AUDITING GROUP POLICIES USING THE CIS-CAT TOOL

Table of Contents

1. Objective

To Identify the compliance level of windows 10 system using CIS-CAT Lite V3

2. Prerequisites

Prerequisites	Version
Tools required	CIS-CAT Lite V3
Operating System	Windows 10, JRE

3. Problem Statement

Hardening is the process which reduces the potential attack surface of the system. Centre for information security (CIS) provides set of benchmark standards to harden the system.

4. Summary

Steps	Description
Step 1	Downloading of CIS-CAT Lite V3
Step2	Installation of CIS-CAT Lite V3
Step3	CIS-CAT Report

Introduction of CIS-CAT Tool :

CIS-Configuration Assessment Tool (CAT) compares the configuration of target systems to the secure configuration settings recommended in machine-readable content. The tool is designed to primarily assess against CIS Benchmark configuration recommendations. The tool provides a conformance report ranging from 0 – 100. Detailed output reports provide remediation guidance for each CIS Benchmark recommendation.

- **CIS-CAT Lite**: It's an free version produces only HTML and supports a subset of CIS Benchmark assessments.
- **CIS-CAT PRO**: Performs assessments over a local or shared internal network, and offers a variety of outputs.

CIS-CAT Lite v3

CIS-CAT Lite can perform Assessment on Local system. CIS CAT Lite v3 supports following benchmarks:

- CIS Apple OSX 10.12 Benchmark
- CIS Google Chrome Benchmark

- CIS Microsoft Windows 10 Enterprise Release 1909 Benchmark
- CIS Ubuntu Linux 18.04 LTS Benchmark

CIS-CAT Lite v4

CIS-CAT Lite can perform Assessment on Local system as well as Remote system. CIS CAT Lite v4 supports following benchmarks:

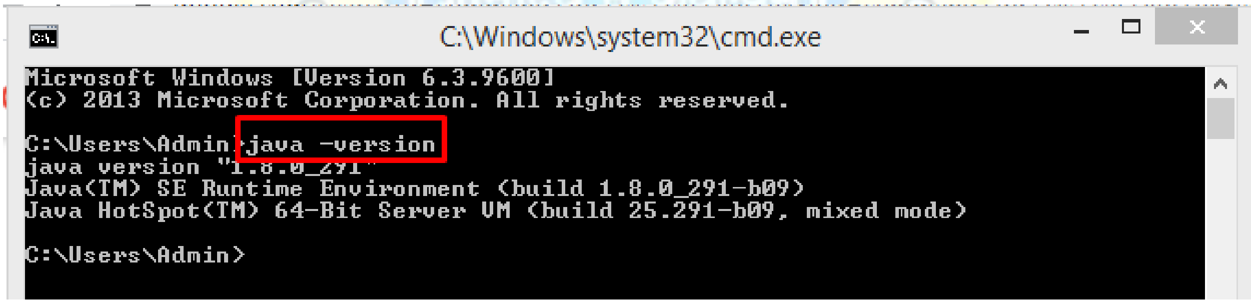
- CIS Controls Assessment Module – Implementation Group 1 for Windows 10 v1.0.3
- CIS Controls Assessment Module – Implementation Group 1 for Windows Server V1.0.0
- CIS Google Chrome Benchmark V2.0.0
- CIS Microsoft Windows 10 Enterprise release 2004 Benchmark v1.9.1
- CIS Ubuntu Linux 18.04 LTS Benchmark v1.9.1

1. Step-1 : Downloading of CIS-CAT Lite

NOTE : Before starting CIS-CAT Assessment we need to check whether java is installed on the system or not.

Open the command prompt and type the command java -version to see the whether java is install or not and what is it's version.

If java is not installed then we have to install java.

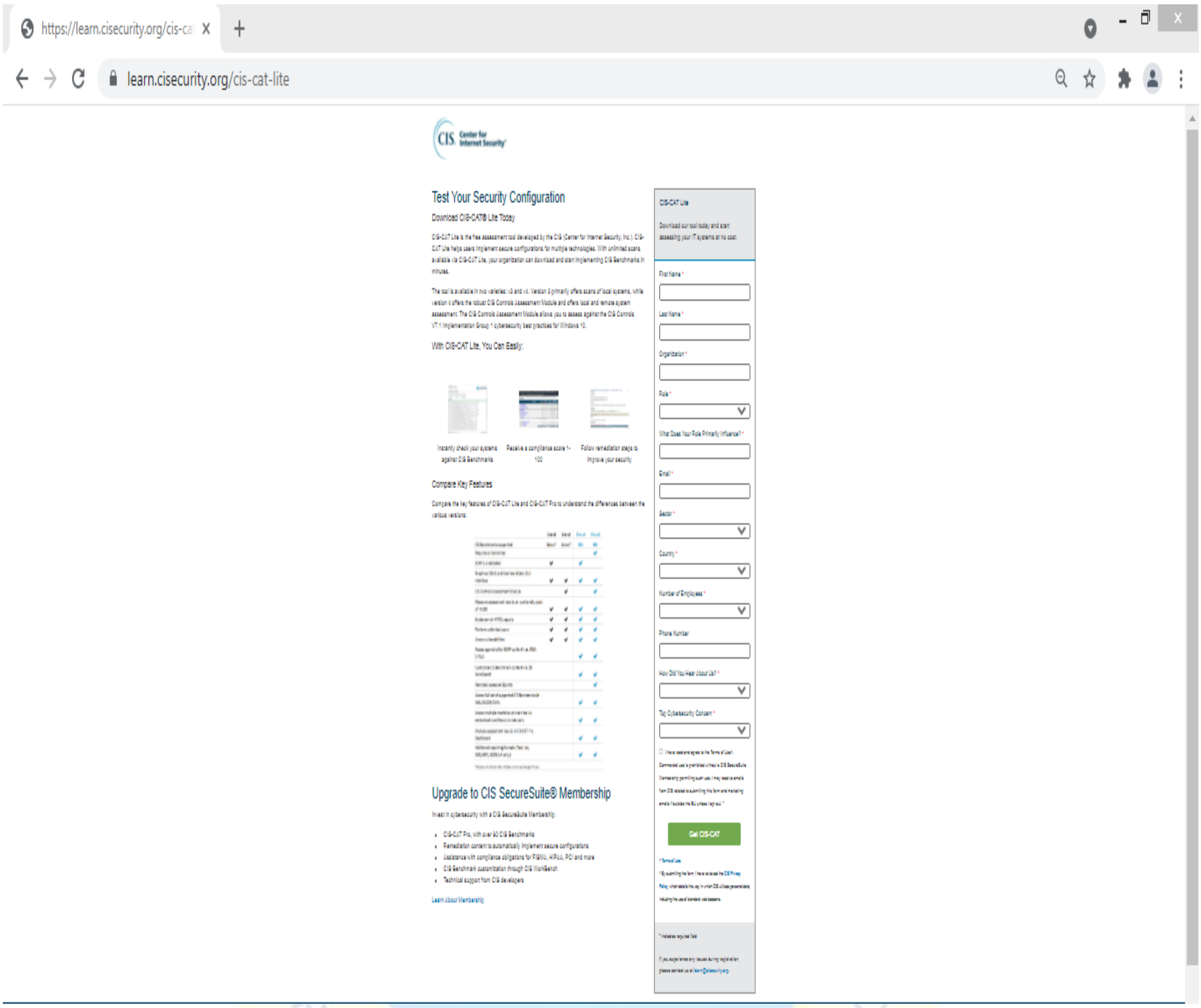


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Admin>java -version
java version "1.8.0_291"
Java(TM) SE Runtime Environment (build 1.8.0_291-b09)
Java HotSpot(TM) 64-Bit Server VM (build 25.291-b09, mixed mode)

