayed.
2. Click the **Discovery Name** link.

   The **Discovery Summary** of that discovery is displayed.

Summary

The summary report provides information about the discovery of the keys in the default branch. It contains the cumulative results of all successful discoveries.

Discovery summary mainly contains four reports:

- **Key Discovery Summary:** This widget gives a count of the discovered host keys and the user keys.

Color Code	Description
Orange	Displays the number of discovered host keys.

Color Code	Description
Blue	Displays the number of discovered user keys.

Clicking the widget redirects you to the **Host Keys/User Keys** tab.

- **Hosts:** This widget gives a count of the existing hosts and the newly discovered hosts.

Color Code	Description
Orange	Displays the number of existing hosts.
Blue	Displays the number of newly discovered hosts.

Clicking the widget redirects you to the **Hosts** tab.

- **User Keys:** This widget gives a count of the newly discovered user keys, missing user keys, and unchanged user keys in the device.

Color Code	Description
Blue	Displays the number of newly discovered user keys.
Yellow	Displays the number of missing user keys.
Green	Displays the number of user keys with no changes.

Clicking the number hyperlink redirects you to the **User Keys** tab.

- **Host Keys:** This widget gives a count of the newly discovered host keys, missing host keys, and unchanged host keys in the device.

Color Code	Description
Blue	Displays the number of newly discovered host keys.
Yellow	Displays the number of missing host keys.
Green	Displays the number of host keys with no changes.

Clicking the number hyperlink redirects you to the **Host Keys** tab.

Hosts

The Hosts tab displays the total number of compliant, non-compliant, weak kex algorithm hosts, weak ciphers, and weak mac algorithm hosts in the host discovery status. Click the number hyperlink to drill down on the metrics.

This helps you monitor the progress of the host discovery efforts, identify the compliance gaps, and prioritize the remediation actions.

Host Keys

The Host Keys tab displays the total number of weak, shared, orphan, and suspicious keys in the key discovery status. Click the number hyperlink to drill down on the metrics.

This helps you track the progress of the key discovery efforts, identify any potential security risks, and prioritize the remediation actions.

User Keys

The User Keys tab displays the total number of weak, shared, orphan, and suspicious keys in the key discovery status. Click the number hyperlink to drill down on the metrics.

This helps you track the progress of the key discovery efforts, identify any potential security risks, and prioritize the remediation actions.

Risk Report

The Risk Report tab contains the same field information as the Dashboard. The only difference is that while Dashboard shows the reports for all the discovered keys and also an option to perform remediation, you can use this page to fetch all the reports for the selected discovery. See Reports.

Scheduler

To discover keys using the Scheduler option:

1. Go to (**Menu**) **> SSH+ > Discovery > Scheduler**.
   The **Scheduler** page is displayed.
2. Displays the following details:

Field description for Scheduler section

Field	description
Scheduler Name	Displays unique scheduler name.
Discovery Mode	Displays the mode of discovery (IP range, subnet, or managed devices).
Recurrence Type	Displays the frequency of the run of the scheduled discovery key instance.

Field	description
Last Execution Time	Displays the date and time of the previous scheduled discovery occurrence details.
Status	Displays the discovery status which are **Completed**, **Scheduled**, and **Paused**. **Note:** Scheduled discovery can be paused or resumed by clicking the pause or resume icon before the occurrence of the discovery.
Description	Displays the details pertaining to the discovery stating the purpose.
Next Execution Time	Displays the date and time of the next scheduled discovery occurrence details.

What to do next:

- To modify the scheduled discovery, click **Discovery Status::Scheduler > Modify**.
- To delete a discovery, select the checkbox next to the **Scheduler name** that has to be deleted and click **Actions > Delete**.

  The selected discovery is deleted from the AppViewX database.

Managing Devices/Hosts

Overview

Before you get started: Ensure that you have enabled the SSH+ ACF to access this functionality by going to **Platform > Identity > Role > Authorized functions.**

You can configure and manage devices (AWS Cloud and Linux servers), enable certificate sync for AppViewX to connect with customer's accounts and discover certificates, enable SSH sync for AppViewX to connect with customer's accounts, and discover host and user keys.

From the **Managing Devices** page, you can:

- Configure devices (AWS Cloud and Linux servers). See Adding Cloud or Adding Server.
- Set user name and passwords to make the devices secure for SSH management. See Adding Credentials.
- Perform action such as export, import, manage, unmanage, or delete a server, or fetch configuration from a server. See Actions.

Adding Credentials

To add credentials for any device:

1. Go to (**Menu**) **> SSH+ > Administration > Device Management**.
   The **Device::Server** page is displayed.
2. Select the device from the tabs.
3. Click the  (**Credential**) icon in the command bar.
   The **Credential** page is displayed. If credentials are set up, a list of credential names with details is displayed in the table.
4. To add a new credential, click + (**Add Credential**) icon in the command bar.
   The **Add Credential** page is displayed with default credentials fields for AppViewX.
   - To set credentials for **AppViewX**:

Field description for AppViewX Credential Details section

Field	Description
***Credential name**	Enter a suitable credential name.
***User name**	Enter a suitable username.
Credential type (Password)	Select one of the options: • **Password:** Enter password and secondary password. • **Identity key:** Enter identity key and passphrase.

Field	Description
Note: Fields indicated with red asterisk (*) symbol are mandatory.	

- To set credentials for **CyberArk**:

Field description for CyberArk Credential Details section

Field Name	Description
***Credential name**	Enter a suitable credential name
Type	Select one of the options: • **Device:** Enter user name, App ID, and user type. • **Amazon (AWS/ELB):** Enter AWS IAM user name, App ID, and AWS access key ID.
Note: Fields indicated with red asterisk (*) symbol are mandatory.	

Note: To configure the API Settings for CyberArk, click the **Cyberark API Settings** button on the right of the screen.

- To set credentials for **Thycotic**:

Field description for Thycotic Credential Details section

Field Name	Description
***Credential name**	Enter a suitable credential name.
***API Profile**	Select the desired API profile from the dropdown list.
Secret Type	Select one of the options: • **Device:** Enter user name. • **Amazon (AWS/ELB):** Enter AWS IAM user name.

Field Name	Description
	Note: Fields indicated with red asterisk (*) symbol are mandatory.

Note: To configure the API Settings for Thycotic, click the **Thycotic API Settings** button on the right of the screen.

Host Inventory

Hosts can be discovered, added, modified, deleted, and decommissioned. The most important feature of this module is discovering the cloud host. Cloud host management helps simplify grouping and access to the host.

- You can discover the hosts that are a part of the AWS cloud.
- When you create access groups based on AWS Tags, it is easier to identify the LDAP user groups associated with the access groups of these hosts.
- The devices can be automatically grouped together based on *AWS Tags* during the run of a cloud host discovery host instance.
- The automatic grouping option can be enabled using a toggle button.
- Alternatively, you can manually create an Access Group by grouping the devices as per your discretion.

- Adding Host
- Viewing Host Inventory
- Actions in Host Inventory

Adding Host

Note: AppViewX SSH+ currently supports only adding servers as hosts.

To add a host:

1. Go to (**Menu**) **> SSH+ > Inventory > Host Inventory**.
2. On the command bar, click **+ Add Host**.

   The **SSH+::Host Inventory > Add Host** page is displayed.

