CyberArk DNA™ User Guide

Version 8.1

DNA 8.1 8/22/2018

Table of Contents

CyberArk DNA™

The IT security landscape keeps changing and, thus, the tools and techniques that are used to defend organizations must also change to compensate and adapt to these changes. No longer can organizations exclusively rely on preventive security technologies, such as firewalls, anti-virus, and standard configurations of user authentication systems. Now organizations need more agile tools to sufficiently protect them from today's most sophisticated attacks and operate with modern operation tools (DevOps tools). The reality is that focused, well-funded, and expert attackers can circumvent all of the commonly used preventive security systems. Privileged accounts are built-in vulnerabilities throughout your infrastructure and are what most attackers look for. Unprotected, unmonitored privileged accounts are the weapon of choice for most of attackers. To compensate for this general weakness, organizations must enhance their detection, investigative, and response capabilities.

CyberArk Discovery and Audit™ (DNA) is an innovative discovery and audit tool that automatically scans an organization's network, typically a complex, manual process, for the following:

- Data related to privileged and non-privileged accounts
- Hard-coded and embedded application credentials on workstations, servers, MSSQL databases, and DevOps
- Potential credential theft risks, including Golden Ticket, Pass-the-Hash, Pass-the-Ticket and Overpass-the-Hash attacks
- SSH key exposure
- Privilege escalation risks

The easy-to-use scanner automatically discovers and analyzes any privileged and non-privileged account within servers and desktops as defined by the user, then generates a report and visual organizational map that evaluates the privileged account security status in the organization. A simple three-step procedure leads to better and more efficient risk management around privileged accounts.

Considerations

In order to provide accurate and meaningful results for the security team, the DNA tool uses powerful methods or technologies that mimic those used by attackers. Before running DNA, it is strongly recommended that deploying organizations assess the related legal requirements both under data protection and telecommunication laws as well as any other applicable laws and regulations on their own behalf. We recommend that IT security personnel verify that corporate employment policies or local laws do not prohibit the scanning or analysis of data streams for network security purposes, because the tool involves scanning, locating and analyzing corporate access credentials.

CyberArk's DNA scanner is a certificate-signed tool that does not require agents to be installed on target systems, making it non-intrusive to the IT environment. However, these network activities may trigger alerts in security applications and tools designed to detect anomalous network traffic, so Security Operations Teams may need to be alerted in advance so that the security work is coordinated and does not disrupt or distract from ordinary security monitoring or management of alerts.

Privileged Access Security Status

DNA enables an organization to scan its network on local machines, on the cloud (Amazon Web Services, Azure, etc.), and in DevOps tools (Ansible), and retrieve a list of all accounts that have access to its machines and places where privileged accounts are used, such as in accounts embedded in Windows Services, Scheduled Tasks, IIS Application Pools, and more. It scans all local and domain accounts that have permission to logon to endpoints with a password or using SSH Keys, whether on Windows or Unix/Linux devices.

Together with basic password-based authenticated users that are detected, DNA identifies private and public SSH keys on Unix and Windows machines in your environment and ascertains the status of each key. DNA distinguishes between the private SSH key and the public SSH key, correlates the potential risk of possible connections and produces a visual organizational map of machines that can be accessed using the detected SSH keys.

In addition to regular service accounts in Windows, there are services that authenticate using Kerberos and are registered in the Active Directory Domain. These accounts have an additional attribute called Service Principal Name (SPN), requesting a SPN domain ticket could allow an attacker to efficiently escalate privileges by creating Silver Tickets or simply impersonate the service account by logging in with the appropriate credentials.

CyberArk DNA can discover all defined Domain Service Accounts according to their Service Principal Name (SPN) attribute.

In Ansible playbooks, DNA identifies the hard-coded user and password keywords that are saved as task parameters, variables and environment variables, and sends alerts about them as these credentials might have the potential to take down an entire Data Center if they fall into the wrong hands

Hard-coded and Embedded Application Credentials

DNA enables organizations to find embedded and hard-coded credentials, and assess the extent to which these passwords can be accessed by unauthorized users on the following platforms:

- WebSphere servers (on Unix/Linux)
- WebLogic servers (on Unix/Linux)
- IIS servers
- Ansible playbooks

A clearly organized report lists the discovered embedded credentials and hard-coded credentials to aid in understanding the current risk and threat caused to servers, applications, and target systems to which the applications connect (e.g. databases).

Credential Theft

Using deep credential theft analysis tools, DNA can indicate which machines are vulnerable to Windows memory credential harvesting (from LSASS and SAM). In addition, DNA assesses the current and potential risk of Golden Ticket, Pass-the-Hash, Pass-the-Ticket and Overpass-the-Hash attacks, a form of credential theft. DNA identifies stored hashes of privileged domain accounts on machines, producing a visual map of machines that are vulnerable to the above mentioned attacks.

Cloud Users and Instance Keys

DNA enables organizations to find IAM users, access keys and SSH key pairs, and asses the risk of leaving them unmanaged and unmonitored. DNA currently supports Amazon Web Services (AWS) platform using the AWS API.

DNA can also integrate with Amazon AWS Inspector to show the number of high severity findings on EC2 instances. AWS recommend to treat these security issue as an emergency and implement an immediate remediation as these high severity findings describe security issues that can result in a compromise of the information confidentiality, integrity, and availability within your assessment target.

Database Accounts

DNA scans MSSQL databases to discover all privileged or non-privileged users on SQL or Windows/Active Directory.

Note:
DNA can scan databases on MSSQL 2012 and 2016.

On any target machine, the DNA may discover multiple MSSQL instances, each used in several databases and each with its own users (database-level object). An account may be either an SQL login account or a Windows login account, and each may have one or more users even though each user can only access one database.

The results of the database accounts scan are only displayed in the Database Scan sheet, and are not represented in the Executive Summary.

Privilege Escalation

DNA discovers and flags potential excessive privileges that have been escalated on Unix and Linux.

The assignment of account privileges can be error-prone on Unix and Linux machines, where the root account is the only privileged account by default, and escalating account privileges is typically and commonly done using an un-centralized sudoers configuration file. Since the sudoers configuration file was not designed for cyber-security, the process of escalating account privileges **may result in excessive privileges for accounts**. DNA detects these excessive privileges and exposes the risk.

Granular, Flexible, Easy to Use

Users can select organizational units (OUs) in the Active Directory or import a list of target machines to scan. For Windows systems, users can determine whether DNA will scan only workstations, only servers, or both workstations and servers contained in the OU. On Unix and Mac devices, DNA will always scan both workstations and servers.

Reporting and Visualizing Threats

The resulting Discovery and Audit report is a comprehensive Excel file that provides an Executive Summary Dashboard as well as detailed information about the current status of each privileged account in your organization, and extensive machine and account information for potential attack vectors pertaining to various Credential Theft attacks (Golden Ticket, Pass-the-Hash, Pass-the-Ticket and Overpass-the-Hash) and SSH key exposure.

The report reveals privileged account security issues, highlights non-compliance of passwords and SSH Keys, vulnerabilities to Credential Theft attacks (Golden Ticket, Pass-the-Hash, Pass-the-Ticket and Overpass-the-Hash) and Insecure Privilege Escalations. The report shows how privileged accounts (those using passwords or SSH Keys) are managed, thus enabling your organization to better manage, secure and automate its privileged account processes. The report displays the following sheets:

- **Windows Sheet** – A list of accounts on Windows and Unix machines (when an Active Directory bridge solution is used) throughout your organization, including detailed information about accounts that can be accessed using SSH Keys, as well as information about each SSH Key, and accounts that are vulnerable to Credential Theft attacks (Golden Ticket, Pass-the-Hash, Pass-the-Ticket and Overpass-the-Hash). The list also includes Service Accounts (embedded Windows credentials) that are being used by certain services to carry out their functions. For example, Windows Services, Scheduled Tasks, IIS Application Pool, IIS Anonymous Authentication, etc.
- **Unix Sheet** – A list of accounts on Unix/Linux machines throughout your organization, including detailed information about accounts that can be accessed using SSH Keys, as well as information about each SSH Key.

- **Domain Scan Sheet** – A list of domain accounts that have the SPN attribute set, including detailed information about the accounts and their SPN Service name as well as the SPN itself.
- **SSH Key Trusts** – The organizational status of all SSH keys, the trusts found between Unix and Windows accounts and machines, their potential exposure, as well as their compliancy status.
- **Hard-Coded Credentials** – A list of hard-coded credentials found in applications running on WebSphere, WebLogic, IIS servers, and DevOps tools playbooks (for Ansible) throughout your organization, including detailed information about where the password was discovered and which target system it is used for (e.g. database).
- **Cloud Users** - A list of all IAM users and Access Keys found on AWS, including detailed information about their privileged policies and compliance which can indicate highly privileged users.
- **Cloud Instances** - A list of all EC2 instances in the selected region (or all regions) and their relevant key pairs. This information can help an organization perform a DNA scan on their cloud assets and enumerate all their EC2 instances information.
- **What is Insecure Priv. Esc.** - An explanation about insecure privileged escalation and how it affects the organization.
- **What are SSH Keys** – A summary of how SSH Keys are used, what their risks are, and how DNA helps you assess the current and potential risk of SSH key exposure in your organization.
- **What is Pass-the-Hash** – An explanation about how Pass-the-Hash attacks work and how DNA helps you to assess the current and potential risk of Pass-the-Hash attacks in your organization.

In addition, visual maps of all the machines in your organization display the following:

- **SSH Keys: Organizational SSH Trust Map** – This map displays the possible SSH key trusts between Unix and Windows accounts and machines in your organization. It distinguishes between the “client side” (private SSH key) and the target system (public SSH key), resulting in relationships between accounts and machines that are based on potential access.
  This map makes it easy and quick to understand on which machines SSH keys have been used throughout the years, and exactly which SSH Key trusts can be used to connect from one machine to another.
- **Pass-the-Hash: Organization Vulnerability Map** – This map displays the machines in your organization that are vulnerable to Golden Ticket[1] and Pass-the-Hash and attacks, as well as the machines that are at fault and threaten the organization.
  This map makes it easy and quick to understand how an attacker can leverage these vulnerabilities in your organization.

You can use these maps to focus on the machines and accounts that require immediate attention to help mitigate the threat quickly.

[1]The Golden Ticket vulnerability is only shown in the Pass-the-Hash map if there is indication of a potential attack.

Agentless and Light

CyberArk's DNA scanner is a certificate-signed tool that does not require agents to be installed on target systems, making it non-intrusive to the IT environment. Target device properties are scanned in read-only mode[1]. Please see the FAQ for a detailed explanation regarding DNA's performance and network bandwidth usage.

[1]Target device properties are scanned in read-only mode, except when scanning for SSH keys on Windows without Cygwin.

Install DNA

This chapter describes how to install DNA.

System Requirements

General Requirements

The minimum requirements for running CyberArk DNA are as follows:

Operating System:	Windows 7, Windows 8/8.1, Windows Server 2008, Windows Server 2012
Disk space:	At least 1GB free disk space

Note:
Scanning from a Windows 7 32-bit machine may result in partial maps generated by DNA. For more information, refer to Known Behavior and Limitations, page 140

License

DNA requires a license. The DNA license includes an expiration date, and limits the number of Windows machines and the number of Linux/Unix machines that can be scanned per scan, both when scanning from an Active Directory and from an imported file. This version of DNA is backwards compatible to support older license versions.

Supported Active Directory

DNA can perform scans on the following Active Directories:

- Microsoft Active Directory 2003, 2008 and 2012

Note:
DNA does not support scanning Active Directory domain controllers

Supported SSH Keys

DNA can discover the following types of SSH keys:

- OpenSSH private keys up to 20 kilobytes
- Private PuTTY

Supported SSH Servers

- OpenSSH Server 6.7 and lower
  - On OpenSSH Server 6.2-6.7, DNA cannot discover the time when an SSH key was last used. For information about configuring the server to log this data, refer to Configure Logging for 'Key Last Used' Data, page 151.

- DNA discovers private and public SSH keys on all OpenSSH servers using SSH2 protocol.

- SunSSH v2.2 and below

Microsoft Office Application

Reports generated by DNA can be viewed in the following Microsoft Office applications:

- Microsoft Excel 2010 and 2013

Note:
DNA is incompatible with Microsoft Office 2007

.NET Framework

- Make sure that .NET Framework 4.5.2 and .NET Framework 3.5 are installed.

In addition, make sure that the Visual C++ 2008 runtime library is installed.

Windows Requirements

The minimum operating system requirements for scanning Windows machines with DNA are as follows:

Credentials for scanning

- Domain Administrator
  or,
- Equivalent Domain User:
  - User with read permissions on the Active Directory
  - User with local administrative rights for Windows

Note:
- In Windows Vista or newer, a user who is not a domain Administrator must be a domain user and must belong to the Administrators group or to a group nested within the Administrators group.
- In older versions of Windows, the domain user can be a member of any privileged group.

Supported target machines

Machine	Windows Version
Workstations:	- Windows 2000*, ** - Windows XP*, ** - Windows Vista - Windows 7 - Windows 8

Machine	Windows Version
	▪ Windows 10
Servers:	▪ Windows 2000*, ** ▪ Windows 2003** ▪ Windows 2008 ▪ Windows 2012

Note:

*By default, the Audit Policy does not audit required events on these platforms. For more information about this requirement, refer to Windows Requirements, page 14, below.

**By default, machines with a single core CPU that run Windows versions will not be scanned for Golden Ticket and Pass-the-Hash vulnerabilities or private SSH keys. This can be changed by configuration parameters in the DNA.exe.config file. For more information about configuring DNA scans on machines with a single core CPU and disabling scanning for Pass-the-Hash vulnerability, refer to Configuration Parameters, page 121.

Supported protocols

The following protocols are supported when accessing the Active Directory:

- LDAP
- LDAPs

Network protocols

- Windows File and Printer Sharing
- Windows (WMI)
- SSH – To discover SSH Keys on Windows machines where Cygwin is installed

For information about how to enable the Windows (WMI) Protocol in your environment, see Enable WMI Ports on Windows Client Machines, page 131.

For more information about the ports that DNA uses to access remote machines, refer to Ports used by DNA, page 150

For information about how to enable the Windows (WMI) Protocol in your environment, see Enable WMI Ports on Windows Client Machines, page 131.

For more information about the ports that DNA uses to access remote machines, refer to Ports used by DNA, page 150

Scan for embedded and hard-coded credentials on IIS servers

Supported Platforms

- IIS 7 and higher

Prerequisites

- Make sure that the machine where DNA runs and all scanned machines are configured for Administrative shares (e.g. C$, etc.).

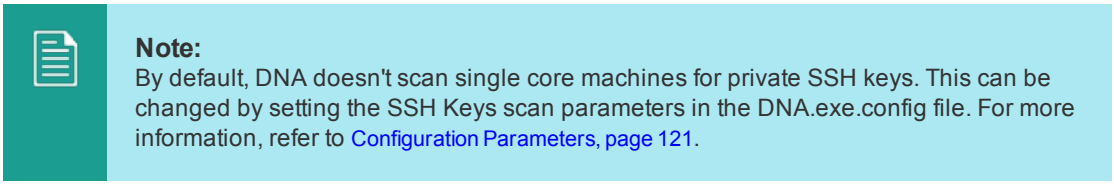
Scanning for SSH keys on Windows machines

DNA can discover SSH keys on Windows machines, either with Cygwin installed or without, in the following ways:

On Windows machines where Cygwin is installed:	. DNA discovers private SSH keys and public SSH keys
On Windows machines where Cygwin is not installed:	. DNA discovers private SSH keys . DNA must use a domain administrative Windows account, and not a local administrative account

Prerequisites

- To enable DNA to discover all the private SSH keys on the machines to scan, the user who will perform the scan must have access to all these keys.



Note:
By default, DNA doesn't scan single core machines for private SSH keys. This can be changed by setting the SSH Keys scan parameters in the DNA.exe.config file. For more information, refer to Configuration Parameters, page 121.

Scanning for cloud users and instances

Supported Platforms

- AWS
- AWS Inspector

Prerequisites

Make sure that the machine where DNA runs can access the AWS console via API.

Supported target windows machines and Cygwin versions

Cygwin versions

- Cygwin 1.7.32 and above

Target Windows machines

Supported target Windows machines where Cygwin is installed:

- Windows 7
- Windows Vista
- Windows 2008
- Windows 2012

Prerequisites

- Make sure that OpenSSH is installed within Cygwin.
- To discover public SSH Keys on Windows, make sure that Cygwin is installed in your environment.
- To scan a Windows machine that has Cygwin installed, the following packages and commands must be installed in Cygwin:
  Packages:
  - openssh-server – This package must be installed.
  - openssh – This package must be installed.
  - sshd daemon – This package must be started and configured.
  - SSH connection – DNA requires an SSH connection to scan machines for SSH Keys.

  Commands
  - ssh-keygen – DNA uses the ssh-keygen command.

Note:

- To make sure the SSH Server is running and available, run the "ssh localhost" command. At the prompt, specify your password. If a new command line is now displayed, your SSH server is listening on the standard SSH port.
- The SSH Server must support password, SSH key, or keyboard interactive authentication, which can be configured in the /etc/ssh/sshd_config file. For more information, refer to Log Error Messages, page 118, in Troubleshooting
- The SSH Server must support password, SSH key, or keyboard interactive authentication, which can be configured in the /etc/ssh/sshd_config file. For more information, refer to Log Error Messages, page 118, in Troubleshooting.
- The SSH Server must support password, SSH key, or keyboard interactive authentication, which can be configured in the /etc/ssh/sshd_config file. For more information, refer to Log Error Messages, page 118, in Troubleshooting.
- By default, machines with a single core CPU will not be scanned for private SSH keys. This can be changed by configuration parameters in the DNA.exe.config file. For more information, refer to Configuration Parameters, page 121.

Additional requirements on target machines

Configure the Audit Policy in the Local Security Policy or Group Policy to audit the following types of events:

- Audit logon events
- Audit system event

For information about how to configure the Audit Policy, see Configure Audit Policy, page 135.

Unix/Linux Requirements

The minimum requirements for scanning a Unix/Linux environment with DNA are as follows:

Credentials for Scanning

To scan Unix/Linux/Mac machines, the following credentials are required:

Note:
These credentials are not relevant to IBM Virtual I/O Server or IBM Hardware Management Console platforms. For information about credentials that are required to scan these machines, refer to the relevant information at the bottom of this page

Type of user	Required Credentials
User with root permissions for Unix/Linux/Mac	It is possible to configure DNA to scan with users who authenticate with a password, as well as SSH Keys
Connected via an Active Directory bridge, using the Active Directory as a source.	. Domain Administrator with root permissions on Unix/Linux/Mac machines or, . Equivalent Domain User: . User with read permissions on the Active Directory . User with root permissions for Unix/Linux  **Note:** To scan using the Active Directory as a source, your organization must use an Active Directory bridge solution. For example: . Centrify DirectControl (DNA does not scan for SSH keys when using AD Bridge on Centrify)
accounts other than root	DNA requires the use of sudo to run commands. Hence, the administrative user account(s) configured to scan with DNA must have permissions to run sudo on the scanned Unix/Linux/Mac machines. For more information, see Configure Root Permissions Using the Sudoers File, page 132.

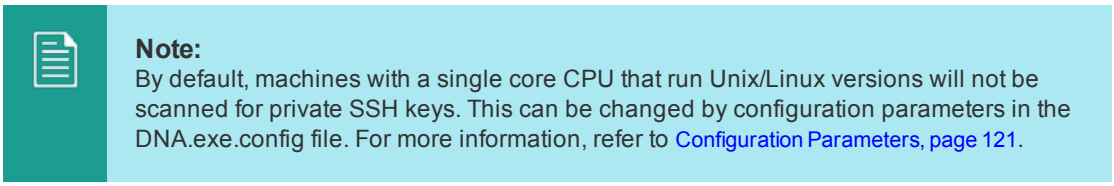
To scan other Unix/Linux machines:

Platform	Required Credentials
ESX machine	root user
IBM VIOS machines	A user with vios.oemsetupenv authorization is required. This authorization allows the user to elevate the shell to

Platform	Required Credentials
	unrestricted shell mode by executing the "oem_setup_env" command.
IBM HMC machines	An hscroot user or any user with the hmcsuperadmin task role.

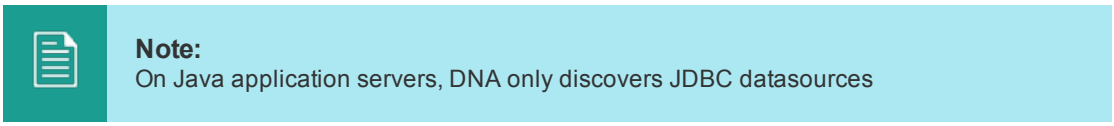
Supported Unix/Linux Platforms

- Workstations and servers:
  - RHEL 4-7.1
  - Solaris Intel and Solaris SPARC 9, 10, 11 – For known limitations, refer to Known Behavior and Limitations, page 140.
  - SUSE 10
  - Fedora 18, 19, 20
  - Oracle Linux 5
  - CentOS 6
  - AIX 5.3, 6.1, 7.1
  - ESXi 5.0 and 5.1
  - IBM Virtual I/O Server 2.2.x
  - IBM Hardware Management Console 7Rx.x and 8Rx.x
  - MacOS Mavericks, Sierra, High Sierra



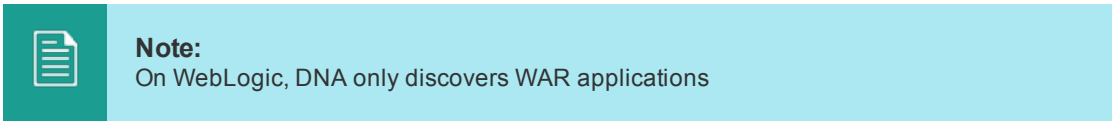
Note:
By default, machines with a single core CPU that run Unix/Linux versions will not be scanned for private SSH keys. This can be changed by configuration parameters in the DNA.exe.config file. For more information, refer to Configuration Parameters, page 121.

Supported Java Application Servers



Note:
On Java application servers, DNA only discovers JDBC datasources

- WebSphere 6.1 and higher (Linux, Solaris, AIX)
- WebLogic 9.x and higher (Linux, Solaris, AIX)



Note:
On WebLogic, DNA only discovers WAR applications

Supported DevOps Platforms

- Ansible version 2.3 and higher on RHEL 4-7.1

Package Prerequisites

To be able to scan a Unix/Linux environment with DNA, the following packages or commands must be installed:

Package or Command	Details
SSH	The openssh-server and openssh packages must be installed, and the sshd daemon must be started and configured. DNA will not be able to scan the machine without an SSH connection. DNA uses the following commands: ssh-keygen
sudo	The sudo package must be installed and configured to enable DNA to perform scan and retrieve account details.  **Note:** . This is only a prerequisite when scanning as a user other than “root”. . DNA supports the following sudo-replacement solutions: . CA Privileged Identity Manager/ControlMinder . Centrify Access Manager/DirectAudit For more information, refer to Unix/Linux Requirements, page 18
lastlog command	This command retrieves the last login date of an account.  **Note:** The command is not required on AIX systems and Solaris

Note:

- To find out if a specific command is installed, run the "which" command. For example, if sudo is installed, the "which sudo" command will return the full path of the sudo command. If sudo is not installed, the “which” command will return: no sudo in /usr/bin /etc /usr/sbin /usr/ucb /usr/bin/.
- To make sure the SSH Server is running and available, run the "ssh localhost" command. At the prompt, specify your password. If a new command line is now displayed, your SSH server is listening on the standard SSH port.
- The SSH Server must support password, SSH Key, or keyboard interactive authentication, which can be configured in the /etc/ssh/sshd_config file. For more information, refer to Log Error Messages, page 118, in Troubleshooting.

Sudo Replacements

DNA supports the following sudo-replacement solutions:

- CA Privileged Identity Manager/ControlMinder – This solution contains the sesudo command.
- Centrify Access Manager/DirectAudit - This solution contains the dzdo command.

AD-Bridge support

DNA supports the following AD-Bridge solutions:

- Centrify Access Manager/AD Bridge
- Quest (OneIdentity) vastool

Installation

DNA installation

1. From the DNA installation package that you will receive from your CyberArk representative, copy the CyberArk DNA zip file to the machine you want to scan from.
2. Extract the contents of the zip file to any directory on your local hard drive.

Note:
Make sure you have full read and write permission for the chosen directory

3. Optionally configure the DNA.exe.config configuration file.
   This file includes the configuration that DNA will use during scanning. For example, you can configure whether or not DNA will scan for Golden Ticket and Pass-the-Hash vulnerabilities, scheduled tasks, and Windows services, and how it will treat non-compliance with the password policy in your organization. For more information about the configuration parameters, refer to Configuration Parameters, page 121.

Use DNA

DNA automatically scans your organization's network, discovers and analyzes privileged and non-privileged accounts, accounts that use passwords and accounts that use SSH Keys, and also discovers potential Credential Theft attacks (Golden Ticket, Pass-the-Hash, Pass-the-Ticket and Overpass-the-Hash).

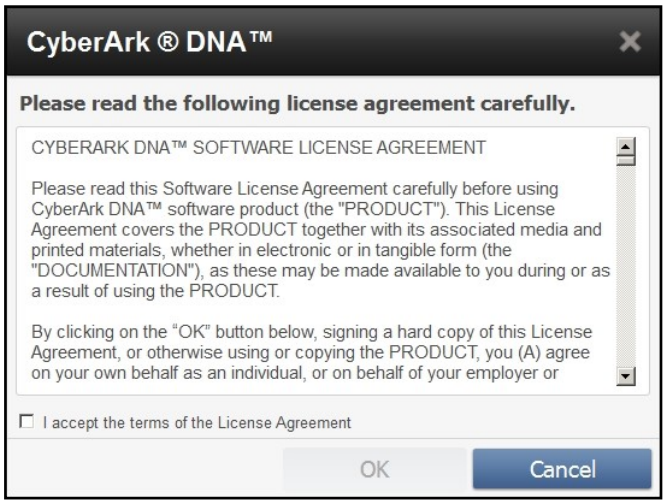
This chapter explains how to run DNA, work with its interface, setup and perform a scan, and view the scan results.

Run DNA for the first time

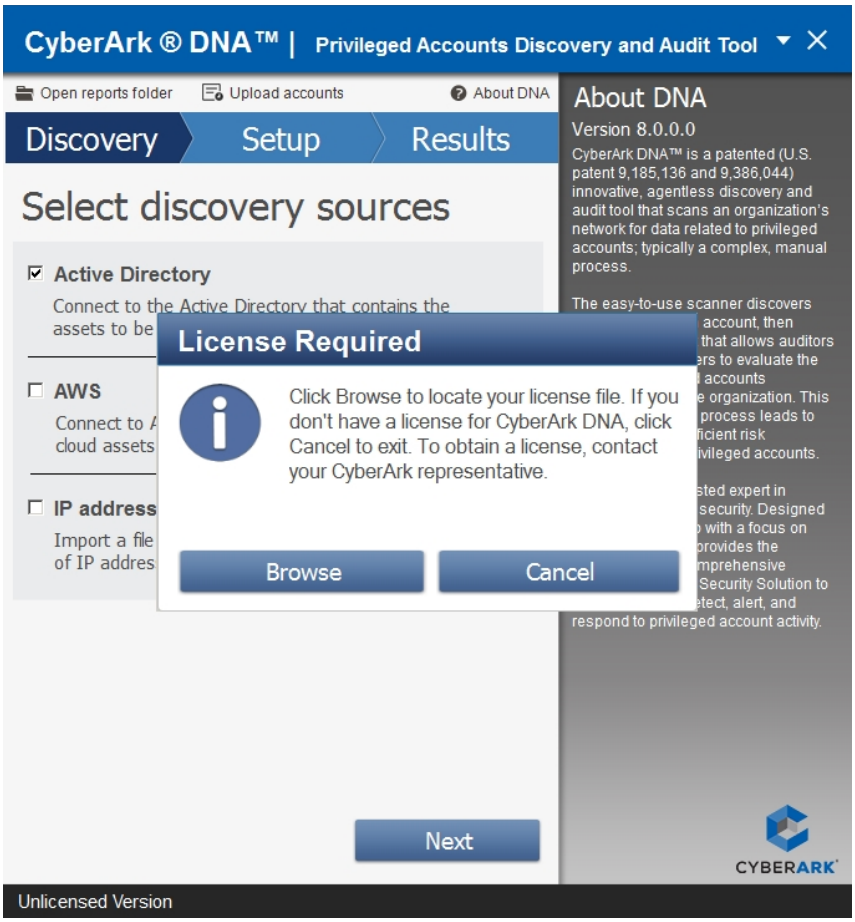
Note:
Running DNA might trigger SIEM system alerts due to the way it scans your network.

Run DNA

1. In the CyberArk DNA executable folder, double-click DNA.exe.
2. The first time that DNA is run, the CyberArk DNA Software License Agreement window appears.

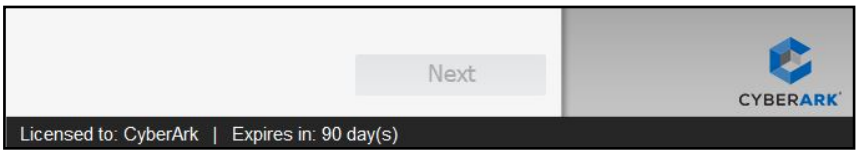


3. Read the license agreement and select the checkbox to accept its terms, then click OK; the CyberArk DNA window appears with the License Required pop-up on top. At the bottom left of the CyberArk DNA window, Unlicensed Version is displayed.

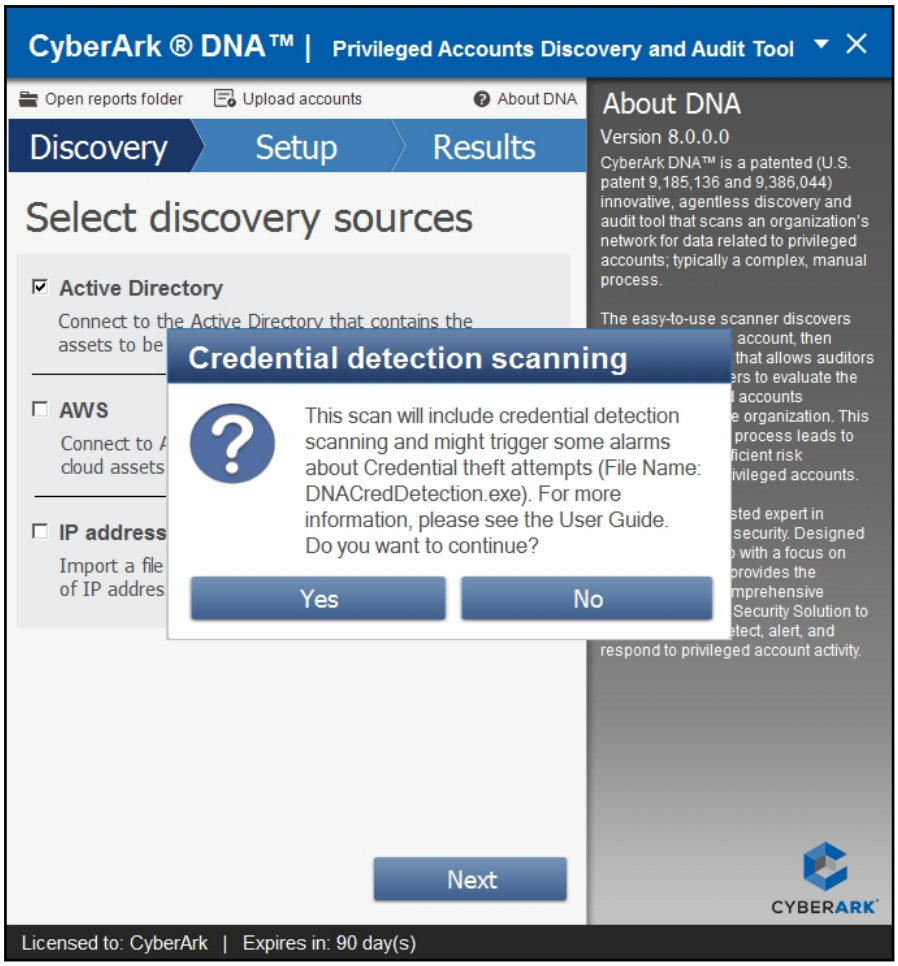


To be able to use DNA, you need a license. The DNA license includes an expiration date and limits the number of Windows machines and the number of Unix/Linux machines that can be scanned per scan, both when scanning from an Active Directory and from an imported file.

4. In the License Required pop-up, click Browse and find the DNALicense.xml file, then choose the file.
   Note that at the bottom left of the CyberArk DNA window, Unlicensed Version has been replaced by information about the license, the licensee and the remaining number of days until the license expires.



Depending on the DNA zip package that you receive, DNA may be configured to detect credential theft vulnerabilities on machines. When this configuration is activated, a window appears for credential detection scanning indicating that this scan might trigger an alert in your SOC systems about credentials theft using the DNACredDetection.exe file.

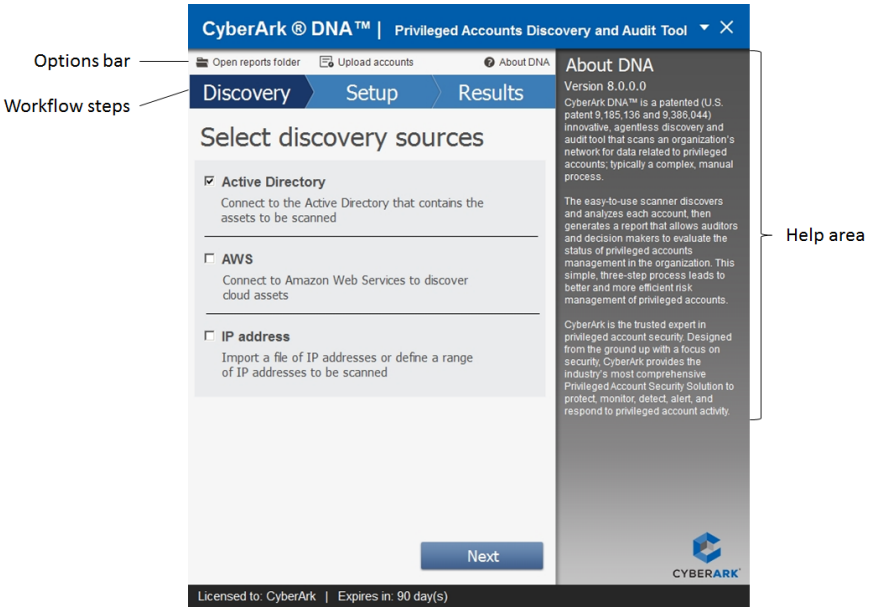


To disable this type of scan, open the DNA configuration file and disable the **ScanVulnerableCredentials** parameter. For more information, refer to DNA Configuration, page 121.