C:\Users\Admin>
```

For Downloading CIS-CAT Lite V3 Open the web browser and type the below url https://learn.cisecurity.org/cis-cat-lite



https://learn.cisecurity.org/cis-ca
learn.cisecurity.org/cis-cat-lite
CIS Center for Internet Security

Test Your Security Configuration

Download CIS-CAT® Lite Today

CIS-CAT Lite is the free assessment tool developed by the CIS (Center for Internet Security, Inc.). CIS-CAT Lite helps users implement secure configurations for multiple technologies. With unlimited scans available via CIS-CAT Lite, your organization can download and start implementing CIS Benchmarks in minutes.

The tool is available in two varieties: v3 and v4. Version 3 primarily offers scans of local systems, while version 4 offers the robust CIS Controls Assessment Module and offers local and remote system assessment. The CIS Controls Assessment Module allows you to assess against the CIS Controls V7.1 Implementation Group 1 cybersecurity best practices for Windows 10.

With CIS-CAT Lite, You Can Easily:

Instantly check your systems against CIS Benchmarks

Receive a compliance score 1-100

Follow remediation steps to improve your security

Compare Key Features

Compare the key features of CIS-CAT Lite and CIS-CAT Pro to understand the differences between the various versions:

	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]				✓
[illegible]	✓		✓	
[illegible]	✓	✓	✓	✓
[illegible]		✓		✓
[illegible]	✓	✓	✓	✓
[illegible]	✓	✓	✓	✓
[illegible]	✓	✓	✓	✓
[illegible]	✓	✓	✓	✓
[illegible]			✓	✓
[illegible]			✓	✓
[illegible]				✓
[illegible]			✓	✓
[illegible]			✓	✓
[illegible]			✓	✓
[illegible]			✓	✓

Upgrade to CIS SecureSuite® Membership

Invest in cybersecurity with a CIS SecureSuite Membership:

- CIS-CAT Pro, with over 80 CIS Benchmarks
- Remediation content to automatically implement secure configurations
