



CA PAM START

Installation and User Guide

Version 1.8

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Table of Contents

Introduction	4
Installation	4
System Requirements	4
Install in 3 Easy Steps	5
User Interface	6
CA-PAM-START Main Tab	6
Scan Status Tab	7
Reports	8
Report Dashboard	8
Detailed Reports	9
CA PAM START Configuration	10
CA-PAM-START.props file	10
Command Line Execution	13
Appendix A: Release Information	14
New Features and Enhancements in 1.8	14
New Features and Enhancements in 1.7	14
New Features and Enhancements in 1.6	14
New Features and Enhancements in 1.5	14

Introduction

CA PAM START (Standalone Access Reporting Tool) is a lightweight remote scanning tool, aimed at helping security professionals locate and understand potential security risks and vulnerabilities in their environments, leading them towards Symantec PAM (Privileged Access Manager) as the ultimate security solution.

The tool supports the scanning of Linux, Windows and Active Directory hosts and provides the scan result in a report. The scan provides account information such as privileged accounts, inactive, expired accounts and certain types of vulnerable accounts and on Linux machines, the scan provides additional information on SSH certificates such as SSH key pairs, orphaned keys, key age, weak keys and trust relationships.

Installation

System Requirements

You can install CA PAM START on:

- Windows
- Linux

The minimum memory should have at least 2 GB.

For best viewing experience, a screen resolution of 1920 x 1080 is recommended.

Install in 3 Easy Steps

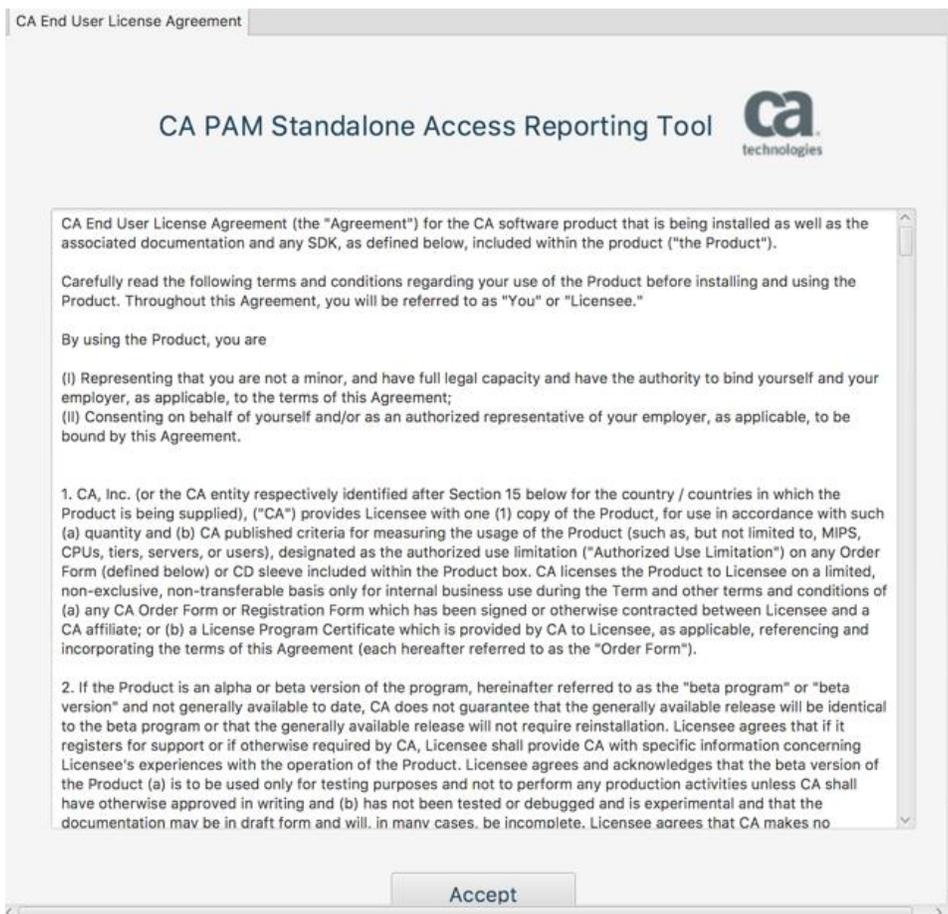
1. Download the PAM-START package for your operating system and extract it to your desired directory.