Understand the DNA User Interface

The DNA user interface

The CyberArk DNA enables you to specify the sources that DNA will use to perform discovery, setup a scan, run it, and view the results.



Each CyberArk DNA window contains the following:

- Workflow steps (e.g., select the discovery source, setup, etc.)
- Options bar – Includes the following options:
  - **Open reports folder** – Enables you to access all reports.
  - **Upload accounts** – Enables you to upload discovered accounts from a DNA DB file to the CyberArk PAS Pending Accounts.
  - **About DNA** – Displays information about CyberArk DNA in the Help area.
- Context-sensitive Help Area – Click “What’s this?” to display help about each section.

The DNA Workflow

The DNA workflow includes the following steps:

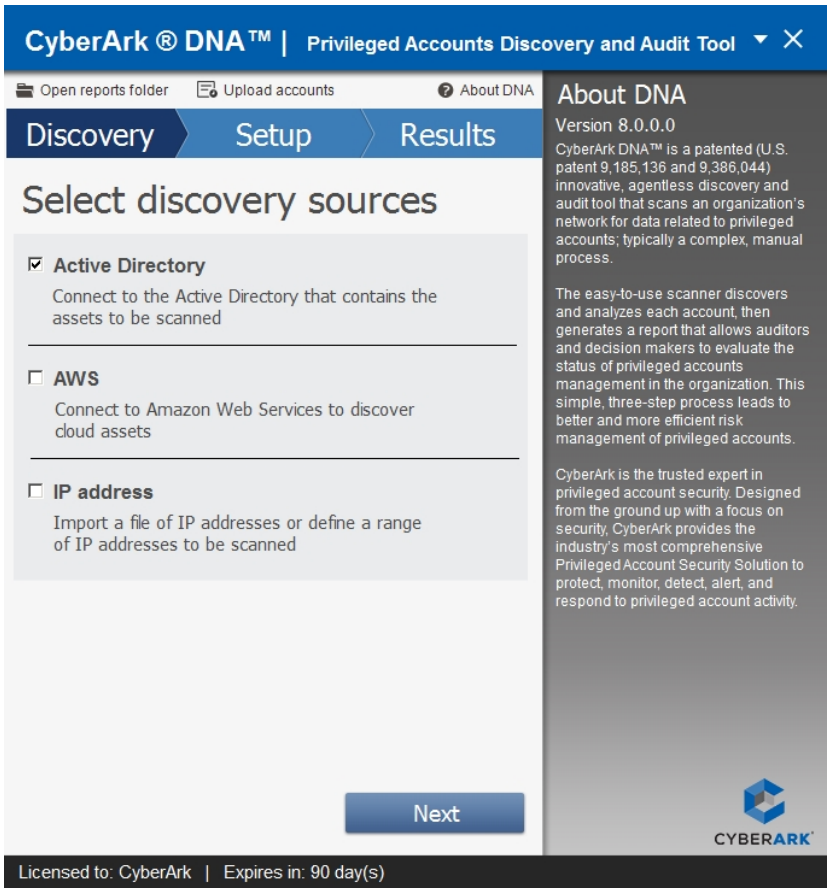
Step	Description
Discovery	Determine the sources that DNA will use to perform discovery. DNA can be configured to scan the assets contained in a specified Active Directory, or the machines listed in a specific file, or both.
Setup	Configure the basic setup of the scan, depending on the sources you selected in the Discovery step. Once you have provided this information, you can start scanning.
Scan	View live data about the scan in progress. When scanning is complete, you can view statistical information about the scan and access the scan report.

Perform a Scan

You can perform a privileged account scan using the following three-step procedure, explained in the sections below:

Select Sources for Discovery

In the Discovery window, select the sources that DNA will use to perform discovery.



Select sources

1. Select one or all of the following options:

Source	Description
Active Directory	DNA will scan the assets contained in the Active Directory that you specify in the Setup window.
AWS Discovery	Connect to Amazon Web Services to discover cloud assets, such as IAM users, Access keys and EC2 instances and EC2 key pairs (in the selected region).
IP	Import a file of machines or define a range of IP addresses to scan. DNA

Source	Description
Address	will scan all detected machines listed in the file or that are active in the IP network range from the Setup window.

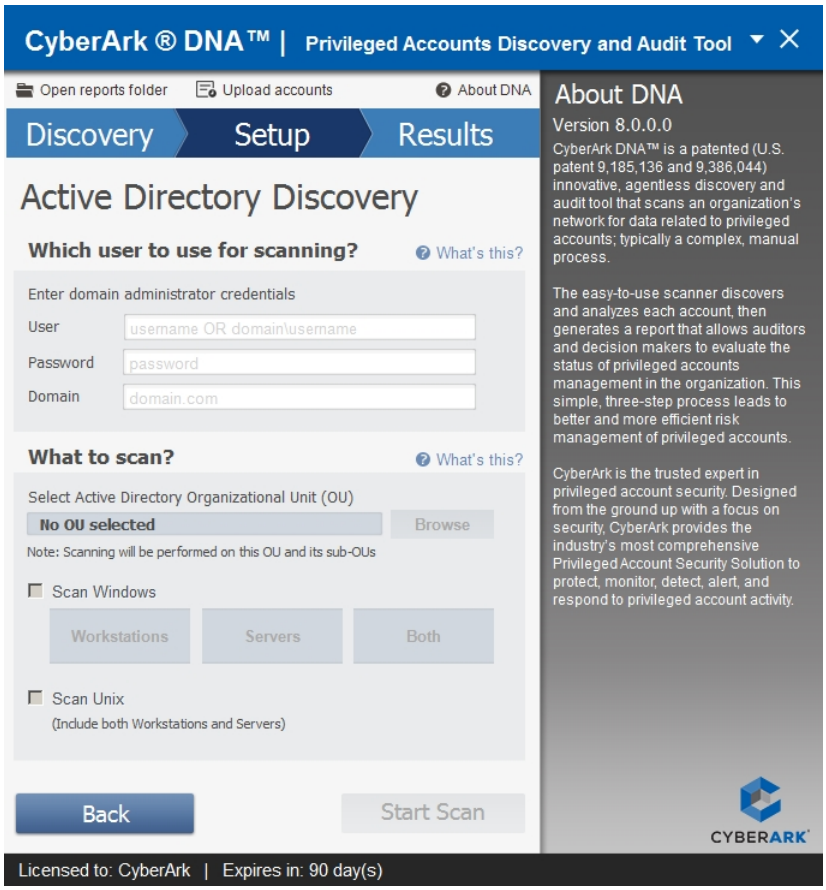
2. Click **Next**; the Setup window appears.

Set up a DNA Scan

The option you choose in the Discovery page determines what is displayed in the Setup page. If you selected multiple options in the Discovery window, the setup pages are displayed according to the list order.

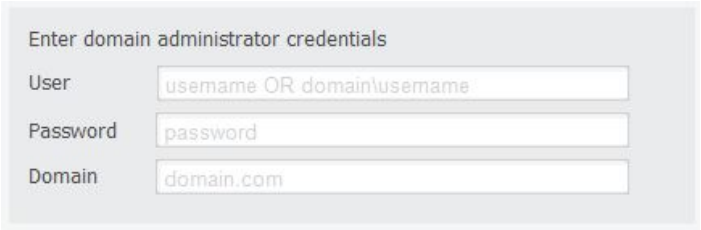
Set up DNA to Scan from an Active Directory

The Active Directory Discovery page enables you to set up DNA to scan from an Active Directory.



Scan from an Active Directory

1. In the Which user to use for scanning? section, specify the credentials the scanner will use to access the Active Directory and to perform the scan.

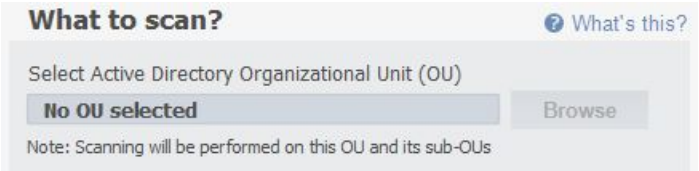


Type the user credentials in the relevant fields.

Note:

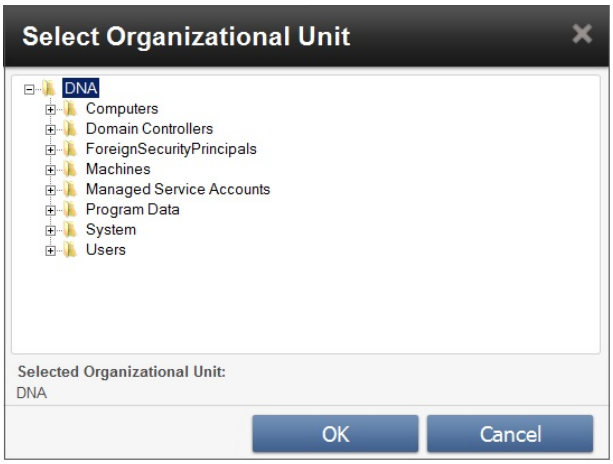
- DNA uses these credentials to connect to the Active Directory's Organizational Unit (OU) and the target machines.
- To connect to the OU, read permission is required.
- To scan both Windows and Unix/Linux/Mac machines via an Active Directory Bridge solution, the credentials must have both of the following permissions:
  - Local administrative permission for Windows
  - Root permission for Unix/Linux machines. This permission is typically configured in the sudoers configuration file.
- If the specified credentials have only local administrative or root permission, you must scan Windows and Unix/Linux/Mac devices in two separate scans, using the relevant credentials for each operating system. For more information, see Run a Scan , page 35.
- You must specify the domain name in the fully-qualified domain name (FQDN) format.
- When you configure DNA to scan a company domain, sub-domains will not be scanned. For example, when you scan the mycompany.com domain, the sub.mycompany.com domain will not be scanned.

2. In the What to scan? Section, specify the target machines to scan for privileged accounts.



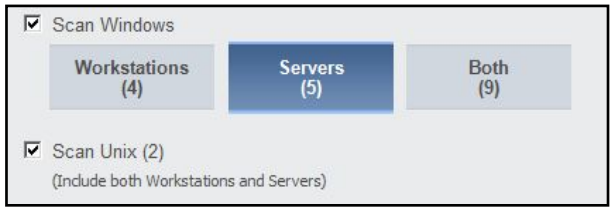
a. Select the Active Directory's Organizational Unit (OU) to scan. Use Browse to find the relevant OU and select it, then click OK; the scanner will scan the selected

OU and all of its sub-OUs.



b. Check the following options:
   - Scan Windows – Check this option to scan Windows machines, then select the items to scan by clicking the relevant button: Workstations, Servers (default), or Both.
     By default, DNA automatically scans the selected Windows machines for risks of Golden Ticket and Pass-the-Hash attacks. This can be configured in the DNA configuration file.
     By default, any MSSQL server found during the Windows scan is scanned for Database users. This can be configured in the DNA configuration file.
     For more information, refer to DNA Configuration, page 121.
   - Scan Unix – Check this option to scan Unix/Linux machines.

     Note:
     On Unix/Linux devices, DNA will always scan both workstations and servers

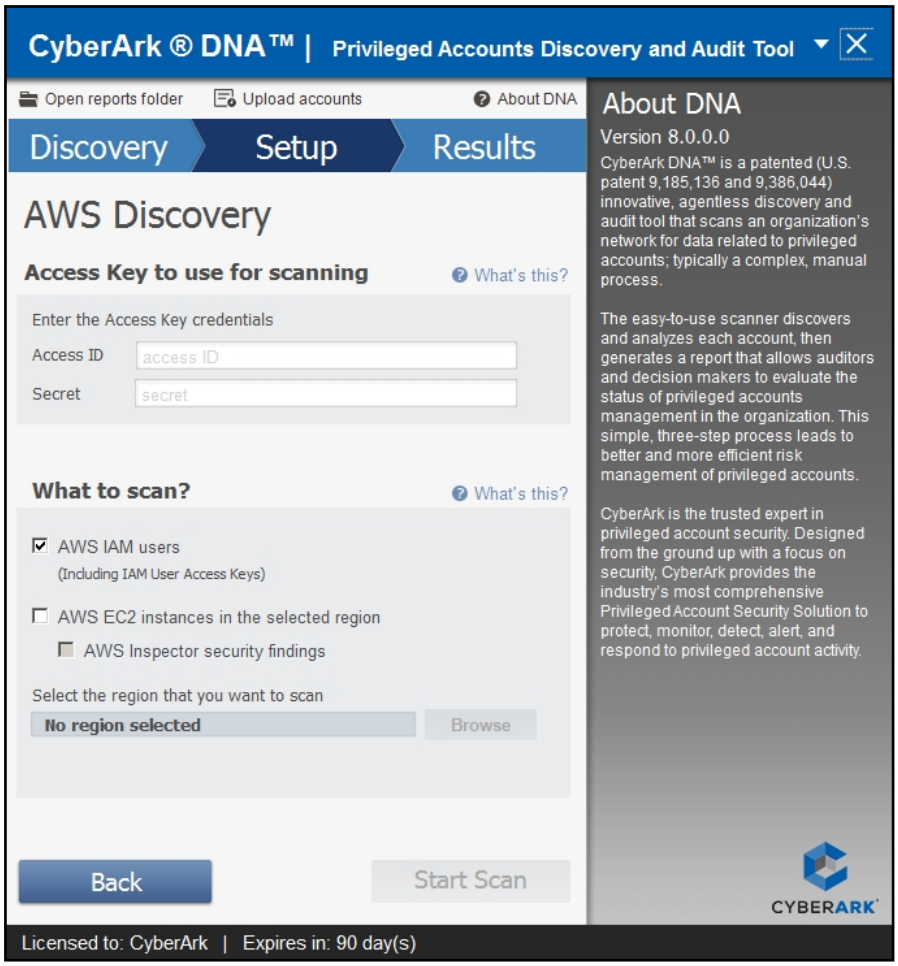
     

     MacOS scan is included in the Unix scan.
     By default, DNA automatically scans the selected Unix/Linux machines for SSH keys exposure. This can be configured in the DNA configuration file. For more information, refer to DNA Configuration, page 121.

3. If you configured DNA to scan from a file/IP range or AWS, as well as from the Active Directory, click **Next** to proceed to the Setup scanning from a file/IP range or AWS window. Otherwise, click **Start Scan**.

Set up DNA to Scan from AWS

The AWS Discovery page enables you to set up DNA to scan from an AWS platform.



Scan from AWS

1. In the Access Key to use for scanning section, specify the access ID and access secret that the scanner will use to access AWS and perform the scan.
   Type the access ID and secret in the relevant fields.

> **Note:**
> - DNA uses these credentials to connect to the AWS console using the AWS API.
> - To run an AWS scan, the user related to the access key provided needs the open read policy. For more specific permissions please refer to the technical FAQ guide.

2. In the What to scan? section, check the following options:
   - IAM users and access keys - Check this option to detail AWS IAM users and their access keys
   - E2 instances and key pairs:
     - Select the required region to scan. By default, all regions are scanned.
     - AWS has a limitation when scanning certain regions, such as AWS GovCloud (US) or China (Beijing).

- Check this option to enumerate the EC2 instances and EC2 key pairs in the selected region.
- AWS Inspector security findings:
  - Check this option to list AWS Inspector information on the selected region for all EC2 instances that have the Inspector agent installed.
  - Selecting this option will sum all high severity security finding in the scanned EC2 instances.

3. If you configured DNA to scan from a file as well as from AWS, click **Next** to proceed to the Setup scanning from a file window. Otherwise, click **Start Scan**.

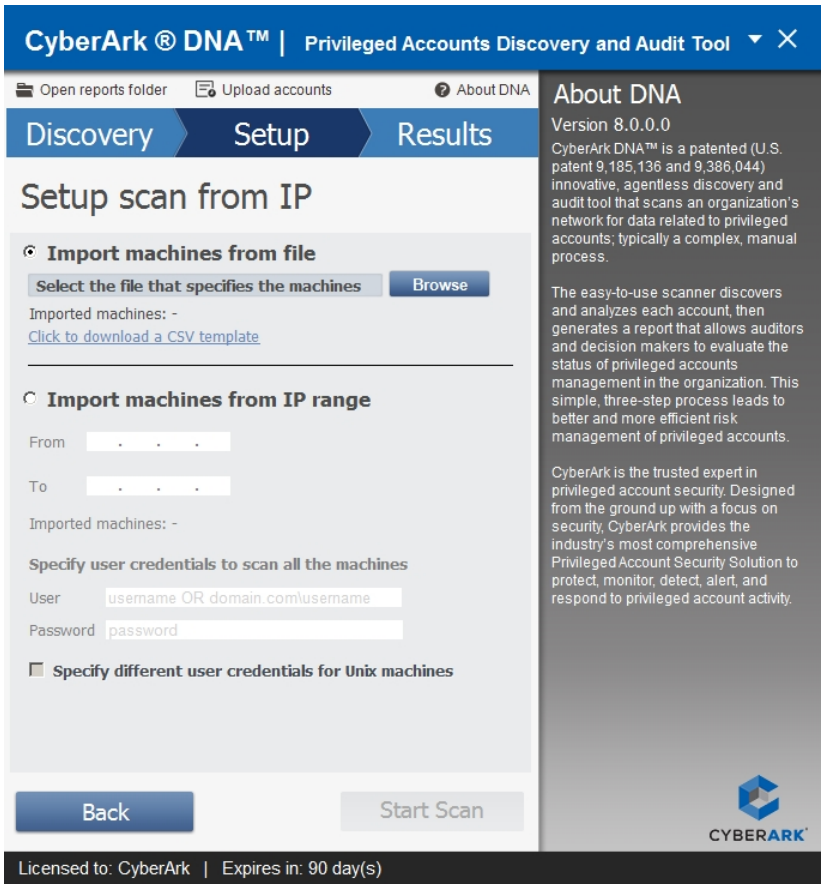
Set up DNA to Scan IP addresses

Note:
- When scanning from a file, make sure that none of the passwords in the imported file contain the file delimiter character, since this might cause the account to be locked out. By default, the delimiter character is a comma ",". For more information, refer to Imported File Issues, page 113, in Troubleshooting.
- To accurately identify machines as "Workstation" or "Server", make sure that the user who will perform the scan is a Domain user. For more information, refer to Scan Limitations, page 140.

The Setup scan from IP page enables you to setup DNA to:

- Scan machines that are not connected to an Active Directory
- Scan an entire network range
- Scan a specific list of machines
- Scan machines by authenticating to them using an SSH Key. For more information, refer to Import a File, page 136.

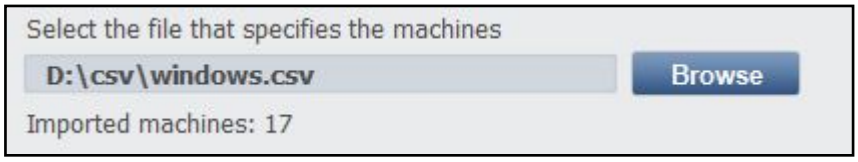
Note:
DNA cannot authenticate to Windows machines with Cygwin using SSH Keys



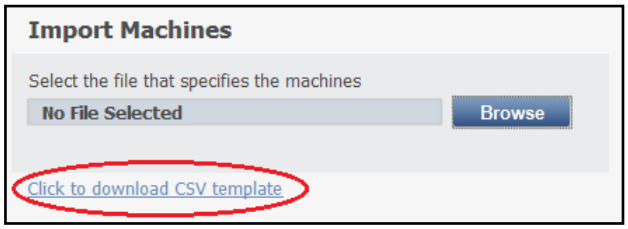
If you specify that DNA will scan from an Active Directory as well as from a file, some machines may be duplicated. In this case, DNA will omit the duplicates. Click Back to return to the Setup scanning from the Active Directory window.

Import machines from file

1. Select **Import machines from file**, then click **Browse**, and select the file that specifies the machines to scan; the number of imported machines is displayed below the field.



2. To download a CSV template that you can use to create your CSV file, click **Click to download CSV template**.



   For more information about importing a file, refer to Import a File, page 136.
3. Click **Start Scan**.

Import machines from IP range

1. Select **Import machines from IP range**.
2. Specify the IP range from which DNA will scan and the IP range to which DNA will scan. Make sure that each number is between 0 and 255.
   The number of machines to scan is displayed.
3. Specify the name and credentials of the user who will run the DNA scan.
4. To specify additional user credentials to access and scan Unix machines, select **Specify different user credentials for Unix machines** and type the user's name and credentials.

5. Click **Start Scan**

Run a Scan

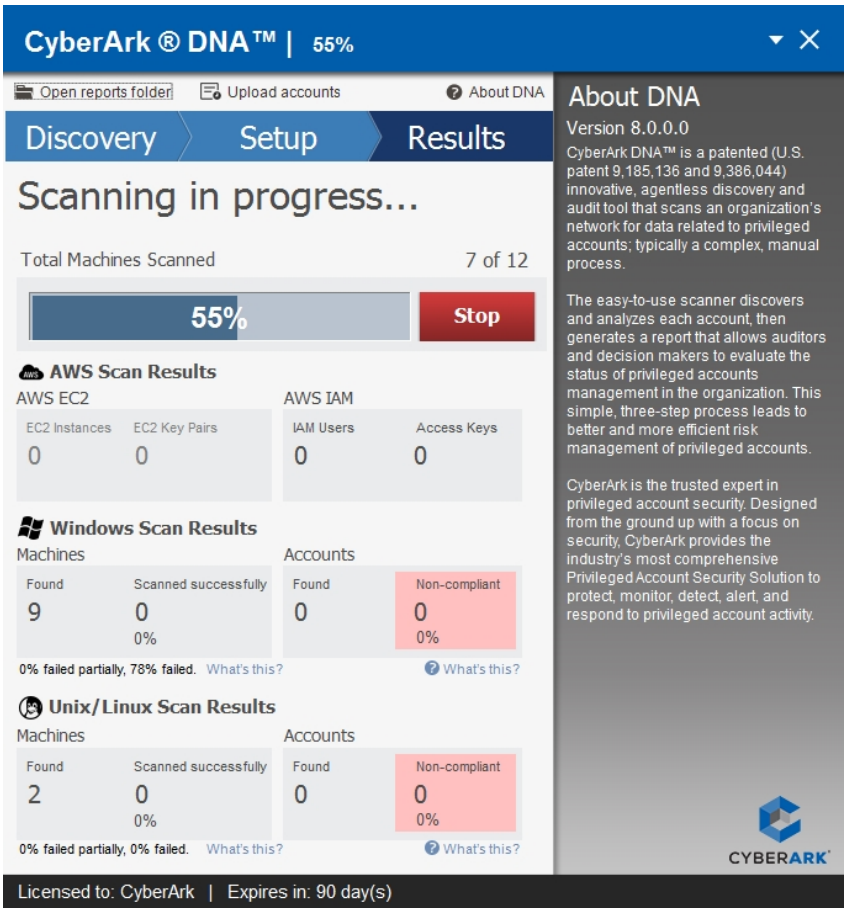
Once you have provided the information required in the Discovery and Setup windows, you can start scanning.

- If the credentials you specified above have both local administrative and root permissions, you can scan both Windows and Unix/Linux devices in a single scan.
- If the specified credentials have only local administrative or root permission, you must scan Windows and Unix/Linux devices in two separate scans, using the relevant credentials for each operating system.
- AWS results are only relevant if you selected the AWS scan and entered the AWS access key credentials.

  Database scanning results will be available if the supplied credentials have the appropriate permissions on the MS SQL servers.

Start the scan

- To run the DNA scan, click **Start Scanning**; the Scan window appears.



Stop the Scan

- To stop the scan before it is complete, click **Stop**.

During scanning, the following live data is displayed:

- Total Machines Scanned - The current number of Windows and Unix/Linux machines scanned. The Progress bar displays the current percentage of scans completed. When the application is minimized, the scanning progress is indicated in the taskbar.
- Windows and Unix/Linux Scan Results

  Machines

  - Found – The total number of Windows and Unix/Linux machines found in the organization.
  - Scanned successfully - The total number of Windows or Unix/Linux machines scanned successfully, along with the current percentage of Windows or Unix/Linux machines scanned.Scanned successfully - The total number of Windows or Unix/Linux machines scanned successfully, along with the current percentage of Windows or Unix/Linux machines scanned.
  - Statistics - Below this information, the following statistics display:
    - Failed partially – The current percentage of Windows or Unix/Linux machines for which at least one but not all types of scans failed due to errors.

- Failed – The current percentage of Windows or Unix/Linux machines for which all scans failed due to errors.

  Errors can occur for a variety of reasons, for example because a machine is offline and not available for scanning, or because of insufficient permissions. For information about specific errors, see the Details section in the report. See also the Troubleshooting section.

Accounts

- Found – The total unique number of Windows and Unix/Linux accounts found in the organization.
- Non-Compliant - The total unique number and percentage of non-compliant Windows or Unix/Linux accounts identified in the scan. An account is considered non-compliant if its password was not changed for a period greater than the threshold value defined in the DNA configuration file.

Note:
Only enabled accounts (as opposed to disabled or “locked-out” accounts) can have a non-compliant status.

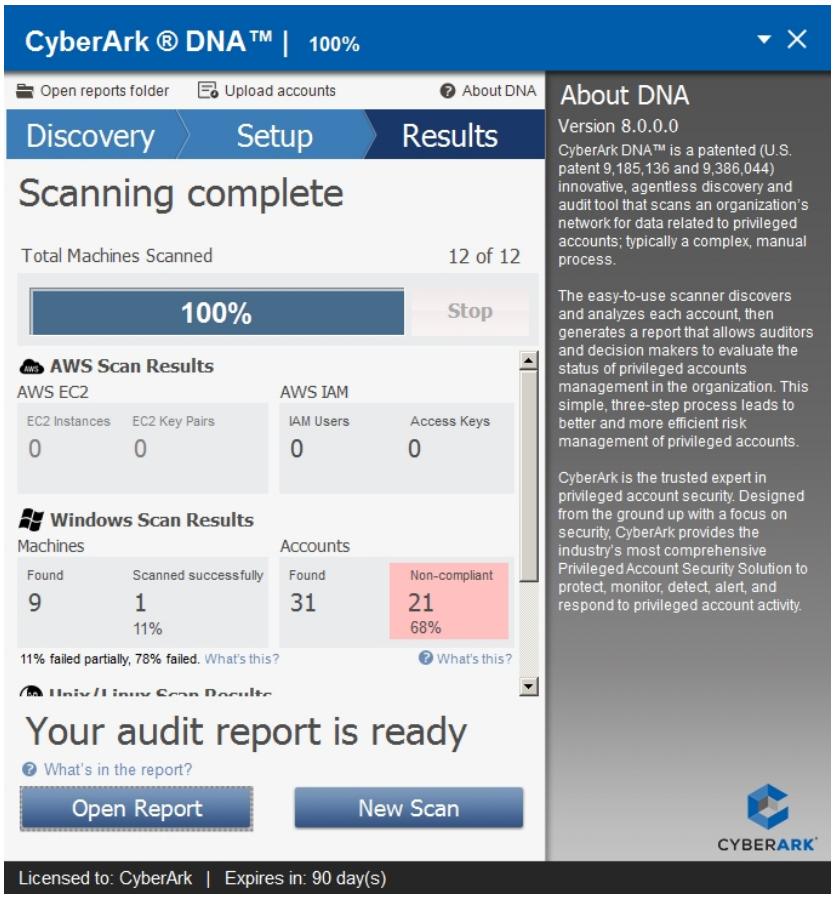
When running an AWS scan, the following AWS Scan Results information is added:

- AWS EC2 instances - The total number of EC2 instances found in the selected region.
- AWS EC2 Key pairs - The total number of EC2 Key Pairs found on the discovered EC2 instances.
- AWS IAM Users - The total number of IAM users found in the AWS console.
- AWS IAM Access Keys - The total number of access keys found on each discovered IAM user.

If only the AWS scan is selected, this information will appear on its own. However, if the AWS scan is selected together with other scans, this information will appear alongside all the information from the other scans.

View the Scan Results

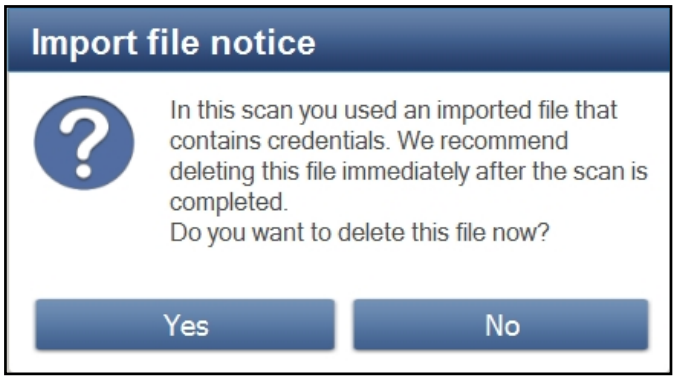
When the scan is complete (or if you pressed the Stop button), the Results window appears.



This window displays the final scanning data. For more information about the displayed scanning data, see Run a Scan , page 35.

You can now open the Discovery and Audit Report, or start a new scan.

- To access the reports and maps, click **Open Report**.
- To start a new scan, click **New Scan**; the Setup window appears; the same user credentials and OU or region that were used in the previous scan will be used and will appear in the relevant fields. CyberArk DNA will generate a new report name with the current date and time in the Report name field. To start the scan, click **Start Scanning**.
- To upload discovered accounts, click **Upload Accounts** at the top of the DNA window. For further information, refer to Upload Accounts, page 40.
- After running a scan using an import file, a warning message recommends that you delete the imported file as it contains credentials in it.


Import file notice
In this scan you used an imported file that contains credentials. We recommend deleting this file immediately after the scan is completed.
Do you want to delete this file now?
Yes
No

Upload Accounts

After DNA discovers accounts in your enterprise, you can initiate an onboarding process to upload accounts listed in the DNA DB file to the Pending Accounts page in the PVWA.

Upload accounts

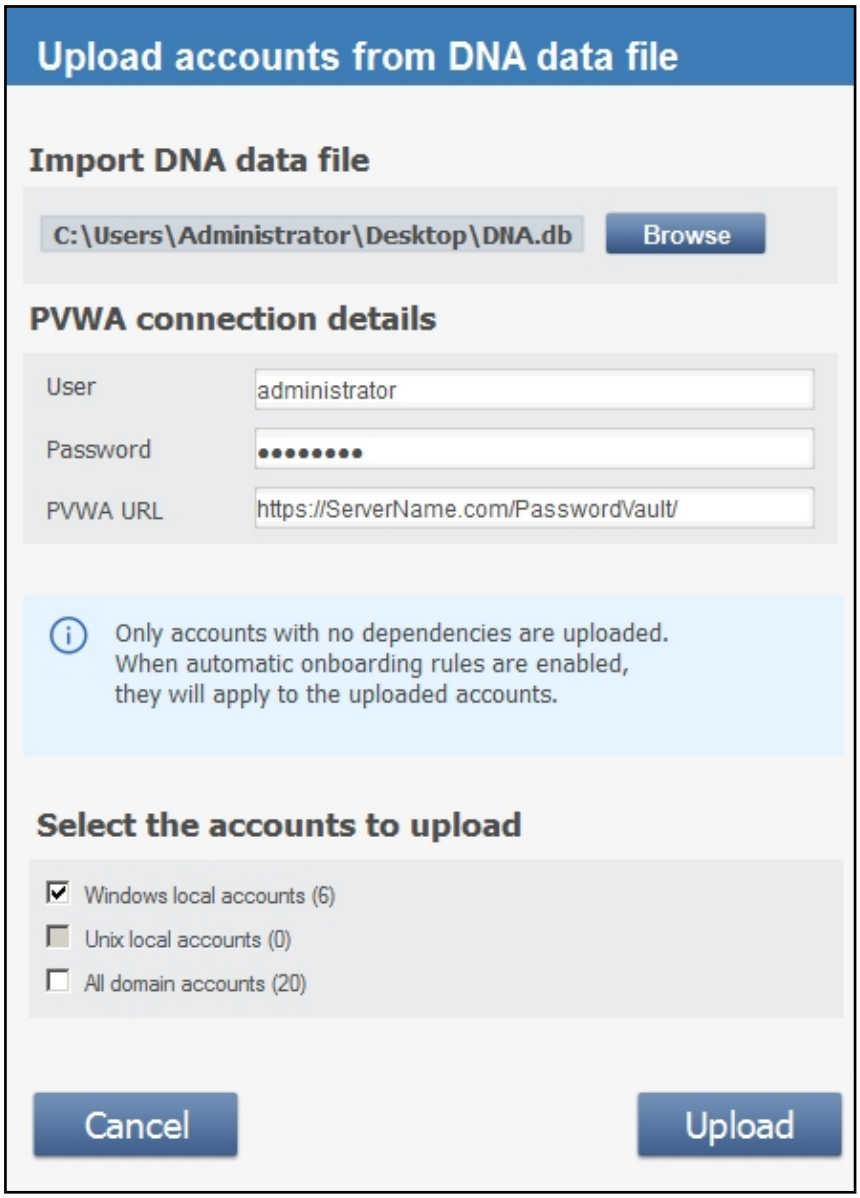
1. In the DNA window, click **Upload accounts**. The Upload accounts window appears.

2. When you initiate this at the end of a scan, the **Import DNA data file** will be filled with the relevant data file of the scan that just ended.
   If this is initiated at a different time (not immediately after a scan), under **Import DNA data file**, click **Browse** to select the DNA DB file reports that include the accounts to onboard to the Pending Accounts.
3. Under **PVWA connection details**, specify the Vault user who will run this process, their Vault password, and the URL of the PVWA to which the accounts will be uploaded (for example: https://MyServer.mydomain.com/PasswordVault).

> **Note:**
> This process only uploads accounts that do not have dependencies.