- Assistance with compliance obligations for FISMA, HIPAA, PCI and more
- CIS Benchmark customization through CIS WorkBench
- Technical support from CIS developers

Learn About Membership

CIS-CAT Lite

Download our tool today and start assessing your IT systems at no cost.

First Name *

Last Name *

Organization *

Role *

What Does Your Role Primarily Influence? *

Email *

Sector *

Country *

Number of Employees *

Phone Number

How Did You Hear About Us? *

Top Cybersecurity Concern *

□ I have read and agree to the Terms of Use^. Commercial use is prohibited without a CIS SecureSuite Membership permitting such use. I may receive emails from CIS related to submitting this form and marketing emails if outside the EU unless I opt out. *

Get CIS-CAT

^Terms of Use.

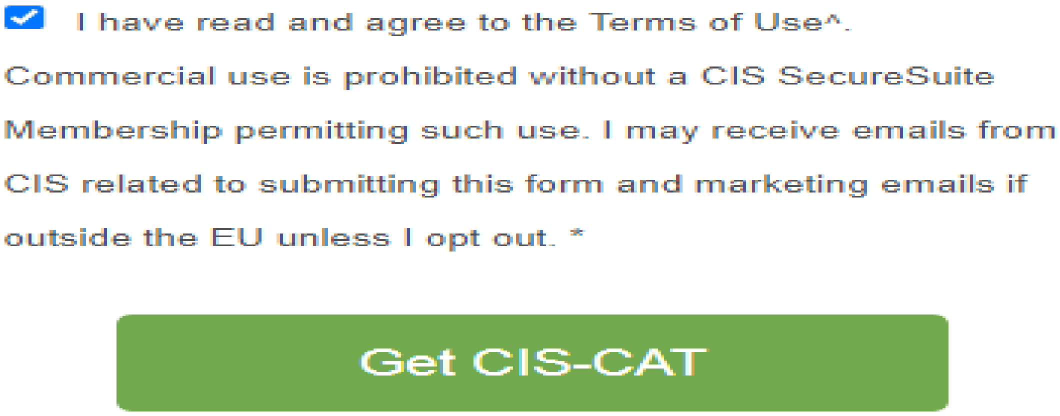
^By submitting the form, I have reviewed the CIS Privacy Policy, which details the way in which CIS utilizes personal data, including the use of standard web beacons.

* Indicates required field

If you experience any issues during registration, please contact us at learn@cisecurity.org.

Fill all the required details to register for CIS-CAT Lite tool.

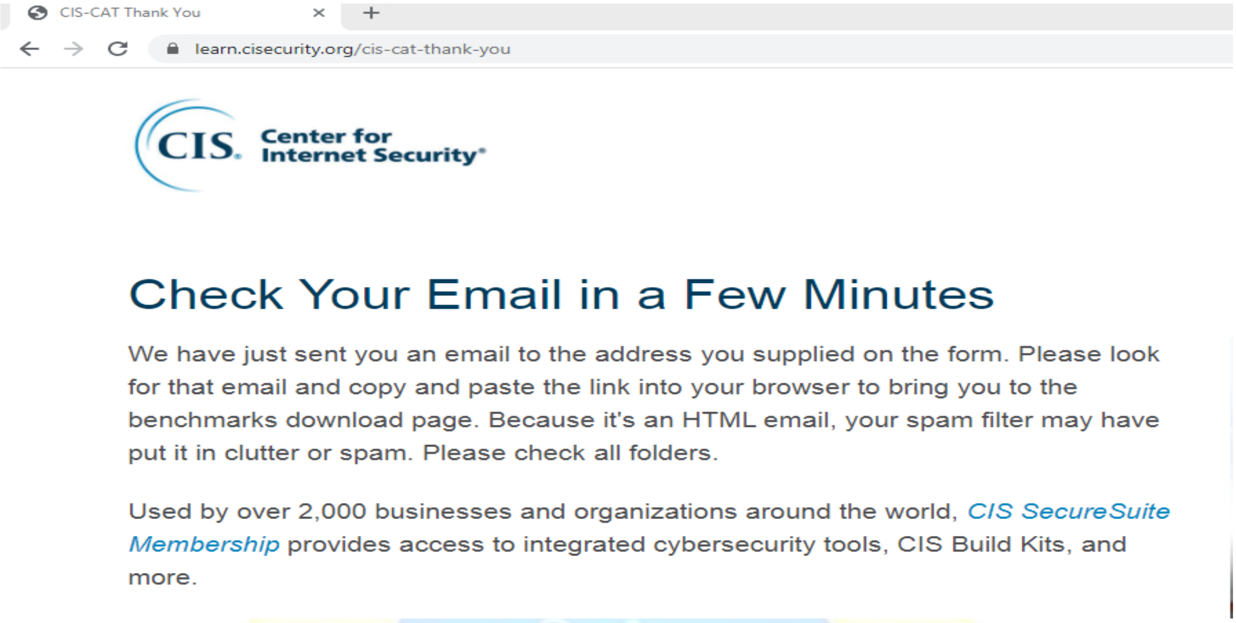
After Entering mandatory details check the Terms of Use. And click on Get CIS-CAT



☑ I have read and agree to the Terms of Use^. Commercial use is prohibited without a CIS SecureSuite Membership permitting such use. I may receive emails from CIS related to submitting this form and marketing emails if outside the EU unless I opt out. *

Get CIS-CAT

After clicking on Get CIS-CAT, browser will redirect to page which prompt to check email in few minutes. In some time an email will receive which have link to download the CIS-CAT Lite.


CIS-CAT Thank You
learn.cisecurity.org/cis-cat-thank-you