Operating System	Extract the package
Windows	Right click on the package and select Extract All from the context menu.
Linux	In the terminal window, run this command: tar zxvf CA-PAM-START-1.7-linux-x64.tar.gz

2. In the bin directory within CA-PAM-START, run the script for your operating system.

Operating System	Run the application
Windows	run-CA-PAM-START.cmd
Linux	run-CA-PAM-START.sh

3. Review the licensing agreement and click Accept if you agree.



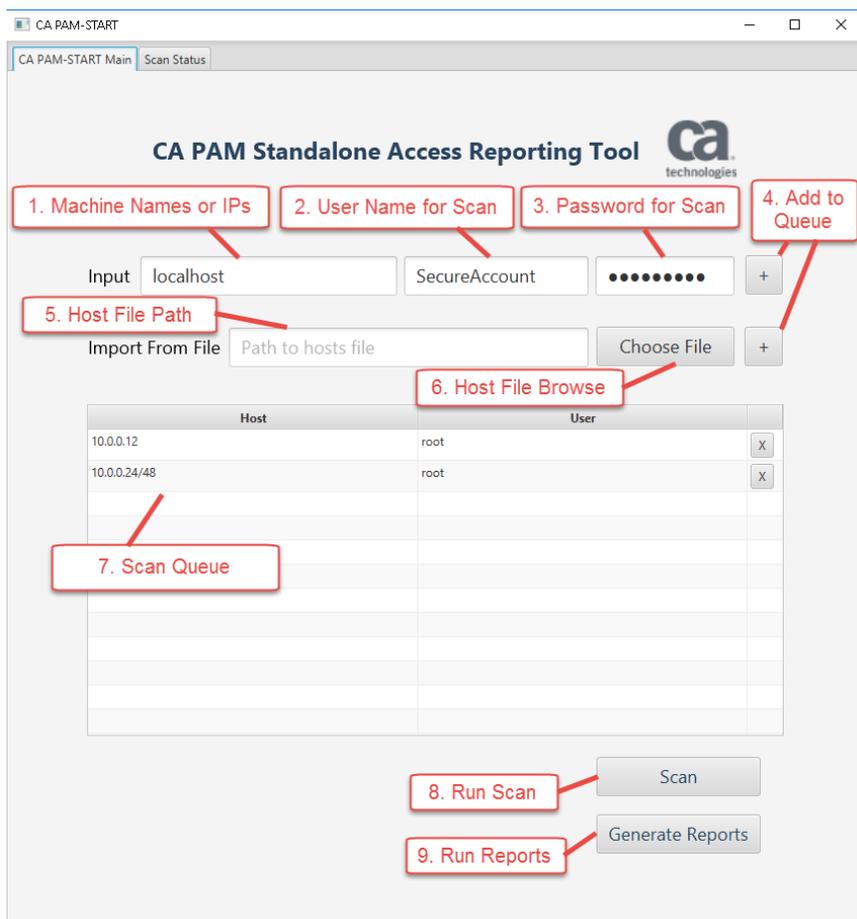
4. You are now up and running with CA PAM START.

User Interface

Here is how you use CA PAM START.

1. Specify the host(s) to scan by either entering the information for each host manually or import them from a file and add them to the scan queue. An example host file can be found in the **CA-PAM-START\example** folder.
2. Start the scan.
3. View the reports.

CA-PAM-START Main Tab



Machine Names or IPs: Enter the hostname or IP address of the machine to scan. A range of IP addresses is also supported. The format can either be in CIDR (Classless Inter-Domain Routing) format such as **192.168.1.0/24** to represent 256 IP addresses from 192.168.1.0 to 192.168.1.255. or simply provide the starting and ending address such as **192.168.1.0-192.168.1.255**.