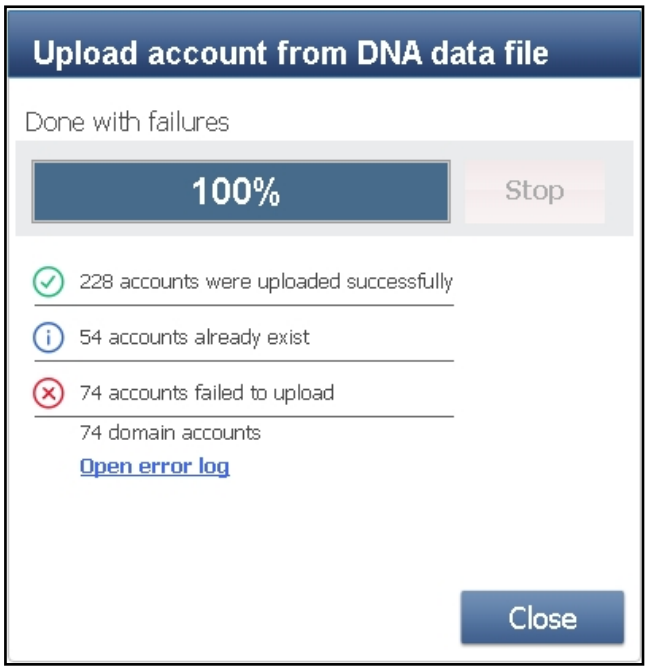
4. Under **Select the accounts to upload**, select the type of accounts in the DNA

report that will be uploaded.



5. Click **Upload**; the DNA uploads the relevant accounts to the Pending Accounts page in the PVWA.

6. If any errors occurred during the upload, after the upload is finished, a link to an error log is displayed so that you can view all the errors that happened during the process.



7. To provision these accounts in the Vault, log onto the PVWA. For more information, refer to *Pending Accounts* in the Privileged Access Security Implementation Guide.

Note:
If Automatic Onboarding Rules have been created, they will be applied to the uploaded accounts. This is relevant to version v10.2 and above.

Use DNA Reports

DNA scans your organization's network, then generates a report and visual organizational maps that evaluate the privileged account security status in your organization.

This chapter describes the DNA report, the organizational Pass-the-Hash Vulnerability map, the organizational SSH Keys Trusts map, and explains how to use these tools to expose security threats in your organization.

Understand DNA Reports

The Discovery and Audit Report is a comprehensive Excel file that provides detailed information about the current status of each privileged account that is identified.

Note:
You cannot view the report file using Microsoft Excel Viewer

The report includes the following Excel sheets:

- Executive Summary Dashboard
- Windows Scan
- Unix Scan
- Domain Scan
- SSH Keys Trust
- Database scan
- Hard-Coded Credentials
- Cloud Users
- Cloud Instances
- What is Insecure Priv. Esc.
- What are SSH Keys?
- What is Pass-the-Hash?
- Scan Errors

Executive Summary Dashboard

The first sheet in the Discovery and Audit Report is the Executive Summary Dashboard, which contains summarized information about the scan using charts and graphs, for a quick and simple overview.

Note:
The results of the database accounts scan are only displayed in the Database Scan sheet, and are not represented in the Executive Summary.

This summary comprises the following main areas:

Area	Summarizes
Machine/Account Data	The scan, the accounts that were discovered and their compliance status. For more information, refer to Machine/Account Data.
Embedded/Hard-Coded Credentials Discovery	the scan for embedded and hard-coded credentials. For more information, refer to Embedded/Hard-Coded Credentials Discovery, page 49.

Area	Summarizes
SSH Keys Discovery	the SSH keys discovery scan, their usage, and their compliance status. For more information, refer to SSH Keys Discovery, page 50.
Credential Theft Vulnerability	The threat and vulnerability status of Pass-the-Hash related attacks. For more information, refer to Credential Theft Vulnerability, page 51.
Cloud Asset Discovery	The cloud discovery scan, their type and their compliance status. For more information, refer to Cloud Asset Discovery, page 53

Machine/Account Data

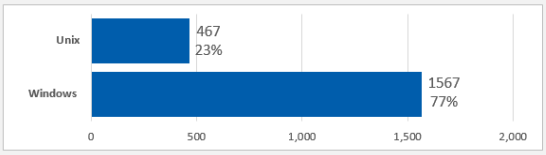
This area displays a summary of the scan, the machines that were scanned, and the accounts that were discovered.

MACHINE/ACCOUNT DATA

ABOUT THE SCAN

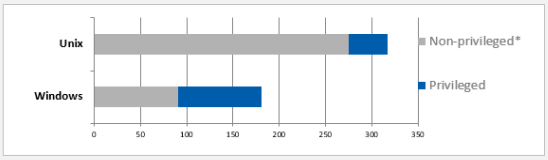
Scan date	Monday December 12 2016 12:12:16
Licensee name	CyberArk
Created by	Administrator
Password policy	Passwords of compliant accounts are changed every 90 days
Windows machine types	Servers and workstations
Windows object types	Accounts, Service Accounts
Unix machine types	Servers and workstations
Unix object types	Accounts
LDAP path	CN=Computers,DC=DNAdom,DC=com

MACHINES SCANNED



O/S	#
Windows	1,567
Unix	467
Total machines scanned	2,034

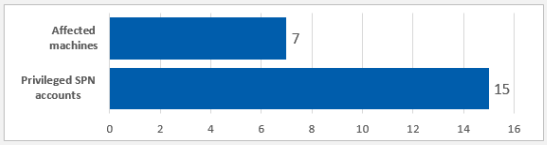
ACCOUNTS DISCOVERED



	Windows	Unix
Non-privileged*	91	275
Privileged	90	42
Total accounts discovered	181	317

* Not including non-privileged account members of the Domain Users group

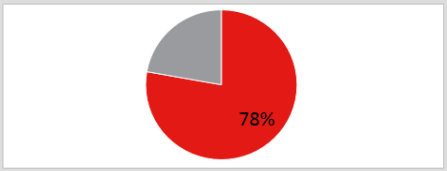
DOMAIN SERVICE ACCOUNTS DISCOVERED



Privileged SPN accounts	15
Affected machines	7

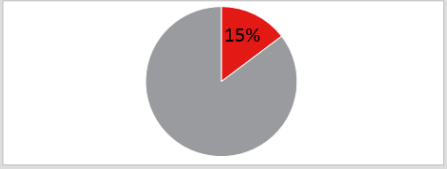
RISK STATUS

WINDOWS COMPLIANCE



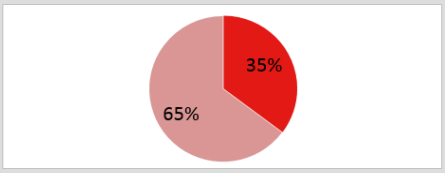
Non-compliant accounts	3,752
Compliant accounts	1,071
Total Windows accounts	4,823

UNIX COMPLIANCE



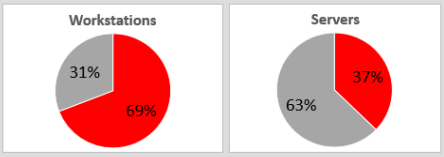
Non-compliant accounts	337
Compliant accounts	1,962
Total Unix accounts	2,299

TOTAL NON-COMPLIANT



Privileged accounts	113
Non-privileged accounts	208

LEAST PRIVILEGE RISK - WINDOWS BUSINESS USERS



	Workstations	Servers
Privileged business users*	56	48
Non-Privileged business users	25	81
Total business users	81	129

* Privileged business users includes all privileged accounts, and excludes the built-in Administrator

It includes the following information:

- About the Scan – A summary of the scan details:

Data	Description
Scan date	The date and time the scan was performed.
Licensee name	The person or organization DNA is licensed to.
Created by	The display name of the user logged on to the machine where CyberArk DNA is run.
LDAP path	The LDAP path used to identify the accounts to scan. **Note:** If the scan was performed on accounts listed in an imported file, the displayed LDAP path will be N/A.
Windows machine types	The type of machines selected for scanning. On Windows machines, this can be Servers, Workstations, or Servers and Workstations.
Windows object type	The type of objects selected for scanning. For Windows, this can be Accounts (privileged accounts and non-privileged accounts) or Service Accounts (embedded Windows credentials) or both.
Unix machine types	The type of machines selected for scanning. On Unix/Linux machines, this is always Servers and Workstations.
Unix object type	The type of objects selected for scanning. For Unix/Linux, this is Accounts (privileged and non-privileged accounts).
Password policy	The current password policy that identifies non-compliant accounts. For more information about how policies work, refer to DNA Configuration, page 121, in Configuration Parameters.

- Machines Scanned – A bar chart that shows the number and percentage of Windows and Unix/Linux devices scanned, displayed by operating system. The number of machines scanned per operating system is displayed below the chart.

Note:
This number includes both machines that were completed successfully and those where the scan completed with issues

- Accounts Discovered – A bar chart that shows the number of accounts detected on Windows and Unix/Linux devices, displayed by operating system. Privileged and non-privileged accounts are displayed in different colors. The number of privileged and non-privileged accounts detected per operating system is displayed below the chart.

Note:
This number does not include non-privileged account members of the Domain Users group

- Domain Service Accounts Discovered – A bar chart that shows the number of domain accounts that have the SPN attribute set and the machines that are affected

- by these SPN. The number of Privileged SPN accounts includes the unique number of users in the domain for each registered Service. A user can appear on several machines and with several registered Services.
- Risk Status – A set of pie charts that reflect the following:

Compliant/non-compliant accounts

The percentage of compliant/non-compliant accounts discovered on Windows and Unix machines during the scan. The exact number of compliant/non-compliant accounts is displayed below each chart.

DNA identifies compliant/non-compliant accounts according to the following criteria:

Compliancy	Indicates ...
Compliant	Accounts that meet organizational and standards compliancy, including a predefined maximum password age, key length, key type, etc.
Non-compliant	Accounts that do not meet organizational and standards compliancy.

Privileged/non-privileged accounts

The percentage of privileged/non- privileged accounts discovered on Windows and Unix machines during the scan. The exact number of privileged/non-privileged accounts is displayed below the chart.

DNA identifies privileged/non-privileged accounts according to the following criteria:

Privilege	Indicates ...
Privileged	Accounts that are accessed by users in the following groups: ▪ On Windows, this includes groups such as Power Users, Administrators, etc. ▪ On Unix, this also includes the root group and users listed in the sudoers file.
Non-privileged	Accounts that are accessed by users in any group not defined as privileged.

For more information, refer to Account Category in “windows and unix scans’

Least Privilege Risk – Windows business users

The percentage of privileged/non-privileged Windows business users. The exact number of each type of user discovered on Workstations and Servers is displayed below each chart.

DNA identifies Windows business users according to the following criteria:

Privileged Windows business users

Users included:	▪ Privileged domain users

- Privileged local users

Users excluded:

- Built-in administrator account of the local machine
- Built-in administrator account of the domain

Non-privileged Windows business users

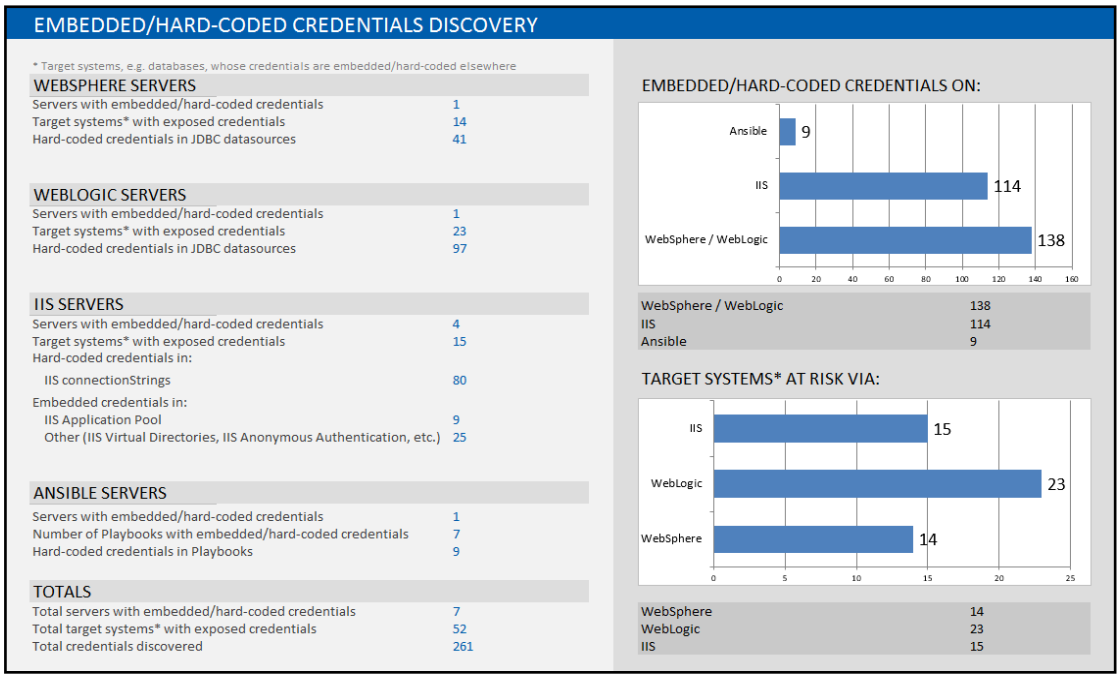
Users included:

- Any non-privileged accounts on Windows privileged domain users

Embedded/Hard-Coded Credentials Discovery

This area displays a summary of the risk that discovered embedded and hard-coded credentials pose, the machines that were scanned, and the accounts that were discovered.

For more information about how embedded or hard-coded credentials are defined, and how and where they are discovered, refer to Embedded and Hard-Coded Credentials, page 146.



It includes the following information:

- Summary (left side) – The number of embedded and hard-coded credentials found on WebSphere, WebLogic, IIS, and Ansible servers, the number of WebSphere, WebLogic and IIS servers or Ansible playbooks with these credentials, and the number of target systems (e.g. databases) or playbooks at risk as a result. This list enables you to see the level of risk that your environment is exposed to at a glance.
- Embedded/Hard-Coded Credentials Data (right side) – The number of embedded and hard-coded credentials discovered during the scan on WebSphere, WebLogic,

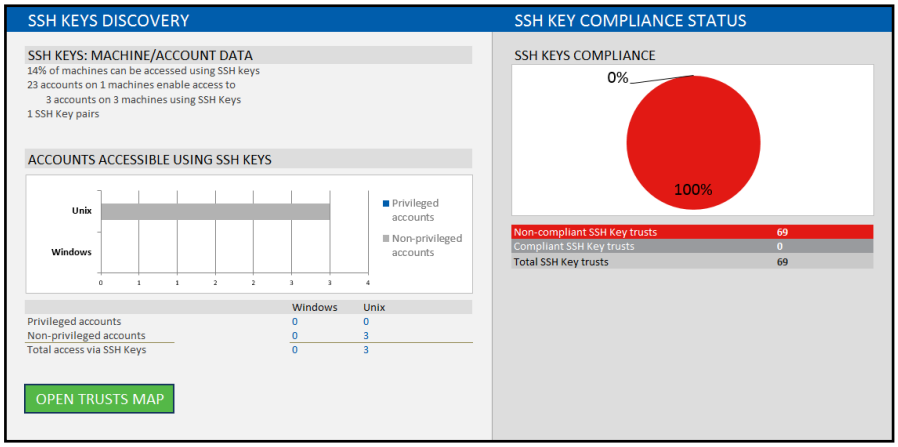
- IIS and Ansible servers. The exact number of credentials found on each server is displayed on and below each chart.
- Target systems at risk (right side) – The number of target systems (e.g. databases) at risk as a result of exposed credentials on WebSphere, WebLogic, IIS, and Ansible servers. The exact number of target systems at risk is displayed on and below each chart.

SSH Keys Discovery

This section displays a summary of the SSH keys discovery scan, their usage, and their compliance status.

DNA discovers private and public SSH keys on Unix and Windows machines in the following ways:

- Unix – DNA discovers private SSH keys in any configured path, and discovers public SSH keys using the authorized keys file used by the OpenSSH server.
- Windows – DNA discovers private and public SSH keys in any configured path. Public SSH keys are discovered using the authorized keys file used by the OpenSSH server running within Cygwin.



It includes the following information:

- Machine/account data – A summary of the accounts that were discovered during the scan that can potentially be used to access machines in your environment. This information includes the percentage of machines in your environment that can be accessed using SSH Keys, as well as the actual number of accounts on machines that enable this type of access.
- Accounts Accessible using SSH Keys – A bar chart that shows the unique number of discovered privileged and non-privileged Unix and Windows accounts that can be accessed using the discovered SSH Keys. The total number of these accounts is displayed below the chart.
- SSH Keys Trusts Map – Display a visual representation of the machines in your organization that can potentially be accessed using SSH keys. To display the map, click OPEN TRUSTS MAP. For more information, refer to Focus on a Specific Machine, page 91.
- Compliance Status – A set of pie charts that reflect the percentage of compliant and

- non-compliant SSH keys and accounts discovered during the scan. The exact number of compliant and non-compliant keys is displayed below each chart.

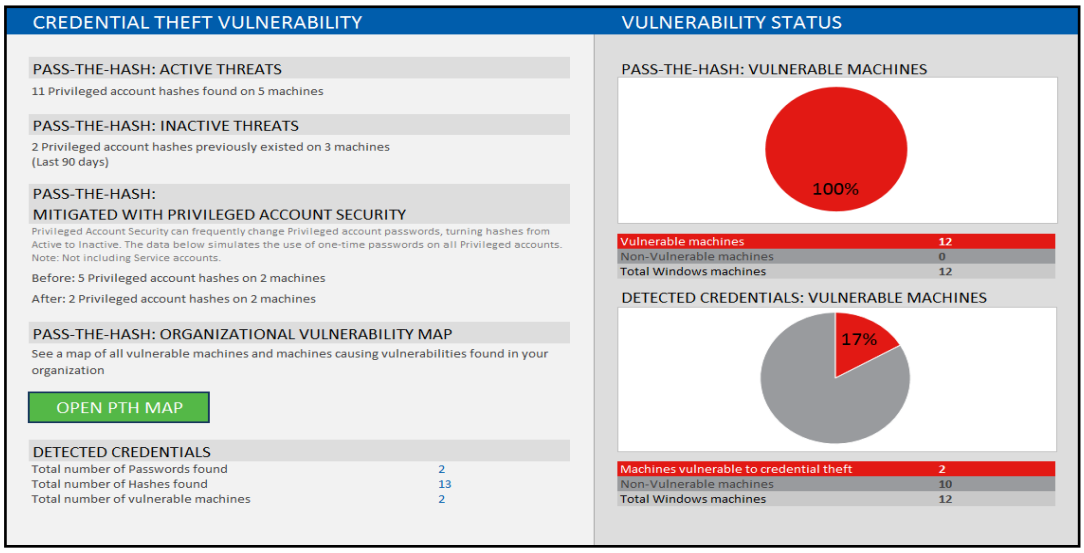
> **Note:**
> SSH Keys are compliant if their key age is lower than or equal to the maximum key age defined in the SSHKeyMaxAgeInDays parameter in the DNA Configuration file. For more information, refer to DNA Configuration, page 121

Alternatively, compliant SSH Keys must meet the defined strength (length and algorithm). For more information about these criteria, refer to SSH Key Compliance Criteria, page 145.

> **Note:**
> SSH Keys are non-compliant if they do not meet one or more of these criteria

Credential Theft Vulnerability

This area displays the threat and vulnerability status of Credential Theft related attacks (Golden Ticket, Pass-the-Hash, Pass-the-Ticket and Overpass-the-Hash).



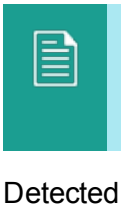
It includes the following information:

- Active threats – These threats indicate stored privileged account hashes that may currently be leveraged against vulnerable machines and cause risk to your organization.
- Inactive threats – These threats indicate privileged account hashes that were previously stored on a machine posed a risk to your organization at that time.
- Mitigated with Privileged Access Security – With Privileged Access Security it is possible to manage Privileged account passwords and frequently change them, turning hashes from Active to Inactive. The data in this section simulates the organization's threat status with the use of one-time passwords on all privileged

- accounts.

Note:
This simulation does not include discovered service account hashes, since they are always stored on the scanned machine. The threat of service account hashes should be mitigated using segmentation and least-privilege security strategy

- Pass-the-Hash: Organization Vulnerability Map – Display a visual representation of the machines in your organization that are vulnerable to Pass-the-Hash attacks as well as the machines that are at fault. To display the map, click OPEN PTH MAP. For more information, refer to The Organizational Pass-the-Hash Vulnerability Map, page 81.



Note:
This map also includes a Golden Ticket attack indication if DNA finds this vulnerability.

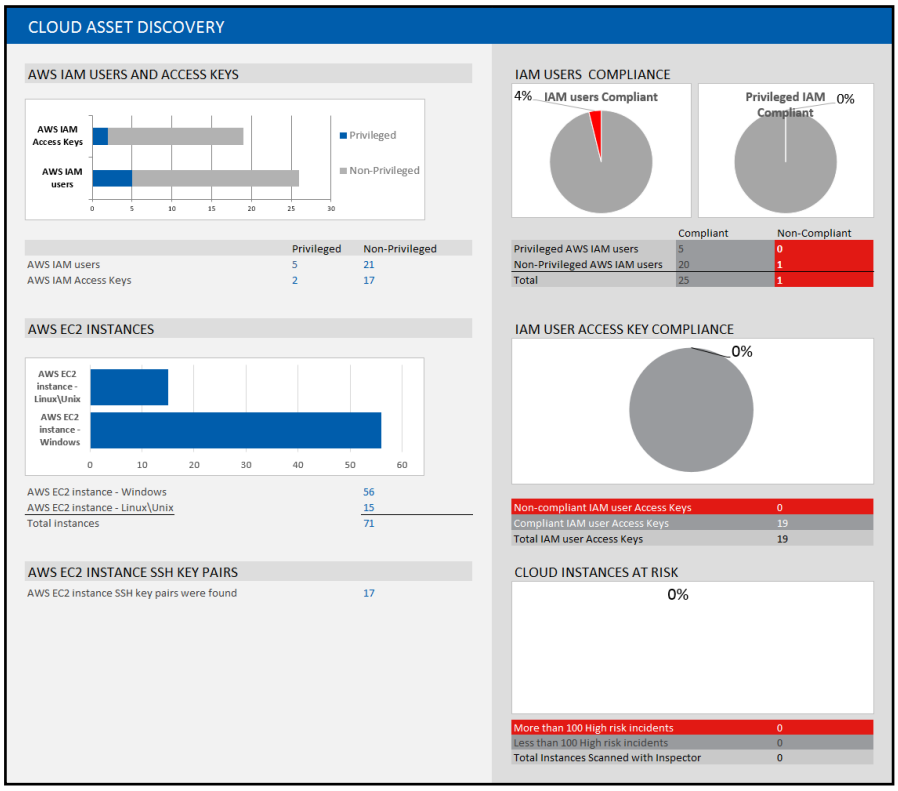
- Detected Credentials - These numbers indicate the actual passwords and hashes found on scanned machines. Using the deep credentials detection, DNA can detect the actual passwords and hashes on a scanned machine. This table summarizes all the passwords and hashes a potential attacker could reveal and emphasizes the risk around endpoint security and managing credentials.
- Vulnerability Status – A set of pie charts that reflect the following:
  - Pass-the-Hash: Vulnerable Machines - A pie chart that reflects the percentage of vulnerable and non-vulnerable machines. Below the chart, the number of vulnerable and non-vulnerable machines and the total number of Windows machines found in the environment is displayed.
  - Detected Credentials: Vulnerable Machines – A pie chart that reflects the percentage of vulnerable machines for credentials theft and non-vulnerable machines. Below the chart, the number of vulnerable and non-vulnerable machines for credentials theft and the total number of Windows machines found in the environment is displayed.

According to DNA's findings, the potential total number of privileged accounts that can cause a risk to the organization due to stored hashes, is the sum of Active and Inactive threats. For example, a combined total of 97 active threats and 277 inactive threats indicates that there are a total of 374 privileged accounts whose hashes can potentially be stored in your organization.

In addition, the total number of potential machines that store hashes is the sum of Active and Inactive threats. For example, a combined total of 347 machines where active threats are stored and 481 machines where inactive threats are stored indicates that there are a total of 828 machines in your organization that can potentially store hashes at any time.

Cloud Asset Discovery

This area displays the total number of credentials found (IAM users, Access Keys and EC2 Key pairs) in a cloud discovery. If AWS Inspector has run as well, this area also displays the amount of high severity security findings on scanned EC2 Instances.

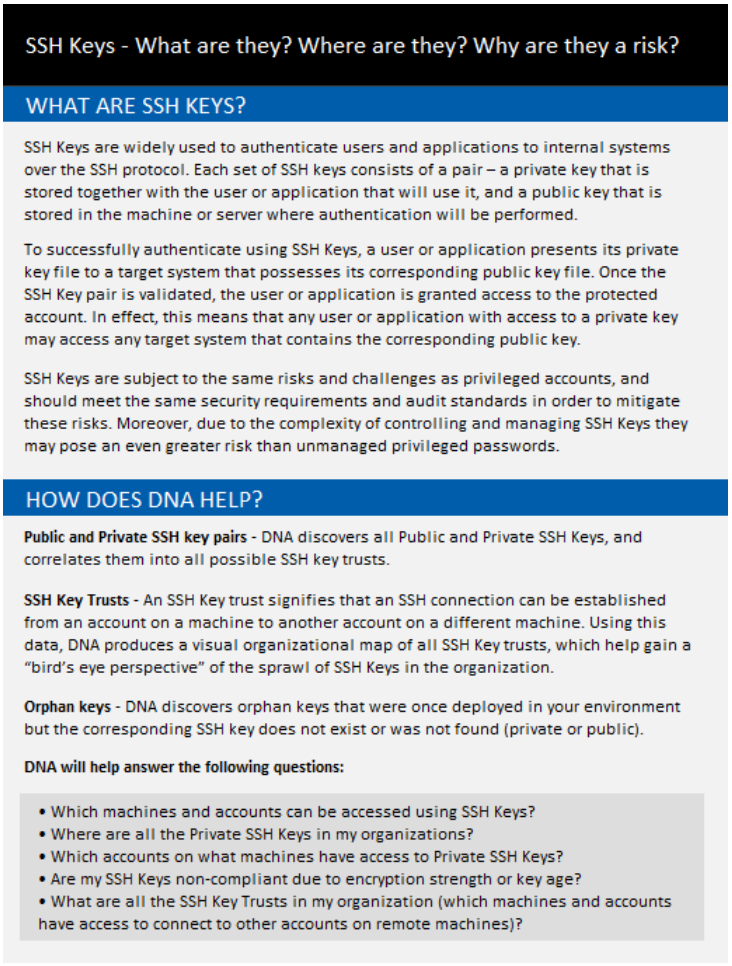


It includes the following information:

- AWS IAM Users and Access Keys (left side) – A summary of accounts and keys that were discovered during the scan. The IAM users and Access Keys are divided by privileged/non-privileged and their compliancy.
- AWS EC2 Instances (left side) - A summary of all EC2 instances found in the discovery, divided by operating system.
- AWS EC2 Instances SSH Key Pairs (left side)- A summary of the number of EC2 instances key pairs found in the discovery.
- IAM Users Compliance (right side) – Two pie charts that describe the overall status of total IAM users compliance and the Privileged IAM users compliance.
- IAM Users Access Keys Compliance (right side) – A pie chart that describes the compliance and non-compliance of IAM Users Access Keys found in the scan.
- Cloud Instances at Risk (right side) – A pie chart that describes the status of EC2 Instances scanned by AWS Inspector. The pie chart describes the number of instances with more and less than 100 high severity security findings, including the total number of EC2 instances that were scanned.

What are SSH Keys?

The 'What are SSH Keys' sheet explains how SSH Keys are used and their risks. It also explains how DNA helps you assess the current and potential risk of SSH key exposure in your organization.



SSH Keys - What are they? Where are they? Why are they a risk?

WHAT ARE SSH KEYS?

SSH Keys are widely used to authenticate users and applications to internal systems over the SSH protocol. Each set of SSH keys consists of a pair – a private key that is stored together with the user or application that will use it, and a public key that is stored in the machine or server where authentication will be performed.

To successfully authenticate using SSH Keys, a user or application presents its private key file to a target system that possesses its corresponding public key file. Once the SSH Key pair is validated, the user or application is granted access to the protected account. In effect, this means that any user or application with access to a private key may access any target system that contains the corresponding public key.

SSH Keys are subject to the same risks and challenges as privileged accounts, and should meet the same security requirements and audit standards in order to mitigate these risks. Moreover, due to the complexity of controlling and managing SSH Keys they may pose an even greater risk than unmanaged privileged passwords.

HOW DOES DNA HELP?

Public and Private SSH key pairs - DNA discovers all Public and Private SSH Keys, and correlates them into all possible SSH key trusts.

SSH Key Trusts - An SSH Key trust signifies that an SSH connection can be established from an account on a machine to another account on a different machine. Using this data, DNA produces a visual organizational map of all SSH Key trusts, which help gain a "bird's eye perspective" of the sprawl of SSH Keys in the organization.

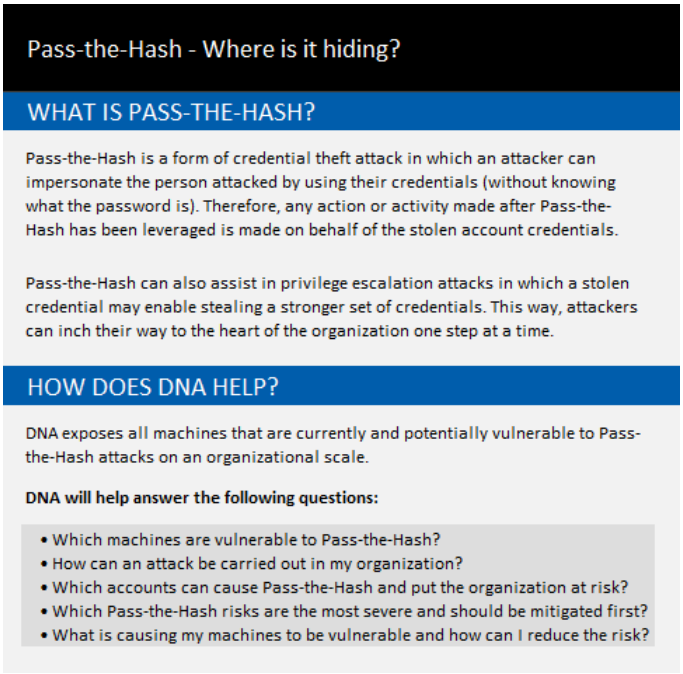
Orphan keys - DNA discovers orphan keys that were once deployed in your environment but the corresponding SSH key does not exist or was not found (private or public).

DNA will help answer the following questions:

- Which machines and accounts can be accessed using SSH Keys?
- Where are all the Private SSH Keys in my organizations?
- Which accounts on what machines have access to Private SSH Keys?
- Are my SSH Keys non-compliant due to encryption strength or key age?
- What are all the SSH Key Trusts in my organization (which machines and accounts have access to connect to other accounts on remote machines)?

What is Pass-the-Hash?

The “What is Pass-the-Hash” sheet explains how Pass-the-Hash attacks work and how DNA helps you assess the current and potential risk of Pass-the-Hash attacks in your organization.



Pass-the-Hash - Where is it hiding?

WHAT IS PASS-THE-HASH?

Pass-the-Hash is a form of credential theft attack in which an attacker can impersonate the person attacked by using their credentials (without knowing what the password is). Therefore, any action or activity made after Pass-the-Hash has been leveraged is made on behalf of the stolen account credentials.

Pass-the-Hash can also assist in privilege escalation attacks in which a stolen credential may enable stealing a stronger set of credentials. This way, attackers can inch their way to the heart of the organization one step at a time.

HOW DOES DNA HELP?

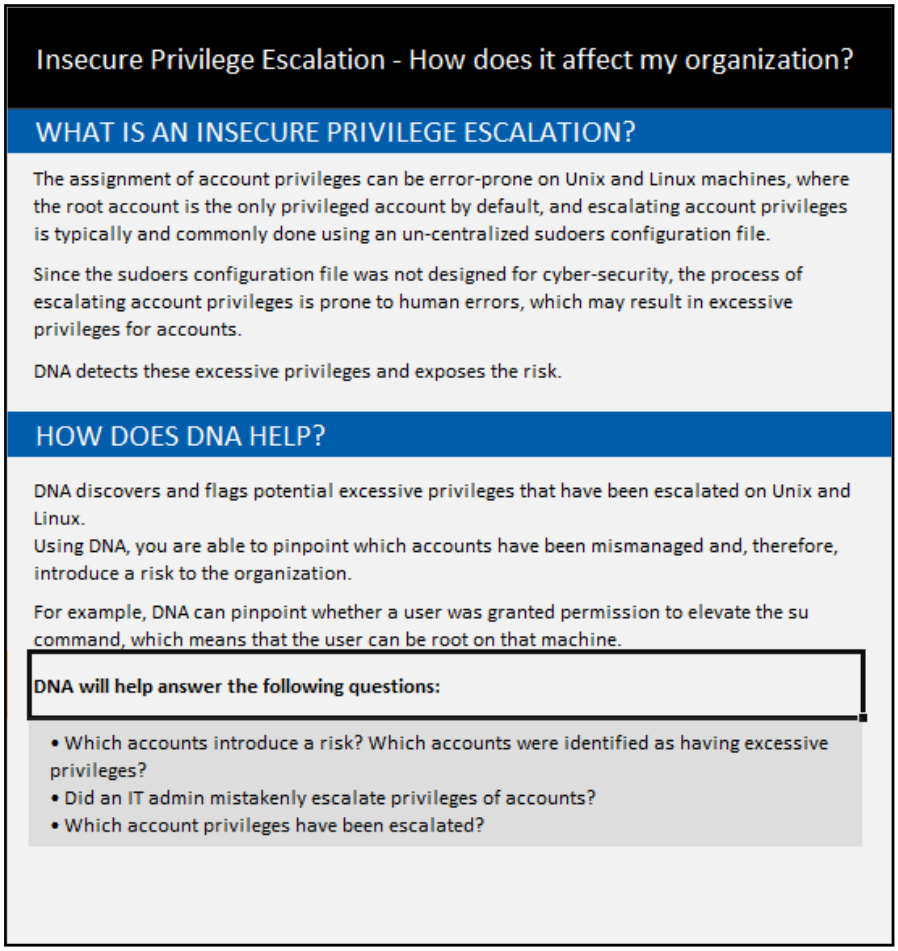
DNA exposes all machines that are currently and potentially vulnerable to Pass-the-Hash attacks on an organizational scale.