3. Enter the following details:

Field description for Add Host section

Field	Description
General information	
***Category**	Select **Server**. Selecting the **Server** option displays the **Port** field.
***Vendor**	Select **Linux**.
***Device Name**	Enter the name of the device. Displays the port used while configuring the device.
Port	This is a non-editable field.
Client	By default, this is turned off. Turning on the toggle button allows you to identify the host as a client. The application infra access groups selected also get mapped to this client.
Access Type	You can choose between **Key** and **Certificate** access modes during host addition. By default, **Certificate** option is selected.
***FQDN / IP Address**	Enter the FQDN or the IP address of the host.
***DataCenter**	Select a datacenter to connect to the host.
***Inventory Action**	Select one of the options: • **Do Not Move:** To avoid the movement of newly discovered keys in the inventory. • **Manage:** To allow the system to manage the newly discovered keys, which are moved to the inventory with **Managed** status. • **Monitor:** To allow the system to monitor the newly discovered keys, which are moved to the inventory with **Monitored** status.
***Discover**	Select one or both of the options: • **User Keys:** To discover user keys. • **Host Keys:** To discover host keys.
***Scan Type**	Select one of the options:

Field	Description
	• **Default:** The system scans the default ssh folders. • **Full:** The system scans the entire location. You can enter the files name/path that you want to exclude from the discovery for non-standard location. Make sure to select the **Sudoer User** checkbox. • **Directory:** The system starts scan in the defined directory. Enter the file name/path you want to exclude/include for non-standard location. **Note:** Changing the scan type clears the File Path table.
File Path	This field is enabled only if you select **Full** or **Directory** as your **Scan Type**. Enter the file/s name/path that you want to exclude/include scan (only for directory scan) from the discovery for non-standard location. File path should always starts with /.
Operation	This field is enabled only if you select **Full** or **Directory** as your **Scan Type**. Select one of the options: • **Exclude:** Disables the scan in the file/s name/path location entered in **File Path**. • **Include:** Enables the scan only in the file/s name/path location entered in **File Path**. **Note:** Multiple folder/path entries can be entered for scan, which are displayed in the consecutive table with respect to **File Path** and **Operation**.
Click **Add.** The File Path table is populated with the operation.	
Credentials	
***Credential Type**	Select one of the options:

Field	Description
	• **Manual entry:** Enter username and password. • **Credential List:** Select the credential details that are already stored in the credential inventory page.
Login Using	Select one of the options: • **Password:** Enter username and password. • **Identity Key:** Click **Upload** and the **Upload SSH Private Key** window opens. Browse for the key file and fill out all the fields. Enter passphrase.
Sudoer User	Enable this checkbox if you want to do a full scan on the entire location. This checkbox is disabled for the **Identity Key** login type. **CAUTION:** Incorrect selection of sudoer access might result in work order failure.
***Access Elevation**	This field appears only on selection of **Sudoer User**.
Assign group	
***Application Infra Access Group**	Select the required **Application Infra Access Group** to which you want to map the onboarded host. The onboarded hosts are associated with the selected Application Infra Access Group. The Application Infra Access Group selection simplifies the grouping of the onboarded hosts and checks the onboarded hosts for user compliance. The onboarded hosts are checked for compliance based on the policy of the Application Infra Access Group it is associated with.
***Key Compliance Group**	Select a value from the dropdown list.
Note: Fields indicated with red asterisk (*) symbol are mandatory.	

4. Click **Create**.

   The host is created in the host inventory.

Viewing Host Inventory

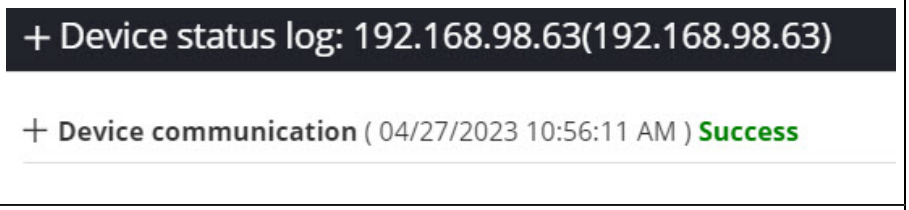
The Host Inventory tab displays the total number of compliant, non-compliant, weak kex algorithm hosts, weak ciphers, and weak mac algorithm hosts in the host discovery status. Click the number hyperlink to drill down on the metrics. This helps you monitor the progress of the host discovery efforts, identify the compliance gaps, and prioritize the remediation actions.

To view the details of the host inventory:

1. Go to (**Menu**) **> SSH+ > Inventory > Host Inventory.**

   The **Host Inventory** page is displayed.

Field description for Host Inventory section

Field	Description
Device name	Displays the name of the device.
FQDN/IP address	Displays the FQDN/IP address of the host.
Host name	Displays the name of the host.
Group	Displays the group associated with the host.
Host Status	Displays the status of the host as: • Managed • Unmanaged • In-Progress • Failed • Unresolved Clicking the hyperlink displays the device status: 
Client	Displays the devices acting as a client.
Access Type	Displays whether key or certificate was selected during host addition.
User	Displays the name of the user onboarding the device.
Port	Displays the port number that is communicating with the host.

Field	Description
Vendor	Displays the vendor associated with the host.
Last sync time	Displays the last sync date and time with the host.
Instance Id	Displays the ID automatically generated by AWS when you launch a new EC2 instance.

Actions in Host Inventory

You can perform any of following actions by selecting the checkbox against the host name and clicking the **Actions** dropdown menu on the **Host Inventory** page:

Action description on Host Inventory page

Action	Description
Modify	You can edit the host inventory.
Delete	You can delete only the active hosts from the host inventory.
Credentials	You can view the credentials of the host keys that are discovered on the device. You can also add, modify, or delete the credentials. See Adding Credentials. You cannot delete the default or active credentials.
Fetch Keys	You can fetch the host key from the host inventory.
Export	You can export the host from the host inventory to .csv or .xls format.
Rotate Host Certificate	You can rotate host certificates from the endpoint directly from the host inventory. A warning message about the implications of the rotation process is displayed. On clicking **Yes**, the existing host certificate is deleted and a new one is created in its place for the selected host.

Adding Server

Note: AppViewX SSH+ currently supports addition of only Linux servers.

To add a server:

1. Go to (**Menu**) **> SSH+ > Administration > Device Management**.

   The **Device::Server** page is displayed.

2. On the command bar, click + (**Add**) icon to add a new server.

   The **Device::Server > Add** page is displayed.