CIS Center for Internet Security

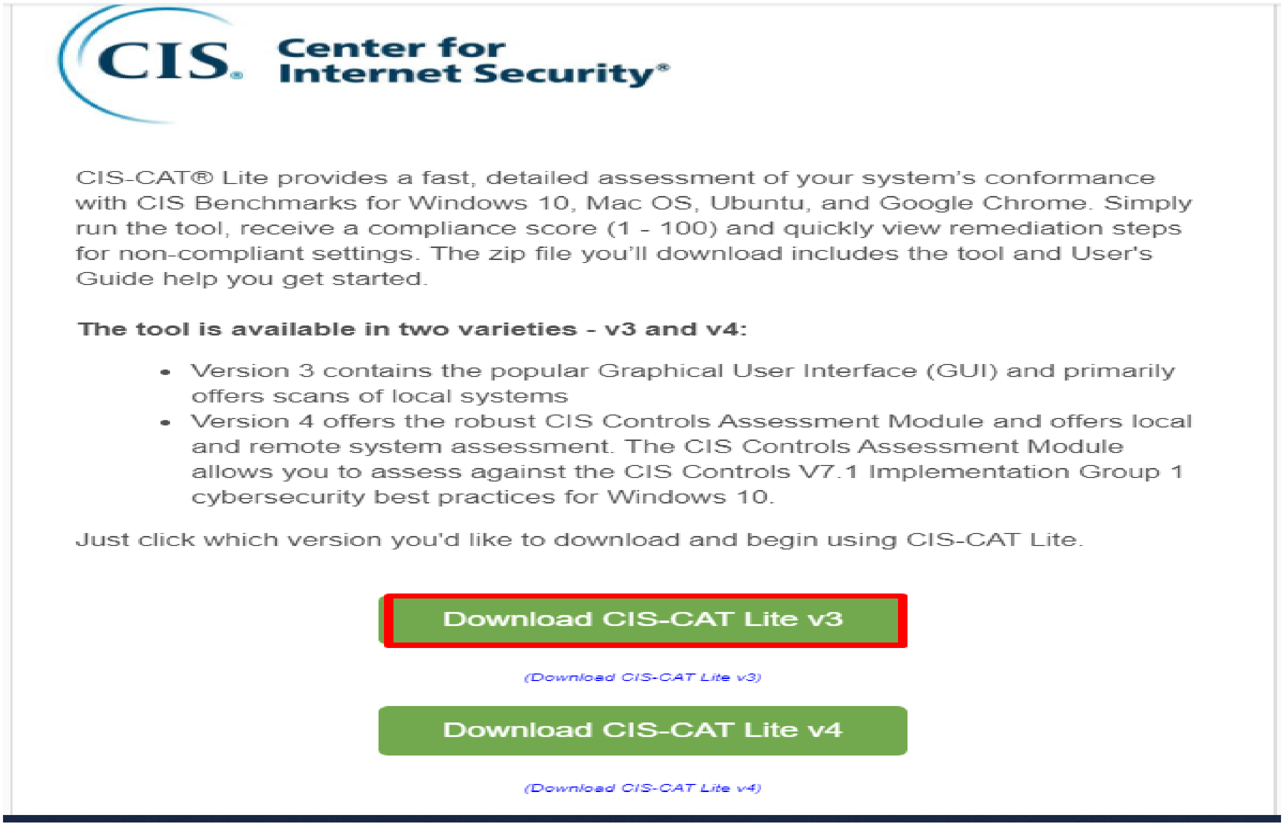
Check Your Email in a Few Minutes

We have just sent you an email to the address you supplied on the form. Please look for that email and copy and paste the link into your browser to bring you to the benchmarks download page. Because it's an HTML email, your spam filter may have put it in clutter or spam. Please check all folders.

Used by over 2,000 businesses and organizations around the world, CIS SecureSuite Membership provides access to integrated cybersecurity tools, CIS Build Kits, and more.

Download the CIS-CAT Lite from the link received through email.

Click on Download CIS-CAT Lite v3. Downloading will be start in few seconds.



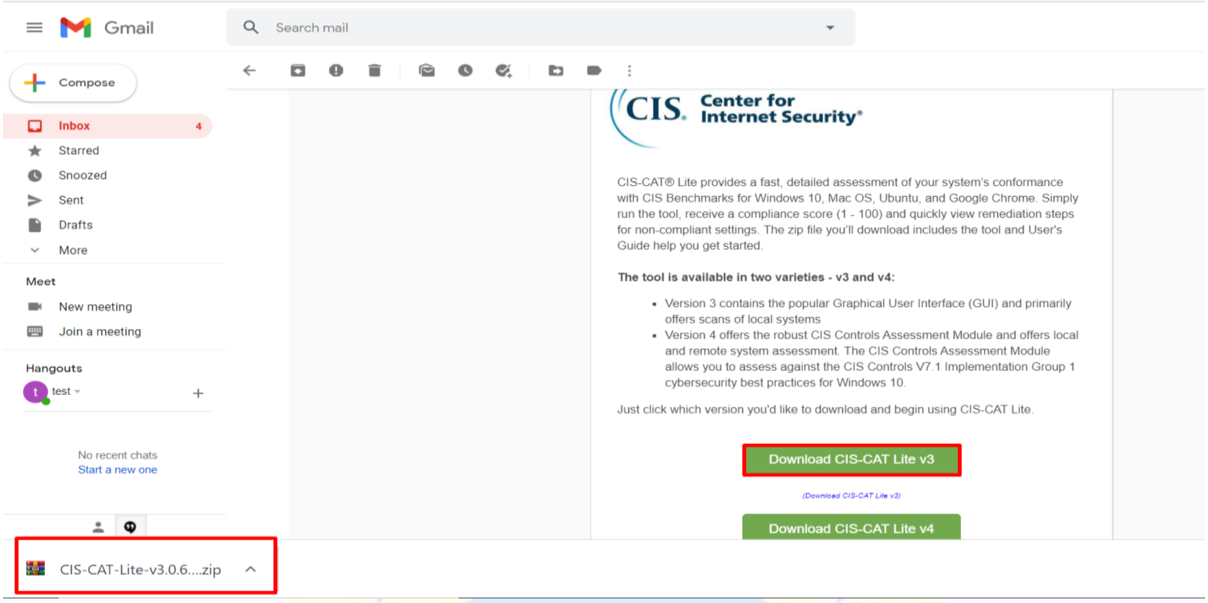
CIS-CAT® Lite provides a fast, detailed assessment of your system's conformance with CIS Benchmarks for Windows 10, Mac OS, Ubuntu, and Google Chrome. Simply run the tool, receive a compliance score (1 - 100) and quickly view remediation steps for non-compliant settings. The zip file you'll download includes the tool and User's Guide help you get started.

The tool is available in two varieties - v3 and v4:

- Version 3 contains the popular Graphical User Interface (GUI) and primarily offers scans of local systems
- Version 4 offers the robust CIS Controls Assessment Module and offers local and remote system assessment. The CIS Controls Assessment Module allows you to assess against the CIS Controls V7.1 Implementation Group 1 cybersecurity best practices for Windows 10.

Just click which version you'd like to download and begin using CIS-CAT Lite.

As we can see zip folder is downloaded.