DNA will help answer the following questions:

- Which machines are vulnerable to Pass-the-Hash?
- How can an attack be carried out in my organization?
- Which accounts can cause Pass-the-Hash and put the organization at risk?
- Which Pass-the-Hash risks are the most severe and should be mitigated first?
- What is causing my machines to be vulnerable and how can I reduce the risk?

What is Insecure Privilege Escalation?

The “What is Insecure Privilege Escalation?” sheet explains what Insecure Privilege Escalation is and how DNA helps you assess the current and potential privilege escalation risk in your organization.



Insecure Privilege Escalation - How does it affect my organization?

WHAT IS AN INSECURE PRIVILEGE ESCALATION?

The assignment of account privileges can be error-prone on Unix and Linux machines, where the root account is the only privileged account by default, and escalating account privileges is typically and commonly done using an un-centralized sudoers configuration file.

Since the sudoers configuration file was not designed for cyber-security, the process of escalating account privileges is prone to human errors, which may result in excessive privileges for accounts.

DNA detects these excessive privileges and exposes the risk.

HOW DOES DNA HELP?

DNA discovers and flags potential excessive privileges that have been escalated on Unix and Linux.
Using DNA, you are able to pinpoint which accounts have been mismanaged and, therefore, introduce a risk to the organization.

For example, DNA can pinpoint whether a user was granted permission to elevate the su command, which means that the user can be root on that machine.

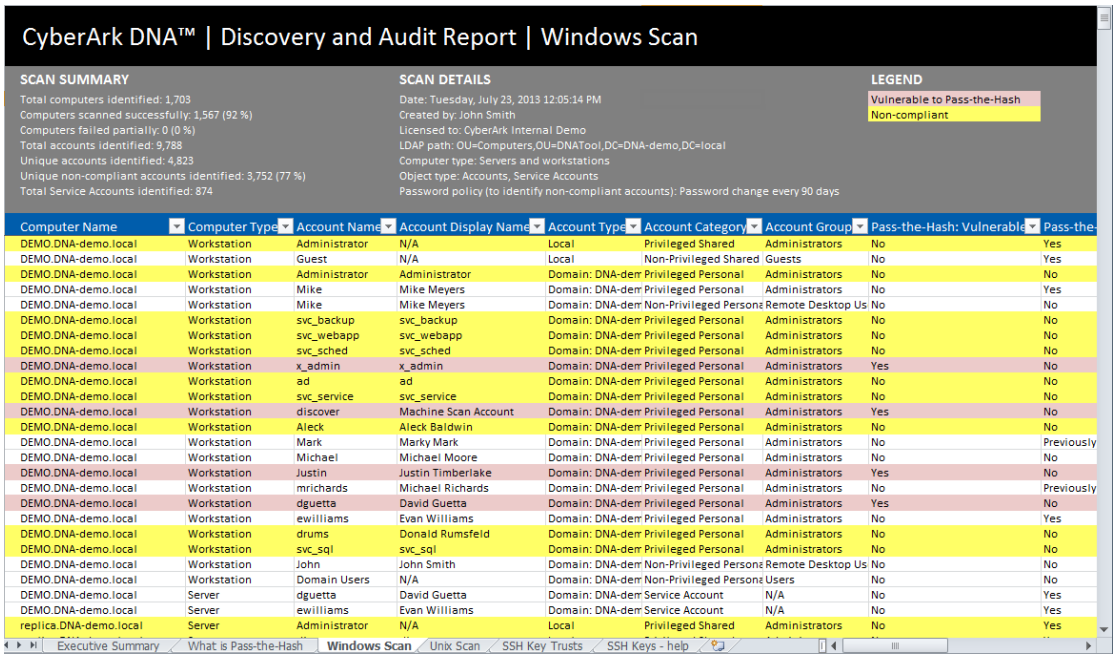
DNA will help answer the following questions:

- Which accounts introduce a risk? Which accounts were identified as having excessive privileges?
- Did an IT admin mistakenly escalate privileges of accounts?
- Which account privileges have been escalated?

Windows and Unix Scans

The DNA scan results for Windows and Unix/Linux/Mac devices are displayed on separate sheets. Each row in the report represents an account or service account identified on a specific machine. An account can appear more than once on the same machine if it belongs to more than one group. If a machine cannot be scanned, its name and type is displayed along with an error indication.

The Scan Summary/Scan Details area at the top of the report offers an at-a-glance, high level overview of the scan results.



CyberArk DNA™ | Discovery and Audit Report | Windows Scan

SCAN SUMMARY
Total computers identified: 1,703
Computers scanned successfully: 1,567 (92 %)
Computers failed partially: 0 (0 %)
Total accounts identified: 9,788
Unique accounts identified: 4,823
Unique non-compliant accounts identified: 3,752 (77 %)
Total Service Accounts identified: 874

SCAN DETAILS
Date: Tuesday, July 23, 2013 12:05:14 PM
Created by: John Smith
Licensed to: CyberArk Internal Demo
LDAP path: OU=Computers,OU=DNATool,DC=DNA-demo,DC=local
Computer type: Servers and workstations
Object type: Accounts, Service Accounts
Password policy (to identify non-compliant accounts): Password change every 90 days

LEGEND
Vulnerable to Pass-the-Hash
Non-compliant

Computer Name	Computer Type	Account Name	Account Display Name	Account Type	Account Category	Account Group	Pass-the-Hash: Vulnerable	Pass-the-
DEMO.DNA-demo.local	Workstation	Administrator	N/A	Local	Privileged Shared	Administrators	No	Yes
DEMO.DNA-demo.local	Workstation	Guest	N/A	Local	Non-Privileged Shared	Guests	No	Yes
DEMO.DNA-demo.local	Workstation	Administrator	Administrator	Domain: DNA-dem	Privileged Personal	Administrators	No	No
DEMO.DNA-demo.local	Workstation	Mike	Mike Meyers	Domain: DNA-dem	Privileged Personal	Administrators	No	Yes
DEMO.DNA-demo.local	Workstation	Mike	Mike Meyers	Domain: DNA-dem	Non-Privileged Persona	Remote Desktop Us	No	No
DEMO.DNA-demo.local	Workstation	svc_backup	svc_backup	Domain: DNA-dem	Privileged Personal	Administrators	No	No
DEMO.DNA-demo.local	Workstation	svc_webapp	svc_webapp	Domain: DNA-dem	Privileged Personal	Administrators	No	No
DEMO.DNA-demo.local	Workstation	svc_sched	svc_sched	Domain: DNA-dem	Privileged Personal	Administrators	No	No
DEMO.DNA-demo.local	Workstation	x_admin	x_admin	Domain: DNA-dem	Privileged Personal	Administrators	Yes	No
DEMO.DNA-demo.local	Workstation	ad	ad	Domain: DNA-dem	Privileged Personal	Administrators	No	No
DEMO.DNA-demo.local	Workstation	svc_service	svc_service	Domain: DNA-dem	Privileged Personal	Administrators	No	No
DEMO.DNA-demo.local	Workstation	discover	Machine Scan Account	Domain: DNA-dem	Privileged Personal	Administrators	Yes	No
DEMO.DNA-demo.local	Workstation	Aleck	Aleck Baldwin	Domain: DNA-dem	Privileged Personal	Administrators	No	No
DEMO.DNA-demo.local	Workstation	Mark	Marky Mark	Domain: DNA-dem	Privileged Personal	Administrators	No	Previously
DEMO.DNA-demo.local	Workstation	Michael	Michael Moore	Domain: DNA-dem	Privileged Personal	Administrators	No	No
DEMO.DNA-demo.local	Workstation	Justin	Justin Timberlake	Domain: DNA-dem	Privileged Personal	Administrators	Yes	No
DEMO.DNA-demo.local	Workstation	mrichards	Michael Richards	Domain: DNA-dem	Privileged Personal	Administrators	No	Previously
DEMO.DNA-demo.local	Workstation	dguetta	David Guetta	Domain: DNA-dem	Privileged Personal	Administrators	Yes	No
DEMO.DNA-demo.local	Workstation	ewilliams	Evan Williams	Domain: DNA-dem	Privileged Personal	Administrators	No	Yes
DEMO.DNA-demo.local	Workstation	drums	Donald Rumsfeld	Domain: DNA-dem	Privileged Personal	Administrators	No	No
DEMO.DNA-demo.local	Workstation	svc_sql	svc_sql	Domain: DNA-dem	Privileged Personal	Administrators	No	No
DEMO.DNA-demo.local	Workstation	John	John Smith	Domain: DNA-dem	Non-Privileged Persona	Remote Desktop Us	No	No
DEMO.DNA-demo.local	Workstation	Domain Users	N/A	Domain: DNA-dem	Non-Privileged Persona	Users	No	No
DEMO.DNA-demo.local	Server	dguetta	David Guetta	Domain: DNA-dem	Service Account	N/A	No	Yes
DEMO.DNA-demo.local	Server	ewilliams	Evan Williams	Domain: DNA-dem	Service Account	N/A	No	Yes
replica.DNA-demo.local	Server	Administrator	N/A	Local	Privileged Shared	Administrators	No	Yes

Executive Summary | What is Pass-the-Hash | Windows Scan | Unix Scan | SSH Key Trusts | SSH Keys - help

Windows Scan sheet

The Windows Scan sheet includes:

- Privileged and non-privileged accounts discovered on all scanned Windows machines.
- Public SSH Keys data. DNA discovers public SSH keys using the authorized keys file used by the OpenSSH server. On Windows, DNA discovers public SSH keys only when the OpenSSH server runs from within Cygwin. For more information, refer to the relevant explanations in the table below.
- Embedded Windows Credentials in locations such as Windows Services, Windows Scheduled Tasks, and IIS configuration files. For more information please see Embedded and Hard-Coded Credentials, page 146.
- Pass-the-Hash data about each Windows account. This data can be used to understand the risk of Pass-the-Hash and Golden Ticket attacks, as well as to prioritize a solution to the risk. For more information, refer to the relevant explanations in the table below.

The following indications help you identify accounts that are at risk:

- The rows highlighted in yellow indicate accounts that are non-compliant with the company's current password policy. Accounts are determined non-compliant if they are older than the maximum account password age specified in the AccountMaxPasswordAgeInDays parameter. For more information, refer to DNA Configuration, page 121, in Configuration Parameters, page 121.
- The rows highlighted in pink indicate accounts that are vulnerable to a Pass-the-Hash attack.

Unix Scan sheet

The Unix Scan sheet includes:

- Privileged and non-privileged accounts discovered on all scanned Unix machines.
- Public SSH Keys data. DNA discovers public SSH keys using the authorized keys file used by the OpenSSH server. For more information, refer to the relevant explanations in the table below.
- Insecure Privilege Escalation details about each Unix account. For more information, refer to the relevant explanations in the table below.

The following indications help you identify accounts that are at risk:

- The rows highlighted in yellow indicate accounts whose password is non-compliant with the company's current password policy or whose SSH key is non-compliant. SSH Keys are non-compliant if they do not meet one or more of the following criteria:
  - The age of the SSH Keys is lower than or equal to the maximum key age defined in the SSHKeyMaxAgeInDays parameter in the DNA Configuration file. For more information, refer to DNA Configuration, page 121, in Configuration Parameters, page 121.
  - The SSH Keys meet the defined strength (length and algorithm). For more information about these criteria, refer to SSH Key Compliance Criteria, page 145.
- The rows highlighted in pink indicate accounts whose privileges have been escalated insecurely.

The tables below explain the statistics included in the Scan Summary/Scan Details area.

SCAN SUMMARY	
Statistic	**Description**
Total machines identified	The total number of machines identified in the specified OU and all of its sub-OUs.
Machines scanned successfully	The total number of machines scanned successfully, and the percentage.
Machines failed partially	The total number of machines for which at least one but not all types of scans failed due to errors, and the percentage.
Total accounts identified	The total number of accounts identified in the scan.

Unique accounts identified	The total number of unique accounts identified in the scan.
Unique non-compliant accounts identified	The total number of unique non-compliant accounts identified in the scan.
Total service accounts identified (Windows only)	The total number of service accounts (embedded Windows credentials) identified in the scan. For a detailed description of embedded Windows credentials, refer to Embedded and Hard-Coded Credentials, page 146.
SCAN DETAILS	
Statistic	**Description**
Date	The current date and time, in the following format: day, month, date, year, time. For example: June 12, 2014 10:33 AM
Created by	The display name of the user logged on to the machine where CyberArk DNA is run.
Licensed to	The name of the company to whom CyberArk DNA is licensed.
LDAP path	The LDAP path used to identify the accounts to scan. **Note:** If the scan was performed on accounts listed in an imported file, the displayed LDAP path will be N/A.
Machine types	The type of machines selected for scanning. . On Windows machines, this can be Servers, Workstations, or Servers and Workstations. . On Unix/Linux machines, it is always Servers, Workstations.
Object types	The type of objects selected for scanning. . In the Windows Scan summary, this can be Accounts (privileged accounts and non-privileged accounts) or Service Accounts (embedded Windows credentials) or both. For a detailed description of embedded Windows credentials, refer to Embedded and Hard-Coded Credentials, page 146. . In the Unix Scan summary, this is Accounts (privileged accounts and non-privileged accounts).
Password policy	The current password policy that identifies non-compliant accounts. For more information about how policies work, refer to DNA Configuration, page 121, in Configuration Parameters, page 121.

The table below explains the columns included in the Windows and Unix scans.

Column	Specifies
Machine Name	The name of the current machine about which information was retrieved.
Machine Type (Windows only)	Whether the machine is a server or a workstation.
Account Name	The login name of the account about which information was retrieved.

Column	Specifies
Local Mapped Account (Unix only)	The local account to which the Active Directory account is mapped. If no local account is mapped, N/A is displayed.
Account Display Name	The account display name as it appears in the account properties. Usually contains a combination of the first and last name of the user.
Account Type	Whether the account is local or domain. In case of a domain account, this field also specifies the domain name.
Account Category	Whether the target account is privileged or non-privileged. For Windows, this column includes the following options: . Privileged Shared - Indicates that the account is local and a member of one of the following local groups: . Administrators . Power Users . Backup operators . Cryptographic operators . Distributed COM Users . Privileged Personal - Indicates that the account is a domain account and a member of one of the following local groups: . Administrators . Power Users . Backup operators . Cryptographic operators . Distributed COM Users . Non-Privileged Shared - Indicates that the account is a non-privileged local account. . Non-Privileged Personal - Indicates that the account is a non-privileged domain account. . Service Account – Indicates that the account is used to run a Windows service, or that it is defined in a scheduled task. The following types of service accounts are supported: . Windows Service . Scheduled Task . IIS Application Pool . IIS Anonymous Authentication . IIS Virtual Directory . IIS Configuration Redirection . IIS Authentication with ASP.NET Impersonation For Unix/Linux, this column includes the following options:
Account Category (cntd)	. Privileged Local - Indicates at least one of the following: . The account is local and a member of GID=0 group. . The account is local and UID=0. . The local account privileges have been escalated using the sudoers file, unless a sudo-replacement solution is used. . In AIX – The account has an "admin" attribute in the /etc/security/user file. . In HMC – The account is local and uses the

Column	Specifies
	hmcsuperadmin task role. . In VIOS – The account is local and uses the vios.oemsetupenv authorization. . Privileged Domain – Indicates at least one of the following: . The domain account is mapped to a local Unix/Linux account that is a member of GID=0 group. . The domain account is mapped to a local Unix/Linux account and is UID=0. . The domain account is mapped to a local Unix/Linux account whose privileges have been escalated using the sudoers file, unless a sudo-replacement solution is used. . In HMC – The domain account is mapped to a local Unix/Linux account that uses the hmcsuperadmin task role. . In VIOS – The domain account is mapped to a local Unix/Linux account that uses the vios.oemsetupenv authorization. . Non-Privileged Local - Indicates that the account is a non-privileged local account. . Non-Privileged Domain - Indicates that the domain account is mapped to a non-privileged local Unix/Linux account.
Account Group	The name of the local group of which the account is a member. . If the account does not belong to any local group, N/A is displayed. . For privileged accounts that were discovered in the sudoers file, *Sudoers file* is displayed. . For privileged accounts that were discovered on HMC machines, *hmcsuperadmin task role* is displayed. . For privileged accounts that were discovered on VIO machines, *vios.oemsetupenv authorization* is displayed.
Privileged Domain Group	The name of the domain group(s) that are a member of the local group stated in the Account Group column and that the user is a member of in the domain. If there is more than one group the group names are separated by semi-comma (';'). In case the user is a direct member of the local group, the value of this column will be N/A
Pass-the-Hash: Vulnerable (Windows only)	Whether or not this account hash was found on any other machine and this machine is, therefore, vulnerable to a Pass-the-Hack attack. Possible values are: . Yes – This account hash was found on another machine, making this machine vulnerable. . No – This account hash was not found on another machine, so this machine is not vulnerable.
Pass-the-Hash: Hash Found (Windows only)	Whether or not a hash for this account was found on this machine. Possible values are: . Yes – A hash for this account was found on this machine.

Column	Specifies
	. No – A hash for this account was not found on this machine. . Previously – A hash for this account was once stored on this machine. It no longer poses a threat, but constitutes a potential threat.
Causes Vulnerability on # of Machines (Windows only)	The number of machines that are vulnerable to a Pass-the-Hash attack, due to a detected stored account hash.
Threat cause (Windows only)	The reason(s) why the hash was stored on this machine. Possible values are: . Local login . Scheduled task was run . Windows Service was run . Machine unlocked . IIS authentication/Powershell script run . Remote command execution . Remote login via RDP . Local offline login
Account Description	The account's description field as it appears in the account properties.
Service Account Type (Windows only)	The type of service account identified. Possible values are: . Windows Service . Scheduled Task . IIS Application Pool . IIS Anonymous Authentication . IIS Virtual Directory . IIS Configuration Redirection . IIS Authentication with ASP.NET Impersonation For a detailed description of embedded Windows credentials, refer to Embedded and Hard-Coded Credentials, page 146.
Service Account Description (Windows only)	The display names of all identified embedded Windows credentials running under local and domain accounts. Possible values for IIS Servers are: . IIS Application Pool: Application Pool Name: <name> . IIS Anonymous Authentication: . Anonymous authentication configured for all sites and applications on the IIS server . Application Name: <name> . Site Name: <name> . IIS Virtual Directory: Virtual Directory Path: <name> . IIS Configuration Redirection: Redirection to: <name> . IIS Authentication with ASP.NET Impersonation: ASP.NET Impersonation: <name> For a detailed description of embedded Windows credentials, refer

Column	Specifies
	to Embedded and Hard-Coded Credentials, page 146.
Compliance Status	The current compliance status of each identified account. **Note:** Only enabled accounts can have a non-compliant status. Rows representing non-compliant accounts are highlighted in yellow. Possible values on Windows machines are: . Compliant – Accounts with a password age smaller than or equal to the maximum password age. . Non-compliant – Accounts with a password age larger than the maximum password age. Note: Only enabled accounts can have a non-compliant status. Rows representing non-compliant accounts appear highlighted in yellow. . N/A – Disabled, locked out, or expired accounts. The reason for non-compliance is displayed in a bold, red value in the Key Age column. Possible values on Unix/Linux machines are: . Compliant – Accounts or SSH Keys with a password/key age lower than or equal to the defined maximum age. In addition, SSH Keys must meet the defined key strength (length and algorithm). . Non-compliant (SSH Key) – SSH keys that are older than the defined maximum SSH keys age and/or whose key strength (length and algorithm) does not meet the specified criteria.
Compliance Status (cntd)	. Non-compliant (Password account) – Accounts that are older than the defined maximum password age. . Non-compliant (Password account, SSH Key) – Accounts or SSH keys that are older than the defined maximum age. In addition, for SSH keys, the key strength (length and algorithm) does not meet the specified criteria. . N/A – Disabled, locked out, or expired accounts or SSH Keys. The reason for non-compliance is displayed in a bold, red value for the Key Age and Key Length fields. For more information about criteria for SSH Keys compliant, refer to SSH Key Compliance Criteria, page 145.
Account State	The current state of an account. This field contains one of the following four values, based on priority (from high to low): 1 = Disabled (Password) 2 = Locked out (Password) 3 = Expired (Password) 4 = Enabled
Password Never Expires	Whether PasswordNeverExpires was defined on the account. This indicates that the user will not be required to change their password based on the domain password policy.
Password Length (Windows Only)	The length of the password in the account.
Credential Type (Windows Only)	The type of credential that was found. Possible values are: . Password . Hash

Column	Specifies
	. Password and Hash . None
Password Age	The current account password age, in days. This will appear as a fraction if the age is less than one day.
Insecure Privilege Escalation	The lines in the sudoers file that enable users other than the root user to bypass predefined rules. These lists are error-prone and may give excessive privileges for accounts.
Insecure Privilege Escalation: Reason	The reason why the identified configuration could be insecure. It may be either of the following: . The sudoers configuration file attempts to restrict the execution of commands using a blacklist. However, it is bad practice to use blacklists, since they are prone to human error and can be bypassed. . The sudoers configuration file attempts to restrict the execution of commands using a whitelist with wildcards. However, it is bad practice to use the "*" wildcard, since it can be bypassed.
Password Last Set	The date and time the password was last set. For more information, see Known Behavior and Limitations, page 140.
Last Login Date	Displays the last date and time that the account was used for login. This value can be affected by local logins as well as remote logins, for example, using an SSH key to connect to a Unix machine. . Local accounts on Windows and Unix – The last date and time the account was used to log into the current machine. . On Windows – If the account has never logged on to the machine, the value will be "Never". . Domain accounts on Windows machines: . If ScanPassTheHash is enabled - The last date and time the account was used to log into the scanned machine. . If ScanPassTheHash is disabled - The last date and time the account was used to log into any machine in the domain. . By default, Pass-The-Hash scanning is not supported on single core machines. Therefore, for accounts on single core machines, DNA will always show the last date and time the account was used to log into any machine in the domain. This can be changed by setting the Pass-The-Hash scan parameter in the DNA.exe.config file. For more information, refer to Configuration Parameters, page 121. . Note: When DNA did not discover any indication of a login, the Last Login Date value will be "Never, based on logs". . Domain accounts on Unix machines – The last date and time the account was used to log into the current machine. . Local Service accounts on Windows – The last date and time the account was used to log into the current machine or that the account was used to run the service.

Column	Specifies
	. Domain Service accounts on Windows – The last date and time the account was used to log into any machine in the domain or that the account was used to run the service. For more information, see Known Behavior and Limitations, page 140. Note: If the dates of the “Last Login Date” and the “Key Last Used” columns are identical, the last logon was done with an SSH key.
Account Expiration Date	The date and time on which the account is configured to expire.
Number of Keys Found	The number of public SSH keys found for this account on this machine. Note: When multiple SSH keys are found, details of the SSH key that poses the most risk is displayed. To view a list of all the SSH keys that were found, display the SSH Key Trusts sheet.
Last Key Update Date	The most recent date and time when the SSH key was last updated. DNA uses the operating system file timestamp to determine the date of the public SSH key. . On Unix/Linux machines and on Windows machines where Cygwin is installed, DNA uses the last modification date. . On Windows machines where Cygwin is not installed, DNA uses the creation date.
Key Age (at least)	The number of days since the public SSH key was last updated. DNA uses the “Last Key Update Date” value to calculate the “Key Age” value. The OpenSSH authorized keys file may contain multiple public SSH keys, and since its last modification date reflects its most recent update, it is not possible to determine the exact age of each key in the file. Therefore, the age that is presented for all public SSH keys in the file should be considered to be at least this age, although it could be older than this.
Key Length	The length of the key in bytes. For more information, refer to * below the table.
SSH Key Algorithm	The algorithm used to create the SSH Key pair. *
SSH Server	The version of the running OpenSSH server.
SSH Key Comment	The comment for configured public SSH Keys. *
Command Run on Login	The command that will be run after connection using this SSH Key (if relevant). *
Key Fingerprint	The fingerprint of the discovered SSH key. The public and private keys of the same trust have the same fingerprint. *
OS Version	The operating system version as defined in the machine’s account in the Active Directory.
Details	If CyberArk DNA was unable to scan a remote machine, this field will contain an error indication, such as “Network path not found” or

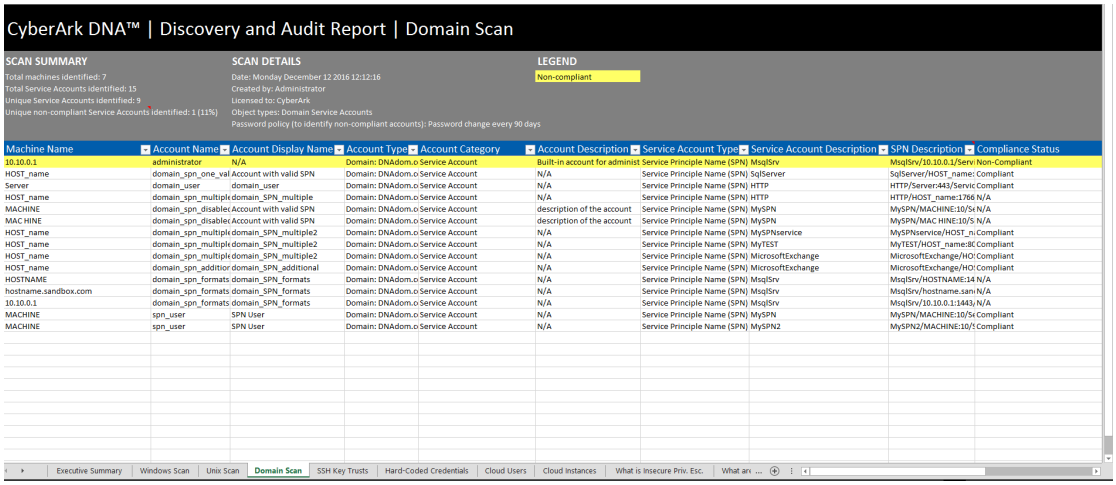
Column	Specifies
	“Access denied”.

Note:
When multiple SSH keys are found for a single account, only the details of the SSH key that poses the most risk is displayed. You can see how many SSH keys were found for this account in the ‘Number of Keys Found’ column. To view a list of all the SSH keys that were found, display the SSH Key Trusts sheet

Domain Scan

The DNA Domain scan results contains information about Domain users' Service Principal Name (SPN). Each row in the report represents a domain service account with a SPN of a specific machine. An account can appear more than once on the same machine or on several machines, depending on the number of services that it is registered to.

The Scan Summary/Scan Details area at the top of the report offers an at-a-glance, high level overview of the scan results.



The rows highlighted in yellow indicate accounts that are non-compliant with the company’s current password policy. Accounts are determined non-compliant if they are older than the maximum account password age specified in the AccountMaxPasswordAgeInDays parameter. For more information, refer to DNA Configuration, page 121, in Configuration Parameters, page 121.

The tables below explain the statistics included in the Scan Summary/Scan Details area.

SCAN SUMMARY	
Statistic	**Description**
Total machines identified	The total number of machines identified that have SPN related to them..
Total service accounts identified	The total number of domain service accounts identified in the scan.

Unique service accounts identified	The total number of unique domain service accounts identified in the scan.
Unique non-compliant service accounts identified	The total number of unique non-compliant domain service accounts identified in the scan.
SCAN DETAILS	
Statistic	**Description**
Date	The current date and time, in the following format: day, month, date, year, time. For example: June 12, 2014 10:33 AM
Created by	The display name of the user logged on to the machine where CyberArk DNA is run.
Licensed to	The name of the company to whom CyberArk DNA is licensed.
Object types	The type of objects scanned. . Domain Service Accounts
Password policy	The current password policy that identifies non-compliant accounts. For more information about how policies work, refer to DNA Configuration, page 121, in Configuration Parameters, page 121.

The table below explains the columns included in the Domain scan.

Column	Specifies
Machine Name	The name of the current machine about which information was retrieved.
Account Name	The login name of the account about which information was retrieved.
Account Display Name	The account display name as it appears in the account properties. Usually contains a combination of the first and last name of the user.
Account Type	This field specifies the domain name of the account.
Account Category	. Service Account – Indicates that the account is used to run a Kerberos registered service. The service name is displayed in the Service Account description column.
Account Description	The account's description field as it appears in the account properties.
Service Account Type	The type of service account identified. This is Service Principle Name (SPN).
Service Account Description	The name of the service as described in the SPN of the domain account.
SPN Description	The real SPN, as written in the account.
Compliance Status	The current compliance status of each identified account. **Note:** Only enabled accounts can have a non-compliant status. Rows representing non-compliant accounts are highlighted

Column	Specifies
	in yellow. Possible values are: . Compliant – Accounts with a password age smaller than or equal to the maximum password age. . Non-compliant – Accounts with a password age larger than the maximum password age. **Note:** Only enabled accounts can have a non-compliant status. Rows representing non-compliant accounts appear highlighted in yellow. . N/A – Disabled, locked out, or expired accounts. The reason for non-compliance is displayed in a bold, red value in the Key Age column.
Account State	The current state of an account. This field contains one of the following four values, based on priority (from high to low): . 1 = Disabled (Password) . 2 = Locked out (Password) . 3 = Expired (Password) . 4 = Enabled
Password Never Expires	Whether PasswordNeverExpires was defined on the account. This indicates that the user will not be required to change their password based on the domain password policy.
Password Age	The current account password age, in days. This will appear as a fraction if the age is less than one day.
Password Last Set	The date and time the password was last set. For more information, see Known Behavior and Limitations, page 140.
Last Login Date	Displays the last date and time that the account was used for login. This value displays the last date and time the account was used to log into any machine in the domain or that the account was used to run the service. can be affected by local logins as well as remote logins, for example, using an SSH key to connect to a Unix machine.
Account Expiration Date	The date and time on which the account is configured to expire.

SSH Key Trusts

DNA discovers private and public SSH keys on Unix and Windows machines in the following ways:

- Unix – DNA discovers private SSH keys in any configured path and discovers public SSH keys using the authorized keys file used by the OpenSSH server.
- Windows – DNA discovers private and public SSH keys in any configured path. Public SSH keys are discovered using the authorized keys file used by the OpenSSH server running within Cygwin.

The SSH Key Trusts sheet displays all discovered trusts between machines and accounts throughout the organization, enabling you to see their exposure The status of the private and public SSH keys is displayed for each trust.

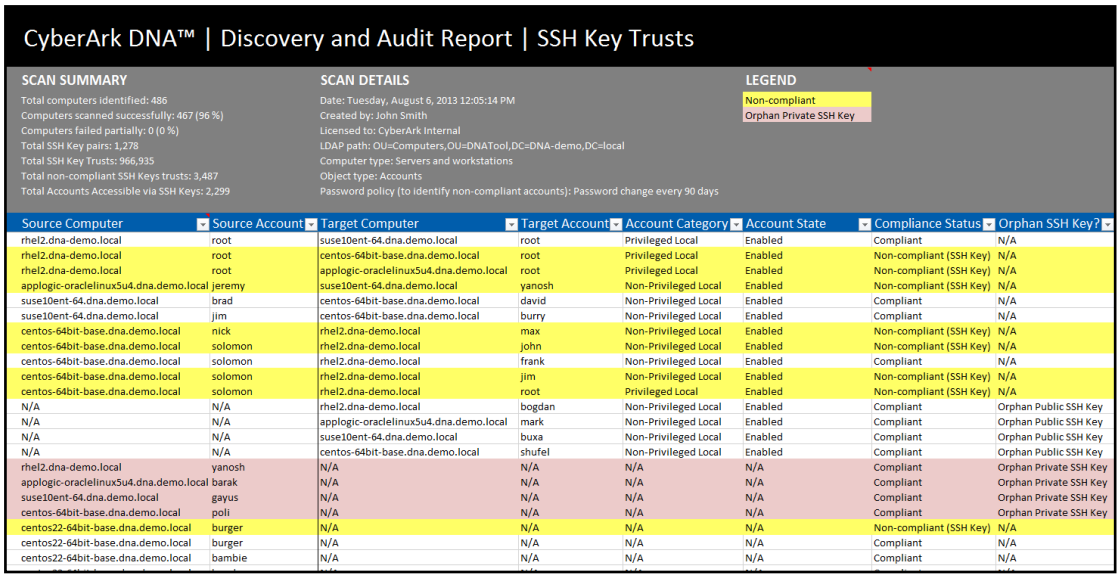
An SSH Key pair consists of two keys; a public SSH key and private SSH key. An SSH Key trust signifies that an SSH connection can be established from an account on a machine to another account on a different machine. Each row in the report represents this trust.

An SSH key can appear more than once for one machine since it may have trusts to multiple public SSH keys on multiple machines.

An “orphan” SSH Key is when one of the keys (public or private) in the SSH key pair was found, but its corresponding SSH key does not exist or was not found (private or public). This may be due to bad practice in SSH key management, or as a result of an unsuccessful scan.

Note:
Private OpenSSH SSH keys that are protected by a passphrase can never be correlated to their public SSH keys since they are encrypted, but they should not be considered “orphan” keys. Private PuTTY SSH keys that are passphrase-protected can be correlated to their public SSH keys, since they include the unencrypted public key

The Scan Summary/Scan Details area at the top of the report offers an at-a-glance, high level overview of the scan results.