3. Select **Linux** from the **Vendors** list.
4. Enter the following details:

Field description for Device Details section

Field	Description
Server details	
***Server name**	Enter a unique name for the server. This helps you identify it easily.
***IP address/FQDN**	Enter the IP address/FQDN.
Data center	Select a data center from the dropdown list.
Communication mode	Select SSH.
***SSH Port**	By default, the port is 22. You can choose to enter a port number.
Cert sync	Select one of the options: • **Managed:** AppViewX connects to the customer's server account and discovers host and user keys. These keys are added to the host and key inventory. Users with the relevant permissions can then perform the required keys-related actions. • **Monitored:** AppViewX connects to the customer's server account and discovers host and user keys. These keys are added to the host and key inventory where the users are allowed to only view the keys. • **Ignored:** AppViewX connects to the customer's server account but host and user key discovery are disabled. **Note:** The device is added only to the device inventory. It is not available in the host inventory.
Credentials	
***Credential Type**	Select one of the options:

Field	Description
	• **Manual entry:** Enter the username and password. • **Credential List - AppViewX:** Select the credential details that are already stored in the credential inventory page. • **SSH:** Enter the username, browse and upload the identity key along with its passphrase.
Service account credentials	
Username	Enter the user name.
Password	Enter the password.
Vendor Specific Details	
Access Elevation	By default, the value is **None**. Select a value from the dropdown list.
Discover Formats	Enter a value to filter the formats to be discovered from the device. By default, all standard formats are discovered.
Certificate details	
Certificate Directory	Provide the directory from where the certificates must be discovered. By default, the system scans for certificates from all the directories.
Scan type	Select one of the options: • **Default:** The system scans for supported certificate formats such as pem, crt, cer, der, kdb, jks, p12, p7, pfx, and adds them to the certificate inventory. • **Aggressive:** The system scans for all keystore files with non-standard extensions.
***Operation**	Select one the options: • **Exclude:** Disables the scan in the specified certificate directory. • **Include:** Enables the scan only in the specified certificate directory.
 **Note:** Fields indicated with red asterisk (*) symbol are mandatory.	

5. Click **Add**.

   The details are populated in the **Certificate Directory** table.

6. Scroll down to the **SSH Details** section. By default, the **SSH Sync Enable** toggle button is turned off.

7. Click **SSH Sync Enable** toggle button to enable SSH sync.
8. Click **Customise** to modify the default settings.
9. Enter the following fields:

Field description for SSH Details section

Field	Description
***Inventory Action**	Select one of the options: • **Do Not Move:** To avoid the movement of newly discovered keys in the inventory. • **Manage:** To allow the system to manage the newly discovered keys, which are moved to the inventory with **Managed** status. • **Monitor:** To allow the system to monitor the newly discovered keys, which are moved to the inventory with **Monitored** status.
***Discover**	Select one or both of the options: • **User Keys:** Discovers user keys. • **Host Keys:** Discovers host keys.
Scan Type	Select one of the options: • **Default:** The system scans the default ssh folders. • **Full:** The system scans the entire location. You can enter the files name/path that you want to exclude from the discovery for non-standard location. • **Directory:** The system starts scan in the defined directory. Enter the file name/path you want to exclude/include for non-standard location.  **Note:** Changing the scan type clears the File Path table.
File Path	This field appears if you select **Full** or **Directory** as your **Scan Type**. Enter the file/s name/path that you want to exclude/include scan (only for directory scan) from the discovery for non-standard location. File path should always starts with '/'.
Operation	This field appears if you select **Full** or **Directory** as your **Scan Type**. Select one of the options:

Field	Description
	• **Exclude:** Disables the scan in the file/s name/path location entered in **File Path**. • **Include:** Enables the scan only in the file/s name/path location entered in **File Path**. **Note:** Multiple folder/path entries can be entered for scan, which are displayed in the consecutive table with respect to **File Path** and **Operation**.
***Host Compliance Group**	Select the required Host Compliance Group to which you want to map the discovered hosts and host keys. The discovered host keys are associated with the selected host compliance group. The host group selection simplifies the grouping of the discovered hosts and checks the discovered hosts for host compliance. The hosts are checked for compliance based on the policy of the host group it is associated with.
***Key Compliance Group**	Select the required Key Compliance Group to which you want to map the discovered keys. The discovered keys are associated with the selected key compliance group. The key group selection simplifies the grouping of the discovered keys and checks the discovered keys for key compliance. The keys are checked for compliance based on the policy of the key group it is associated with.
***Application Infra access group**	Select the Application Infra Access Group(s) to which you want to map the onboarded host. To add new group name, type a name in the above text box and press Enter.
Note: Fields indicated with red asterisk (*) symbol are mandatory.	

10. Click **Save**.

The host is created and displayed in the host inventory.

Multiple devices can be configured for the same vendor.

What to do next:

- To add credentials to the server, see Adding Credentials.
- To perform any of the actions such as export, import, manage, unmanage, or delete a server, or fetch configuration from a server, see Actions.

Adding Cloud

Note: AppViewX SSH+ currently supports addition of only AWS cloud devices.

1. Go to (**Menu**) **> SSH+ > Administration > Device Management**.
   The **Device::Server** page is displayed.
2. Click **Cloud** tab.
   The **Device::Cloud** page is displayed.
3. On the command bar, click + (**Add**) icon to add a new cloud device.
   The **Device::Cloud > Add** page is displayed. By default, AWS is selected from the **Vendors** list.
4. Enter the following fields:

Field description for AWS Device Details section

Field	Description
Basic Information	
***Account Type**	Select **Cross or Federated** to authenticate using the assumed role.
***Account Name**	Enter a unique name. It cannot be an account name that is already in the cloud inventory. Name can be alphanumeric and contain hyphen (-) and period (.).
***Account Number**	Enter a valid AWS account number.
Account Description	Enter a description that helps identify your account from the cloud inventory.
Proxy Required	Select the checkbox if you want to create it as a proxy.
***Default Region**	Select the region from the dropdown list for API communication.

Field	Description
***Data Center**	Select a datacenter to connect to the host.
Credentials	
***Credential type**	Select one of the options: • **Manual Entry:** Enter username and password. • **Credential List:** Select the credential details that are already stored in the credential inventory page.
***Access Key ID**	Enter the access key ID.
***Secret Access Key**	Enter the secret access key. **Note:** To authenticate requests, use both the access key ID and the secret access key.
Discover resources	
Auto Discover Resources	By default, this is turned off. Turn on the toggle button to discover all cross or federated/child accounts of the provided master account details.
Advanced Settings	By default, this is turned off. Turn on the toggle button to customize the auto-discovery process.
***Auto Discovery Mode**	Select one or both of the options.
***Service**	Select **EC2 (EC2 instance)** from the dropdown list.
***Service Region**	Click **Fetch Region** to fetch the service regions for the provided account information.
Cert Sync	Select one of the options: • **Managed:** AppViewX connects to the customer's server account and discovers host and user keys. These keys are added to the host and key inventory. Users with the relevant permissions can then perform the required keys-related actions. • **Monitored:** AppViewX connects to the customer's server account and discovers host and user keys. These keys are added to the host and key inventory where the users are allowed to only view the keys.

Field	Description
	• **Ignored:** AppViewX connects to the customer's server account but host and user key discovery are disabled. **Note:** The device is added only to the device inventory. It is not available in the host inventory.
Auto Sync	By default, this is turned off. Turn on the toggle button to auto sync based on trigger or schedule.
EC2 Services	
Communication mode	Keep the default selection.
Certificate Discovery Mode	Keep the default selection.
***S3 Deployment Type**	Enter the S3 deployment type that can be a centralized S3 bucket.
***S3 Bucket Name**	Click the **Settings** icon and fill out the mandatory fields in the **ARN Advanced Settings** window that pops up.
Note: Fields indicated with red asterisk (*) symbol are mandatory.	