CIS-CAT® Lite provides a fast, detailed assessment of your system's conformance with CIS Benchmarks for Windows 10, Mac OS, Ubuntu, and Google Chrome. Simply run the tool, receive a compliance score (1 - 100) and quickly view remediation steps for non-compliant settings. The zip file you'll download includes the tool and User's Guide help you get started.

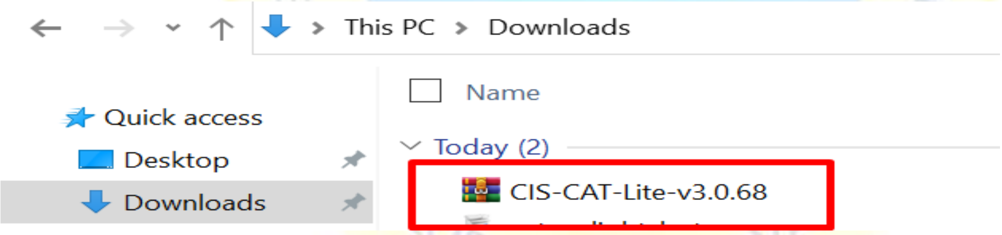
The tool is available in two varieties - v3 and v4:

- Version 3 contains the popular Graphical User Interface (GUI) and primarily offers scans of local systems
- Version 4 offers the robust CIS Controls Assessment Module and offers local and remote system assessment. The CIS Controls Assessment Module allows you to assess against the CIS Controls V7.1 Implementation Group 1 cybersecurity best practices for Windows 10.

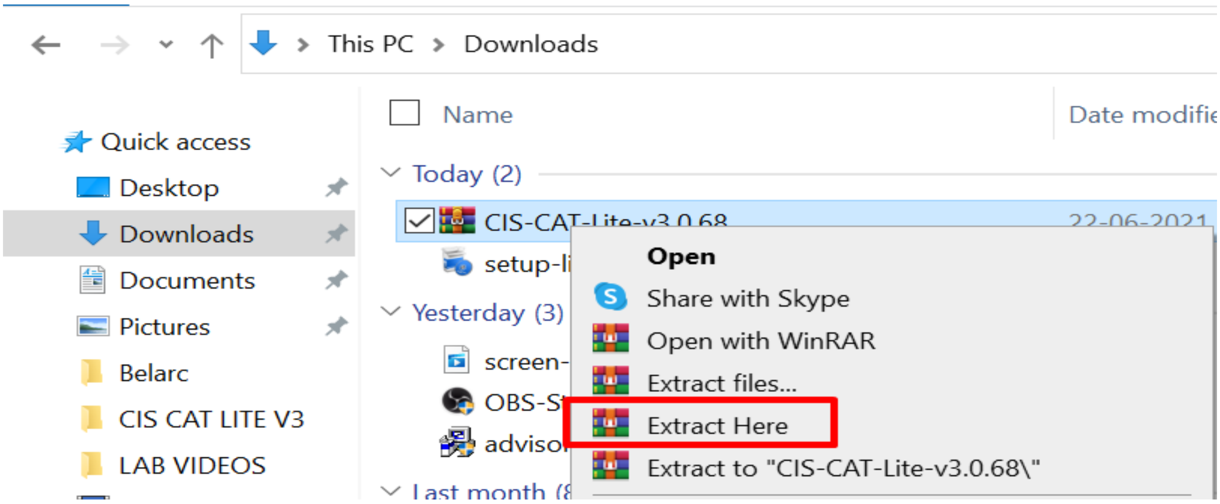
Just click which version you'd like to download and begin using CIS-CAT Lite.

2. Installation of CIS-CAT Lite V3

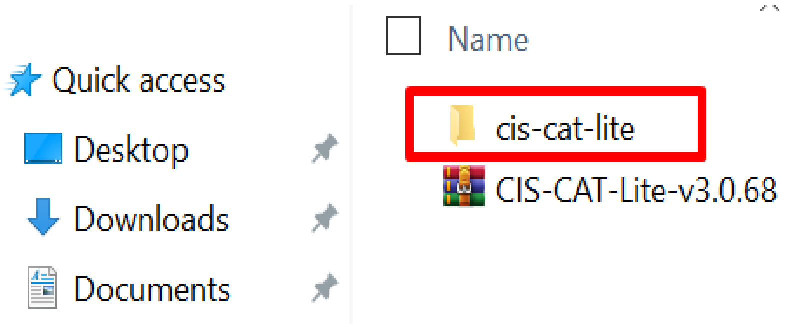
The Zip folder is downloaded in downloads folder



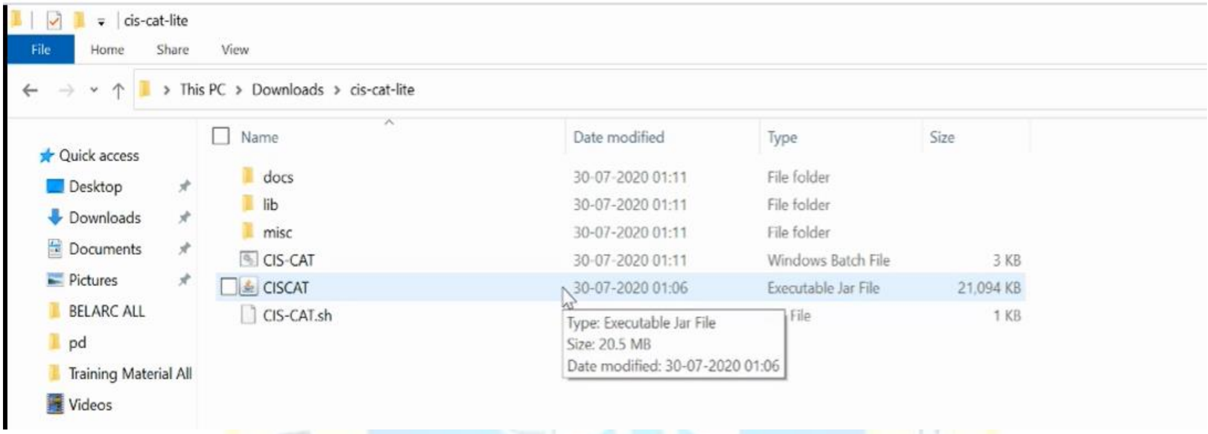
Right click on the downloaded CIS-CAT Lite v3 zip folder and click on Extract here.



After extracting Zip folder cis-cat-lite folder will be appear as shown in screenshot below.



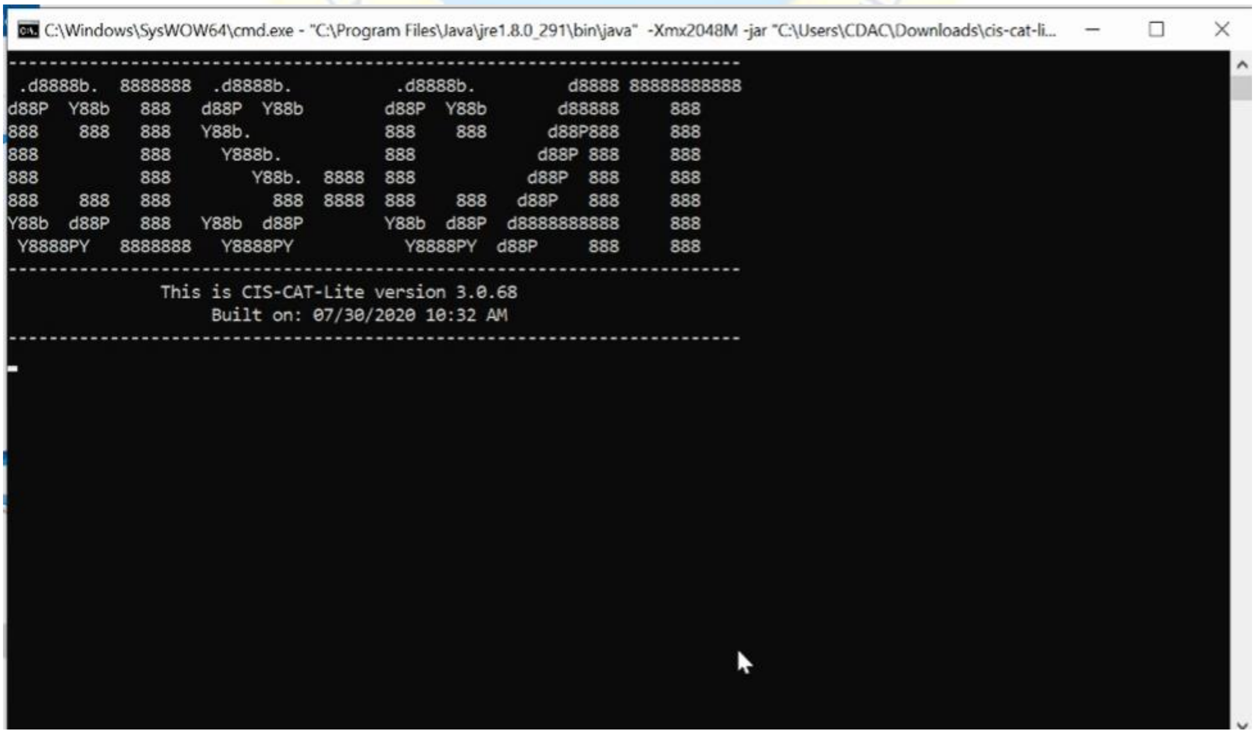
Open the cis-cat-lite folder



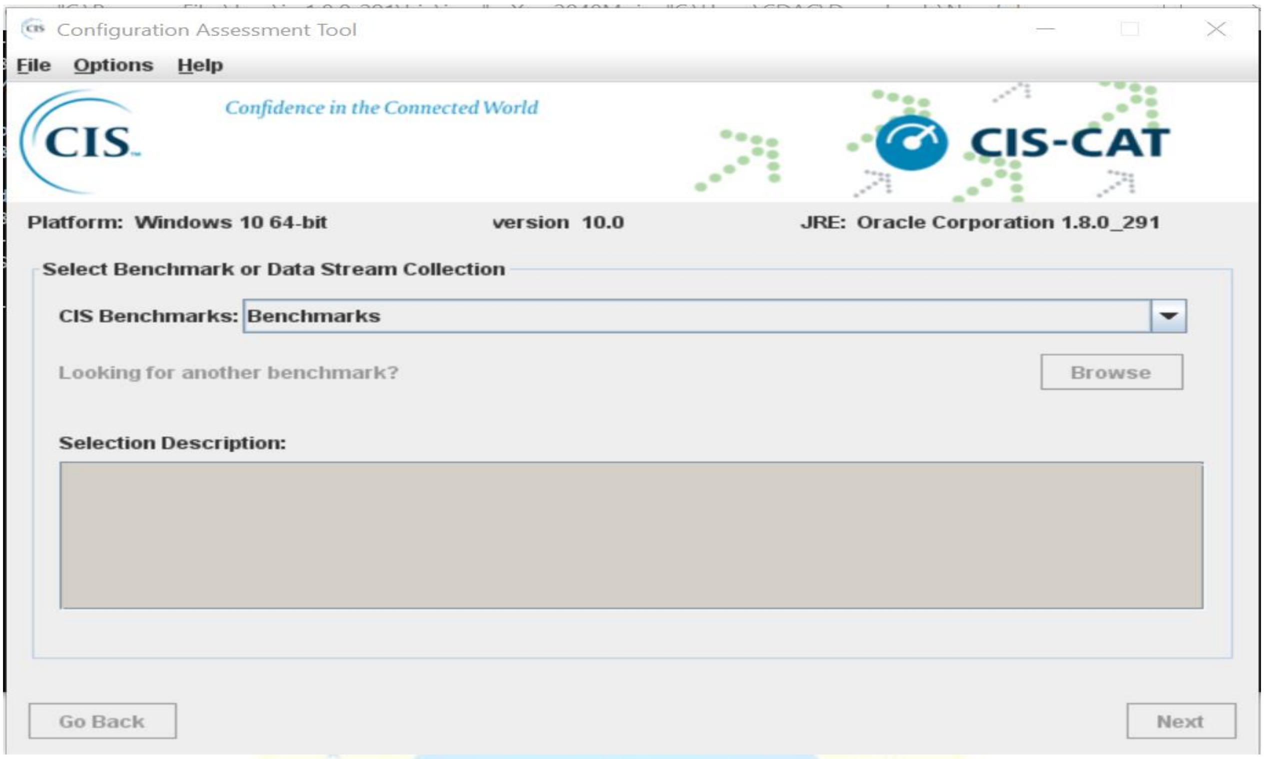
Name	Date modified	Type	Size
docs	30-07-2020 01:11	File folder	
lib	30-07-2020 01:11	File folder	
misc	30-07-2020 01:11	File folder	
CIS-CAT	30-07-2020 01:11	Windows Batch File	3 KB
CISCAT	30-07-2020 01:06	Executable Jar File	21,094 KB
CIS-CAT.sh		File	1 KB

Type: Executable Jar File
Size: 20.5 MB
Date modified: 30-07-2020 01:06

As we can see CISCAT Executable jar File is there. Double click on it. The below window will appear.


C:\Windows\SysWOW64\cmd.exe - "C:\Program Files\Java\jre1.8.0_291\bin\java" -Xmx2048M -jar "C:\Users\CDAC\Downloads\cis-cat-li...