CyberArk DNA™ | Discovery and Audit Report | SSH Key Trusts

SCAN SUMMARY

Total computers identified: 486
Computers scanned successfully: 467 (96 %)
Computers failed partially: 0 (0 %)
Total SSH Key pairs: 1,278
Total SSH Key Trusts: 966,935
Total non-compliant SSH Keys trusts: 3,487
Total Accounts Accessible via SSH Keys: 2,299

SCAN DETAILS

Date: Tuesday, August 6, 2013 12:05:14 PM
Created by: John Smith
Licensed to: CyberArk Internal
LDAP path: OU=Computers,OU=DNATool,DC=DNA-demo,DC=local
Computer type: Servers and workstations
Object type: Accounts
Password policy (to identify non-compliant accounts): Password change every 90 days

LEGEND

Non-compliant
Orphan Private SSH Key

Source Computer	Source Account	Target Computer	Target Account	Account Category	Account State	Compliance Status	Orphan SSH Key?
rhel2.dna-demo.local	root	suse10ent-64.dna.demo.local	root	Privileged Local	Enabled	Compliant	N/A
rhel2.dna-demo.local	root	centos-64bit-base.dna.demo.local	root	Privileged Local	Enabled	Non-compliant (SSH Key)	N/A
rhel2.dna-demo.local	root	applogic-oraclelinux5u4.dna.demo.local	root	Privileged Local	Enabled	Non-compliant (SSH Key)	N/A
applogic-oraclelinux5u4.dna.demo.local	jeremy	suse10ent-64.dna.demo.local	yanosh	Non-Privileged Local	Enabled	Non-compliant (SSH Key)	N/A
suse10ent-64.dna.demo.local	brad	centos-64bit-base.dna.demo.local	david	Non-Privileged Local	Enabled	Compliant	N/A
suse10ent-64.dna.demo.local	jim	centos-64bit-base.dna.demo.local	burry	Non-Privileged Local	Enabled	Compliant	N/A
centos-64bit-base.dna.demo.local	nick	rhel2.dna-demo.local	max	Non-Privileged Local	Enabled	Non-compliant (SSH Key)	N/A
centos-64bit-base.dna.demo.local	solomon	rhel2.dna-demo.local	john	Non-Privileged Local	Enabled	Non-compliant (SSH Key)	N/A
centos-64bit-base.dna.demo.local	solomon	rhel2.dna-demo.local	frank	Non-Privileged Local	Enabled	Compliant	N/A
centos-64bit-base.dna.demo.local	solomon	rhel2.dna-demo.local	jim	Non-Privileged Local	Enabled	Non-compliant (SSH Key)	N/A
centos-64bit-base.dna.demo.local	solomon	rhel2.dna-demo.local	root	Privileged Local	Enabled	Non-compliant (SSH Key)	N/A
N/A	N/A	rhel2.dna-demo.local	bogdan	Non-Privileged Local	Enabled	Compliant	Orphan Public SSH Key
N/A	N/A	applogic-oraclelinux5u4.dna.demo.local	mark	Non-Privileged Local	Enabled	Compliant	Orphan Public SSH Key
N/A	N/A	suse10ent-64.dna.demo.local	buxa	Non-Privileged Local	Enabled	Compliant	Orphan Public SSH Key
N/A	N/A	centos-64bit-base.dna.demo.local	shufel	Non-Privileged Local	Enabled	Compliant	Orphan Public SSH Key
rhel2.dna-demo.local	yanosh	N/A	N/A	N/A	N/A	Compliant	Orphan Private SSH Key
applogic-oraclelinux5u4.dna.demo.local	barak	N/A	N/A	N/A	N/A	Compliant	Orphan Private SSH Key
suse10ent-64.dna.demo.local	gayus	N/A	N/A	N/A	N/A	Compliant	Orphan Private SSH Key
centos-64bit-base.dna.demo.local	poli	N/A	N/A	N/A	N/A	Compliant	Orphan Private SSH Key
centos22-64bit-base.dna.demo.local	burger	N/A	N/A	N/A	N/A	Non-compliant (SSH Key)	N/A
centos22-64bit-base.dna.demo.local	burger	N/A	N/A	N/A	N/A	Compliant	N/A
centos22-64bit-base.dna.demo.local	bambie	N/A	N/A	N/A	N/A	Compliant	N/A

For the SSH Key Trusts sheet, the rows highlighted in pink indicate orphan private SSH keys (that do not use a passphrase). Orphan private SSH keys constitute bad practice in SSH key management, since their public SSH key counterpart is missing. Orphan private SSH keys can be used to re-create their public SSH key counterpart, which will then be used to establish and configure new SSH key trusts “under the radar”.

The tables below explain the statistics included in the Scan Summary/Scan Details area.

SCAN SUMMARY	
Statistic	**Description**
Total machines identified	The total number of machines identified in the specified OU and all of its sub-OUs.
Machines scanned successfully	The total number of machines scanned successfully, and the percentage.
Machines failed partially	The total number of machines for which at least one but not all types of scans failed due to errors, and the percentage.
Total accounts identified	The total number of accounts identified in the scan.
Unique accounts identified	The total number of unique accounts identified in the scan.
Unique non-compliant accounts identified	The total number of unique non-compliant accounts identified in the scan.
Total service accounts identified (Windows only)	The total number of service accounts (embedded Windows credentials) identified in the scan.
SCAN DETAILS	
Statistic	**Description**
Date	The current date and time, in the following format: day, month, date, year, time. For example: June 12, 2012 10:33 AM
Created by	The display name of the user logged on to the machine where

	CyberArk DNA is run.
Licensed to	The name of the company to whom CyberArk DNA is licensed.
LDAP path	The LDAP path used to identify the accounts to scan. **Note:** If the scan was performed on accounts listed in an imported file, the displayed LDAP path will be N/A.
Machine types	The type of machines selected for scanning. . On Windows machines, this can be Servers, Workstations, or Servers and Workstations. . On Unix/Linux machines, it is always Servers, Workstations.
Object types	The type of objects selected for scanning. This can be a combination of accounts (embedded and hard-coded credentials), privileged accounts and non-privileged accounts.
Password policy	The current password policy that identifies non-compliant accounts. For more information about how policies work, refer to DNA Configuration, page 121, in Configuration Parameters, page 121.

The table below explains the columns included in the SSH Key Trusts scan.

Column	Specifies
Source Machine	The name of the machine where the private SSH key was found.
Source Account	The name of the account that has access to the private SSH key that was found. This is determined using the file permissions as well as the directory that the key resides in.
Target Machine	The name of the machine where the public SSH key was found.
Target Account	The name of the account to which the detected SSH key enables access. This is determined using the permissions that are granted to the authorized keys file.
Account Category	Whether the target account is privileged or non-privileged. This column includes the following options: . Privileged Local - Indicates at least one of the following: . The account is local and a member of GID=0 group. . The account is local and UID=0. . The local account privileges have been escalated using the sudoers file. . In AIX – The account has an "admin" attribute in the /etc/security/user file. . In HMC – The account is local and uses the hmcsuperadmin task role. . In VIOS – The account is local and uses the vios.oemsetupenv authorization. . Privileged Domain – Indicates at least one of the following:

Column	Specifies
	. The domain account is mapped to a local Unix/Linux account that is a member of the GID=0 group. . The domain account is mapped to a local Unix/Linux account and is UID=0. . The domain account is mapped to a local Unix/Linux account whose privileges have been escalated using the sudoers file. . In HMC – The domain account is mapped to a local Unix/Linux account that uses the hmcsuperadmin task role. . In VIOS – The domain account is mapped to a local Unix/Linux account that uses the vios.oemsetupenv authorization. . Non-Privileged Local - Indicates that the account is a non-privileged local account. . Non-Privileged Domain - Indicates that the domain account is mapped to a non-privileged local Unix/Linux account.
Account State	The current state of an account. This field contains one of the following four values, based on priority (from high to low): 1 = Disabled 2 = Locked out 3 = Expired 4 = Enabled
Compliance Status	The current compliance status of each identified account. Possible values are: . Compliant – Accounts or SSH Keys with a password/key age lower than or equal to the defined maximum age. In addition, SSH Keys must meet the defined key strength (length and algorithm). . Non-compliant (SSH Key) – SSH keys that are older than the defined maximum SSH keys age and whose key strength (length and algorithm) does not meet the specified criteria. . Non-compliant (Password account) – Accounts that are older than the defined maximum password age. . Non-compliant (Password account, SSH Key) – Accounts or SSH keys that are older than the defined maximum age. In addition, for SSH keys, the key strength (length and algorithm) does not meet the specified criteria. . N/A – Disabled, locked out, or expired accounts or SSH Keys. . The reason for non-compliance is presented using a red and bold value for the Key Age and Key Length fields. . For more information about criteria for SSH Keys compliant, refer to SSH Key Compliance Criteria, page 145.
Orphan SSH Key?	If a pair of SSH keys were once deployed in your environment but one of the key pair could not be found during the scan, this

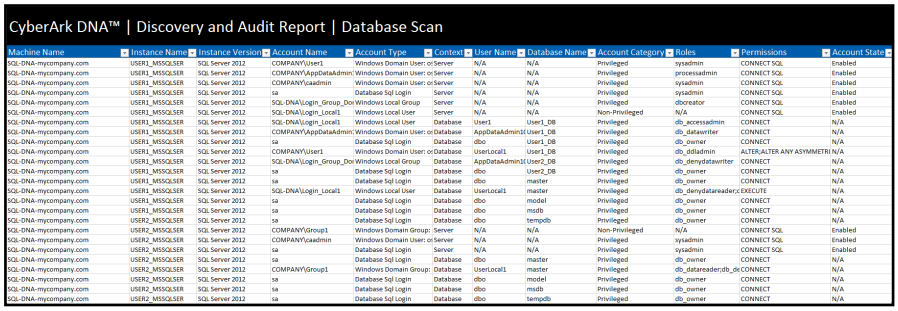
Column	Specifies
	indicates which single key was discovered.
Key Length	The length of the SSH keys.
Key Algorithm	The algorithm used to generate the SSH keys.
Passphrase Encryption	Whether or not a passphrase was used to encrypt the private SSH key and, if so, the type of encryption that was used. If a passphrase was not used, the value will be: . Passphrase Not Used
Key Last Used	The date and time when the SSH key trust was last used. This information is taken from the syslog on the OpenSSH server. If no usages were discovered by DNA, the value will show “Never, based on logs”. . The syslog includes the IP address of the source machine and the fingerprint of the SSH key. However, it does not contain account names and, therefore, it is not possible to determine without doubt which source account was used. DNA correlates the use of SSH keys based on the account that currently has permission to the key that was used, based on the fingerprint. . The discovered trust may be newer than the discovered Key Last Used date, since the data is extracted from the syslog, which contains historic data. It is possible that trust was previously used, then deleted, and then put in place again. . The syslog includes the IP address of the source machines and the fingerprint of the SSH key. However, it is possible that DNA will encounter an IP address of a machine that was not scanned. In this scenario, this will be marked in the ‘Source Machine’ column with “(from SSH log)”, and the following message will appear in the “Details” column: “DNA discovered the use of an SSH key from a Source Machine that was not scanned. It is possible that the IP has changed since use or that the machine was not scanned by DNA. See troubleshooting for more details.”
Last Trust Update Date	The date when the trust between a private and public SSH key was established. DNA uses the operating system file timestamp to determine this value. . On Unix/Linux machines and on Windows machines where Cygwin is installed, DNA uses the last modification date. . On Windows machines where Cygwin is not installed, DNA uses the creation date.
Trust Age (at least)	The number of days that have passed since the SSH key trust was established. DNA uses the “Last Trust Update Date” value to calculate the “Trust Age (at least)” value. Since the most recent date of the two timestamps of the private and

Column	Specifies
	public SSH keys is used, the Trust Age should be considered to be at least this age, and could be older than this. . On Unix/Linux machines and on Windows machines where Cygwin is installed, DNA uses the last modification date to determine the public and private SSH key age. . On Windows machines where Cygwin is not installed, DNA uses the creation date to determine the private SSH key age. . The OpenSSH authorized keys file may contain multiple public SSH keys and, since its last modification date reflects its most recent update, it should be considered to be at least this age, although it could be older than this. . When DNA correlates a trust between a private SSH key and a public SSH key, their dates are compared. The more recent date of the two values is presented in the "Trust Age (at least)" column. This date reflects the closest value to the number of days since the SSH Trust was established.
Key Age (at least)	The number of days since the private and/or public SSH key was created or last updated. DNA uses the "Last Key Update Date" value to calculate the "Key Age (at least)" value. DNA uses the operating system file timestamp to determine this value. . On Unix/Linux machines and on Windows machines where Cygwin is installed, DNA uses the last modification date to determine the public and private SSH key age. . On Windows machines where Cygwin is not installed, DNA uses the creation date to determine the private SSH key age. . The OpenSSH authorized keys file may contain multiple public SSH keys and, since its last modification date reflects its most recent update, it is not possible to determine the exact age of each key in the file. Therefore, the age that is presented for all public SSH keys in the file, should be considered to be at least this age, although it could be older than this. . When DNA correlates a trust between a private SSH key and a public SSH key, their dates are compared. The older date of the two values is presented in the "Key Age (at least)" column. This date reflects the closest value to the number of days since the SSH Key was created.
Key Comment	The comment in the public SSH key.
Command Run on Login	The command that is configured to run after the keys have established a connection, if any.
Private Key Type	The type of private SSH key that was detected. This column

Column	Specifies
	displays one of the following values: . OpenSSH . PuTTY
Private Key Path	The path and filename of the private SSH key.
Public Key Path	The path and filename of the public SSH key.
Key Fingerprint	The fingerprint of the discovered SSH key. The public and private keys of the same trust have the same fingerprint.
Details	If CyberArk DNA was unable to detect a connection using an SSH key, this field will specify the reason. For example, “SSH connections are disabled” or “The SSH server configuration does not allow the account to connect via SSH”.

Database Scan

DNA uses the Windows credentials of a domain user that has the **sysadmin** server role to log onto the target machine and discover users in MSSQL databases for local SQL or Windows/Local or domain users. The scan detects both privileged and non-privileged users.


CyberArk DNA™ | Discovery and Audit Report | Database Scan

Machine Name	Instance Name	Instance Version	Account Name	Account Type	Context	User Name	Database Name	Account Category	Roles	Permissions	Account State
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	COMPANY\User1	Windows Domain User: or	Server	N/A	N/A	Privileged	sysadmin	CONNECT SQL	Enabled
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	COMPANY\AppDataAdmin	Windows Domain User: or	Server	N/A	N/A	Privileged	processadmin	CONNECT SQL	Enabled
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	COMPANY\saadmin	Windows Domain User: or	Server	N/A	N/A	Privileged	sysadmin	CONNECT SQL	Enabled
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	sa	Database Sql Login	Server	N/A	N/A	Privileged	sysadmin	CONNECT SQL	Enabled
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	SQL-DNA\Login_Group_Do	Windows Local Group	Server	N/A	N/A	Privileged	dbcreator	CONNECT SQL	Enabled
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	SQL-DNA\Login_Local1	Windows Local User	Server	N/A	N/A	Non-Privileged	N/A	CONNECT SQL	Enabled
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	SQL-DNA\Login_Local1	Windows Local User	Database	User1	User1_DB	Privileged	db_accessadmin	CONNECT	N/A
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	COMPANY\AppDataAdmin	Windows Domain User: or	Database	AppDataAdmin1	User1_DB	Privileged	db_datawriter	CONNECT	N/A
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	sa	Database Sql Login	Database	dbo	User1_DB	Privileged	db_owner	CONNECT	N/A
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	COMPANY\User1	Windows Domain User: or	Database	UserLocal1	User1_DB	Privileged	db_ddladmin	ALTER;ALTER ANY ASYMMETRI	N/A
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	SQL-DNA\Login_Group_Do	Windows Local Group	Database	AppDataAdmin1	User2_DB	Privileged	db_denydatawriter	CONNECT	N/A
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	sa	Database Sql Login	Database	dbo	User2_DB	Privileged	db_owner	CONNECT	N/A
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	sa	Database Sql Login	Database	dbo	master	Privileged	db_owner	CONNECT	N/A
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	SQL-DNA\Login_Local1	Windows Local User	Database	UserLocal1	master	Privileged	db_denydatareader;c	EXECUTE	N/A
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	sa	Database Sql Login	Database	dbo	model	Privileged	db_owner	CONNECT	N/A
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	sa	Database Sql Login	Database	dbo	msdb	Privileged	db_owner	CONNECT	N/A
SQL-DNA-mycompany.com	USER1_MSSQLSER	SQL Server 2012	sa	Database Sql Login	Database	dbo	tempdb	Privileged	db_owner	CONNECT	N/A
SQL-DNA-mycompany.com	USER2_MSSQLSER	SQL Server 2012	COMPANY\Group1	Windows Domain Group:	Server	N/A	N/A	Non-Privileged	N/A	CONNECT SQL	Enabled
SQL-DNA-mycompany.com	USER2_MSSQLSER	SQL Server 2012	COMPANY\saadmin	Windows Domain User: or	Server	N/A	N/A	Privileged	sysadmin	CONNECT SQL	Enabled
SQL-DNA-mycompany.com	USER2_MSSQLSER	SQL Server 2012	sa	Database Sql Login	Server	N/A	N/A	Privileged	sysadmin	CONNECT SQL	Enabled
SQL-DNA-mycompany.com	USER2_MSSQLSER	SQL Server 2012	sa	Database Sql Login	Database	dbo	master	Privileged	db_owner	CONNECT	N/A
SQL-DNA-mycompany.com	USER2_MSSQLSER	SQL Server 2012	COMPANY\group1	Windows Domain Group:	Database	UserLocal1	master	Privileged	db_datareader;db_de	CONNECT	N/A
SQL-DNA-mycompany.com	USER2_MSSQLSER	SQL Server 2012	sa	Database Sql Login	Database	dbo	model	Privileged	db_owner	CONNECT	N/A
SQL-DNA-mycompany.com	USER2_MSSQLSER	SQL Server 2012	sa	Database Sql Login	Database	dbo	msdb	Privileged	db_owner	CONNECT	N/A
SQL-DNA-mycompany.com	USER2_MSSQLSER	SQL Server 2012	sa	Database Sql Login	Database	dbo	tempdb	Privileged	db_owner	CONNECT	N/A

The table below explains the columns included in the Database Scan sheet.

Column	Specifies
Machine name	The name of the server where the DB is installed.
Instance name	The name of the specific instance of the DB in the server.
Instance Version	The type of the database/instance and its version.
Account name	The name of the entity that can connect to the Server.
Account Type	The login authentication type. Possible values: Local, Domain: <domain name>, Database.
Context	Whether the account is on the context of the server or the database.
User name	The name of the entity that can connect to the database itself. If a login has several users, each user will have a separate line in the report.
Database name	The name of the database. There may be only one database per user.
Account Category	Whether the account is privileged or not. Possible values: Privileged, Non-Privileged.
Roles	A list of the database/instance roles (either of the login or the user) that this account belongs to, separated by ';'.
Permissions	A list of all the permissions of the login/user separated by ';' that this user has over the database.
Account State	Whether the account is enabled/disabled/locked/expired in the DB/Windows.

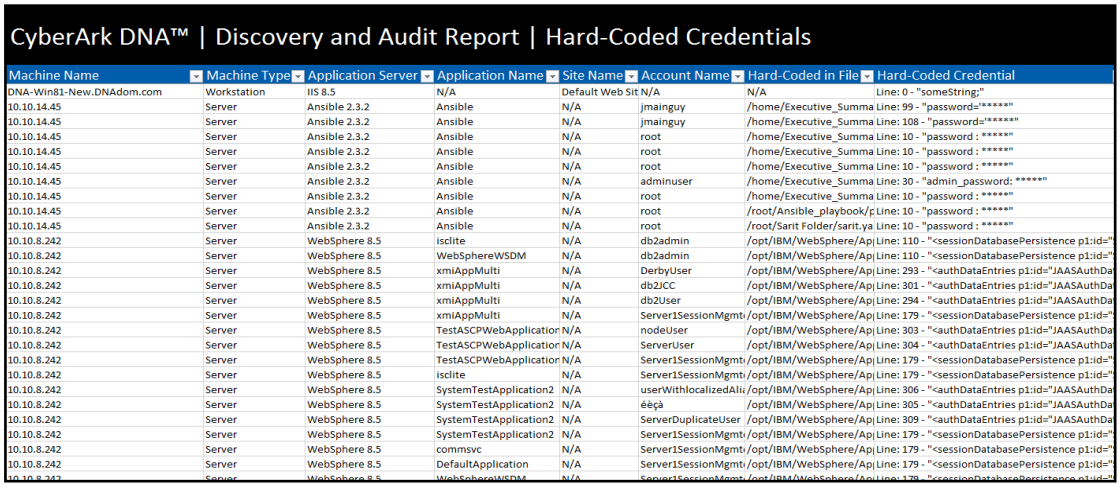
Hard-Coded Credentials

The Hard-Coded Credentials sheet displays the DNA scan results for hard-coded credentials discovered in files stored on machines in your enterprise. Each row in the report represents a credential that was discovered.

Applications use credentials to establish connections to a remote target machine or system. On WebSphere and WebLogic servers, DNA discovers such hard-coded credentials in data sources and on IIS servers. For Ansible Playbooks, DNA discovers hard-coded credentials in tasks, variables and other areas of the playbook. If a machine cannot be scanned, its name and type is displayed with an error indication.

For more information, refer to Embedded and Hard-Coded Credentials, page 146.

If the scan does not find any hard-coded credentials, this sheet will not be created.



CyberArk DNA™ | Discovery and Audit Report | Hard-Coded Credentials

Machine Name	Machine Type	Application Server	Application Name	Site Name	Account Name	Hard-Coded in File	Hard-Coded Credential
DNA-Win81-New.DNAdom.com	Workstation	IIS 8.5	N/A	Default Web Sit	N/A	N/A	Line: 0 - "someString;"
10.10.14.45	Server	Ansible 2.3.2	Ansible	N/A	jmainguy	/home/Executive_Summa	Line: 99 - "password='*****"
10.10.14.45	Server	Ansible 2.3.2	Ansible	N/A	jmainguy	/home/Executive_Summa	Line: 108 - "password='*****"
10.10.14.45	Server	Ansible 2.3.2	Ansible	N/A	root	/home/Executive_Summa	Line: 10 - "password : *****"
10.10.14.45	Server	Ansible 2.3.2	Ansible	N/A	root	/home/Executive_Summa	Line: 10 - "password : *****"
10.10.14.45	Server	Ansible 2.3.2	Ansible	N/A	root	/home/Executive_Summa	Line: 10 - "password : *****"
10.10.14.45	Server	Ansible 2.3.2	Ansible	N/A	adminuser	/home/Executive_Summa	Line: 30 - "admin_password: *****"
10.10.14.45	Server	Ansible 2.3.2	Ansible	N/A	root	/home/Executive_Summa	Line: 10 - "password : *****"
10.10.14.45	Server	Ansible 2.3.2	Ansible	N/A	root	/root/Ansible_playbook/p	Line: 10 - "password : *****"
10.10.14.45	Server	Ansible 2.3.2	Ansible	N/A	root	/root/Sarit Folder/sarit.ya	Line: 10 - "password : *****"
10.10.8.242	Server	WebSphere 8.5	isclite	N/A	db2admin	/opt/IBM/WebSphere/Ap	Line: 110 - "<sessionDatabasePersistence p1:id="
10.10.8.242	Server	WebSphere 8.5	WebSphereWSDM	N/A	db2admin	/opt/IBM/WebSphere/Ap	Line: 110 - "<sessionDatabasePersistence p1:id="
10.10.8.242	Server	WebSphere 8.5	xmiAppMulti	N/A	DerbyUser	/opt/IBM/WebSphere/Ap	Line: 293 - "<authDataEntries p1:id="JAASAuthDa
10.10.8.242	Server	WebSphere 8.5	xmiAppMulti	N/A	db2JCC	/opt/IBM/WebSphere/Ap	Line: 301 - "<authDataEntries p1:id="JAASAuthDa
10.10.8.242	Server	WebSphere 8.5	xmiAppMulti	N/A	db2User	/opt/IBM/WebSphere/Ap	Line: 294 - "<authDataEntries p1:id="JAASAuthDa
10.10.8.242	Server	WebSphere 8.5	xmiAppMulti	N/A	Server1SessionMgmt	/opt/IBM/WebSphere/Ap	Line: 179 - "<sessionDatabasePersistence p1:id="
10.10.8.242	Server	WebSphere 8.5	TestASCPWebApplication	N/A	nodeUser	/opt/IBM/WebSphere/Ap	Line: 303 - "<authDataEntries p1:id="JAASAuthDa
10.10.8.242	Server	WebSphere 8.5	TestASCPWebApplication	N/A	ServerUser	/opt/IBM/WebSphere/Ap	Line: 304 - "<authDataEntries p1:id="JAASAuthDa
10.10.8.242	Server	WebSphere 8.5	TestASCPWebApplication	N/A	Server1SessionMgmt	/opt/IBM/WebSphere/Ap	Line: 179 - "<sessionDatabasePersistence p1:id="
10.10.8.242	Server	WebSphere 8.5	isclite	N/A	Server1SessionMgmt	/opt/IBM/WebSphere/Ap	Line: 179 - "<sessionDatabasePersistence p1:id="
10.10.8.242	Server	WebSphere 8.5	SystemTestApplication2	N/A	userWithlocalizedAli	/opt/IBM/WebSphere/Ap	Line: 306 - "<authDataEntries p1:id="JAASAuthDa
10.10.8.242	Server	WebSphere 8.5	SystemTestApplication2	N/A	éèçà	/opt/IBM/WebSphere/Ap	Line: 305 - "<authDataEntries p1:id="JAASAuthDa
10.10.8.242	Server	WebSphere 8.5	SystemTestApplication2	N/A	ServerDuplicateUser	/opt/IBM/WebSphere/Ap	Line: 309 - "<authDataEntries p1:id="JAASAuthDa
10.10.8.242	Server	WebSphere 8.5	SystemTestApplication2	N/A	Server1SessionMgmt	/opt/IBM/WebSphere/Ap	Line: 179 - "<sessionDatabasePersistence p1:id="
10.10.8.242	Server	WebSphere 8.5	commsvc	N/A	Server1SessionMgmt	/opt/IBM/WebSphere/Ap	Line: 179 - "<sessionDatabasePersistence p1:id="
10.10.8.242	Server	WebSphere 8.5	DefaultApplication	N/A	Server1SessionMgmt	/opt/IBM/WebSphere/Ap	Line: 179 - "<sessionDatabasePersistence p1:id="

The table below explains the columns included in the Hard-coded Credentials sheet.

Column	Specifies
Machine Name	The name of the current machine about which information was retrieved.
Machine Type	Whether the machine is a server or a workstation.
Application Server	The name of the application server where the account was discovered. Possible values are: . IIS version . WebSphere version . WebLogic version . Ansible
Application Name	The name of the application that uses the discovered credentials. For credentials that are not linked to any application, eg, in IIS, 'Credentials not in use by any application' will be displayed.
Site Name	The name of the IIS website where the hard-coded credentials are stored. For credentials discovered on

Column	Specifies
	WebSphere, WebLogic application, or Ansible servers, 'N/A' will be displayed.
Account Name	The user name of the credential about which information was retrieved.
Hard-Coded in File	The name of the file in which the credentials are hard-coded. ▪ Credentials discovered on WebSphere are either stored in a security.xml or server.xml file. ▪ Credentials discovered on WebLogic are stored in a jdbc-xxxx.xml file. ▪ Credentials discovered on Ansible servers are usually stored in playbooks. The full pathname is listed. For example, /Ansible/Playbooks/site.yml
Hard-Coded Credential	The credentials that are hard-coded and its location in the file. The password itself is replaced by asterisks.
Password Length	The number of characters in the password. For credentials that are encrypted, N/A will be displayed. Note: Empty passwords connection strings will not be displayed.
Target System Address	The IP address or DNS of the target system where the discovered account will be used. N/A – Indicates that the credentials were discovered in an Ansible playbook.
Target System Type	The type of system where the discovered account will be used. Possible values are: ▪ Database ▪ Web ▪ Active Directory ▪ N/A – Indicates that DNA didn't recognize the target system type from the connection string, or that the credentials were discovered in an Ansible playbook.
OS Version	The operating system version as defined in the machine's account in the Active Directory.
Details	If CyberArk DNA was unable to scan a remote machine, this field will contain an error indication, such as "Network path not found" or "Access denied".

Cloud Users

The Cloud Users sheet displays the DNA scan results for Cloud Users and Access Keys discovered in AWS scans. Each row in the report represents a credential that was discovered, either an IAM user or an Access Key.

IAM Access Keys are related to an IAM user and have the same permissions as them. Discovering all the IAM users, their policies and other privileged relevant data helps in assessing the risk with each IAM user or Access Key. Privileged users in the AWS console can have devastating results if not managed and monitored correctly according to a password policy.

For more information, refer to Configure AWS Scan Policies, page 133

If the AWS scan is not selected, this sheet will not be created.

Cloud Instances

The Cloud Instances sheet displays the DNA scan results for Cloud Instances discovered in AWS scans. Each row in the report represents an EC2 Instance with relevant details about the instance and key pair (if found). A key pair for an instance should be used only for certain cases. An instance that has a public DNS is more vulnerable and exposed to attacks.

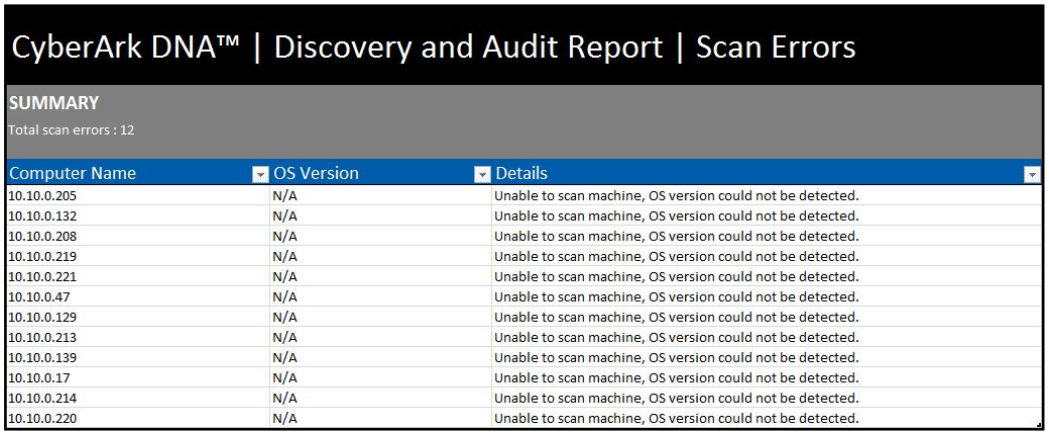
If **AWS Inspector scan** was selected and AWS Inspector data is available on the scanned instances, additional data about the instance findings will be displayed.

For more information, refer to Configure AWS Scan Policies, page 133

If the AWS scan is not selected, this sheet will not be created.

Scan Errors

The final sheet in the Discovery and Audit Report is the Scan Errors sheet. This sheet contains basic scan errors, such as connectivity errors, DNS errors and OS detection errors. The errors are listed in the Details column of each row.



CyberArk DNA™ | Discovery and Audit Report | Scan Errors

SUMMARY

Total scan errors : 12

Computer Name	OS Version	Details
10.10.0.205	N/A	Unable to scan machine, OS version could not be detected.
10.10.0.132	N/A	Unable to scan machine, OS version could not be detected.
10.10.0.208	N/A	Unable to scan machine, OS version could not be detected.
10.10.0.219	N/A	Unable to scan machine, OS version could not be detected.
10.10.0.221	N/A	Unable to scan machine, OS version could not be detected.
10.10.0.47	N/A	Unable to scan machine, OS version could not be detected.
10.10.0.129	N/A	Unable to scan machine, OS version could not be detected.
10.10.0.213	N/A	Unable to scan machine, OS version could not be detected.
10.10.0.139	N/A	Unable to scan machine, OS version could not be detected.
10.10.0.17	N/A	Unable to scan machine, OS version could not be detected.
10.10.0.214	N/A	Unable to scan machine, OS version could not be detected.
10.10.0.220	N/A	Unable to scan machine, OS version could not be detected.

The errors that are listed in this sheet are also stored in the scan log file which is created for each scan. For more information, refer to Logging, page 104.

The Organizational Pass-the-Hash Vulnerability Map

CyberArk Discovery and Audit draws a vulnerability map of Golden Ticket and Pass-the-Hash attacks that can be leveraged between machines in the organization. In a Pass-the-Hash attack, the privileged account hash is passed from one machine to another. The Golden Ticket attack risk discovered by DNA determines if a hash can be used to leverage a Pass-the-Hash attack to log in to the Domain Controller and can then be used to steal the Golden ticket (AKA “KRBTGT”). This is represented in the Organizational Vulnerability Map using directional arrows from one machine to another.

Each machine on the map is either Vulnerable, Causes vulnerability, or both (Causes vulnerability and vulnerable).

- Causing vulnerability - Machines cause vulnerabilities due to detected Active threats, which indicate stored privileged account hashes that may currently be leveraged against vulnerable machines and expose your network to Golden Ticket and Pass-the-Hash attacks. For more information, refer to Executive Summary Dashboard, page 44.
- Vulnerable - Machines are vulnerable because an Active threat was identified on another machine, and the stored privileged account hash has access to this machine.

  For example:
  - A stored privileged account hash was found on Machine A.
  - The privileged account whose hash was found has access to Machine B and can, therefore, be passed from Machine A to gain access to Machine B.
  - Machine A is flagged as Causes vulnerability.
  - Machine B is flagged as Vulnerable.
- Causing vulnerability and vulnerable – Machines that are both:
  - Flagged as Causing vulnerability because privileged account hashes were found on them.
  - Flagged as Vulnerable because privileged account hashes were found elsewhere that cause a vulnerability on them.