5. Scroll down to the **SSH Details** section. By default, the **SSH Sync Enable** toggle button is turned off.
6. Click **SSH Sync Enable** toggle button to enable SSH sync.
7. Click **Customise** to modify the default settings.
8. Enter the following fields:

Field description for SSH Details section

Field	Description
***Auto-Create Application Infra access group**	By default, this toggle button is turned off. Access groups can be auto-created based on the tags available for an AWS host during discovery. Users with permissions to an access group can automatically be authenticated to all the hosts belonging to the access group.
***Inventory Action**	Select one of the options:

Field	Description
	• **Do Not Move:** To avoid the movement of newly discovered keys in the inventory. • **Manage:** To allow the system to manage the newly discovered keys, which are moved to the inventory with **Managed** status. • **Monitor:** To allow the system to monitor the newly discovered keys, which are moved to the inventory with **Monitored** status.
***Host Compliance Group**	Select the required Host Compliance Group to which you want to map the discovered hosts and host keys. The discovered hosts are associated with the selected host compliance group. The host group selection simplifies the grouping of the discovered hosts and checks the discovered hosts for hosts compliance. The hosts are checked for compliance based on the policy of the hosts group it is associated with.
***Key Compliance Group**	Select the required Key Compliance Group to which you want to map the discovered keys. The discovered keys are associated with the selected key compliance group. The key group selection simplifies the grouping of the discovered keys and checks the discovered keys for key compliance. The keys are checked for compliance based on the policy of the key group it is associated with.
Scan Type	Select one of the options: • **Default:** The system scans the default ssh folders. • **Full:** The system scans the entire location. You can enter the files name/path that you want to exclude from the discovery for non-standard location. • **Directory:** The system starts scan in the defined directory. Enter the file name/path you want to exclude/include for non-standard location. **Note:** Changing the scan type clears the File Path table.
***Discover**	Select one or both of the options:

Field	Description
	• **User Keys:** Discovers user keys. • **Host Keys:** Discovers host keys.
File Path	This field appears if you select **Full** or **Directory** as your **Scan Type**. Enter the file/s name/path that you want to exclude/include scan (only for directory scan) from the discovery for non-standard location. File path should always starts with '/'.
Operation	This field appears if you select **Full** or **Directory** as your **Scan Type**. Select one of the options: • **Exclude:** Disables the scan in the file/s name/path location entered in **File Path**. • **Include:** Enables the scan only in the file/s name/path location entered in **File Path**. **Note:** Multiple folder/path entries can be entered for scan, which are displayed in the consecutive table with respect to **File Path** and **Operation**.
Note: Fields indicated with red asterisk (*) symbol are mandatory.	

9. Click **Add**.
   The added details are populated in the consecutive table.

What to do next:

- To add credentials to the cloud device, see Adding Credentials.
- To perform any of the actions such as export, import, manage, unmanage, or delete a server, or fetch configuration from a server, see Actions.

Actions

To do any of the following actions on the command bar, select the checkbox against the device.

Action Descriptions on Command Bar

Icon	Action	Description
	Terminal connect	Click to open the terminal connect page of the device.
	Delete	Click **Yes** on the confirmation popup window. The device is deleted from the inventory.
	Credential	Click to add credentials for the server. See Adding Credentials.
	Manage	Click **Yes** on the confirmation popup window. Configuration fetch is triggered, and the device status is changed to *Managed* in the device inventory. **Note:** With the introduction of the Cert License Enforcement; Server Auto discovery of EC2 instances will be on-boarded with certificate status as *Monitored*, even if *Managed* state is configured in the device account configuration.
	Unmanage	Click **Yes** on the confirmation popup window. Configuration fetch is triggered, and the device status is changed to *Unmanaged* in the device inventory.
	Export	Select one of the options: • **All Columns:** Select this option if you want to export all information about the device. • **Displayed columns:** Select this option if you want to export only the information that is visible on the screen. • **Columns to modify data and import:** Select this option if you want to export device details to make modifications and then import the data into the device inventory. The data is exported to an Excel (.xls) format.

Action Descriptions on Command Bar (continued)

Icon	Action	Description
	Import	1. Click **Import** to be redirected to the import cloud page. 2. Download the sample <.csv> or <.xls> file. 3. Update the details. 4. Click to browse and upload the files. The Cloud details are updated in the cloud inventory.
	Fetch config	A popup message, *Fetch config has been triggered for the device(s)* appears. The configuration is fetched from the device.
	Device Settings	Click to change the **Certificate details** section.

Access Control

Overview

Before you begin: To access this functionality, ensure that you have enabled the right ACF permissions under SSH+ by going to **Platform > Identity > Role > Authorized functions.**

With access control, you can access terminals to manage and monitor all the hosts on your network from a single platform to perform various tasks such as running scripts, executing commands, and troubleshooting issues.

You can access terminals using the **Open with Password** option if you know the password or click the **Name** hyperlink of the infra access group once you have been granted access to the group (See Requesting Access to Terminals).

Requesting Access to Terminals

To request access to terminal:

1. Go to (**Menu**) **> SSH+ > Access Control**.
   The **Terminal Access Control** page is displayed.
2. Click the **Name** hyperlink of the infra access group to which you want to request access.
   The access request form is displayed.
3. Enter the following fields:

Field description for Access Request section

Field	Description
***Access Mode**	Select one of the options: • **AppViewX Terminal:** Select this option if you are selecting only infra access group. • **Client:** Select this option if you have mapped infrastructure access group to a client or a set of client. The client are populated in the Device name box. You can search or select the ones you want access to. • **Unmanaged Clients:** Select this option to add devices outside of AppViewX. You can select between generating keys via AppViewX or uploading your own public keys thus ensuring secure and customized access to unmanaged clients. The download option has a disabled PEM format field and an optional password field when AppViewX is selected for key generation. The signed keys are downloadable as a PEM file from the Infra Access Group inventory as long as the access request is valid. AppViewX signs the user-uploaded key with a certificate validity for the requested access duration. The user can choose to protect the downloaded keys (zip file) with a password or leave them unprotected. The download option is disabled when the PEM format field without a password for the upload key is selected.
***Application Infra Name**	This is the infra access group for which you are requesting access. This is a non-editable field.

Field	Description
Available Host(s)/ Available Client(s)	This field is displayed on selecting the **Client** option. Select one or more hosts/ client from the section. Click the **Refresh** icon to see the latest list.
***Access Duration**	You can key in a value in the text field after selecting **Hours** or **Days** option from the dropdown list. Maximum hours cannot exceed 23. **Note:** The access duration kicks in from the time the administrator grants access to the time requested. Once the access duration elapses, the access is revoked.
Comments	Enter the reason you want access to the infra access group.
Note: Fields indicated with red asterisk (*) symbol are mandatory.	

4. Click **Request Access.**
   A message, *Your access request was sent successfully for approval; once request is approved, you can access SSH terminal* appears. The Access Status changes to *Pending Approval.* Once the administrator approves the request, the Access Status changes to *Accessible*. If the access request is rejected, then the Access Status changes to *Access Denied.*

What to do next

You can directly access the terminal by clicking the **Name** hyperlink of the infra access group. See Accessing Host Terminals.

Viewing Terminal Access Control Page

To request access to terminal:

Go to (**Menu**) **> SSH+ > Access Control**.
The **Terminal Access Control** page is displayed.

Field description for Terminal Access Control page

Field	Description
Name	Displays the name of the infra access group.