To scan Active Directory, enter the hostname in this format: **<hostname>:<port>**.

User Name for Scan: Enter a user account with necessary permissions to perform scan on specified machine(s).

To scan an Active Directory domain, enter the connection string for the AD domain admin user credential such as **CN=Administrator,CN=Users,dc=mydomain,dc=com**.

To scan local Windows accounts, enter a local Windows administrator account such as **Administrator**.

To scan Linux accounts, enter a Linux user with root privileges such as **root**.

Password for Scan: Enter the password for the specified user account.

If you want to encrypt the password for security purposes, you can use the utility provided in the **password_encryption_tool** directory. See the README.txt in that directory for more information.

Add to queue: Click the + button to add the host to scan into the scan queue in the table below. The queue processes multiple scan requests in a single scan job. This allows individual user accounts to be provided against individual machines or network IP segments.

Host File Path: Enter the path to any pre-populated host file you might have available. A sample host file is provided in the install directory in the example directory.

Host File Browse: Click this button to browse for the pre-populated hosts file on your local file system.

Scan Queue: The queue displays all scan requests that have been submitted by clicking the plus buttons above. The individual scan requests are placed into this queue and the system processes all scan requests in a batch job.

Run Scan: Click this button to execute the scan job and run all the scan requests that are placed into the scan queue.

Run Reports: Once the scan job has completed, click the Generate Reports button to launch the report set for the completed scan.

Scan Status Tab



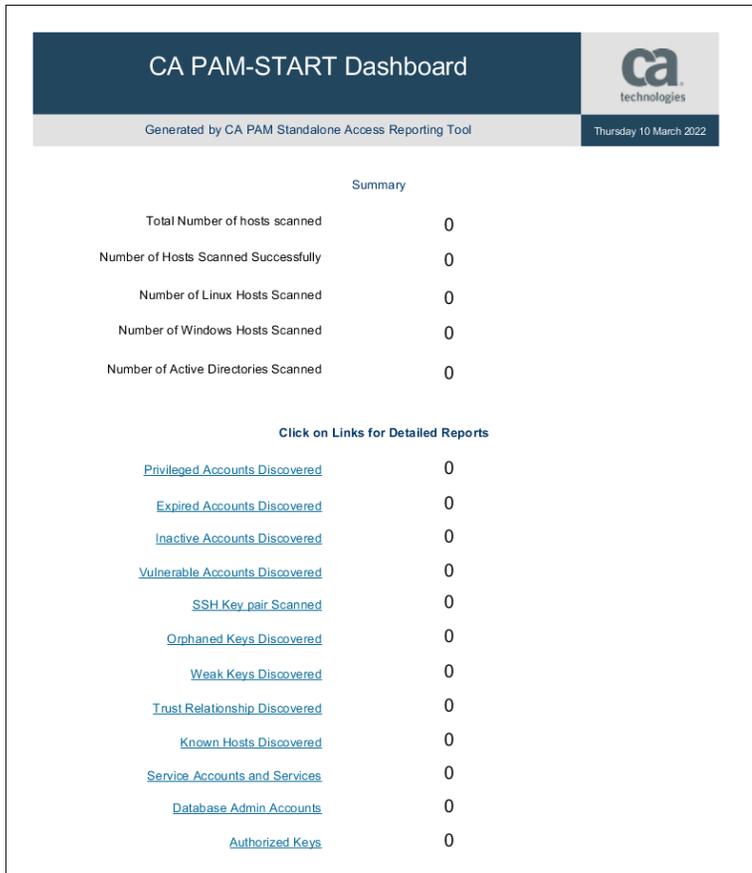
Scan Job Status: Scan Status tabs are generated for each Scan Job executed showing real-time scanning progress.

Scan Job Results: Scan job results allow you to monitor the progress of the scan. Ensure the scan has completed successfully before running the Generate Reports button in the CA-PAM-START Main tab.

Reports

Report Dashboard

The Report Dashboard provides a summary of the scan results.