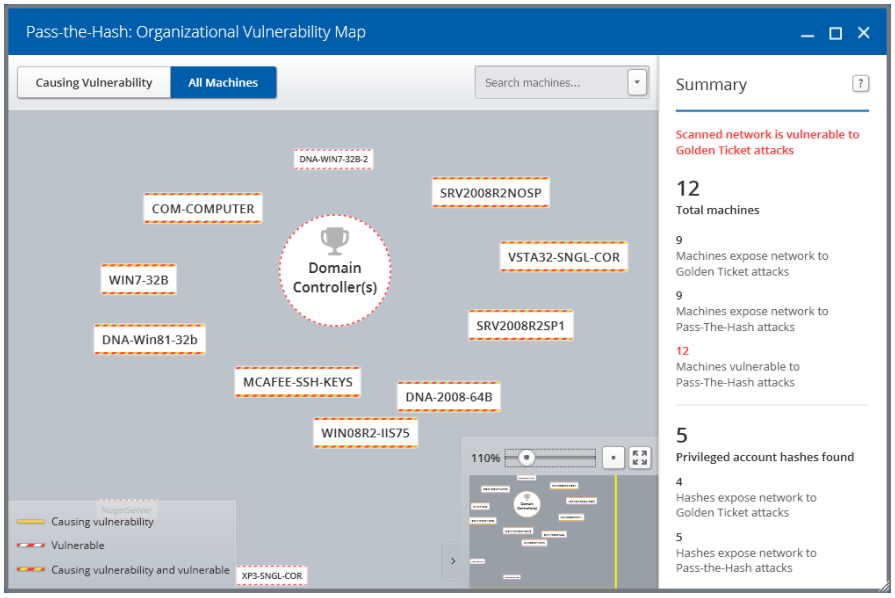
Display the Map

1. Set up DNA to scan for Pass-the-Hash vulnerabilities. For more information on how to configure the scan, see Set up a DNA Scan, page 29.
2. After the scan completes, open the report. In the Executive Summary Dashboard, in the Credential Theft Vulnerability section, click OPEN PTH MAP.
3. The Pass-the-Hash: Organizational Vulnerability Map is displayed, together with a Browse window. Select the relevant map file, and click Open.

Understand the Map

Overview

When you open a map, the Summary is displayed in the right pane.



This includes the following information:

Details	Indicates ...
Vulnerability status	If the scanned network is vulnerable to Golden Ticket attacks, a message is displayed at the top of the summary pane.
Vulnerable machines	The total number of machines that were scanned and are displayed on the map and the breakdown of machines that expose your network to Golden Ticket and Pass-The-Hash attacks and vulnerabilities. **Note:** The number of total machines is not the sum of Machines causing vulnerabilities and Vulnerable machines because these two groups overlap. Machines can both cause vulnerabilities and can be vulnerable.
Privileged account hashes	The total number of privileged account hashes displayed on the map and the breakdown of privileged account hashes that expose your network to Golden Ticket and Pass-The-Hash attacks.

Machine Nodes Layout

Nodes Layout

The machine nodes are laid out by relevance of a Golden Ticket or Pass-the-Hash attack. If a privileged account hash can be passed from Machine A to Machine B, the machine nodes will be laid out close together.

Nodes Shapes

Servers/workstations are presented as a rectangular node. The Domain Controller is presented as a round node.

Nodes Size

The size of the machine nodes is set according to the number of machines they cause a vulnerability on, making it easy to find the more important machines.

Legend

On the bottom left of the map, you can see a list of the machine types at any time.

Note:
All machines that are part of a Golden Ticket or Pass-the-Hash attack are displayed. If a machine is not vulnerable or does not cause a vulnerability, it is not displayed. Therefore, it is possible for a machine to be included in the report, but not appear on the map.

Mini Map

At the bottom right of the map, the mini-map can be used to zoom in/out and move around the main map.

Select the Machines to Display

You can determine the machines that are displayed in the map using the following options.

Machines causing vulnerability/all machines

It is possible to display only machines that cause vulnerabilities or machines that are both vulnerable and cause vulnerabilities, using the filter buttons at the top left corner of the map.

- Click **Causing Vulnerability** to display only the machines in your organization that cause vulnerabilities.
- Click **All Machines** to display all the machines in your organization that are either vulnerable or cause vulnerabilities, or both.

Search for a machine

Search for a machine and focus on it in one of the following ways:

- In the Search machines dropdown box, write the machine name,

Or,

- Click on the arrow, find and click on the relevant machine.

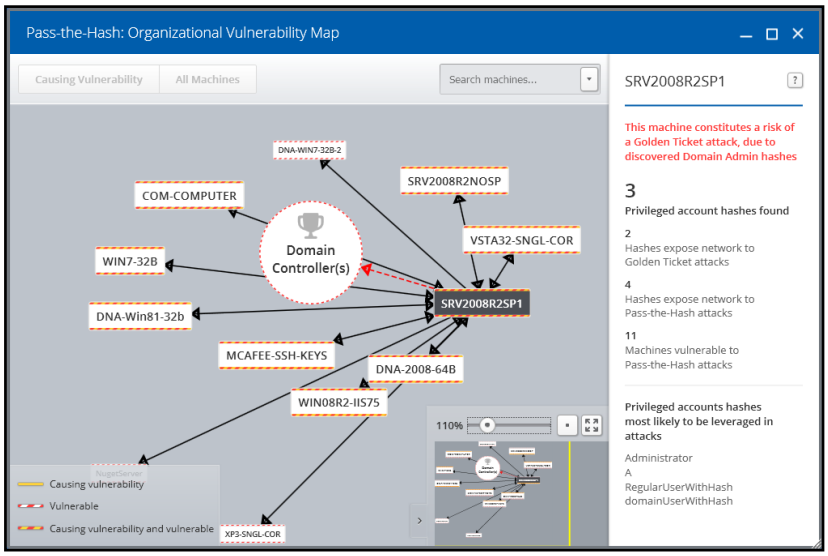
Focus on a Specific Machine

View information about a specific machine in any of the following ways:

To view ...	Do the following ...
Vulnerabilities	To view all possible vulnerabilities involving a certain machine, click its name.
Direction	The directional arrows represent the direction in which a privileged account hash can be passed. - The machine on the originating side of the arrow is the machine that causes the vulnerability from where the attacker can pass a privileged account hash from. - The machine on the target side of the arrow is the vulnerable machine to which the attacker can pass a privileged account hash.
Machine	When you select a machine name, the right pane shows information that is specific to that machine: - Vulnerability status – If the scanned machine is vulnerable to a Golden Ticket attack, a message is displayed at the top of the summary pane. - Status of exposure to attacks – The total number of privileged account hashes found on the selected machine is displayed with a breakdown of the number of privileged account hashes found on the selected machine that expose the network to Golden Ticket and Pass-the-Hash attacks.

To view ...	Do the following ...
	▪ Status of vulnerability to Pass-the-Hash attacks – The number of privileged account hashes found on the selected machine that cause Pass-the-Hash attack vulnerabilities on other machines and a list of the privileged account hashes that are most likely to be leveraged in Pass-the-Hash attacks.

View a possible Golden Ticket attack



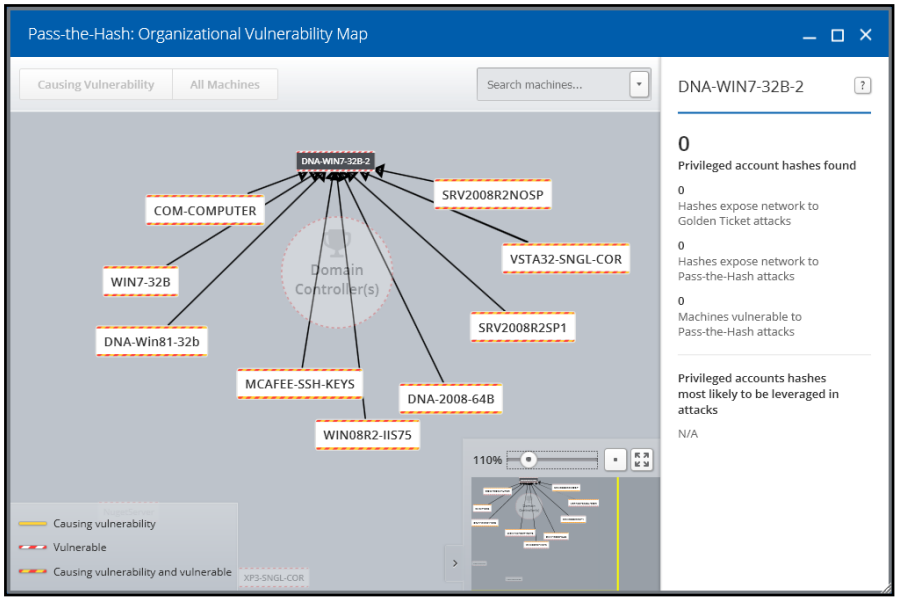
You can view possible Golden Ticket attacks in the Organizational Vulnerability Map of your scanned network in either of the following ways:

- Select the Domain Controller. If your network is vulnerable to a Golden Ticket attack, arrows point to all machines that put the network at risk of a Golden Ticket attack.

Or,

- Select any machine. If a hash is discovered on the selected machine that can be exploited for a Golden Ticket attack, an arrow points to the Domain Controller.

View possible Pass-the-Hash attacks



- In the Organizational Vulnerability Map, select any machine. If your network is vulnerable to a Pass-the-Hash attack, arrows point to the vulnerable machines.

The SSH Keys Trusts Map

CyberArk Discovery and Audit produces a visual organizational map of all SSH key trusts that can be used on the different machines in your organization. The nodes presented on the map represent machines in your organization with public or private SSH keys. When SSH keys are exposed, they can be used to access multiple machines. This is represented in the SSH Keys: Organizational Trust Map where directional arrows indicate all the discovered SSH Key trusts between the selected machine and other machines.

Each machine on the map is either Compliant or Non-compliant.

- Compliant - Machines where only compliant SSH Keys are stored. This means that all the SSH Keys on this machine have a key age that is lower than or equal to the predefined maximum SSH Key age, and that all the SSH Keys' strength (length and algorithm) meet the specified criteria. For more information, refer to Executive Summary Dashboard, page 44.
- Non-compliant – Machines are non-compliant if even one SSH Key stored on it is not compliant.

Display the Map

1. Set up the DNA scan. During each scan, DNA automatically scans the selected machines for SSH keys exposure. For more information on how to configure the scan, see Set up a DNA Scan, page 29.
2. After the scan completes, open the report. In the Executive Summary Dashboard, in the SSH Keys Discovery section, click OPEN TRUSTS MAP.
3. The SSH Keys: Organizational Trust Map is displayed, together with a Browse window. Select the relevant map file, and click Open.

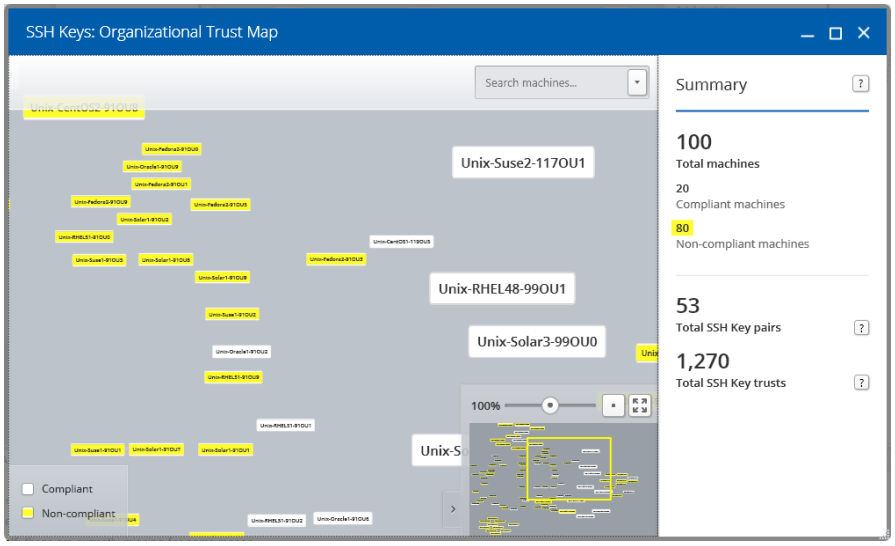
Auto-zoom

When the Organizational Trust Map is displayed, the machine where the most non-compliant SSH Keys are stored will be zoomed onto, making it easy to focus on the machine that most requires immediate attention.

Understand the Map

Overview

When you open a map, the Summary is displayed in the right pane.



This includes the following information:

Details	Indicates ...
Total machines	The total number of machines displayed on the map.
Compliant machines	The number of machines in the organization where only compliant SSH Keys are stored.
Non-compliant machines	The number of machines in the organization where non-compliant SSH Keys are stored.
Total SSH Key pairs	The total number of SSH Key pairs found on all machines on the map.
Total SSH Key trusts	The total number of SSH connections that can be established from an account on one machine to another account on a different machine in the map.

Machine Nodes Layout and Size

Nodes Layout

The machine nodes are laid out by relevance of SSH key exposure. If SSH Keys on a machine can be used to access other machines, the machine nodes will be laid out close together.

Nodes Size

The size of the machine nodes is set according to the number of total accounts that can connect to this machine. This reflects the number of “locations” that this machine can be connected to using SSH Keys.

Legend

On the bottom left of the map, you can see a list of the machine types at any time.

Note:
All machines where SSH Keys are stored are displayed. If an SSH Key is not stored on a machine, it is not displayed in this map.

Mini Map

At the bottom right of the map, the mini-map can be used to zoom in/out and move around the main map.

Select the Machines to Display

You can determine the machines that are displayed in the map using the following options.

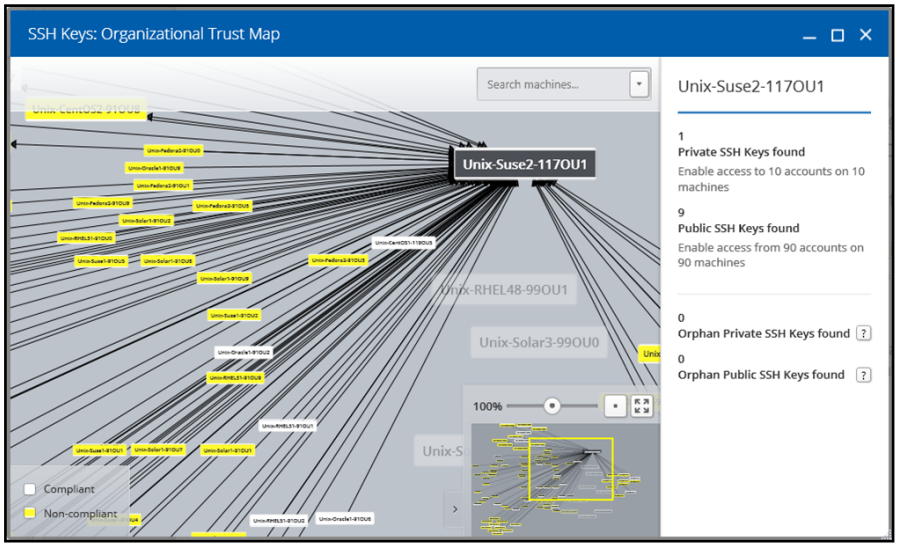
Search for a Machine

Search for a machine and focus on it in one of the following ways:

- In the Search machines dropdown box, write the machine name,

Or,

- Click on the arrow, find and click on the relevant machine.



Focus on a Specific Machine

View information about a specific machine in any of the following ways:

To view ...	Do the following ...
SSH Key exposures	To view all SSH Key exposures involving a certain machine, click its name.
Direction	The directional arrows represent the direction in which an SSH Key trust can be used to access another machine. ▪ The machine on the originating side of the arrow is the machine where the private SSH key that enables access is stored. ▪ The machine on the target side of the arrow is the machine where the corresponding public SSH key is stored and, therefore, can be accessed.
Machine	When you select a machine name, the right pane shows information that is specific to that machine: ▪ Private SSH Keys found – The number of private SSH keys found on the selected machine. Additional information describes how many accounts can be accessed on other machines in the map using these SSH keys. ▪ Public SSH Keys found – The number of public SSH keys found on the selected machine. Additional information describes how many accounts can be accessed from other machines in the map using these SSH keys. ▪ Orphan Private/Public SSH Keys found – The number of orphan private/public SSH keys found on the selected machine.

Use DNA Reports to Expose Security Threats

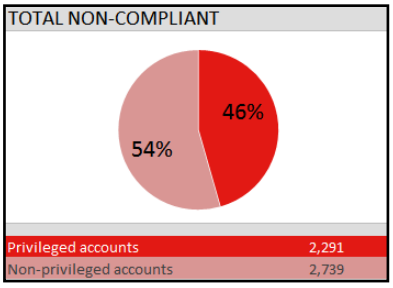
The DNA Report provides detailed information about the machines in your organization and the users and user groups that have access to them.

Account Scan

Scenario 1: How many non-compliant privileged accounts do I have?

In the Executive Summary

- In the Compliance Status section, the TOTAL NON-COMPLIANT chart shows the percentage of non-compliant privileged and non-privileged accounts, as shown below:



In the Scan Report

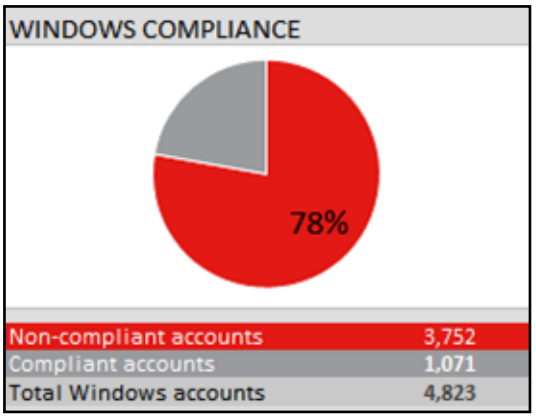
1. Filter the Compliance Status column to show only Non-compliant records.
2. Filter the Account Category column to show only Privileged Shared/Local and Privileged Personal/Domain records. This displays a list of all non-compliant privileged accounts.
3. Optional: Filter the Machine Type column to show only Server. This displays a list of all non-compliant privileged accounts that can log into servers.

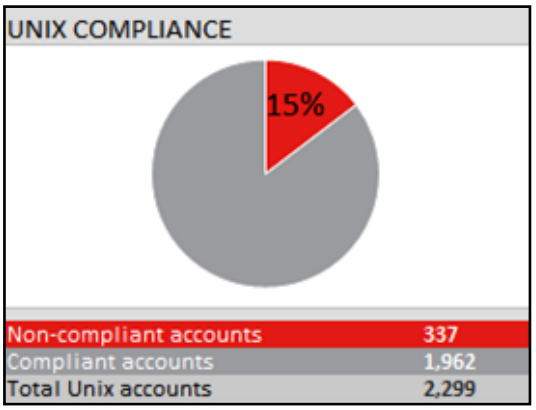
Non-compliant privileged accounts that can log into servers have a higher severity than those that can only log into workstations.

Scenario 2: How many non-compliant Windows or Unix/Linux accounts do I have?

In the Executive Summary

- In the Compliance Status section, the two top pie charts on the right show the percentage of non-compliant accounts for Windows and Unix/Linux, as shown below:

- 



In the Scan Report

- In the Windows Scan and Unix Scan sheets, filter the Compliance Status column to show only Non-compliant records.

Scenario 3: Which Unix account privileges have been escalated mistakenly?

- In the Unix Scan sheet, filter the Account Group column to show only *Sudoers file* records.

  This displays a list of all privileged accounts on Unix/Linux machines throughout the organization that were given additional privileges via sudoers files.
- In the Unix Scan sheet, filter the Insecure Privilege Escalation column to show only records that have values.

  Of the privileged accounts that were given additional privileges, this displays a list of all the accounts whose privilege might have been escalated accidentally.

  See the Insecure Privilege Escalation: Reason column for the reason.

Sudoers files are difficult to maintain. Accounts found in sudoers files may have accidentally been given the wrong privileges.

Scenario 4: In the last quarter, were any local privileged accounts used to log into servers?

1. Filter the Account Category column to show only Privileged Shared/Local records. These are the local privileged accounts, such as Administrator.
2. Filter the Machine Type column to show only Server.

This displays a list of all local privileged accounts that can access servers. The Last Login Date column shows the last date and time that the account was used to log into the correlated machine.

This information shows when the account was last used to log into each machine.

Scenario 5: Do my servers have 'backdoor' accounts? How do I find all local privileged non built-in accounts?

1. Filter the Account Category column to show only Privileged Shared/Local records. These are the local privileged accounts, such as Administrator.
2. Filter the Machine Type column to show only Server.
3. In Account Description, clear Built-in account for administering the machine/domain.

This displays a list of all local non built-in privileged accounts that can access servers. The accounts may have been:

- Left unintentionally by decommissioned applications. They may be leveraged maliciously as 'backdoors' to the advantage of attackers.
- Created by malware.
- Created by a third-party contractor without informing IT. Contractors may create such local privileged accounts to aid in their work while not considering security implications.

Local privileged accounts are considered high risk due to their enhanced permissions.

Scenario 6: Which non-privileged accounts can access my servers?

1. Filter the Account Category to show only Non-privileged Shared/Local and Non-privileged Personal/Domain records.
2. Filter the Machine Type column to show only Server.

This displays a list of all non-privileged accounts that can potentially log into the organization's servers.

It is bad practice to allow personal or shared non-privileged users to log into servers.

Embedded and Hard-Coded Credentials Scan

This section describes a variety of typical scenarios that show how DNA can help you discover embedded credentials and hard-coded credentials that are exposed in your organization.

Scenario 1: Which credentials have been exposed by being embedded throughout my organization? How many are non-compliant?

In the Windows Scan sheet

- Filter the Account Category column to show only Service Account records. This will show only accounts that have been embedded into different locations.
- To find out which are non-compliant, filter the Compliance Status column to show only Non-compliant records

You can now analyze how these accounts can be leveraged maliciously. The Service Account Type and Service Account Description columns help you understand in which locations (e.g. Windows Services, Scheduled Tasks, IIS Application Pool, IIS Anonymous Authentication, etc.) each account is used; most likely for actions such as backup, database connections, running scheduled scripts, and so on.

It is best practice to be aware of Service Accounts used throughout your organization. Service Accounts are likely to have privileged rights, and should therefore be compliant with organizational policy.

Scenario 2: Where are embedded credentials being used?

In the Windows Scan sheet

- Filter the Account Category column to show only Service Account records.

This displays a list of your organization's service accounts.

You can now analyze how these accounts may be leveraged maliciously. The Service Account Type and Service Account Description columns help you understand how each account is used; most likely for actions such as backup, database connections, running scheduled scripts, and so on.

This information is essential to IT personnel in planning Privileged Identity Management.

Scenario 3: Which credentials have been hard-coded into connectionStrings on IIS servers and where?

In the Hard-Coded Credentials sheet

- DNA presents all instances of discovered connectionStrings on WebSphere, WebLogic and IIS servers.
- The Machine Name column displays the name of machine where the connectionString was discovered.
- The Account Name column displays the extracted usernames from the discovered connectionStrings.
- The Hard-Coded Credential column displays the connectionString that was discovered. However, if the discovered connectionString does not contain a password, it will not be displayed.
- This information helps you understand which credentials were encoded, where they have been found, in which files they've been hard-coded, and enables a bird's eye view of the state of hard-coded credentials on IIS servers.

CyberArk recommends eliminating any embedded or hard-coded credential to decrease the risk of malicious exploitation.

Scenario 4: How secure are my DevOps playbooks?

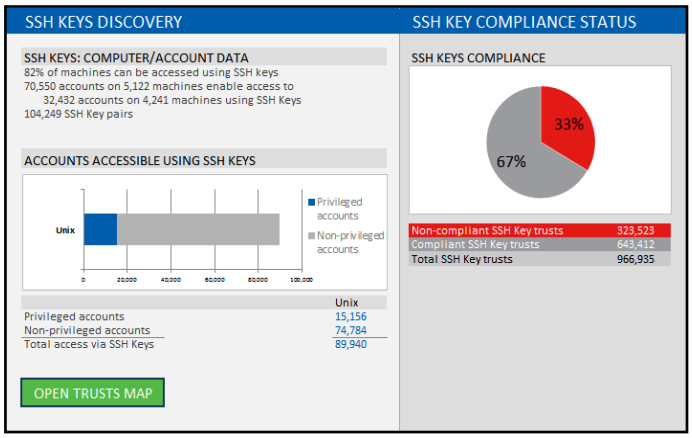
In the Hard-Coded Credentials sheet

- In the changing world of IT, where DevOps tools are becoming more popular and organization development teams use the CI/CD pipeline to develop faster, credentials sometimes get left behind.
- DNA presents all instances of discovered hard-coded credential in Ansible playbooks. The Hard-Coded Credential column displays the credentials in the Ansible playbook that could potentially be used by an attacker. Seeing credentials with a Password Length is a good indicator of un-protected credentials.
- CyberArk recommends eliminating any embedded or hard-coded credentials to decrease the exposure of privileged credentials that are being used as part of the CI/CD pipeline.

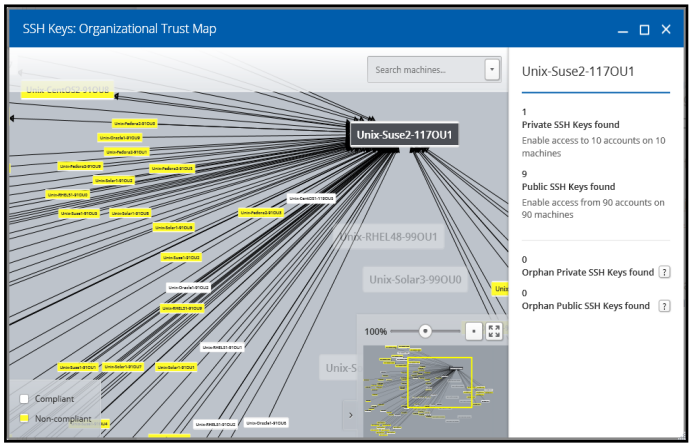
SSH Keys Scan

This section describes a variety of typical scenarios that show how DNA can help you discover SSH Key exposure in your organization.

Some of these scenarios recommend that you refer to the DNA Executive Summary that is described in detail in Executive Summary Dashboard, page 44.



Other scenarios recommend that you refer to the SSH Keys: Organizational Trust Map that is described in detail in Focus on a Specific Machine, page 84.



Scenario 1: Which accounts enable access to machines via SSH keys?

In the Unix Scan sheet

- Filter the # of Keys Found column to show only records with a value higher than 0. This will show only accounts that have a public SSH key associated to them.

This displays a list of accounts that users who have access to the correlating private SSH key can use to establish an SSH connection to them and, thus, gain access to their privileges.

Scenario 2: How many SSH Key pairs do I have?

In the Executive Summary

- In the SSH Keys Compliance section, under SSH KEYS: MACHINE/ACCOUNT DATA you can see the total number of SSH Key pairs

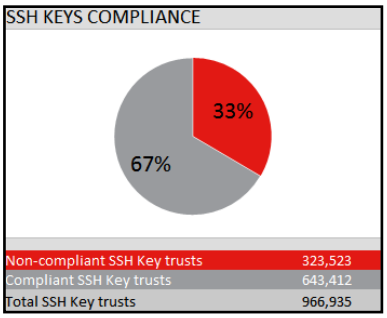
In the SSH Key Trusts sheet

- For all SSH Key row in the SSH Key Trusts sheet, get the unique Key Fingerprint to see the unique number of SSH Key pairs detected.

Scenario 3: How many non-compliant SSH Key Trusts do I have?

In the Executive Summary

- In the SSH Keys Compliance section, the pie chart shows the percentage of non-compliant SSH Key Trusts, as shown in the following screenshot:



- Non-compliant SSH Key Trusts are determined according to non-compliance of either the private or public SSH key, or both. This number provides insight into the number of possible SSH connections, from machine to machine, that may be used with non-compliant SSH keys.

In the SSH Key Trusts sheet

- Filter the Compliance Status column to show only Non-compliant (SSH Key) and Non-compliant records.

This shows a list of all non-compliant SSH Key Trusts.

Scenario 4: How many Accounts are accessible by SSH Keys?

In the Executive Summary

- In the SSH Keys Compliance section, under SSH KEYS: MACHINE/ACCOUNT DATA, you can see the total number of accounts that are accessible with SSH Keys and the percentage of machines that are accessible with SSH Keys.

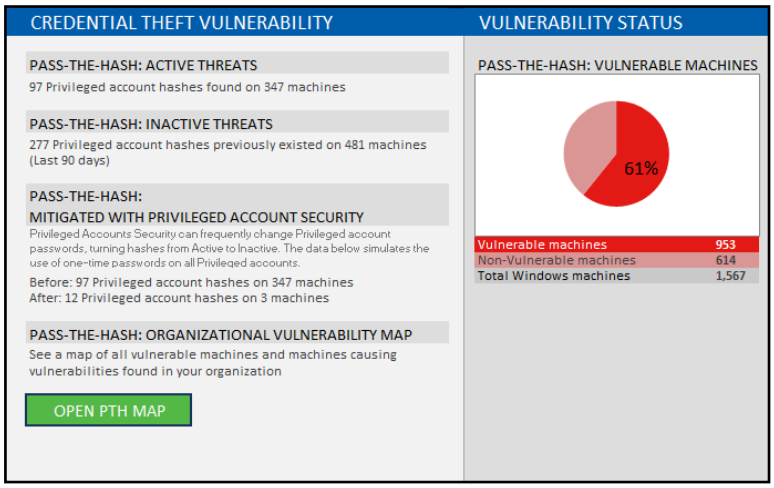
In the SSH Key Trusts sheet

- The total number of accessible accounts is the number of unique target accounts that can be accessed using these keys.
- Only target accounts are "Accessible". Source accounts enable access to target accounts.
- Filter the distinct target accounts and target machines.

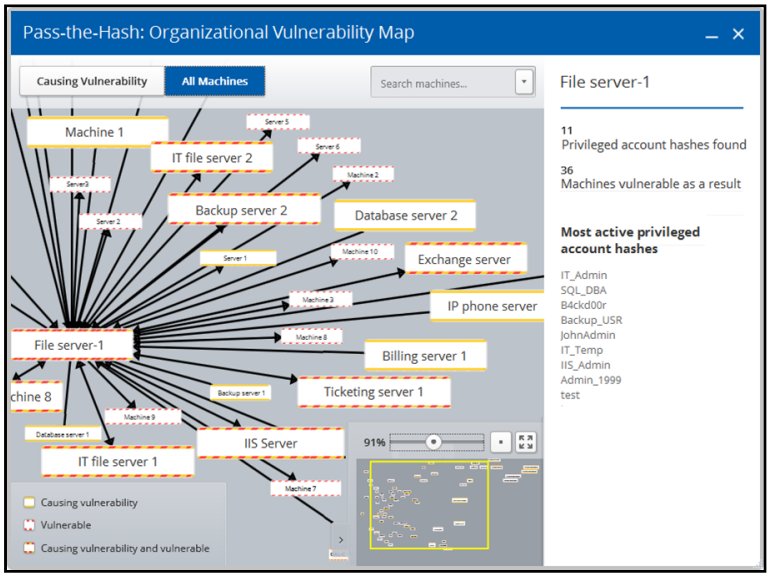
Pass-the-Hash Vulnerabilities Scan

This section describes a variety of typical scenarios that show how DNA can help you expose Golden Ticket and Pass-the-Hash vulnerabilities in your organization.

Some of these scenarios recommend that you refer to the DNA Executive Summary that is described in detail in Executive Summary Dashboard, page 44.



Other scenarios recommend that you refer to the Pass-the-Hash Organizational Vulnerability Map that is described in detail in The Organizational Pass-the-Hash Vulnerability Map, page 81.



Scenario 1: How many Privileged account hashes were found and, as a result, how many vulnerable machines are there?

In the Executive Summary Dashboard

In the Credential Theft Vulnerability section, do the following:

- In the Pass-the-Hash: Active Threats section, the number of the unique privileged account hashes, and the total number of machines on which the hashes were found is displayed.
- On the right, in the Vulnerability Status section, the pie chart shows the percentage of vulnerable machines in the entire organization, as a result of the Active Threats described on the left.

The percentage of vulnerable machines points out the magnitude of the Golden Ticket and Pass-the-Hash problem.

In the Organizational Vulnerability Map

In the Executive Summary Dashboard, in the Credential Theft Vulnerability section, do the following:

1. Click OPEN MAP then, In the dialog, choose the map file to open.
2. On the right pane of the Organizational Vulnerability Map, the number of Machines causing vulnerabilities, Vulnerable machines and Privileged account hashes found is specified.

In the Windows Scan Sheet

- Filter the Pass-the-Hash: Vulnerable to show only records with Yes.

All vulnerable privileged accounts are displayed. Privileged accounts are vulnerable on a specific machine because the Privileged account hash was found on another machine.

- Filter the Pass-the-Hash: Hash Found to show only records with Yes.

All privileged accounts whose hashes were found on a certain machine are displayed.

Scenario 2: Which machines cause a vulnerability on a certain machine? Which machines are made vulnerable due to a certain machine?

In the Organizational Vulnerability Map

In the Executive Summary Dashboard, in the Credential Theft Vulnerability section, do the following:

1. Click OPEN PTH MAP. In the dialog, choose the map file to open.
2. Use the Search field to find a machine to be analyzed, or click any machine on the map.

The map shows all machines that cause a vulnerability on this machine, and/or all machines that are made vulnerable due to this machine. See the legend at the bottom left of the map for more information.

Scenario 3: Which accounts cause vulnerabilities on the most machines?

In the Organizational Vulnerability Map

- The size of a machine (node) represents how many vulnerabilities it causes. The bigger the size, the more vulnerabilities it causes on machines in the organization.

Focusing on the larger machines first will make it easier to prioritize and mitigate Golden Ticket and Pass-the-Hash threats more quickly.

In the Scan Report

1. Filter the Pass-the-Hash: Hash Found to show only records with Yes.
2. Sort Causes Vulnerability On # of Machines by largest to smallest.

This displays a list of all privileged accounts whose hash has been found, sorted by the number of machines on which they cause a vulnerability.

The first account on the list causes the most vulnerabilities in the organization, and so on.

Scenario 4: What if Privileged Access Security were implemented in my organization? How would that help me mitigate Pass-the-Hash?

In the Executive Summary Dashboard

In the Credential Theft Vulnerability section, do the following:

- In the Pass-the-Hash: Mitigated with Privileged Access Security section, a “before and after” simulation is given.

This shows the number of active privileged account hashes before implementing Privileged Access Security and after implementing the use of one-time passwords for all privileged accounts found by DNA.

Scenario 5: Which workstation may be a starting point for a Pass-the-Hash attack?

In the Windows Scan sheet

1. Filter the Pass-the-Hash: Hash Found to show only records with Yes.
2. Filter the Machine Type to show only records with Workstation.
3. Filter the Account Type to show only domain records.

This displays a list of all workstations on which Privileged hashes have been found.

Workstations are often the first step in a Pass-the-Hash attack, since they are the most susceptible to APTs.

Scenario 6: Which Privileged account hashes were once stored, no longer cause vulnerabilities, but constitute an underlying threat?