Field	Description
Host(s) Count	Displays the count of the hosts associated with the infra access group.
Access Status	Displays the access status of the infra access group: • **N/A:** Initial status when you do not have access to the group. • **Pending Approval:** Status when you have sent the access request and are awaiting approval form the administrator. • **Accessible:** Status when the administrator grants access to the group. • **Access Denied:** Status when the administrator rejects access to the group. • **Expired:** Status once your access to the group is expired for the requested duration. You can request access for the same group again by raising an access request. • **Failed:** Status when the access request fails for some reason. You can try raising the access request once more.
Access Mode	Displays the access mode for the terminal: • AppViewX Terminal • Client • Unmanaged Clients
Logs	Click **View** to open the log. The log displays details about the user who has access to the infra access group, access mode (whether SSH if it was accessed after granting approval or credential if password was used to access the terminal), status (whether access is active or expired), when the access request was initiated, when the access was terminated, and for how long the access was granted. You can export the logs in .CSV or PDF format.

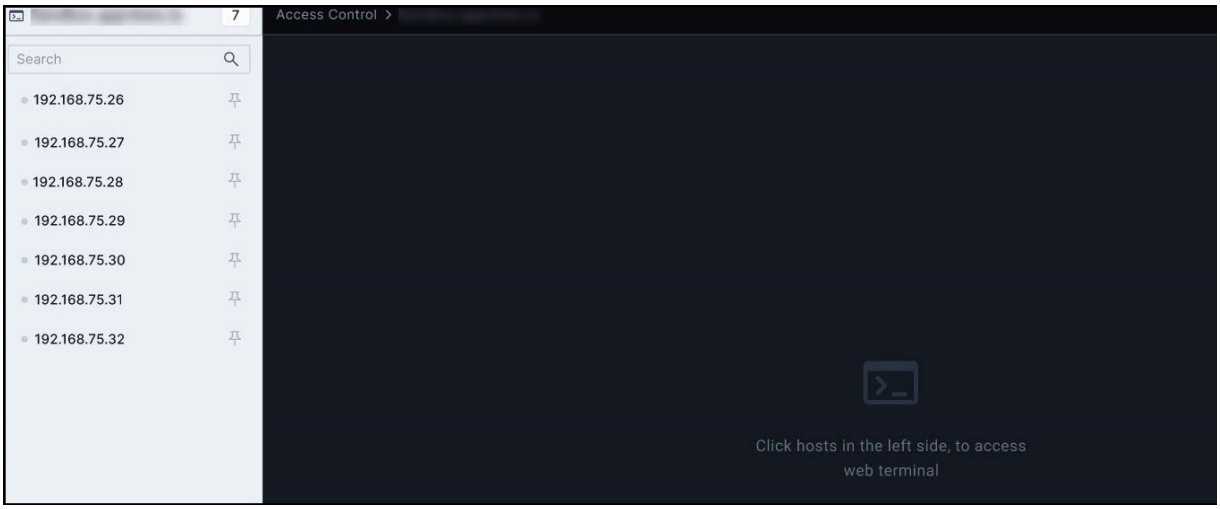
Accessing Host Terminals

You can access the host terminals in any of the following ways:

- If you have the password to the infra access server, then click the **Open with Password** option on the **Access Request** page.
- If you do not have the password to the infra access server, then request access as described in Requesting Access to Terminals. Once access is granted, you can:
  - Click the **Name** hyperlink of the infra access group.
  - Access the terminals from the **Device Management** page or the **Host Inventory** page by clicking the  (**Terminal Connect**) icon.

To access the host terminal:

1. Go to (**Menu**) **> SSH+ > Access Control**.
   The **Terminal Access Control** page is displayed.
2. Click the **Name** hyperlink of the infra access group.
   The terminal page opens with all the associated hosts as shown.



3. Click any of the hosts to access the web terminal.
4. Enter your credentials.
   You can now perform various tasks such as running scripts, executing commands, and troubleshooting issues.

Note:

- You can access more than one host at a time within each infra access group. On selecting multiple hosts, the hosts open in the split screen view. You can alternate between split or tab view by clicking using () icon on the RHS of the page.
- You can pin only four terminals for better access and management using the (**Pin**) icon.

Adding Infra Access Groups

Infra Access Group

- Creating an access group lets you enable access to a user or a group of users to all the hosts in the access group with a single instruction/selection.
- A host can be associated with one or more access groups. A host can remain unassociated with an access group as well.
- You can create an Infra Access Group by two different methods:
  - Auto-create during the cloud host scan

    Auto-created access groups are created automatically by reading the AWS tags of the host during cloud host discovery. The system forms the groups dynamically based on these AWS tags. The cloud host discovery does a periodic scan. The system detects any tag change that may occur due to an action on the device. This change could be due to some action performed by the cloud administrator. Once the system identifies the change in tags of the host, it switches the host to the Infra Access Group of the host based on its new tag. The system also ensures withdrawal of access that was provisioned to the host previously. If this change causes the device to associate with an existing auto-created access group, the other devices in the new access group are automatically provisioned with access to this device.

  - Manually created through the Infra Access Group tab

    Manually created access groups are just groups and do not have the above-mentioned intelligence. It is meant to create access group on-premises devices as well. See Adding Infra Access Group.

Adding Infra Access Group

Before you begin: To access this functionality, ensure that you have enabled the right ACF permissions under SSH+ by going to **Platform > Identity > Role > Authorized functions.**

To add an infra access group:

1. Go to (**Menu**) **> SSH+ > Groups > Infra Access Group**.

   The **Infra Access Group** page is displayed.

2. On the command bar, click **+Add New Groups**.

   The **Infra Access Group > Create** page is displayed.

3. In the **General Information** section, enter the following:

   Field description for General Information section

Field	Description
***Group Name**	Enter a unique name.
Description	Enter details regarding the group stating the purpose.
Managed Devices/ Instances	Select the managed devices/instances to be associated with the group.
Client	Select the clients to be associated with the group.

   Note: Fields indicated with red asterisk (*) symbol are mandatory.

4. Click **Create**.

   An Infra Access Group is created and displayed in the inventory.

5. Click the number displayed in the **Associated Machine Count** column.

   The popup window displays the **List of Devices** associated with the machine.

What to do next:

Modify or delete an infra user group by selecting the checkbox against the group name and selecting **Modify** or **Delete** from the **Actions** menu.

Managing Host Key and User Key Inventories

Overview

Before you begin: To access this functionality, ensure that you have enabled the right ACF permissions under SSH+ by going to **Platform > Identity > Role > Authorized functions.**

SSH uses SSH keys to encrypt communicate with a remote system. SSH keys usually come in pairs comprising a public and a private key and are used to grant access to authorized personnel to critical systems such as cloud, on-premise servers, and network devices. The public key (or host key) can be freely shared and is used to encrypt data sent to remote server or user; the private key (or user key) must only be with the user and be kept secret as it is used to decrypt data sent from remote server or user. It is generated by the local machine and kept in a secure location

This chapter guides you through all the actions that can be carried out on the keys. Actions on keys such as deletion, status change, export, and upload of keys are possible.

From the **Inventory** page, you can:

- View details of the user key and host key. See Viewing User/Host Key Inventory.
- Delete, change status, export, upload user key or host key. See Actions in Key Inventory.
- Discover and add hosts to the host inventory. See Adding Host.
- View details of the hosts. See Viewing Host Inventory.
- Decommission inactive hosts or delete active hosts, add credentials to the host server, fetch host key from the host inventory, and export details of the host to a .csv or .xls format. See Actions in Host Inventory.

Key Inventory

The keys inventory displays the details about the keys. You can also perform various actions on the keys by selecting them from the **Actions** dropdown list. Selecting any action directs you to the respective action page under the **Action** section.