```
------------------------------------------------------------------------
 .d8888b.  8888888  .d8888b.          .d8888b.        d8888 88888888888
d88P  Y88b   888   d88P  Y88b        d88P  Y88b      d88888     888
888    888   888   Y88b.             888    888     d88P888     888
888          888     Y888b.          888           d88P 888     888
888          888        Y88b.  8888  888          d88P  888     888
888    888   888          888  8888  888    888  d88P   888     888
Y88b  d88P   888   Y88b  d88P        Y88b  d88P d8888888888     888
 Y8888PY   8888888   Y8888PY           Y8888PY  d88P     888     888
------------------------------------------------------------------------
               This is CIS-CAT-Lite version 3.0.68
                    Built on: 07/30/2020 10:32 AM
------------------------------------------------------------------------
```


Configuration Assessment Tool
File
Options
Help
CIS
Confidence in the Connected World
CIS-CAT
Browse
Go Back
Next

Platform: Windows 10 64-bit version 10.0 JRE: Oracle Corporation 1.8.0_291

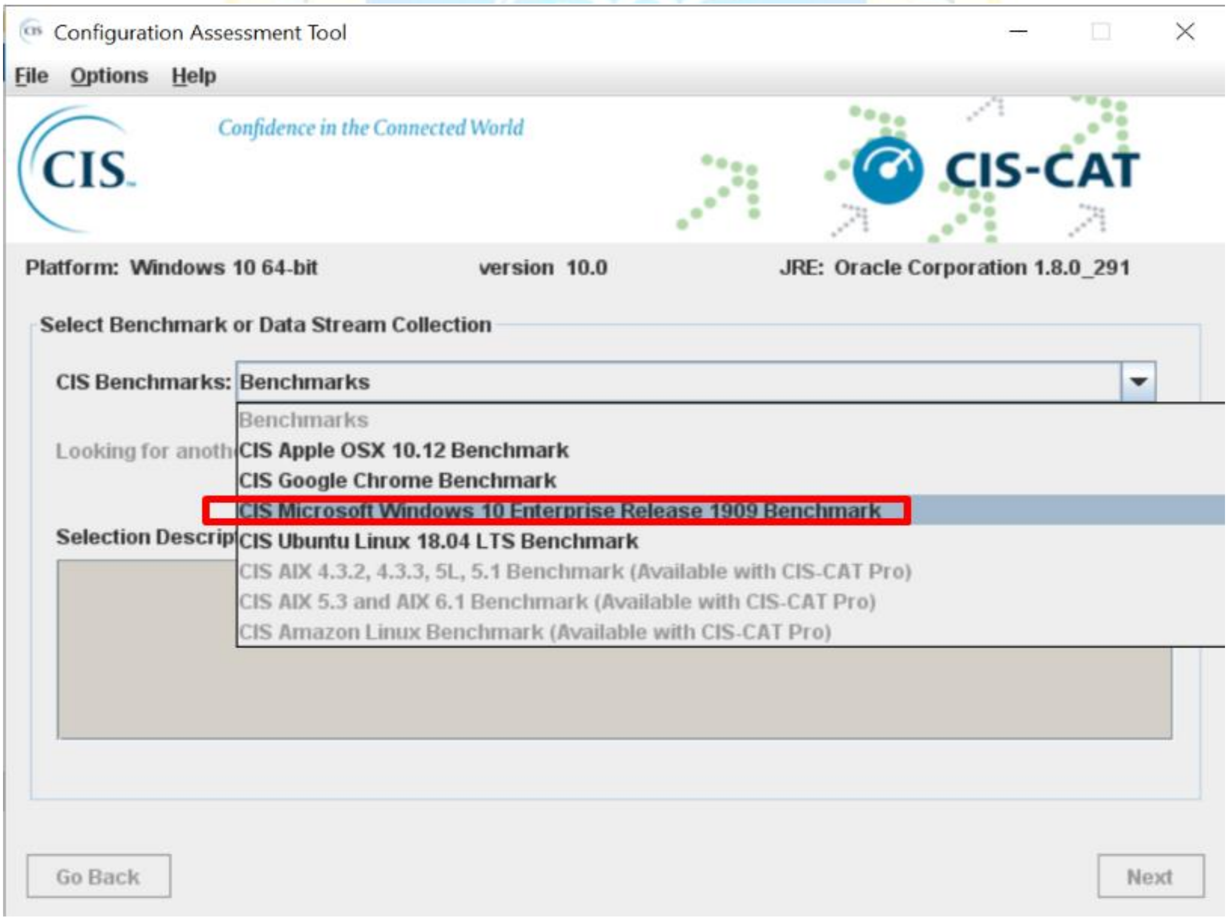
Select Benchmark or Data Stream Collection

CIS Benchmarks: Benchmarks

Looking for another benchmark?

Selection Description:

Select the CIS Microsoft Windows 10 Enterprise Release 1909 Benchmark from the dropdown.


Configuration Assessment Tool
File
Options
Help
CIS