In the Executive Summary Dashboard

in the Credential Theft Vulnerability section, do the following:

- In the Pass-the-Hash: Inactive Threats section, the number of unique privileged accounts hashes, and the total number of machines on which privileged account hashes were stored previously is displayed.

Hashes are deleted by Windows in certain scenarios, such as when logging off or restarting the machine.

In the Windows Scan sheet

1. Filter the Pass-the-Hash: Hash Found to show only records with Previously.
2. Filter the Account Category to show only Privileged Shared, Privileged Personal, and Service Account records.
3. Filter the Account Type to show only domain records.

This displays a list of all privileged accounts whose hash has been previously stored on the machine, but is no longer stored. Hashes are removed in certain scenarios, such as when logging off or restarting the machine.

These privileged hashes may become an imminent threat the next time they are used.

Scenario 7: Why are hashes stored on my servers?

1. Filter the Pass-the-Hash: Hash Found to show only records with Yes.

2. Filter the Machine Type to show only records with Server.
3. Filter the Account Category to show only Privileged Shared, Privileged Personal, and Service Account records.
4. Filter the Account Type to show only domain records.

This displays a list of all servers on which Privileged hashes have been found. The Threat Cause column shows the reasons that hashes have been stored on the server.

For example: Remote command execution, Remote login via RDP.

Scenario 8: How many machines are exposed to credentials theft?

In the Executive Summary

- In the DETECTED CREDENTIALS: VULNERABLE MACHINES graph, you can see the number of machines that are vulnerable to credentials theft.

In the Scan Report

- In the Windows Scan sheet, filter the Credential Type column to include Password, Hash and 'Password and Hash'.
- The unique number of Machine names is the number of machines that are exposed to credentials theft techniques.

Sharing DNA Report Data with CyberArk

We encourage you to share your Report data with CyberArk to help us improve our products. Report data can be shared securely using the automatically generated obfuscated report data, which includes a scrambled version of all sensitive data from the scan, such as usernames and machine names. As part of the scrambling process, the data will be salted and hashed irreversibly by the SHA-256 cryptographic hash function. The obfuscated report data is in an SQLite database, which can be viewed using any SQLite viewer.

To enable convenient sharing, DNA always saves an obfuscated version of the Report data of the latest scan.

Share the Automatically Generated Obfuscated Report Data

1. Navigate to the DNA folder.
2. Locate the obfuscated database file, named "DNA_obfuscated.db".
3. To view the obfuscated database you can use any SQLite viewer.
4. To view the obfuscation tool log, open DNA.DbObfuscation.log.

Run the DNA Obfuscation Tool Manually

During scanning, DNA creates a temporary database that it deletes afterwards. To be able to obfuscate the database manually, first configure DNA so that it will not delete the temporary database:

- In the DNA configuration file, add the DeleteDB key with the value No.

Then perform the following steps:

1. Run a scan.
2. Open a command line window, and navigate to the DNA folder.

3. Run the DNA.DbObfuscation.exe app with the following parameters:

Parameter	Description	Possible Values
-i	The input database filename.	"DNA.db" ".\DNA.db" "C:\DNA\DNA.db"
-o	The output database filename (optional). If this parameter is not specified, the output file name will be: "**[input file name]_ obfuscated.db**"	"out.db" ".\dna_pth.db", "C:\Users\guest\Desktop\pth.db"
-s	A salt value used for obfuscation (optional). If this parameter is not specified, the obfuscation tool will choose a random salt value.	"this is a salt" "12345" "0x22fb3304a1"

4. To view the obfuscation tool log, open DNA.DbObfuscation.log.

DNA.DbObfuscation.exe –i "DNA.db" –o "DNA_obfuscated.db" –s "salt value"

Logging

During each scan, the DNA creates log files in the DNA\Log folder to monitor DNA activity and status during that scan.

At the end of the scan, these log files are stored in a zip file called DNA_Package_Logs_YYYY-MM-DD_hh_mm_ss-PM/AM.zip. This zip file includes the entire DNA\Log folder.

For example, a zipped file of a scan that began on March 10, 2016, at 10.00pm would be called DNA_Package_Logs_2016-03-10_10_00_00-PM.zip.

You can send this zipped file to your CyberArk representative for analysis and troubleshooting.

Troubleshooting

The troubleshooting options in this chapter guide you through the main issues that may occur when using DNA.

Errors reported by DNA always start with the letters DNA, for example “DNAPR188E”. Errors that do not start with these letters may have been returned by the operating system or certain libraries. In such cases, it is recommended to search online for the error string.

For more information, contact your CyberArk support representative.

Scanning Issues

General scanning errors and issues are displayed

Problem	General scanning errors and issues are displayed while scanning Unix/Linux machines. In the console log, the following error is displayed: "**DNAPR188E Timeout occurred while waiting for user prompt**".
Possible Solutions	These errors indicate a timeout that may occur while DNA awaits output from the SSH shell. . In the configuration file, modify the SSHExpectInputTimeoutInSeconds parameter as follows: 1. In the DNA.exe.config file, increase the timeout value of the SSHExpectInputTimeoutInSeconds parameter. 2. Rerun DNA and check the results. If necessary, increase the timeout value again. Note: This will increase scan time.
Problem	General scanning errors and issues are displayed while scanning Unix/Linux machines. In the console log, the following error is displayed: **"DNAPR189E Timeout occurred while waiting for command prompt."**
Possible Solutions	These errors indicate a timeout that may occur while DNA awaits output from the SSH shell. . In the configuration file, modify the SSHExpectInputTimeoutInSeconds parameter as follows: 1. In the DNA.exe.config file, increase the timeout value of the SSHExpectInputTimeoutInSeconds parameter. 2. Rerun DNA and check the results. If necessary, increase the timeout value again. Note: This will increase scan time.
Problem	General scanning errors and issues are displayed while scanning Unix/Linux machines. In the console log, the following error is displayed: "**DNAPR199E Command execution timed out.**"
Possible Solutions	This error indicates a timeout that may occur while DNA awaits output from the SSH shell after a command is run. . In the configuration file, modify the SSHCommandExecutionTimeoutInSeconds parameter as follows: 1. In the DNA.exe.config file, increase the timeout value of

the SSHCommandExecutionTimeoutInSeconds parameter.
2. Rerun DNA and check the results. If needed, increase timeout value again.

The scan failed on Windows machines

Problem	The scan failed partially on many Windows machines. When the scan is complete, the percentage of Windows machines where the scan failed partially is higher than expected. Scans on a machine fail partially when at least one but not all types of scans on it fail due to errors. For more information, see the Run a Scan , page 35 section.
Possible Reasons	Certain protocols that DNA requires to be able to scan machines successfully may be blocked, for example by firewalls.
Solution	Make sure no firewalls are blocking DNA traffic. See the Windows Requirements, page 14 section for required protocols, and Enable WMI Ports on Windows Client Machines, page 131 for an explanation of how to enable WMI for Windows.
Problem	The scan failed on many of the Windows machines. When the scan is complete, the percentage of Windows machines where the scan failed is higher than expected.
Possible Reasons	. The credentials used for the scan are not administrative. . Some of the scanned machines may be powered off or not accessible.
Possible Solutions	. Make sure the supplied credentials have local administrative privileges on the local scanned machines. It is recommended to use domain administrative credentials. . Make sure the machines with the returned error function properly and are accessible from the machine that runs DNA.

The scan failed on Unix/Linux machines

Problem	The scan failed on many of the Unix/Linux machines. When the scan is complete, the percentage of Unix/Linux machines where the scan failed is higher than expected.
Possible Reasons	. The credentials used for the scan are not root. . Some of the scanned machines are powered off or not

	accessible. . SSH is not enabled on the scanned machine. . The user does not have permission to connect via SSH.
Possible Solutions	. Make sure the credentials supplied to DNA have root privileges when using the sudo command on the local scanned machines. For more information, see Configure Root Permissions Using the Sudoers File, page 132. . Make sure the machines with the returned error function properly and are accessible from the machine that runs DNA. . In the Details column of the DNA Report, find the machine that returned the error for more information about its cause.

The scan runs for a prolonged time

Problem	DNA runs for a prolonged time during Windows scanning.
Possible Reasons	A known issue on Windows machines causes the WMI protocol to hang. Refer to the Microsoft WMI Troubleshooting Guide for more information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa394603(v=vs.85).aspx.
Possible Solutions	Configure the DistributedScans parameter in the configuration file to All to enable DNA to use multiple processes and to timeout when the hanging occurs.
Problem	The following message is displayed: "**DNAPR110E An error occurred during a scan server proxy call. Remote process ID: <process>, scanned machine address: <address>.**"
Possible Reasons	This error indicates a timeout that may occur while DNA waits for a scan to be finished.
Possible Solutions	In the configuration file, add the DistributedScansTimeoutInSeconds parameter as follows: 1. In the DNA.exe.config file, increase the timeout value of the DistributedScansTimeoutInSeconds parameter. The default value is 1800 seconds (30 minutes). 2. If DNA is running, close and reopen it to load the new configuration value. 3. Rerun DNA and check the results. If necessary, increase the timeout value again. **Note:** This will increase scan time.
Problem	DNA hangs on "initializing scan" for a long time during an IP Range scan
Possible Reasons	When scanning a large IP range segment, DNA might take

	some time to identify all "live" machines.
Possible Solutions	In the configuration file, add the PingIntervals and PingTimeoutInMilliseconds parameters as follows: 1. In the DNA.exe.config file, set the value of PingIntervals to 2 (default is 4) and set the PingTimeoutInMilliseconds to 500 (default is 1000). 2. If DNA is running, close and reopen it to load the new configuration value. 3. Rerun DNA and check the results. If necessary, decrease these values and run again.

The user running the scan doesn't have required authorization

Problem	The following error message appeared in the log "**DNAPR196E Failed to parse LsHmcUser row on remote machine X; row input - 'HSCL350B The user does not have the appropriate authority.'**"
Possible Reason	The user running the DNA scan doesn't have the required authorization on the remote machine.
Possible Solution	Make sure that the account used to run the scan has the hmcsuperadmin task role.

The scan cannot detect the OS version

Problem	The following message appears in the Details column of the Scan errors sheet: "Unable to scan machine, OS version could not be detected." AND The following message appears in the machine logs "DNAPR242I Cannot detect OS version for remote machine {machine address}."
Possible Reasons (Unix machines)	. The SSH server is disabled . The SSH port is blocked by a firewall. . This Unix flavor is not supported by DNA. For a list of supported platforms, refer to Unix/Linux Requirements, page 18.
Possible Solutions (Unix machines)	Check the OpenSSH server settings on the target machine: . Make sure that the OpenSSH server is installed. . Make sure that the SSH server (sshd daemon) is running and listening on the standard SSH port (port 22). . Make sure that the SSH Server allows one of the following:

	. PasswordAuthentication . PubkeyAuthentication . keyboard-interactive . Make sure that the scanning user is allowed to connect via SSH to the target machine. . Make sure that the scanning machine is not blocking SSH outgoing connections, and that port 22 is not blocked by a firewall (Windows Built-in firewall or any other 3rd party firewall software/hardware). To check the above, try to logon to your target machines with PuTTY or any other preferred SSH client.
Possible Reason (Windows machines)	. The scanning user doesn't have administrative privileges on the target machine. . Windows File and Printer Sharing is not enabled on the target machine or another network protocol is blocked by a firewall.
Possible Solution (Windows machines)	. Make sure that all network protocols are enabled on all the target machines to scan and that firewalls do not block this type of traffic. For more information, refer to Windows Requirements, page 14. . Make sure that the scanning account has administrative privileges on the target machines (i.e., is a member of the built-in Administrators group). . The UAC on the target machine may block the local administrator login. Try to run the scan with the Domain administrator's credentials.

DNA could not finish a scan

Problem	The following message is displayed: "Important: DNA encountered issues when scanning at least one Windows machine. All files and processes may not have been removed. See troubleshooting info in the DNA User Guide for actions required." OR The following message is displayed in the DNA report: "DNA timed out while scanning a Windows machine. All files and processes may not have been removed. See troubleshooting info in the DNA User Guide for actions required."
Possible Reason	A power shortage or network outage may have caused the Windows SSH Keys scan cleanup to fail. There were leftover files unhandled by the ScanVulnerableCredentials scan (credentials theft)
Possible Solution	1. A CSV file, called DNACleanup.csv, is created in the DNA directory. This file contains a list of Windows machines on which leftover files might have been left after

a scan.
   - If the credentials required to scan these machines were imported using the file import feature, they are included in the CSV file.
   - If the credentials were specified manually when an AD scan was initiated, they are not included in the CSV file.
2. After analyzing the reason for the failure, rerun DNA on the machines marked in the CSV file to enable a successful scan.
   i. Open the CSV file and check that the user credentials required to access the machines to scan are included.
   ii. Rerun the DNA scan using the file import feature.
3. Once the scan is completed, DNA will clean up the left over files. For more information about the scan, refer to the DNA Configuration, page 121 parameter.

DNA discovered an SSH key from a machine that was not scanned

Problem	The following message is displayed: "DNA discovered the use of an SSH key from a Source Machine that was not scanned. It is possible that the IP has changed since use or that the machine was not scanned by DNA. See troubleshooting for more details."
Possible Reason	DNA may have encountered an IP address of a machine that was not scanned.

Possible solution	- Check if the relevant machine was scanned and, if it wasn't, check why not.
	  - If the scan failed on this machine, find out why. After analyzing the reason for the failure, rerun the DNA on this machine.
	  - If the machine was not included in the scan, include it and run the scan again.

DNA cannot resolve the IP of a machine listed in the imported file

Problem	The following message is displayed: "**DNA can't resolve the IP of a machine contained in the imported file. An error with one of the following codes is displayed: DNAPR228E, DNAPR229E, DNAPR233E, DNAPR234I, or DNAPR249E.**"

Possible Reasons	An incorrect DNS record for the machine to scan was specified, OR There is no communication with the DNS machine.
Possible Solution	1. If you specified a machine name, make sure that the DNS record corresponds to the machine to scan. 2. Make sure that the DNA can communicate with the DNS machine. 3. Try to ping the machine through the command line.

DNA cannot start scanning

Problem	The following error message is displayed in the log and the Scan error sheet: "**Cannot start scanning machine {machine address}. Machine is unavailable. Ping request timed out.**"
Possible Reason	A machine did not respond to a ping request.
Possible Solution	. It is possible that the scanned machine is configured not to respond to ping requests. If so, in the DNA configuration file, set PingMachineBeforeScan to No, Or, 1. If you specified a machine name, make sure that the DNS record corresponds to the machine to scan. 2. 3Make sure that the DNA can communicate with the DNS machine. 3. Try to ping the machine through the command line.

DNA cannot detect a connection using an SSH key

Problem	If CyberArk DNA was unable to detect a connection using an SSH key, the Details field in the SSH Keys Trust report will specify the reason. For example, "**SSH connections are disabled" or "The SSH server configuration does not allow the account to connect via SSH**".
Possible Reason	The discovered trust may be newer than the discovered Key Last Used date, since the data is extracted from the syslog, which contains historic data. It is possible that trust was previously used, then deleted, and then put in place again.
Possible Solution	This is not an error.

DNA failed to discover MS SQL instances

Problem	DNA failed to discover MS SQL instances with the following error: "DNAPR856E Failed to retrieve MS SQL server instances. Error: Microsoft.SqlServer.Management.Smo.FailedOperationException: An exception occurred in SMO while trying to manage a service. → Microsoft.SqlServer.Management.Sdk.Sfc.EnumeratorException: Failed to retrieve data for this request. → System.Management.ManagementException: Invalid class "
Possible Reason	DNA scans for MS SQL instances using the SMO library that, in turn, uses the WMI Provider that is installed with the SQL Server. In this case, DNA returned an "Invalid class" error, which indicates an issue with the MSSQL WMI Provider.
Possible Solution	Use the following workaround: https://support.microsoft.com/en-us/help/956013/error-message-when-you-open-sql-server-configuration-manager-in-sql-se

Imported File Issues

DNA cannot read a target machine name

Problem	When a file is imported, an error message is displayed in the console log. For example: "**Invalid value specified in CSV file {filename}, line {line number}, first column. Machine address contains invalid characters. Valid characters are: letter, number, period, underscore, hyphen.**"
Possible Reasons	A machine name may contain invalid characters, or it may be missing.
Possible Solutions	Refer to the error message in the console log for an explanation of the issue and how to resolve it. For more information about importing a file, refer to Import a File, page 136.

DNA doesn't scan all the listed machines

Problem	When a file is imported, no machines or fewer machines were imported.
Possible Reasons	The CSV file template was changed for version 5.0, and you may have imported a previous version of this file.
Possible Solutions	Get the latest CSV file format from DNA:

1. In the "Setup scanning from a file" page, click "Click on download CSV template" to access the most up-to-date template file.
2. Copy the content of the old CSV file and paste it into the new CSV template file.

DNA cannot retrieve information from the Active Directory

Problem	When scanning using the File Import method, the following errors occurred while trying to retrieve information from the Active Directory: ▪ Unable to retrieve account information due to lack of domain credentials. ▪ Unable to retrieve group information due to lack of domain credentials.
Possible Reasons	The domain address is missing from the "Domain (optional)" column.
Possible Solutions	To scan with a domain account, specify the domain address in the "Domain (optional)" column. To scan with a local account, leave the "Domain (optional)" column empty. DNA will assume that this is a local credential and will not try to connect to the Active Directory domain.

Delimiter characters are included in passwords

Problem	The following error message appears: **WARNING: When using "Scan from file"**, make sure that none of the passwords in the imported file contain the "<delimiter>" character, since this could cause the account to be locked out! For more information, see Troubleshooting in the DNA User Guide.
Possible Reasons	This message always appears.

Possible Solutions Make sure that password values in the imported file, which contain the same character as the delimiter specified in the ScanFromFileCsvDelimiter parameter, are properly escaped, as explained below:

- Password values that contain the delimiter value, should be surrounded by double quotes. By default, the delimiter value is a comma.
- Password values that contain double quotes should be surrounded by double quotes and each literal double quote should be escaped by adding another double quote that immediately precedes it.

Note: Any field can be quoted, but only fields that contain the delimiter character or quotes MUST be quoted.

For example:

Original text	Escaped text
test	test
list, of, items	"list, of, items"
go" he said	“go"" he said”
"go" he said	"""go"" he said"

Report Issues and Messages

DNA cannot scan the password age

Problem	The report shows a Password Age of 0 for all Unix/Linux accounts.
Possible Reasons	▪ The “shadow” file was not read successfully on all Unix/Linux machines. ▪ DNA may have encountered errors while scanning.
Possible Solutions	▪ Make sure the credentials supplied to DNA have root privileges when using the sudo command on the local scanned machines. ▪ Check the console log for errors.

DNA cannot scan the DNA machine

Problem	The report shows an error when scanning the machine from which DNA is run.
Possible Reasons	Service account scans are not supported on the machine where CyberArk DNA is running. For more information, see Known Behavior and Limitations, page 140. The following error appears in the DNA Report: “User credentials cannot be used for local connections”.
Possible Solutions	To scan the specified machine, run DNA from a different machine.

DNA cannot read the Excel file

Problem	When users open the DNA report, the following message appears: “Excel found unreadable content in [FILENAME]. Do you want to recover the contents of the workbook? [...]”.
Possible Reasons	The size of the Excel file was reached due to very long DNA results.
Possible Solutions	Repair the Excel file to solve the problem. If it does not, try limiting the scan to a smaller OU to decrease the length of the results.

DNA cannot resolve group members

Problem	When users open the DNA report, the following message appears: “Unable to resolve one or more group members. Cannot access trusted domain”

Possible Reasons	CyberArk DNA cannot access a trusted domain or another domain in the forest to resolve all the group members.

DNA cannot resolve the domain group

Problem	**When users open the DNA report, the following message appears: "Unable to resolve the domain group"**
Possible Reasons	CyberArk DNA detected a domain group but could not find the group in the domain. Therefore, it cannot resolve the group or any of its members.

DNA cannot detect the OS version

Problem	The following error message is displayed in the Windows Scan sheet, Details column of the DNA report: **"Unable to scan machine, OS version could not be detected."**
Possible Reasons	DNA failed to detect the OS version.

DNA cannot resolve the IP address of the machine to scan

Problem	The following error message is displayed in the DNA report: **"Failed to resolve IP address of {0}**."
Possible Reasons	DNA failed to resolve the machine's IP address from the host name given in the CSV file.

Log Error Messages

DNA cannot start scanning

Problem	The following error message is displayed in the log and the Scan error sheet to indicate that a machine did not respond to a ping request: “Cannot start scanning machine {machine address}. Machine is unavailable. Ping request timed out."
Possible Reasons	The machine is down, or failed to respond to the ping request for another reason.
Possible Solutions	. Make sure the machine is up and connected to the network. . Make sure that the ICMP protocol is not blocked in the machine firewall or in your environment.

DNA cannot authenticate to the machine to scan

Problem	The following error message is displayed in the trace log of the machine: "No suitable authentication method found to complete authentication."
Possible Reasons	In the scanned machine, the relevant authentication method was not configured.

Possible Solutions	Configure SSH Server password authentication support in the /etc/ssh/sshd_config configuration file, as follows:
	1. Logon to your host. This can be done locally or by using your preferred SSH2 client, for example PuTTY.
	2. Specify the following command:
	`vi /etc/ssh/sshd_config`
	3. Press the i key and search for the PasswordAuthentication or PubkeyAuthentication line, depending on the type of authentication you want to configure.
	4. Change its value from no to yes, then press Esc followed by wq to save the file and exit.
	5. Restart the SSH server to apply the changes:
	`/etc/init.d/SSH restart`

DNA cannot access the Database

Problem	The following error message is displayed in the log and the Scan error sheet to indicate that DNA could not log onto a specific database: “Failed to logon to <DB_Version> on <Machine_Name> using username <Supplied_Username>. Error: <Return error from the DB>"
Possible Reasons	The supplied credentials aren't strong enough to scan the database.
Possible Solutions	Use credentials that will enable you to access the database and scan it.

Appendices

Configuration Parameters

DNA Configuration

CyberArk DNA allows you to configure various parameters in the DNA.exe.config configuration file, which is located in the same directory as the DNA.exe file. The table below describes the configurable parameters.

TraceLogActive	
Description	Whether or not a trace log will be written when the tool is run.
Acceptable Values	Yes/No
Default Value	Yes
LogPath	
Description	The default path to which the trace and console logs are written.
Acceptable Values	Path
Default Value	\log
ReportPath	
Description	The default path to which reports are written. [DNA Path] refers to the location DNA is run from. You can also specify an absolute path, for example: C:\MyDNA\MyReports
Acceptable Values	Path
Default Value	[DNA Path]\Reports
MaxThreadNumber	
Description	The default number of machines that DNA can scan concurrently.
Acceptable Values	Number up to 100
Default Value	10
AccountMaxPasswordAgeInDays	
Description	The maximum account password age, as defined in the company's current password policy. DNA uses this parameter to determine the compliance status of each account. Specify -1 to prevent checking the compliance status. By default, the password age limit is taken from the group policy in the domain. This parameter value is only used if the group policy cannot be found. If CyberArk DNA cannot find the group policy and this parameter does not specify a password age limit, DNA will assume that passwords never expire.

Acceptable Values	Number
Default Value	90
SSHExpectInputTimeoutInSeconds	
Description	The maximum time, in seconds, DNA will wait for a shell prompt after running a command.
Acceptable Values	Number
Default Value	60
SSHCommandExecutionTimeoutInSeconds	
Description	The maximum time, in seconds, DNA will wait for an SSH command to execute. When an SSH command times out, DNA will continue to run the next command. This parameter must be configured in correlation to the DistributedScansTimeoutInSeconds, which can override it and should be set to at least ten times greater than this value.
Acceptable Values	Number
Default Value	180
SSHPort	
Description	The port that DNA will use to connect to target machines using SSH.
Acceptable Values	Number
Default Value	22
PassTheHashTimeFrameInDays	
Description	The timeframe in days for which DNA will retrieve data, when scanning for Pass-the-Hash vulnerabilities, including Golden Ticket attack vulnerabilities.
Acceptable Values	. Minimum possible value: 1 . Maximum possible value: 365
Default Value	90
ScanFromFileCsvDelimiter	
Description	The CSV delimiter of the import file. The default delimiter is ",". This is a hidden parameter that can be changed to any other supported CSV delimiter.
Acceptable Values	String
Default Value	“,”
DeleteDB	
Description	Whether or not the DNA database file (DNA.db) is deleted when DNA is closed. . Set this parameter to Yes to delete the database file when DNA is closed.

	. Set this parameter to No to save the database file using the following name format DNA_{Date}_{time}.db. For example, DNA_2015-05-06_04-47-49-PM.db.
Acceptable Values	Yes/No
Default Value	Yes
AccountTypeScanFilter	
Description	The type of accounts that will be scanned.
Acceptable Values	. Domain - Only domain users . Local - Only local users . All – Domain and local users
Default Value	All
Windows Accounts scan (Windows only)	
AccountCategoryScanFilter	
Description	The local groups that will be scanned for accounts.
Acceptable Values	. Privileged: . Administrators . Power Users . Backup operators . Cryptographic operators . Distributed COM Users . NonPrivileged: All other local groups . All: Both privileged and non-privileged local groups
Default Value	All
ScanWindowsServices	
Description	Whether or not Windows Services will be scanned.
Acceptable Values	Yes/No
Default Value	Yes
ScanScheduledTasks	
Description	Whether or not Scheduled Task will be scanned.
Acceptable Values	Yes/No
Default Value	Yes
ScanPassTheHash	
Description	Whether or not DNA will scan for Pass-the-Hash vulnerabilities, including Golden Ticket attack vulnerabilities.
Acceptable Values	Yes/No
Default Value	Yes

ScanDomainServices	
Description	Whether or not DNA will scan Domain Service Accounts (SPN).
Acceptable Values	Yes/No
Default Value	Yes
DistributedScans	
Description	Whether or not DNA will dedicate a process for each target machine scan and terminate after a timeout. When this parameter is set to “All”, DNA will use multiple processes by creating a separate process for each target machine scan, and will timeout after a preconfigured amount of time, set in the DistributedScansTimeoutInSeconds parameter. When this parameter is set to “None”, DNA will run in a centralized manner and will not use a separate process for every target machine. This configuration might cause a failure in one of the target machines which will cause DNA to be unresponsive. The number of machines that can be scanned concurrently in each of the aforementioned configurations is set in the MaxThreadNumber parameter.
Acceptable Values	All/None
Default Value	All
DistributedScansTimeoutInSeconds	
Description	The maximum time, in seconds, that DNA will wait for a distributed scan to execute. This parameter overrides the following parameters and therefore must be configured in correlation to their values: . SSHCommandExecutionTimeoutInSeconds – For best practice, the DistributedScansTimeoutInSeconds parameter must be at least ten times higher than the SSHCommandExecutionTimeoutInSeconds parameter. . WindowsCommandExecutionTimeoutInSeconds – For best practice, the DistributedScansTimeoutInSeconds parameter must be at least 300 seconds higher than the WindowsCommandExecutionTimeoutInSeconds parameter.
Acceptable Values	Number
Default Value	1800 seconds (30 minutes)
WindowsCommandExecutionTimeoutInSeconds	
Description	The maximum time, in seconds, DNA will wait for a Windows command to execute. When a Windows command times out, DNA will stop scanning the current Windows machines, since it is highly likely that the rest of the commands will also time out. It is recommended to increase the default value of the WindowsCommandExecutionTimeoutInSeconds parameter,

	when configuring the SSHKeyScanPathsOnWindows parameter for DNA to scan paths other than the default. This parameter must be configured in correlation to the DistributedScansTimeoutInSeconds, which can override it and should be set to at least 300 seconds greater than this value.
Acceptable Values	Number
Default Value	400
UseLDAPS	
Description	Whether or not to use LDAPS (LDAP over SSL) when connecting to Active Directory.
Acceptable Values	Yes/No
Default Value	No
PingMachineBeforeScan	
Description	Whether or not DNA will ping a machine before starting to scan it. Disable this parameter to scan machines that are configured not to return a ping, possibly for security reasons. Note: Windows machines on the Azure cloud do not return a ping. Disable this parameter to scan these machines.
Acceptable Values	Yes/No
Default Value	Yes
PingIntervals	
Description	The number of intervals that DNA will wait for the Ping command to run. This is a hidden parameter.
Acceptable Values	Number
Default Value	4
PingTimeoutInMilliseconds	
Description	The Ping command timeout in milliseconds. This is a hidden parameter.
Acceptable Values	Number
Default Value	1000
Credentials Detection Scan	
ScanVulnerableCredentials	
Description	Whether or not a scan will search endpoints for vulnerable credentials.
Acceptable Values	Yes/No
Default Value	Yes
SSH Keys Scan	

ScanSSHKeysOnUnix	
Description	Whether or not DNA will scan for SSH Keys on Unix machines.
Acceptable Values	Yes/No
Default Value	Yes
ScanPrivAndPubSSHKeysOnWindowsViaCygwin	
Description	Whether or not DNA will scan private and public SSH keys on machines where Cygwin is installed.
Acceptable Values	Yes/No
Default Value	Yes
ScanPrivSSHKeysOnWindowsNotViaCygwin	
Description	Whether or not DNA will scan for private SSH keys on machines where Cygwin is not installed. DNA uses a proprietary method of scanning endpoints, which is different from the read-only protocols and APIs that DNA uses regularly for all other scans. During the scan, DNA copies mini agents from the scanning machine to each scanned machine. These mini agents scan the Windows machine locally for private SSH keys and then securely communicate the information back to the scanning machine. Once the mini agent has completed its task, it ends all processes and deletes itself from the scanned machine. To verify that no processes or files have been left on the scanned machine, the scanning machine remotely verifies that the processes have been completed successfully. Note: In the case of a power or network outage, the processes may not have fully succeeded, and files might be left over on the scanned machines. For more information about the steps required to clean up these machines, refer to Scanning Issues, page 106, in Troubleshooting, page 105.
Acceptable Values	Yes/No
Default Value	No
SSHKeyScanPathsOnUnix	
Description	The path where DNA will search for private SSH keys on Unix machines.
Acceptable Values	Path, including the following: . Multiple paths, separated by space character. . Wildcards
Default Value	/home /root /export/home (UNIX home directories paths)
SSHKeyScanPathsOnWindows	
Description	The path where DNA will search for private SSH keys on Windows machines.

Acceptable Values	Path. Specify multiple paths separated by a space character. To specify paths that contain a space, eg, c:\documents and settings, surround the path with apostrophes.
Default Value	c:\users 'c:\document and settings'
SSHKeyMaxAgeInDays	
Description	The maximum account SSH Key age. This parameter determines the compliance status of each account.
Acceptable Values	Number Specify -1 to prevent checking the compliance status.
Default Value	365
DiscoverSSHKeysInBinaryFiles	
Description	Whether or not DNA will discover private SSH keys in binary files. This parameter is only relevant when scanning Unix machines and Windows machines with Cygwin, not when scanning Windows machines without Cygwin.
Acceptable Values	Yes/No
Default Value	No
SSHScanSingleCore	
Description	Whether or not DNA will scan SSH keys in a UNIX environment with only one CPU.
Acceptable Values	Yes/No
Default Value	No
DNAExecSSHScanSingleCore	
Description	Whether or not DNA will scan SSH keys in a Windows environment with only one CPU.
Acceptable Values	Yes/No
Default Value	No
PassTheHashScanSingleCore	
Description	Whether or not DNA will scan for Pass-the-Hash attacks in an environment with only one CPU.
Acceptable Values	Yes/No
Default Value	No
Cloud Assets Scan	
AWSRequestTimeoutInSeconds	
Description	The maximum time, in seconds, DNA will wait for an AWS command to execute. When an AWS command times out, DNA will stop scanning the current AWS machines, since it is

	highly likely that the rest of the commands will also time out.
Acceptable Values	Number
Default Value	20
Hard-Coded Credentials	
ScanHardCodedCredentialsInIIS	
Description	Whether or not a scan will search on IIS servers for embedded and hard-coded credentials.
Acceptable Values	Yes/No
Default Value	Yes
ScanHardCodedCredentialsInWebSphere	
Description	Whether or not a scan will search on WebSphere application servers for embedded and hard-coded Unix credentials.
Acceptable Values	Yes/No
Default Value	Yes
WebSphereInstallationPaths	
Description	Additional WebSphere installation paths that DNA will scan.
Acceptable Values	Full path name
Default Value	/opt/IBM/WebSphere/AppServer /usr/IBM/WebSphere/AppServer
ScanHardCodedCredentialsInWebLogic	
Description	Whether or not a scan will search on WebLogic application servers for embedded and hard-coded Unix credentials.
Acceptable Values	Yes/No
Default Value	Yes
WebLogicInstallationPaths	
Description	Additional WebLogic installation paths that DNA will scan.
Acceptable Values	Full path name
Default Value	/u01 /u02 /disk01 /disk02
ScanHardCodedCredsInDevOpsTools	
Description	Whether or not a scan will search playbooks on Ansible servers for embedded and hard-coded Unix credentials.
Acceptable Values	true/false
Default Value	true
AnsiblePlaybookScanPathsOnUnix	

Description	The default Unix path where DNA will search for Ansible Playbooks.
Acceptable Values	Full path of folder on Unix. Separate multiple values with a space delimiter.
Default Value	=/home /root
AD Bridge Integration	
ScanADBridge	
Description	Whether or not DNA will scan all machines for domain accounts. **Note:** This is a hidden parameter.
Acceptable Values	. Yes – DNA will scan all machines for local and domain accounts. . No – DNA will scan all machines for local accounts only.
Default Value	Yes
Database Accounts Scan	
ScanDatabase	
Description	Whether or not DNA will scan MSSQL databases for SQL or Windows/Active Directory databases users.
Acceptable Values	Yes/No
Default Value	Yes

Unix/Linux-Specific Configuration

When scanning Unix/Linux devices, CyberArk DNA uses various parameters in the UnixPrompts.ini configuration file. This file is located in the same directory as the DNA.exe file, and can be customized if certain scenarios occur. For more information, see Troubleshooting, page 105.

The table below describes the configurable parameters.