The **User Key Inventory** page displays:

- Key Pair with Passphrase indicated by ()
- Key Pair without Passphrase indicated by ()
- Public Key Only indicated by ()
- Private Key Only indicated by ()

The **Host Key Inventory** page displays:

- Active hosts indicated by green. These hosts can be deleted.
- Inactive hosts indicated by red. These hosts can be decommissioned.

- Viewing User/Host Key Inventory
- Actions in Key Inventory

Viewing User/Host Key Inventory

The User/Host Keys tab displays the total number of weak, shared, orphan, and suspicious keys in the key discovery status. Click the number hyperlink to drill down on the metrics. This helps you track the progress of the key discovery efforts, identify any potential security risks, and prioritize the remediation actions.

To view the user/host key inventory:

1. Go to  (**Menu**) **> SSH+ > Inventory > Key Inventory**.
2. Select **User Key Inventory** or **Host Key Inventory**.

   The **SSH+::User Key** page is displayed.

Field Description in user/Key Inventory

Field	Description
Key name	Displays the name of the key.
Associated Users	This field is applicable only for the user key. Displays the users associated with the key.
Client Endpoint(s)	Displays the count of client machines associated with the key.

Field	Description
	You can view the list of the hosts associated with the key as a client machine.
Host Endpoint(s)	Displays the count of host machines associated with the key. You can view the list of the hosts associated with the key as a host machine.
Age	Displays the age of the key. For example, if the key was created 5 days earlier, it displays as *5 Days*.
Fingerprint	Displays the fingerprint of the key.
Encryption	This field is applicable only for the user key. Displays the encryption type of the key.
Length	Displays the bit-length of the key.
File Path(s)	Displays the file path of the key inventory.
Risk Status	Displays the status of the key as weak, shared, orphan, or suspicious.
Comment	Displays any comments with regards to the key.
Group	Displays the name of the group associated with the key.
Certificate Count	Displays the number of certificates associated with the key. Click the hyperlink to see a popup window with the following fields: • **Principals**: Displays SSH certificate attribute. • **CA name**: Displays the CA name associated with the key. • **Serial Number**: Displays the serial number of the key. • **Certificate Status**: Displays the certificate status of the key. • **Valid From**: Displays the start date of the key validity. • **Valid To**: Displays the end date of the key validity. • **Expires In**: Displays how long before the key expires. • **Extensions**: Displays the extensions of the key.
Status	Displays the status of the key. The statuses are:

Field	Description
	• Managed • Monitored
Key Validity	Displays the validity of the key.

Actions in Key Inventory

You can perform the following actions from the **Key Inventory** page.

Action description on Key Inventory page

Action	Description
Change status	You can change the status of a key to **Managed** or **Monitored**.
Export	You can export the user or host key from their respective inventory in .csv or .xls format.
Upload User SSH key	**Note:** This field appears only for User Key Inventory. **Field description for Upload SSH key section** **Field** / **Description** ***Key File** — Click **Search** icon to browse for the file. ***Key Group** — Select key group from the dropdown list. **Note:** A key is associated with a key group that is associated with a policy. Based on the selection of the key group, it is decided if the key needs a work order approval. The key is also checked for compliance with the key policy associated with the **Key Group**. ***Key Name** — Enter a unique name for the key. This helps you identify it easily. **Passphrase** — Enter a passphrase

Action description on Key Inventory page (continued)

<table>
<tr><th>Action</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Confirm Passphrase</td><td>Enter the passphrase again to confirm.</td></tr>
<tr><td>*Validity</td><td>Select validity from the dropdown list. This determines the duration for which the key is valid.</td></tr>
<tr><td>Comment</td><td>Enter remarks specific to the key.</td></tr>
</table>
Note: Fields indicated with red asterisk (*) symbol are mandatory.
</td></tr>
<tr><td>Revoke</td><td>Note: This field appears only for User Key Inventory.

You can only revoke certificates that are associated with keys that have a private key and key pair (public + private). If the selection has even one key that is a public key, then revoke is disabled.</td></tr>
<tr><td>Rotate</td><td>You can rotate any type of key from hosts with multiple keys through the user and host key age report thus mitigating service disruptions.

Note: Rotating keys can result in access loss and authentication problems. Proceed with caution and ensure proper backup and alternative authentication methods are in place.
The selected keys are rotated according to the rotation configuration specified in the respective key policies.</td></tr>
<tr><td>Delete</td><td>You can:</td></tr>
</table>

Action description on Key Inventory page (continued)

Action	Description
	• **Delete from Inventory:** Deletes the keys from the AppViewX inventory and not the actual hosts. • **Delete from Endpoints:** Deletes the keys from the host endpoints. **Note:** If you try deleting keys from hosts with only one key, then a warning message about the potential service disruption is displayed.

Risk Dashboard

Reports

The dashboard provides several components that track SSH traffic and log interaction with devices. You can use this dashboard to look at the risks associated with SSH and their severity. This dashboard provides detailed information identifying critical and high device risks for administrators to mitigate and secure before management of a device is compromised.

Risk Report

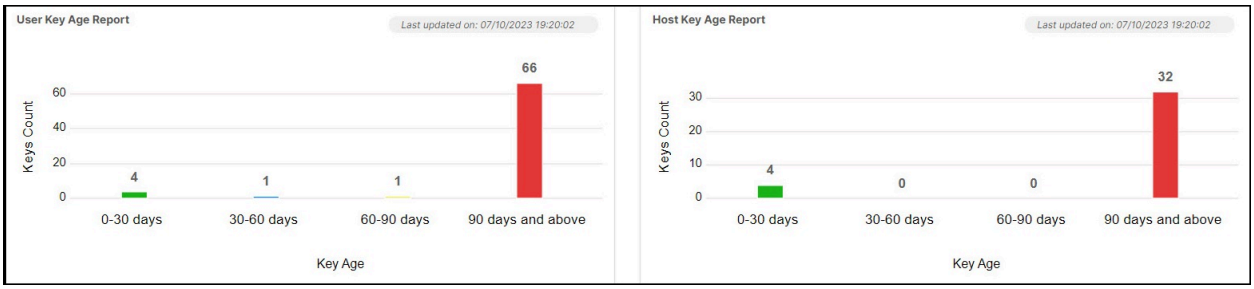
The Risk Report provides information about risks from the discovery of the default branch. It contains cumulative results of successful discovery.

Click the **Count** hyperlink to fetch more details such as key name, group, length, age, encryption and so on based on the key type.

You can identify and remediate weak, shared, suspicious, and orphan host/user keys from the dashboard to keep the infrastructure secure. To perform remediation actions, see Remediation Actions. For description of keys, see Glossary.