The screenshot shows the CA PAM-START Dashboard. The header includes the title "CA PAM-START Dashboard" and the CA Technologies logo. Below the header, it states "Generated by CA PAM Standalone Access Reporting Tool" and the date "Thursday 10 March 2022".

The main content area is titled "Summary" and contains the following data:

Total Number of hosts scanned	0
Number of Hosts Scanned Successfully	0
Number of Linux Hosts Scanned	0
Number of Windows Hosts Scanned	0
Number of Active Directories Scanned	0

Below the summary, there is a section titled "Click on Links for Detailed Reports" with the following hyperlinks and counts:

Privileged Accounts Discovered	0
Expired Accounts Discovered	0
Inactive Accounts Discovered	0
Vulnerable Accounts Discovered	0
SSH Key pair Scanned	0
Orphaned Keys Discovered	0
Weak Keys Discovered	0
Trust Relationship Discovered	0
Known Hosts Discovered	0
Service Accounts and Services	0
Database Admin Accounts	0
Authorized Keys	0

In the Detailed Reports section, you can view the detailed report of the scan for each specific area by clicking the hyperlink for the individual report.

Here is a sample Expired User Report.



The screenshot shows a browser window displaying the "Expired User Report". The title is "Expired User Report" and the subtitle is "List of expired users on your network". The report was generated by the CA PAM Standalone Access Reporting Tool on Friday 22 June 2018.

The report contains a table with the following data:

Host Name	User Account	Expiration Date
test01.ca.com	expireuser	2018-January-01

Detailed Reports

This table describes what kind of information is available in each detailed report.

Detailed Report	Description
Privileged Users	<p>Privileged Users are users who are members in the following groups that will be scanned by CA PAM START.</p> <p>WINDOWS:</p> <p>Windows local administrators</p> <p>AD: Administrators</p> <p>AD: Account Operators</p> <p>AD: Backup Operators</p> <p>AD: Print Operators</p> <p>AD: Server Operators</p> <p>AD: Cert Publishers</p> <p>AD: Domain Admins</p> <p>AD: Enterprise Admins</p> <p>AD: Schema Admins</p> <p>Linux: root wheel adm admin</p>
Expired Accounts	Expired accounts are users whose passwords have already expired.
Inactive Accounts	<p>Inactive accounts are users that have been inactive or not changed their password for a certain number of days. The default is 90 days.</p> <p>The default value can be changed by modifying the following attribute in the CA-PAM-START\conf\CA-PAM-START.props file.</p> <p>minimumNumberOfDaysForInactiveUser=90</p>
Vulnerable Accounts	These are Windows accounts that are vulnerable to the "Pass the Hash" attack.
SSH Key Pairs	These are public and private key pairs found in the common SSH locations. Note: for Linux hosts only.
Orphaned Keys	Orphaned keys are SSH keys where their public keys are not found with their private keys in the common SSH locations. Note: for Linux hosts only.
Weak Keys	Weak keys are SSH keys that are not encrypted with a passphrase. Note: for Linux hosts only.
Trust Relationships	SSH trust relationships discovered on target server.
Known Hosts	A list of hostnames defined in known_host files on Linux servers.
Service Accounts	Service accounts are defined as Windows Service and Linux process run-as users.
Database Accounts	Database admin accounts.
Authorized Keys	Authorized keys and their private keys.

CA PAM START Configuration

CA-PAM-START.props file

This feature provides the ability to configure a number of options for scanning SSH private, public and authorized keys in the **conf/CA-PAM-START.props** configuration file. These options are **global settings** and they apply to all the hosts in the scan.