LoginPassword	
Description	A regular expression that matches a password request by the login process.
SudoPassword	
Description	A regular expression that matches a password request by a Unix/Linux system when using sudo. DNA uses this regular expression to match the request in order to run commands using sudo.
SudoError	
Description	A regular expression that matches an error received when commands are run using sudo. DNA uses this regular expression to match the sudo errors.

The following parameters enable DNA to support Unix/Linux flavors for which the required files are located in non-standard folders. If DNA does not find a file in the default path, it will use the relevant path parameter to search for it.

Specify the parameters in the table below in the Paths section of the UnixPrompts.ini file. In each parameter, specify the full path, including the file name, as shown in the following example:

```
[Paths]
sudoerPath=/usr/local/etc/sudoers
```

Separate multiple paths with a semicolon (;).

passwdPath	
Description	A list of paths to the possible location of the passwd file.
groupPath	
Description	A list of paths to the possible location of the group file.
shadowPath	
Description	A list of paths to the possible location of the shadow file.
sudoerPath	
Description	A list of paths to the possible location of the sudoers file.

Enable WMI Ports on Windows Client Machines

To enable the Windows (WMI) Protocol in your environment:

1. Make sure the Windows Management Instrumentation service startup type is set to Automatic.
2. For your operating system, do the following:
   - Windows 7 - In the firewall settings for your local or Group policy, under Inbound Rules, make sure Windows Management Instrumentation (WMI-In) is enabled and allowed for the Domain profile.
   - Windows Vista - In the firewall settings for your local or Group policy, click the Exceptions tab and enable the Windows Management Instrumentation (WMI) exception.
   - Windows XP - Run the following commands from the commands prompt:
     - netsh firewall set service RemoteAdmin enable.
     - netsh firewall add portopening protocol=tcp port=135 name=DCOM_ TCP135.
     - netsh firewall set portopening tcp 445 smb enable.

Configure Root Permissions Using the Sudoers File

When scanning Unix/Linux machines, DNA requires the use of sudo to run commands. Hence, the administrative user account(s) configured to scan with DNA must have permissions to run sudo on the scanned Unix/Linux machines.

Note:
DNA supports the sudo-replacement solutions that are listed in Sudo Replacements, page 21

Configure root permissions for the administrative user account configured to scan with DNA:

1. Connect to the Unix/Linux machine with the root user.
2. Run the following command to display the sudoers file: "visudo".
3. Add the following line:

```
[username] ALL=(ALL) NOPASSWD: ALL
```

Replace “[username]” with the name of the user running DNA.
Alternatively, if you prefer not to enable full root privileges to the user, the following list includes the commands that DNA requires for the user to be able to run with root privileges:

Platform	Command
Linux	ls, test, cat, lastlog, grep, find, ssh-keygen, date, sh
AIX	ls, test, cat, grep, ssh-keygen, istat, sh
Solaris	ls, test, cat, grep, find, ssh-keygen, sh

4. Save the sudoers file.

Configure AWS Scan Policies

IAM scans require the following policy:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iam:GenerateCredentialReport",
 "iam:GetAccessKeyLastUsed",
 "iam:GetAccountAuthorizationDetails",
 "iam:GetAccountPasswordPolicy",
 "iam:GetCredentialReport",
 "iam:GetUser",
 "iam:ListAccessKeys"
 ],
 "Resource": "*"
 }
 ]
}
```

The built-in policy that allows IAM scans is called **IAMReadOnlyAccess**. The following example shows a possible policy document.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iam:GenerateCredentialReport",
 "iam:GenerateServiceLastAccessedDetails",
 "iam:Get*",
 "iam:List*"
 ],
 "Resource": "*"
 }
 ]
}
```

The EC2 scan requires the following policy:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
```

```
 "Action": [
 "ec2:DescribeInstances",
 "ec2:DescribeKeyPairs"
 ],
 "Resource": "*"
 }
 ]
}
```

The built-in policy that allows EC2 scans is called **AmazonEC2ReadOnlyAccess**. The following example shows a possible policy document.

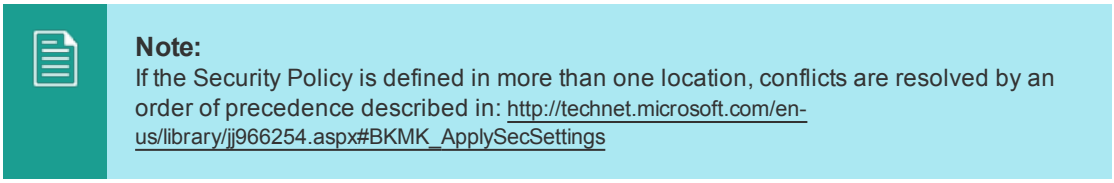
```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2:Describe*",
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": "elasticloadbalancing:Describe*",
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "cloudwatch:ListMetrics",
 "cloudwatch:GetMetricStatistics",
 "cloudwatch:Describe*"
 ],
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": "autoscaling:Describe*",
 "Resource": "*"
 }
 ]
}
```

Configure Audit Policy

DNA requires the Audit Policy to audit the following two types of events:

- Audit logon events.
- Audit system events

This can be configured through the Local Security Policy on endpoints or on the domain level through the Global Policy Management Editor.



Note:
If the Security Policy is defined in more than one location, conflicts are resolved by an order of precedence described in: http://technet.microsoft.com/en-us/library/jj966254.aspx#BKMK_ApplySecSettings

Configure the Audit Policy

1. In Local Policies, display Audit Policy.
2. Change Audit logon events and Audit system events to audit Success.

Import a File

DNA can import a file that specifies which Windows or Unix/Linux machines in your organization it will scan. The imported file must include a list of machines and the administrative credentials for each machine.

When setting up a scan for Windows machines, specify the user(s) who will be used to scan and their password(s).

When setting up a scan for Unix/Linux machines, specify the user(s) who be used to scan and their password(s) or SSH Key(s). For more information, refer to Scan Unix/Linux machines using a Password or an SSH Key, page 137.

Note:
DNA v5 does not support file import formats from previous versions

File Format

To be imported into DNA successfully, the file must meet the following requirements:

- The file must be in CSV format. To download a CSV template that you can use to create your CSV file, in the Setup scanning from a file window, click the link Click to download CSV template.
- It must include the following columns, in this order:
  - Server name/IP – The DNS name or IP address of a machine.
  - Username – The username to be used for scanning the machine.
  - Password – The user's password. Specify either the password or the SSH key in the "SSH Key" column, but not both.
  - Domain – The domain address, if the account is a domain account. This is optional.
  - SSH Key – The filename of the private SSH key that will authenticate the user and enable them to connect to a remote machine. For information about where to store the private SSH key, refer to Scan Unix/Linux machines using a Password or an SSH Key, page 137. Specify either the private SSH key or the user's password in the "Password" column, but not both.
  - It is also possible to use a passphrase-protected SSH Key. If you choose to do so, specify the passphrase in the "Passphrase" column.
  - DNA supports the following private keys in OpenSSH format:
    - RSA
    - DSA
  - The following encryption algorithms are supported:
    - DES-EDE3-CBC
    - DES-EDE3-CFB
    - DES-CBC
    - AES-128-CBC

- AES-192-CBC
- AES-256-CBC

- Passphrase – The passphrase that protects the SSH Key specified in the “SSH Key” column.

Note:
- The names of the columns do not need to be the same as above.
- The first row of the CSV must include the column headers.
- The CSV delimiter must be a comma: “,”.The delimiter can be changed in the CsvFileImportDelimeter parameter in the DNA configuration file.
- The credentials in the file must have local administrative or root privileges for the machines to be scanned. If DNA is configured to scan for Golden Ticket and Pass-the-Hash vulnerabilities, domain administrator credentials must be given; in this case, local administrative credentials are insufficient and are not supported.
- Make sure to delete the file used for this scan at the end of the scan, as it contains sensitive credentials.

Example

The following example shows the contents of a CSV file:

	A	B	C	D	E	F	G
1	Important note: Do not configure DNA to scan machines with Private SSH Keys that invoke						
2	Server name/IP	Username	Password	Domain (Optio	SSH Key Fi	Passphrase (Optional)	
3	machine1	user1	123456	domain.com			
4	10.10.0.10	administrat	admin				
5	10.10.0.1	root			key1		
6	10.10.0.2	root			key2	myKey	
7							

Scan Unix/Linux machines using a Password or an SSH Key

DNA can be configured to scan with users who authenticate in either of the following ways:

- Password authentication
- SSH Key authentication

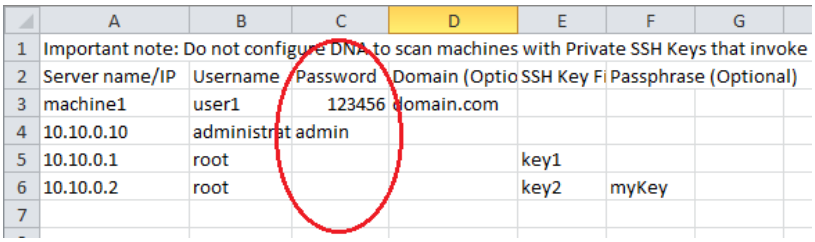
For more information about configuring these authentication methods, refer to the relevant procedure below.

Scan with a Password

1. Download a template of the CSV file where you will specify the Windows machines to scan and their administrative credentials.
   a. In the DNA Discovery window, select Scan from File, then click Next; the Setup scanning from a file page appears.
   b. Click Click to download CSV template; the CSV template file is downloaded your local machine.
2. Open the CSV file and specify the details of the machines to scan, as explained in File

Format, page 136. Make sure you specify the following column:

- Password – Specify the password of the user that will enable them to connect to the specified remote machine and scan it.



	A	B	C	D	E	F	G
1	Important note: Do not configure DNA to scan machines with Private SSH Keys that invoke						
2	Server name/IP	Username	Password	Domain (Optio	SSH Key Fi	Passphrase (Optional)	
3	machine1	user1	123456	domain.com			
4	10.10.0.10	administrat	admin				
5	10.10.0.1	root			key1		
6	10.10.0.2	root			key2	myKey	
7							

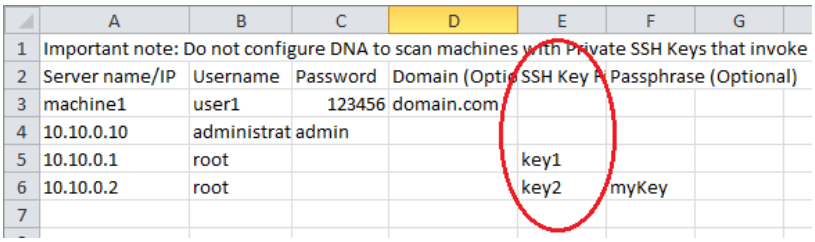
3. Make sure that the SSH Key column is empty. You cannot specify both a password and an SSH Key.
4. Set up the DNA scan, as described in Set up a DNA Scan, page 29.

Scan with an SSH Key

In order to scan machines that require authentication using an SSH key, DNA must have access to the private SSH keys.

Note:
DNA cannot authenticate to Windows machines with Cygwin using SSH Keys

1. Save the private SSH keys that will be used to authenticate to the remote machine in the DNA\PrivateSSHKeys folder on the DNA machine.
2. Download a template of the CSV file where you will specify the Unix/Linux machines to scan and their administrative credentials.
   a. In the DNA Discovery window, select Scan from File, then click Next; the Setup scanning from a file page appears.
   b. Click Click to download CSV template; the CSV template file is downloaded your local machine.
3. Open the CSV file and specify the details of the machines to scan, as explained in File Format, page 136. Make sure you specify the following columns:
   - SSH Key – Specify the filename of the private SSH key that will authenticate the user and enable them to connect to a remote machine and scan it.
   - Passphrase – If you specified an SSH Key that is passphrase-protected, specify the passphrase that protects the SSH Key specified in the SSH Key column.



	A	B	C	D	E	F	G
1	Important note: Do not configure DNA to scan machines with Private SSH Keys that invoke						
2	Server name/IP	Username	Password	Domain (Optio	SSH Key Fi	Passphrase (Optional)	
3	machine1	user1	123456	domain.com			
4	10.10.0.10	administrat	admin				
5	10.10.0.1	root			key1		
6	10.10.0.2	root			key2	myKey	
7							

4. Make sure that the Password column is empty. You cannot specify both a password and an SSH Key.
5. Set up the DNA scan, as described in Set up a DNA Scan, page 29.

Note:

- Make sure that the key that is being used, is not configured to automatically run a command on the target machine after authentication. If this sort of key was used, the command will be run and the connection will immediately disconnect. DNA cannot scan the remote machine when this sort of key is used.
- When running commands using sudo, make sure that a password isn't required.
- Make sure to delete the file used for this scan at the end of the scan, as it contains sensitive credentials.

Known Behavior and Limitations

This version of CyberArk DNA has the following known behavior and limitations:

Known Behaviors

- Unix built-in system accounts (UID between 1 to 100) that cannot login will be filtered out of the report.
- Windows services with built-in users are filtered out.
- In some scenarios, DNA credentials detection (LSASS scan) will result in wrong information about domain accounts, as if they were local accounts.
  - Most cases are recorded in the scan log file
  - If an error occurs, the credential data is not reported. Usually, other credential detection scans also retrieve similar credentials data about the user and report it correctly.

Scan Limitations

- Service account scans are not supported on the machine where CyberArk DNA is running.
- When scanning Unix/Linux machines, CyberArk DNA supports only the English locale when extracting data for the Last login date column.
- CyberArk DNA does not support PSOs (fine grained policies), therefore the password policy will be retrieved from the group policy.
- To determine the Last login date information, i.e., the last time an account logged into a machine, DNA uses the lastlogontimestamp attribute. This attribute is replicated on the different Domain Controllers in the Active Directory, hence its value may vary. Once in 14 days the AD synchronizes the value across all DCs. Since DNA does not enumerate through all Domain Controllers, the information DNA reports will be a maximum of 14 days old.
- To determine the Password Last Set information, i.e., the last time a password was changed for an account, DNA uses the LastPasswordSet property of the UserPrincipal class. This property is replicated on the different Domain Controllers in the Active Directory, hence its value may vary. Once in 14 days the Active Directory synchronizes the value across all DCs. Since DNA does not enumerate through all Domain Controllers, the information DNA reports will be a maximum of 14 days old.
- The Last Login Date column will display N/A for scanned Solaris machines.
  - When scanning HMC, the Key Length column shows the following values:
  - In the Unix Scan sheet, the Key Length column always displays N/A.
  - In the SSH Key Trusts sheet, the Key Length column only displays a value if a private SSH key was found on a non-HMC machine. Otherwise, it displays N/A.
- CyberArk DNA crashes when the current user is denied write access to the DNA folder.
- Scanning AIX and ESXi via an AD Bridge solution is not supported.

- On HMC machines:
  - In the DNA report, the following columns will display N/A: Compliance Status, Account State, Password Never Expires, Password Age, Password Last Set, Account Expiration Date.
  - If the scanned machine is connected to a domain via an AD Bridge, domain users will not be discovered.
- Currently, when setting UseLDAPS to “yes”, only Windows accounts (including accounts used in Windows Services and Scheduled Tasks) will be discovered using LDAPS. All other scans, such as Pass-the-Hash and SSH Key discovery, will use LDAP.
- DNA does not take the order of rules in the sudoers file into consideration. If there are multiple rules, DNA will present them all.
- When scanning for SSH keys on Windows machines where Cygwin is not installed, DNA must use a domain administrative Windows account, and not a local administrative account.
- By default, DNA will not scan single core machines for private SSH keys. This is relevant for both Windows and Unix. This can be changed by setting the SSH Keys scan parameters in the DNA.exe.config file. For more information, refer to Configuration Parameters, page 121.
- CyberArk DNA does not scan for SSH keys when using AD Bridge on Centrify.
- When using a non-administrator user (local or domain), DNA displays all machines in the Machine Type column as Servers even though some scanned machines may be Workstations.
- DNA discovers Hard-Coded Credentials on WebSphere in the default installation location and any other WebSphere running working paths. In addition, you can set the WebSphereInstallationPaths parameter to scan additional WebSphere paths. Likewise, DNA discovers Hard-Coded Credentials on WebLogic in the default installation location and any other WebLogic running working paths. In addition, you can set the WebLogicInstallationPaths parameter to scan additional WebLogic paths.
- If the user removes the default paths from this parameter DNA will still scan the default installation paths. However, if the user changes the default path, DNA will only scan the paths specified in this parameter and will not scan the default installation paths.
- The Database scan is based on the supplied Windows credentials, whether using Active Directory Scan or IP Address scan.

Report Limitations

- Special characters, such as ®, may display incorrectly in the OS Version column of the report.
- Due to Microsoft Excel report size restrictions, the report is limited to 1,048,576 rows. For an average environment, this limitation means approximately 40,000 target machines per scan. Use the filtering options in the configuration file (AccountTypeScanFilter, AccountCategoryScanFilter) to limit the number of accounts identified on each target machine.
- Currently, the Database scan is shown only as raw data and does not have any representation in the Executive summary.

Pass-the-Hash Limitations

- On Windows versions prior to Vista, if a machine name is identical to the domain name, DNA will not analyze PTH for that machine (a.k.a. false negatives).
- DNA may falsely report detected hashes for local and domain accounts that have a blank password.
- In order for DNA to find exposed hashes on the scanning machine itself, do one of the following:
  - Configure the local or domain built-in Administrator account as the credentials that the scanner will use to perform the scan.
  - Log into the machine running DNA with the local or domain built-in Administrator account, then run DNA. You can configure any domain administrative account as the credentials that the scanner will use to perform the scan.
  - Run DNA using “Run as Administrator”. You can configure any domain administrative account as the credentials that the scanner will use to perform the scan.
- The CPU usage in machines running Windows versions prior to Vista rises when scanning for Pass-the-Hash, and may reach as high as 100% between a few seconds and a few minutes. Since machines with a single core CPU may experience an effect on performance, they are not supported by default and will not be scanned for Pass-the-Hash and Golden Ticket risks. This can be changed by configuration parameters in the DNA.exe.config file. For more information, refer to Configuration Parameters, page 121.
- On Windows 2000, DNA cannot correctly identify inactive hashes. DNA overcomes this by marking accounts in the Pass-the-Hash: Hash Found column in the following way:

Account activity	Status
Accounts that have logged on in the past three days	Yes
Accounts that logged on more than three days ago	Previously

- When a password is changed in the Active Directory but is not updated in a Windows Service or Scheduled Task, the report will show “Yes” in the Pass-the-

- Hash: Hash Found column. This is a known false positive. The value should be “Previously”, since the hash is obsolete from the moment the password is changed in the Active Directory.
- When running DNA on a 32-bit machine, the Pass-the-Hash: Organizational Vulnerability Map may display only partial information.

Hard-Coded Credentials Scanning Limitations

- DNA only discovers Hard-Coded Credentials on IIS servers in the default installation location.

File Import Limitations

- When DNA scans a machine using local administrative credentials, it may detect domain groups and accounts. DNA can’t use local credentials to gather data about domain accounts. As a result, some Report fields will display N/A.
- When a file with IP addresses of machines is imported into DNA, Scheduled Task service accounts found on those machines will appear as domain accounts even if they are local accounts.
- When DNA scans using a source file, do not include machines on multiple or sub-domains as the Golden Ticket attack discovery will not run.
- When DNA scans using a source file, Windows business users detection is not supported. DNA tries to identify the Operating System type (Workstation\Server) according to the machine’s Operating System property but, in some cases, the Windows machine can be identified wrongly.

SSH Key Scanning Limitations

- DNA cannot detect SSH Key trusts for passphrase protected Private OpenSSH SSH Keys, since they are encrypted. Private PuTTY SSH keys that are passphrase-protected can be correlated to their public SSH keys, since they include the unencrypted public key.
- When running DNA on a 32-bit machine, the SSH Keys: Organizational Trust Map may display only partial information.
- DNA supports SSH Keys up to 10K in length.
- When scanning for SSH Keys on Solaris, the last modified date is always in GMT.
- When scanning for SSH Keys on Windows, the "Users" and "Documents and Settings" folders must be specified in English.
- DNA scans the permissions of the SSH key file, and the directory that the key file resides in, but not directories above that.
- DNA cannot scan passphrase protected private SSH keys that end with a null byte, therefore they will not appear in the report.
- The CPU usage in machines running Unix/Linux when scanning for private SSH keys, and may reach as high as 100% between a few seconds and a few minutes. Since machines with a single core CPU may experience an effect on performance, they are not supported by default and will not be scanned for SSH keys trusts. This can be changed by configuration parameters in the DNA.exe.config file. For more information, refer to Configuration Parameters, page 121.

- DNA cannot authenticate to Windows machines with Cygwin using SSH keys.
- DNA discovers ECDSA* and Ed25519 SSH keys on Windows with the following limitations:
  - The key length is not discovered
  - Trusts will not be discovered for these keys
- DNA will not discover SSH keys on Windows machines, when scanning via Cygwin, when the SSH keys are stored in a folder that did not inherit its permissions from the parent folder.

SSH Key Compliance Criteria

SSH Keys are non-compliant if they meet any of the following criteria:

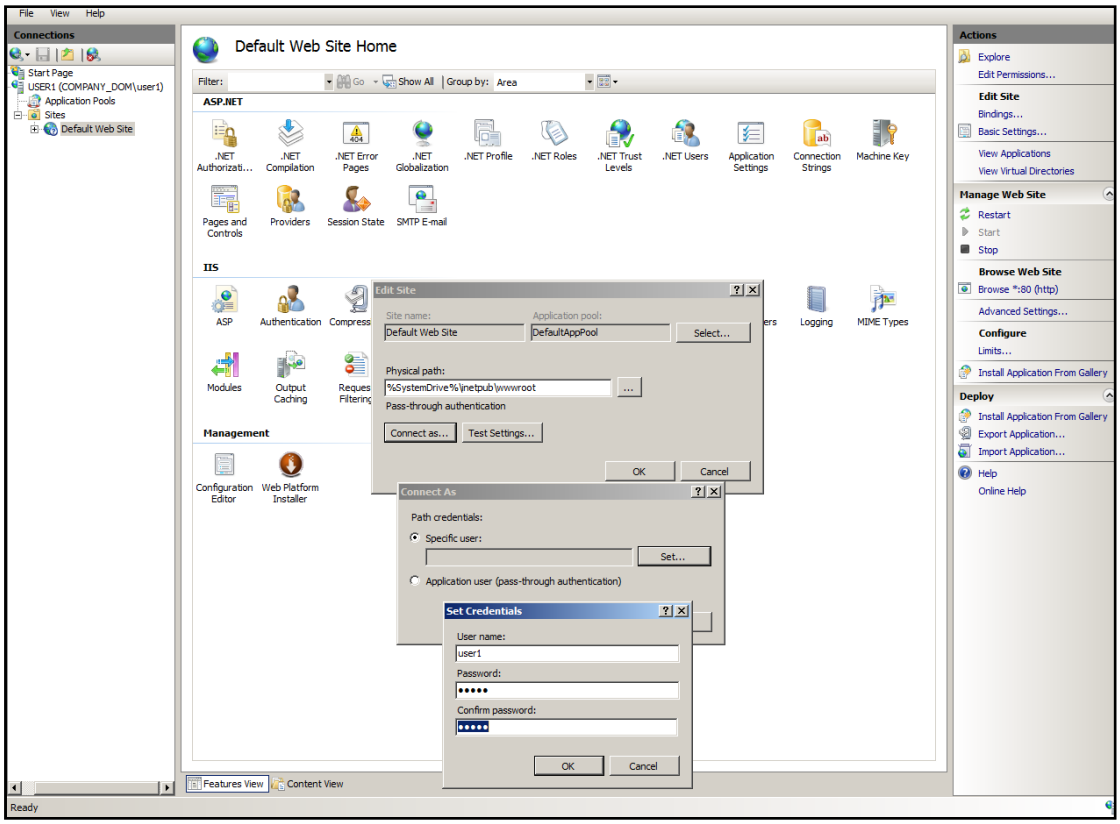
- ECDSA is used for the “Key Algorithm”, as it does not meet CyberArk’s security standards.
- RSA or DSA are used for the “Key Algorithm” and the “Key Length” is below (not including) 2048. SSH Keys of this length can be brute-forced more easily than SSH Keys that use 2048 or more bits.
- ECDSA or Ed25519 are used for the “Key Algorithm” and the “Key Length” is below (not including) 256. SSH Keys of this length can be brute-forced more easily than SSH Keys that use 2048 or more bits.
- The “Key Age” or “Trust Age” is higher than the value specified in the “SSHKeyMaxAgeInDays” parameter in the DNA configuration file.

Embedded and Hard-Coded Credentials

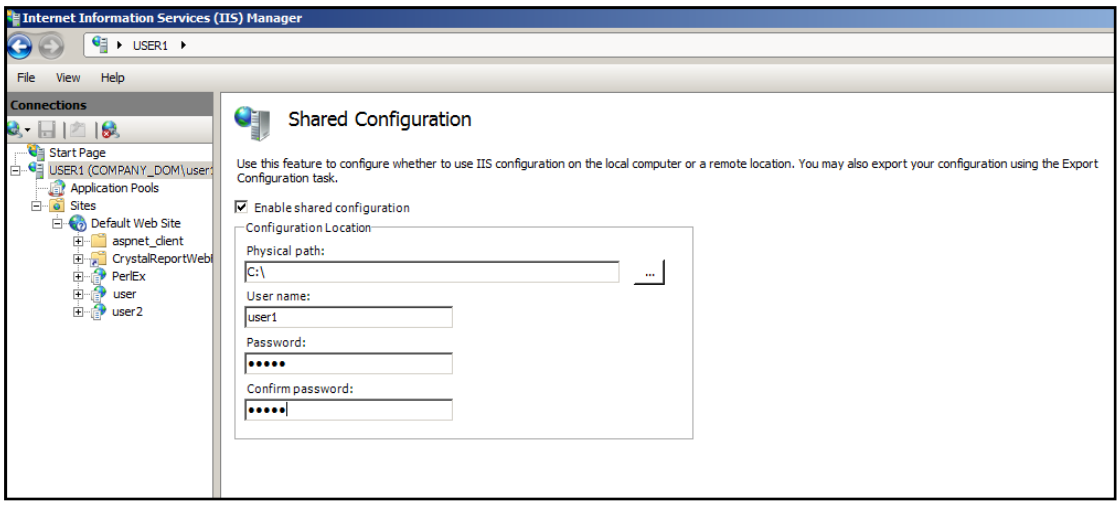
DNA detects the following types of hard-coded and embedded credentials:

- Embedded credentials – These are Windows credentials that are embedded in various locations. Credentials are discovered in the following:
  - Windows Services
  - Windows Scheduled Tasks
  - IIS Server – These credentials are stored in configuration files on the IIS server, and are used to establish connections, such as a connection to a database or web site, or a file system directory on a local or remote shared directory, as shown in the following examples:

Creating a Connection to a Default Web Site



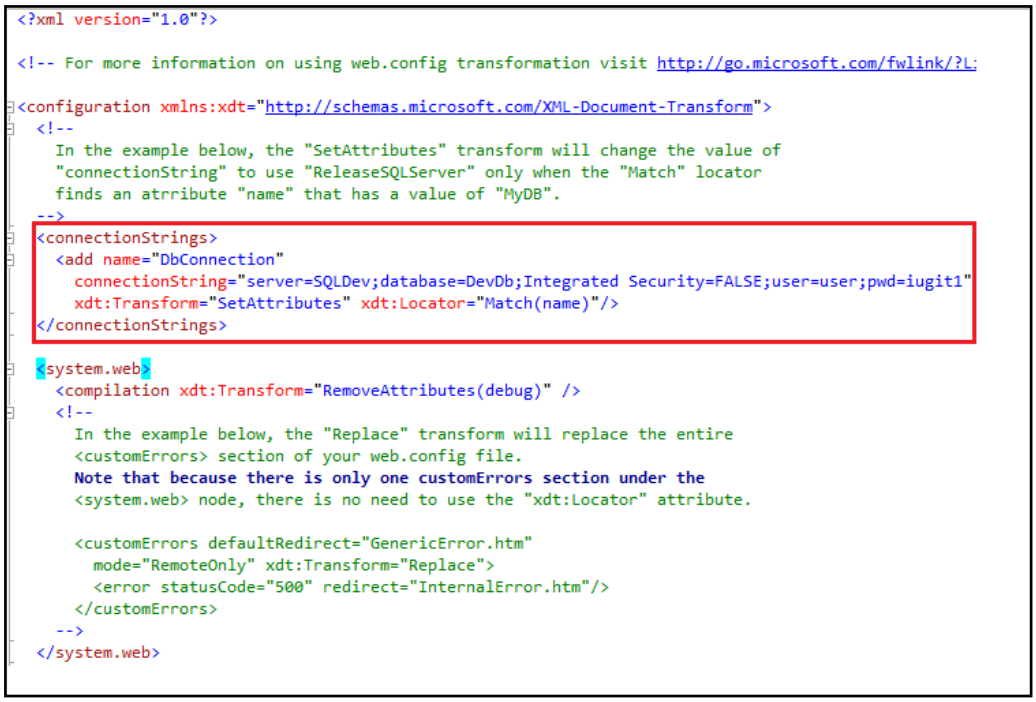
Creating a Shared Configuration Connection



DNA discovers embedded Windows credentials on IIS Servers and categorizes the types listed in the table below. DNA extracts username and password (masked) attributes, as well as path and name attributes. DNA extracts this data from different locations and sections in various IIS configuration files.

Type	Element/attribute	File
IIS Application Pool	Element: processModel	applicationHost.config
IIS Anonymous Authentication	Element: anonymousAuthentication	applicationHost.config, web.config
IIS Virtual Directory	Element: Application → virtualDirectory	applicationHost.config
IIS Configuration Redirection	Element: configurationRedirection Attribute: path	redirection.config
IIS Authentication with ASP.NET Impersonation	Element: identity	web.config, machine.config

- Hard-coded credentials – These are credentials that are manually entered into applications running on WebSphere and IIS servers, as shown in the following example of an IIS configuration file:



```
<?xml version="1.0"?>

<!-- For more information on using web.config transformation visit http://go.microsoft.com/fwlink/?L:

<configuration xmlns:xdt="http://schemas.microsoft.com/XML-Document-Transform">
  <!--
    In the example below, the "SetAttributes" transform will change the value of
    "connectionString" to use "ReleaseSQLServer" only when the "Match" locator
    finds an atrribute "name" that has a value of "MyDB".
  -->
  <connectionStrings>
    <add name="DbConnection"
      connectionString="server=SQLDev;database=DevDb;Integrated Security=FALSE;user=user;pwd=iugit1"
      xdt:Transform="SetAttributes" xdt:Locator="Match(name)"/>
  </connectionStrings>

  <system.web>
    <compilation xdt:Transform="RemoveAttributes(debug)" />
    <!--
      In the example below, the "Replace" transform will replace the entire
      <customErrors> section of your web.config file.
      Note that because there is only one customErrors section under the
      <system.web> node, there is no need to use the "xdt:Locator" attribute.

      <customErrors defaultRedirect="GenericError.htm"
        mode="RemoteOnly" xdt:Transform="Replace">
        <error statusCode="500" redirect="InternalError.htm"/>
      </customErrors>
    -->
  </system.web>
```

Discover Public SSH Keys

DNA uses the value of the AuthorizedKeysFile parameter in the sshd_config file to analyze the public SSH keys that were configured.

If DNA cannot find this parameter in the sshd_config file, DNA uses the following default values:

- [user home folder]/.ssh/authorized_keys
- [user home folder]/.ssh/authorized_keys2

Ports used by DNA

CyberArk DNA uses the following ports to discover accounts and SSH keys on remote machines:

Port	Use case
22	To connect to target machines using SSH. This port can be configured by the SSHPort parameter in the DNA.exe.config file.
88	Used for KDC services (only relevant to domain controllers). This port must be accessible both through network-based and host-based firewalls.
135, 137, 138, 139	To connect to target machines using NetBIOS ports. These ports must be accessible on host-based firewalls.
389/636	To connect to target machines using the LDAP service (only relevant to domain controllers). This port must be accessible both through network-based and host-based firewalls (LDAP=389, LDAPS=636).
443	To access the AWS Console via AWS API and scan AWS.
445	To connect to target machines using SMB/TCP. This port must be accessible on host-based firewalls.
4431	To discover SSH keys on Windows machines without Cygwin. This port is not configurable.
1433	To connect to MSSQL databases
49153	To communicate in TCP with the remote machine, and enables users to view the Event Log.
49154	To get the list of Scheduled Tasks from the remote machine for remote viewing and administration.
49155, 49156	To get the list of Local Services from the remote machine for remote viewing and administration.

Configure Logging for 'Key Last Used' Data

By default, the OpenSSH server (sshd) logs to the AUTH facility of syslog, at the INFO level. To record more information, such as SSH keys last used, increase the logging level to VERBOSE.

This section describes how to configure the OpenSSH server to log the date and time when an SSH key was last used.

On OpenSSH Server 6.2.x and below on Unix and Cygwin

1. In the sshd_config file (usually on /etc/ssh/sshd_config), set the LogLevel parameter to verbose.
2. In the sshd_config file, make sure the SyslogFacility parameter is set to AUTH.
3. Restart sshd service after these changes.
4. In the syslog.conf file, do the following:
   a. Set the syslog log level according to the selected syslog system (Syslog\RSyslog\NG-syslog):
      - On syslog-ng – Include the info level filter (for example: *.=info)
      - On rsyslog or syslog – Include the info log level and higher (for example: *.=info)
   b. Specify a path where the log files will be saved. You can specify either a local or remote path that is mounted on the local machine.
5. In both files, add the syslog facility that will bind the above values (for example: syslog.* /var/log/fac_syslog).

Note:
These changes will apply for future SSH Key Last Used data and not past events.

On deployments where AD Bridge is configured

This is relevant for Centrify AD-Bridge.

1. In the sshd_config file, set the log level to verbose or higher.
2. In the /etc/centrifydc/ssh/sshd_config file, set the log level to verbose or higher. This value must be the same as the value set in step 1.
3. In the syslog.conf.in file, do the following:
   a. Set the syslog log level:
      - On syslog-ng – Include the info level filter
      - On rsyslog or syslog – Include the info log level and higher
   b. Specify a path where the log files will be saved. You can specify either a local or remote path that is mounted on the local machine.
4. In both files, add the syslog facility that will bind the above values.