Confidence in the Connected World
CIS-CAT
Go Back
Next

Platform: Windows 10 64-bit version 10.0 JRE: Oracle Corporation 1.8.0_291

Select Benchmark or Data Stream Collection

CIS Benchmarks: Benchmarks

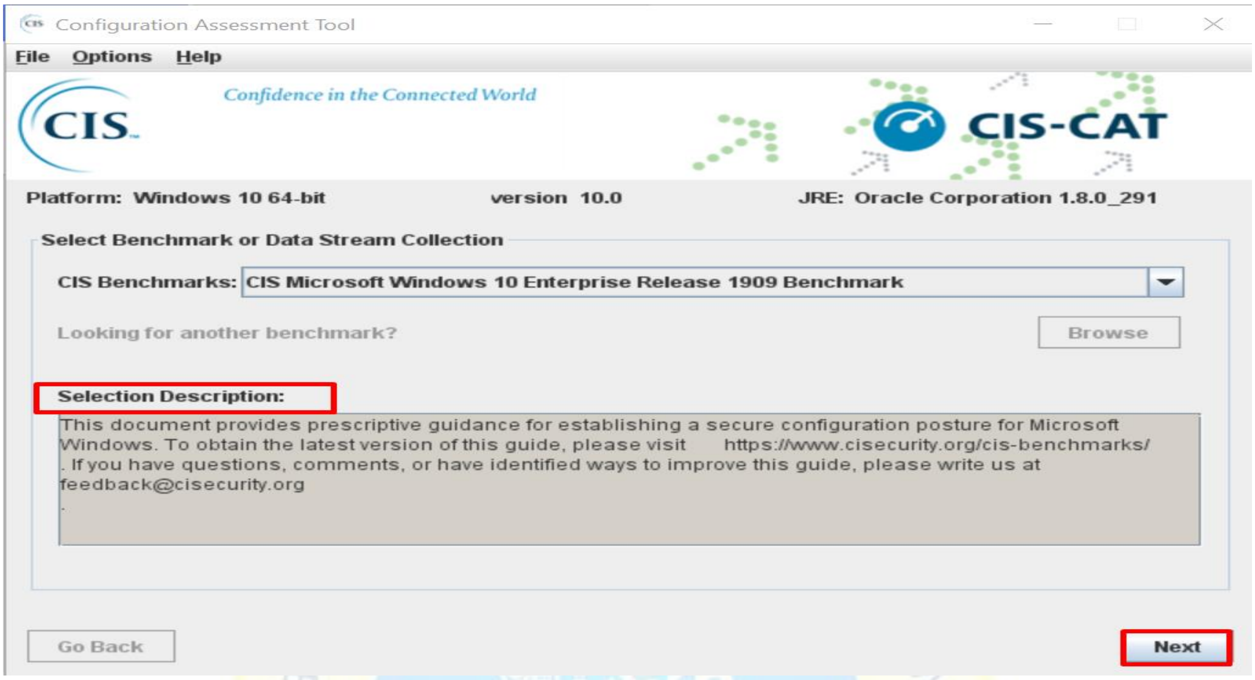
Looking for anoth

Selection Descrip

Benchmarks
CIS Apple OSX 10.12 Benchmark
CIS Google Chrome Benchmark
CIS Microsoft Windows 10 Enterprise Release 1909 Benchmark
CIS Ubuntu Linux 18.04 LTS Benchmark
CIS AIX 4.3.2, 4.3.3, 5L, 5.1 Benchmark (Available with CIS-CAT Pro)
CIS AIX 5.3 and AIX 6.1 Benchmark (Available with CIS-CAT Pro)
CIS Amazon Linux Benchmark (Available with CIS-CAT Pro)

In Selection Description box we can see the description about selected benchmark.

Click on Next.



Configuration Assessment Tool
File Options Help
CIS
Confidence in the Connected World
CIS-CAT

Platform: Windows 10 64-bit   version 10.0   JRE: Oracle Corporation 1.8.0_291

Select Benchmark or Data Stream Collection

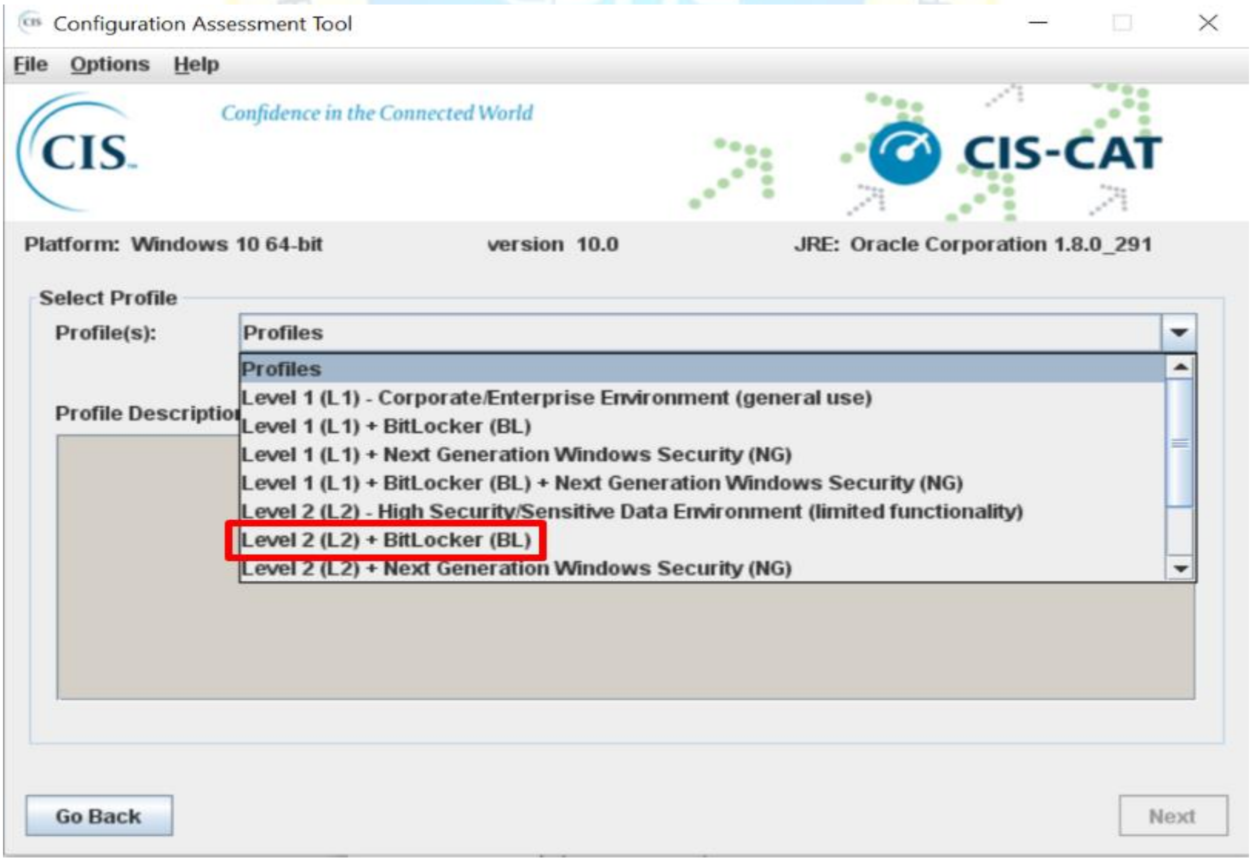
CIS Benchmarks: CIS Microsoft Windows 10 Enterprise Release 1909 Benchmark

Looking for another benchmark?

Selection Description:

This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Windows. To obtain the latest version of this guide, please visit https://www.cisecurity.org/cis-benchmarks/ . If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org
.

From Profiles dropdown select a profile.