This section of the CA-PAM-START.props contains properties for the task pool and should not be changed.

```
#task queue related properties
acquireIncrement=10
initialPoolSize=10
maxPoolSize=50
minPoolSize=10
maxStatements=128
queueSize=100000
```

This section of the CA-PAM-START.props file allows specification of an SSH key to use to run scans on Linux servers and is an alternative to providing per server user name and password. It also contains PowerShell parameters and an inactive days parameter for the Inactive Users Report.

```
#specify the SSH key you will use to access linux servers. Put the absolute path
#to the private key file here. Add the public key to the targeted Linux server
#openSSH key format only
privateKeyFile=c:\\keys\\mykey.ppk
privateKeyPassphrase=RGGzPRuofZVoFZ3WSV5e/XjfMg==
minimumNumberOfDaysForInactiveUser=90
powershellPath=C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
# Maximum time before powershell scan times out in seconds
maxPSScanTimeout=180
```

#The following items have NOT yet been implemented for the current version:

This section of the CA-PAM-START.props file contains parameters that allow for the definition of scanning locations to scan in addition to the default locations.

```
#Use commas to separate multiple values
additionalDirectoriesToScanForSshKeys=
#Additional AD groups (sAmAccountName) to scan separated by commas
additionalADGroupsToScanForPrivUsers=
#Additional Linux groups to scan separated by commas
additionalLinuxGroupsToScanForPrivUsers=
```

This section of the **CA-PAM-START.props** file allows for customization of SSH Key scanning.

```
# -----
# SSH Scanning.
```

```
# -----
# Specifies whether SSH key scanning should include the known_hosts file.
# Options are:
#     Y - scan for known_hosts file
#     N - scan is not performed for known_hosts file
scan_known_hosts_file=Y

# Specifies whether SSH key scanning should include private key file.
# Options are:
#     Y - scan private key file
#     N - skip private key file
scan_private_key_file=Y

# Specifies whether to search users residing in the loadable I&A module in
# addition to the local file on AIX platform.
# Options are:
#     Y - search users in the loadable I&A module
#     N - skip users in the loadable I&A module
scan_aix_ldap_users=Y

# Specifies the loadable I&A module used for searching AIX LDAP users.
aix_load_module=VAS

# Specifies whether scanning of SSH keys should include users residing on a NFS
# mount residing in the NFSDIR/{user}/.ssh directory.
# Options are:
#     Y - include users residing in the NFSDIR/{user}/.ssh directory
#     N - skip users residing on a NFS mount point
scan_nfs_directory=Y

# Specifies the NFS directory to scan for SSH keys.
nfs_directory=/export/rwdg

# Specifies whether scanning of SSH keys should include additional directory.
scan_include_directory=Y

# Specifies the location of an additional directory to scan for SSH keys.
include_directory=/etc/ssh/site

# Specifies whether scanning of SSH keys should skip symbolic links for private
# key files. It is a common practice to create symbolic links for private key
# files to identity and this might create more orphan keys. Hence, skipping
# these private key files can help to avoid some noises in the scan result.
# Options are:
#     Y - skip symbolic links for private key files
#     N - include symbolic links for private key files in the scanning
skip_symbolic_links=Y

# Specifies the list of users that should be excluded from the Authorized Keys
# report.
authorized_keys_filter='operator','aiuser','daemon','dhcpcserv','dladm','ftp','ike
user','lp','mysql','netadm','netcfg','noaccess','nobody','nobody4','openldap','pk
g5srv','smmsp','zfssnap','svctag','sys','unknown','webservd','xvm','bin','lpd'
```

This section of the **CA-PAM-START.props** file allows for specification of a custom SSH Key scanning script to use as an alternative to the built-in script. Note the WARNING.

```
# Specifies the absolute path of a custom script to use for scanning SSH keys.  
#  
# WARNING: Please be mindful with what you modify in the custom script. It is  
# important that the order and format of the data fields collected by the script  
# remains as it is as this is the manner the scan results are parsed and  
# deciphered.  
custom_sshkey_script=
```

Command Line Execution

CA PAM START can be executed from the command line. Running `run-CA-PAM-START.<cmd|sh>` with `--help` displays the help text below.

Symantec PAM Standalone Reporting Tool
Copyright 2014-2021 Broadcom, Inc. All rights reserved.

```
run-CA-PAM-START.<cmd|sh>
```

```
[--help]
```

```
[--conf=<START configuration file>]
```

```
[--show=true|false]
```

```
[--targets=<host configuration file>]
```

```
[--output=<csv file>]
```

`--help` Prints this help message.

`--conf` Specifies the file that contains the global configuration.