Key Age Reports

Displays the following reports in a bar chart:



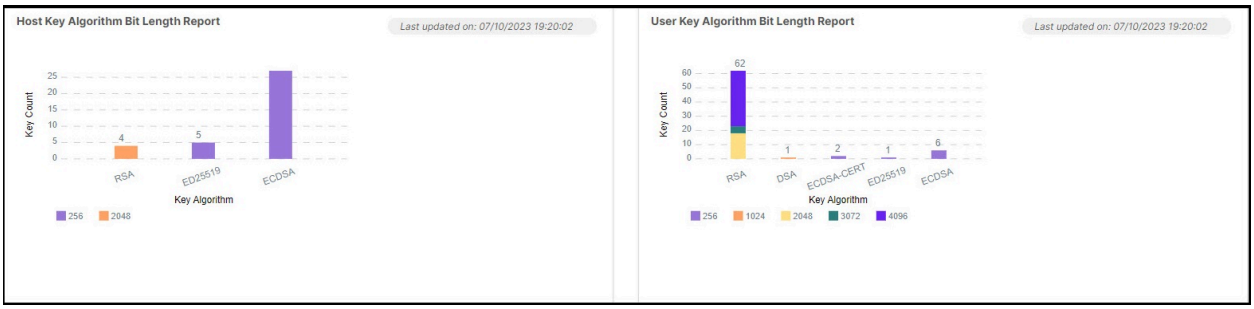
- **User Key Age Report:** A bar chart displaying the groupwise number of keys (y-axis) based on the following user key age (x-axis):
  - 0 to 30 days
  - 30 to 60 days
  - 60 to 90 days
  - 90 days and above
- **Host Key Age Report:** A bar chart displaying the groupwise number of keys (y-axis) based on the following host key age (x-axis):
  - 0 to 30 days
  - 30 to 60 days
  - 60 to 90 days
  - 90 days and above

Click the graph on the widget to fetch details of the client endpoints, host endpoints, associated users, key name, and the group.

You can also rotate and delete keys from hosts with multiple keys through the user and host key age report thus mitigating service disruptions.

Key Algorithm Bit Length Reports

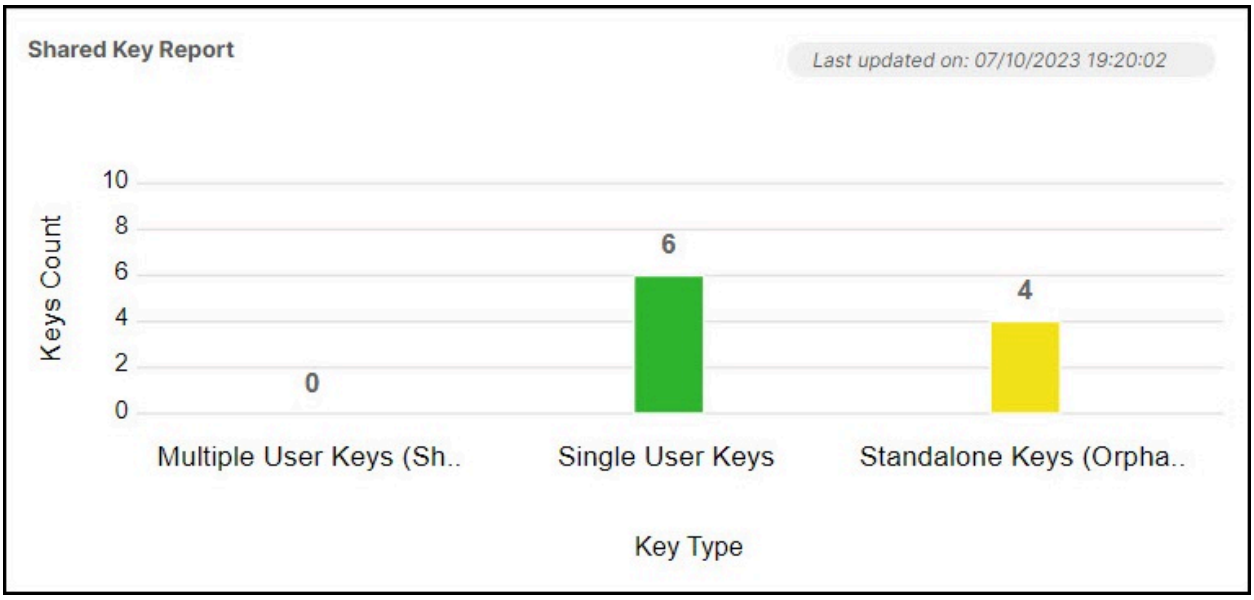
Displays a stacked bar chart to filter keys based on key bit length and key algorithm:



- **User Key Algorithm Bit Length Report:** A stacked bar chart displaying the groupwise number of key size (y-axis) based on the user key size and algorithm (x-axis). The user key sizes are 256, 384, 521, 1024, 2048, 3072, 4096 while the key algorithms are RSA, DSA, RSA1, ED25519, ECDSA.
- **Host Key Algorithm Bit Length Report:** A stacked bar chart displaying the groupwise number of key size (y-axis) based on the host key size and algorithm (x-axis). The host key sizes are 256 and 2048 while the key algorithms are RSA, ED25519, ECDSA.

Shared Key Report

Displays the key count (y-axis) based on the following key type (x-axis) as a bar chart.

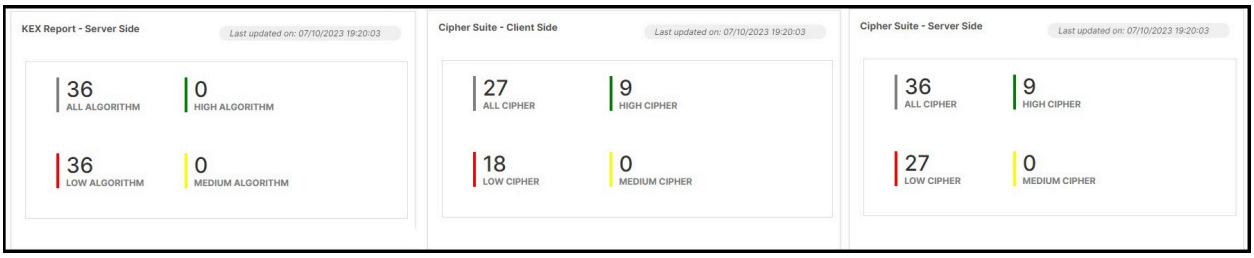


- **Multiple User Keys (Shared):** The number keys that are associated with multiple users and in the key group.
- **Single User Keys:** The number keys that are associated with a single user and in the key group.
- **Standalone Keys (Orphan):** The number of keys on standalone machines associated with the key group.

Click the graph on the widget to fetch details of the client endpoints, host endpoints, associated users, key name, and the group.

Server-Side Reports

Displays the following reports:

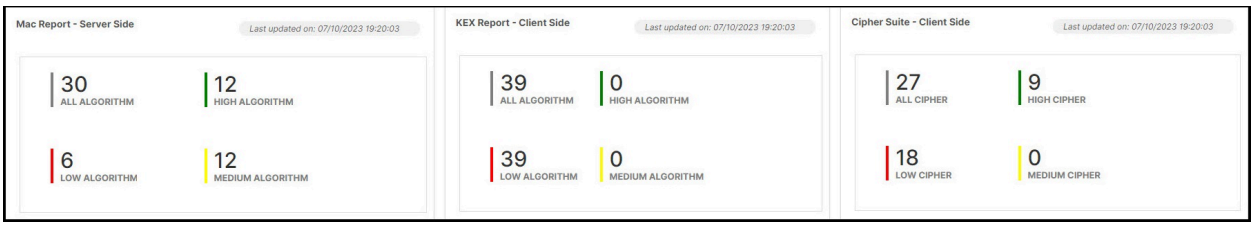


- **Cipher suite report:** This report provides the following numerical representation of All Cipher, High Cipher, Low Cipher, and Medium Cipher in the widget.
- **KEX report:** This report provides the following numerical representation of All Algorithm, High Algorithm, Low Algorithm, and Medium Algorithm in the widget.
- **Mac report:** This report provides the following numerical representation of All Algorithm, High Algorithm, Low Algorithm, and Medium Algorithm in the widget.