`--show` Shows the application when running in the command line mode.
Default is false.

`--targets` Specifies the file that contains a list of hosts and their configuration options to scan when running in the command line mode.

`--output` Specifies the csv file for storing the result of the SSH scanning when running in the command line mode.
Default is output.csv in the bin directory.

```
run-CA-PAM-START.cmd --targets=host_file.txt
```

```
run-CA-PAM-START.cmd --targets=host_file.txt --output=out.csv
```

```
run-CA-PAM-START.cmd --targets=host_file.txt --output=out.csv --show=true
```

A.1 Appendix A: Release Information

A.1.1 New Features and Enhancements in 1.8

A.1.1.1 Customize the Scanning of SSH Keys with Custom Scripts

In this release, a custom script can be used to customize the scanning of SSH keys for hosts in a specific target environment beyond the coverage provided by the default scanning script.

A.1.2 New Features and Enhancements in 1.7

A.1.2.1 AIX Scanning

This feature added support for scanning AIX hosts.

A.1.2.2 Command Line Support

This feature enables the scanning tool to perform the scanning from the command line in addition to the interactive graphical user interface. As a result, the scanning can now be automated by embedding the scan tool into the organization's dev ops operations.

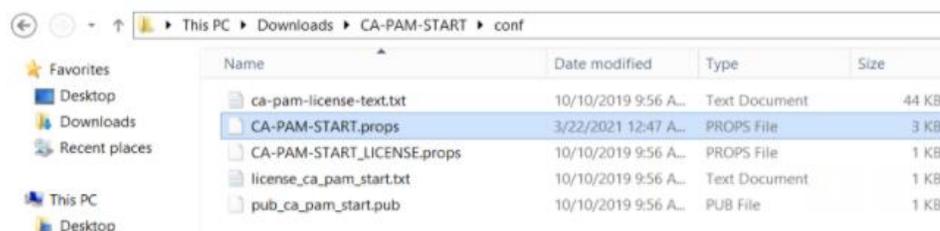
A.1.3 New Features and Enhancements in 1.6

Bug fixes

A.1.4 New Features and Enhancements in 1.5

A.1.4.1 Customize the Scanning of SSH Keys

This feature provides the ability to configure a number of options for scanning SSH private, public and authorized keys in the **conf/CA-PAM-START.props** configuration file. These options are **global settings** and they apply to all the hosts in the scan.



```

# -----
# SSH Scanning.
# -----
# Specifies whether SSH key scanning should include the known_hosts file.
# Options are:
#   Y - scan for known_hosts file
#   N - scan is not performed for known_hosts file
scan_known_hosts_file=Y

# Specifies whether SSH key scanning should include private key file.
# Options are:
#   Y - scan private key file
#   N - skip private key file
scan_private_key_file=Y

# Specifies whether to search users residing in the loadable I&A module in
# addition to the local file on AIX platform.
# Options are:
#   Y - search users in the loadable I&A module
#   N - skip users in the loadable I&A module
scan_aix_ldap_users=Y

# Specifies the loadable I&A module used for searching AIX LDAP users.
aix_load_module=VAS

# Specifies whether scanning of SSH keys should include users residing on a NFS
# mount residing in the NFSDIR/{user}/.ssh directory.
# Options are:
#   Y - include users residing in the NFSDIR/{user}/.ssh directory
#   N - skip users residing on a NFS mount point
scan_nfs_directory=Y

# Specifies the NFS directory to scan for SSH keys.
nfs_directory=/export/rwdg

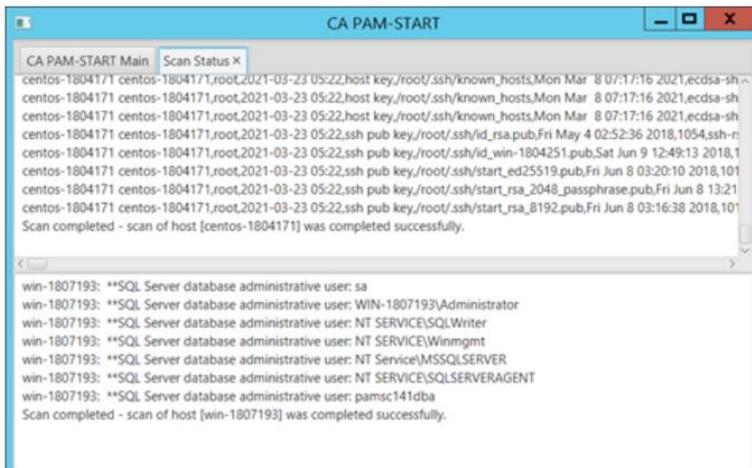
# Specifies whether scanning of SSH keys should include additional directory.
scan_include_directory=Y

# Specifies the location of an additional directory to scan for SSH keys.
include_directory=/etc/ssh/site

# Specifies whether scanning of SSH keys should skip symbolic links for private
# key files. It is a common practice to create symbolic links for private key
# files to identity and this might create more orphan keys. Hence, skipping
# these private key files can help to avoid some noises in the scan result.
# Options are:
#   Y - skip symbolic links for private key files
#   N - include symbolic links for private key files in the scanning
skip_symbolic_links=Y

# Specifies the list of users that should be excluded from the Authorized Keys
# report.
authorized_keys_filter='operator','aiuser','daemon','dhcpcserv','dladm','ftp','ik

```



A.1.4.2 Customize the Scanning of SSH Keys for a Specific Host

In addition to global SSH configuration, each individual host can be scanned using its own SSH configuration file when any of those configurations is different from the rest of the hosts. The host specific configuration is defined in the text-based host file that is used to supply the list of hosts and its credentials for bulk scanning.

Here is a sample configuration.

```
# blank lines separate records
# consecutive non-empty lines make up a record
#
# first line is the hostname
# second line is the username
# third line is the password
# additional lines in the record defines host specific configuration
# that overrides the global configuration settings defined in the
# conf/CA-PAM-START.props file.

# Linux server scan
host.example.com
root
password
scan_known_hosts_file=Y
scan_private_key_file=Y
scan_aix_ldap_users=Y
aix_load_module=VAS
scan_nfs_directory=Y
nfs_directory=/export/rwdg
scan_include_directory=Y
include_directory=/etc/ssh/site
skip_symbolic_links=Y
```

A.1.4.3 New Reports for SSH Keys

Two new reports are now available to provide more information on SSH keys.

- Known Hosts Discovered
- Authorized Keys

SSH Known Hosts Scan Report		ca technologies
Scan result of the SSH known hosts on your network		
Generated by CA PAM Standalone Access Reporting Tool		Sunday 11 April 2021

Host Name	User Account	Known Hosts
centos-1804171	operator	"10.10.10.10"
centos-1804171	operator	"127.0.0.1"
centos-1804171	operator	"[swatgit.ca.com]:2222"
centos-1804171	operator	"centos-1804171"
centos-1804171	operator	"centos-1804171.example.com"

SSH Authorized Keys Report

Scanning result of the users' SSH authorized keys on your network

Generated by CA PAM Standalone Access Reporting Tool

This report contains information on all the authorized keys and their private keys if they can be discovered during the scanning process. This report is generated by a list of users defined in the configuration file to remove users that need not be included in this report.

Host	User	Key Fingerprint	File	Modified	Public Key	Host	User	Fingerprint
centos-1804171	root	SHA256: S/F8ZUrSCpMrB8U+g0+WQb0 Ocwo4wUfvnHGBAu65boQ	/root/. ssh/authorized _keys	Thu Jun 14 00:31:32 2018	null		null	null
centos-1804171	root	SHA256: jq+1UPAvVFzxdshLb/pSwdX8O CoF7n3uwI7pleOA3C0	/root/. ssh/authorized _keys	Thu Jun 14 00:31:32 2018	null		null	null
centos-1804171	root	SHA256: um/8Lp7CldOCxSgwoeU9H+H2 lmX3ips5NSGGIpRo6kY	/root/. ssh/authorized _keys	Thu Jun 14 00:31:32 2018	null		null	null