Hover the mouse over the numbers and click it to fetch details of the host name, IP address/FQDN, algorithm, OS type, version, and group.

Client-Side Reports

Displays the following reports:



- **Cipher suite report:** This report provides the following numerical representation of All Cipher, High Cipher, Low Cipher, and Medium Cipher in the widget.
- **KEX report:** This report provides the following numerical representation of All Algorithm, High Algorithm, Low Algorithm, and Medium Algorithm in the widget.
- **Mac report:** This report provides the following numerical representation of All Algorithm, High Algorithm, Low Algorithm, and Medium Algorithm in the widget.

Hover the mouse over the numbers and click it to fetch details of the host name, IP address/FQDN, algorithm, OS type, version, and group.

Actions

- Click **Export** to export the details to .csv or .xls format.
- Click **View in Inventory** to view the inventory listing of the categories on that page.

Remediation Actions

Before you begin: To access this functionality, ensure that you have enabled the right ACF permissions under SSH+ by going to **Platform > Identity > Role > Authorized functions.**

You can identify and remediate weak, shared, suspicious, and orphan host/user keys from the dashboard to keep the infrastructure secure.

1. Go to  (**Menu**) **> SSH+ > Dashboard**.
   The **Dashboard** page is displayed.
2. On the **Risk Report,** click **Remediation Option** against the host/user key category.
   A popup window of the selected host/user key is displayed along the details of the key name, host endpoints, associated users, and file path.
3. Click the checkbox against the key(s) you want to remediate.
4. You can perform one of the following actions:
   a. **Rotate:** The selected keys are regenerated and pushed to the host endpoints.
   b. **Delete:** The selected keys are deleted from the host endpoints and key inventory.
   c. **Acknowledge:** The selected keys are acknowledged and excluded from the risk report for the duration specified in the associated key policy. The keys, however, continue to be present in the key inventory.
   Selecting any of the actions opens a confirmation window.
5. Click **Confirm** to proceed.

Creating Key Policy and Group

Overview

Before you begin: To access this functionality, ensure that you have enabled the right ACF permissions under SSH+ by going to **Platform > Identity > Role > Authorized functions.**

Policy is configured to define the attributes of a key to belong to the key group. A key is compliant only if it matches the attributes defined in the associated policy.

From the **Policies** page, you can add, modify, or delete a key policy. See Creating Key Policy.

You can bring together keys under a key group. A key can be part of only one group associated with a policy (key policy for the key group). This group to policy association can be done from the key inventory or from the policy create/edit page. By default, the system has a default key group to accommodate all keys that are not manually associated with any other group. See Adding Key Compliance Group.

Key Policy

The key policy plays an important part while generating an SSH key. If the key is associated with a key policy that requires an approval and implementation of the work order of the actions initiated on the key, then you have to continue the process of key creation in the holistic view. You can set the key to rotate automatically while creating the policy.

Compliance check for a group is triggered if a key is added or deleted from the key group. Compliance check for keys and key rotation are also triggered based on the new key group.

You cannot delete the default key policy, but you have the option to change the settings. The default policy is associated with all the key groups.

Note: You can associate a particular policy with a single key group or multiple key groups. The key configuration is based on the associated policy. The discovered keys are checked for compliance against the policy associated with them. The system marks the key as non-compliant in the inventory if the compliance check fails.

Creating Key Policy

To create a key policy:

1. Go to  (**Menu**) **> SSH+ > Policies > Key Policy**.

   The **Key Policy** page is displayed.
2. On the command bar, click **+Create policy**.
3. Enter the following details:

Field description for Key Policy section

Field	Description
Policy details	
***Policy Name**	Enter a unique name for the policy.
Description	Enter details of the policy stating the purpose.
Compliance Configuration	
***Key Algorithm**	Select a value from the dropdown list. You can select more than one value.
***Key Size**	Select a value from the dropdown list. You can select more than one value.
Rotation Configuration	
***Key Rotation Period**	Select a value from the dropdown list.
***Key Algorithm**	Select a value from the dropdown list.
***Key Size**	Select a value from the dropdown list.
Note: Fields indicated with red asterisk (*) symbol are mandatory.	

4. Click **Create**.

   A key policy is created and added to the key inventory.

What to do next:

- Modify or delete a key policy by selecting the checkbox against the policy name and selecting **Modify** or **Delete** from the **Actions** menu.
- Associate the policy with a key compliance group. See Adding Key Compliance Group.

Key Compliance Group

By default, all the LDAP users are mapped to the Default Requestor group. A user can be associated with a single user group. Whenever a requestor is added to a group, a compliance check is triggered to check if the key is compliant or not.

Adding Key Compliance Group

To add a key compliance group:

1. Go to (**Menu**) **> SSH+ > Groups > Key Compliance Group**.

   The **Key Compliance Group** page is displayed.

2. On the command bar, click **+Add New Groups**.

   The **Key Compliance Group > Create** page is displayed.

3. In the **General Information** section, enter the following:

   Field description for General Information section

Field	Description
***Group Name**	Enter a unique name. This helps you identify it easily.
Description	Enter details regarding the group stating the purpose.
***Requestor**	Select the requestor(s) to be associated with the group.
***Requestor Policy**	Select the required policy to be associated with the requestor group.

Note: Fields indicated with red asterisk (*) symbol are mandatory.

4. Click **Create**.

   A key compliance group is created and displayed in the inventory.

What to do next:

- Modify or delete a key compliance group by selecting the checkbox against the group name and selecting **Modify** or **Delete** from the **Actions** menu.

Glossary

Term definition

Term	Definition
SSH	Secure Socket Shell (SSH), also known as simply Secure Shell, is a cryptographic protocol used to enable secure access to remote servers and devices over the internet using SSH keys.
Host key	A host key is a key that is used to identify the server. It is generated by the server and shared with the client during the initial connection setup. The client uses this key to verify the identity of the server before establishing a connection.
Public key	A public key is used to encrypt data and verify digital signatures. It can be freely distributed, and anyone can use it to encrypt data or verify digital signatures. It is also used to establish a secure connection between the client and the server.
Private key	A private key is a secret key that is used to decrypt data and create digital signatures. It must be kept secret and never shared with anyone. The private key is used to authenticate the user and establish a secure connection with the server.
Suspicious key	A key that is found in non-standard location without a server side. Suspicious keys are discovered only when the **Scan Type** is selected as **Full**.
Shared key	A key found on more than one client machine.
Orphan key	A key found on server without a client side.
SSH key	SSH keys are used to encrypt communicate with a remote system. SSH keys usually come in pairs comprising a public and a private key and are used to grant access to authorized personnel to critical systems such as cloud, on-premise servers, and network devices.
SSH key rotation	The process of changing the cryptographic keys used for secure communication between two devices, such as a client and a server.
User key	A user key is a public key that is associated with a particular user account on the server. It is used to authenticate the user and establish a secure connection with the server.

Term definition (continued)

Term	Definition
Weak user key	A key that is weakened over a period of time or because of inferior key algorithm or size.
Weak host key	A key that is weakened over a period of time or because of inferior key algorithm or size.