Configuration Assessment Tool
File Options Help
CIS
Confidence in the Connected World
CIS-CAT

Platform: Windows 10 64-bit   version 10.0   JRE: Oracle Corporation 1.8.0_291

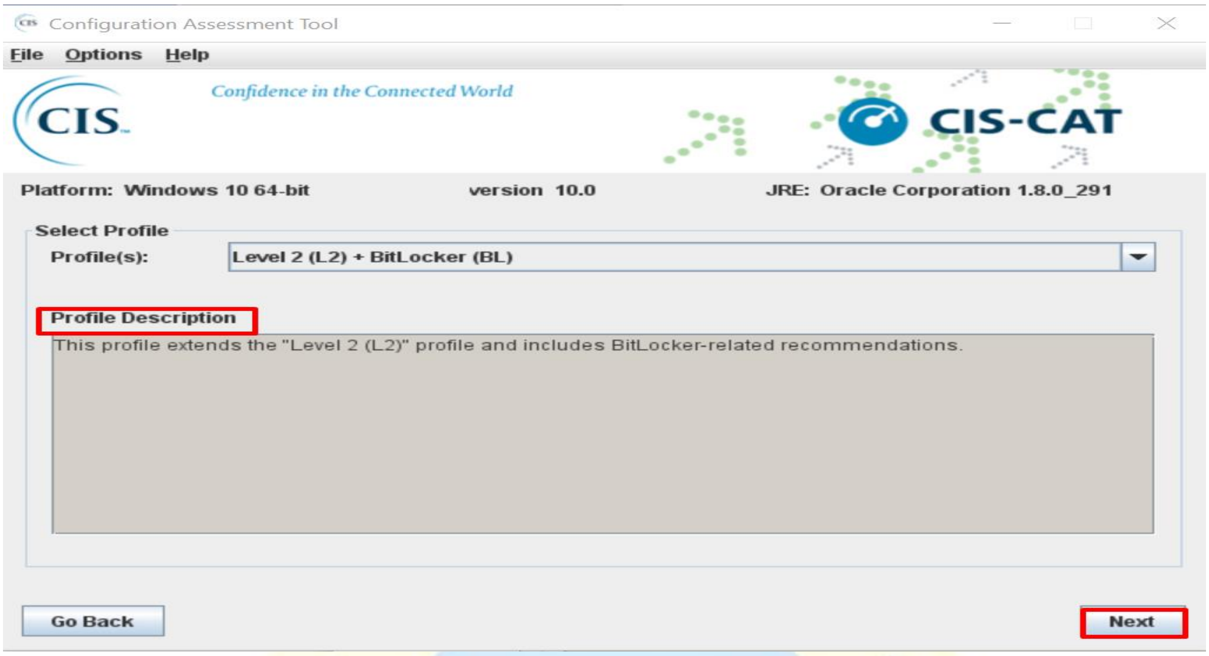
Select Profile

Profile(s): Profiles

- Profiles
- Level 1 (L1) - Corporate/Enterprise Environment (general use)
- Level 1 (L1) + BitLocker (BL)
- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)
- Level 2 (L2) + BitLocker (BL)
- Level 2 (L2) + Next Generation Windows Security (NG)

Profile Descriptio

In profile description box we can see description about the selected profile. Click on Next.



Configuration Assessment Tool

Platform: Windows 10 64-bit version 10.0 JRE: Oracle Corporation 1.8.0_291

Select Profile

Profile(s): Level 2 (L2) + BitLocker (BL)

Profile Description

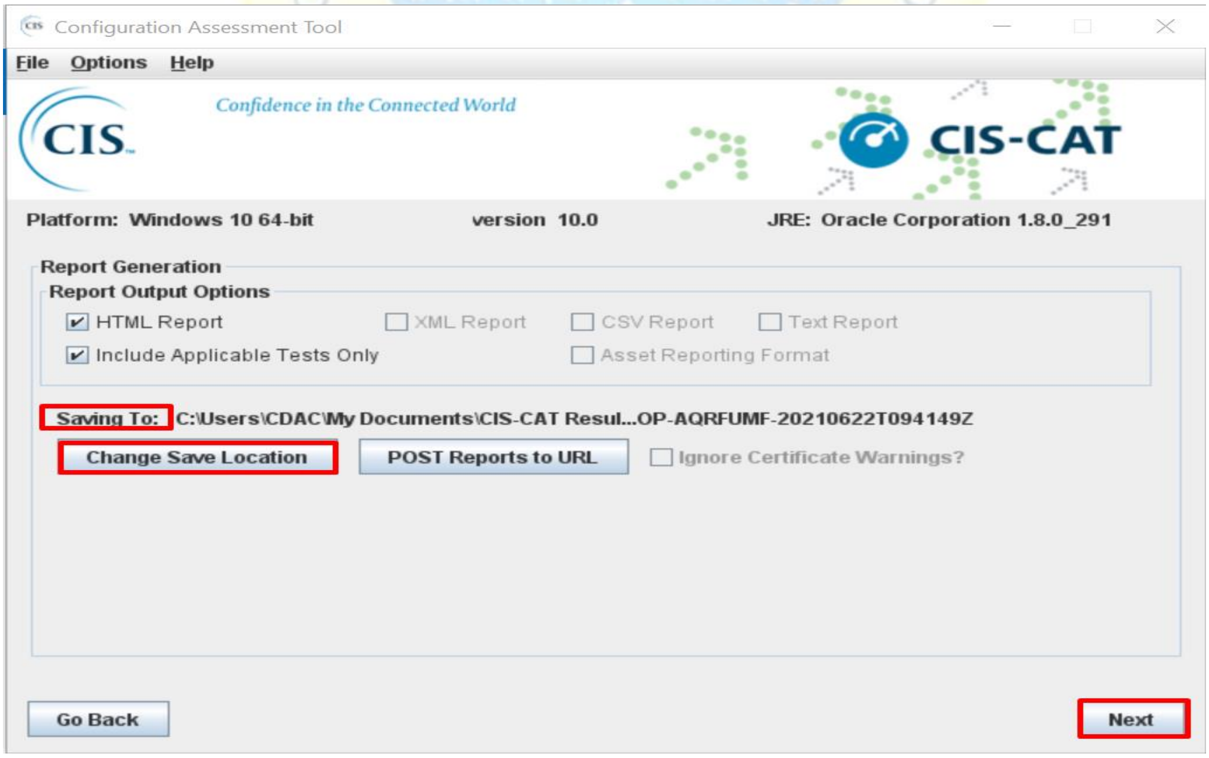
This profile extends the "Level 2 (L2)" profile and includes BitLocker-related recommendations.

In CIS-CAT Lite V3 the report output options will be selected by default.

In Saving To We can see the report generated path.

If we want to change download location then we can change it by clicking Change Save Location.

Click on Next to proceed further.



Configuration Assessment Tool

Platform: Windows 10 64-bit version 10.0 JRE: Oracle Corporation 1.8.0_291

Report Generation

Report Output Options

☑ HTML Report □ XML Report □ CSV Report □ Text Report

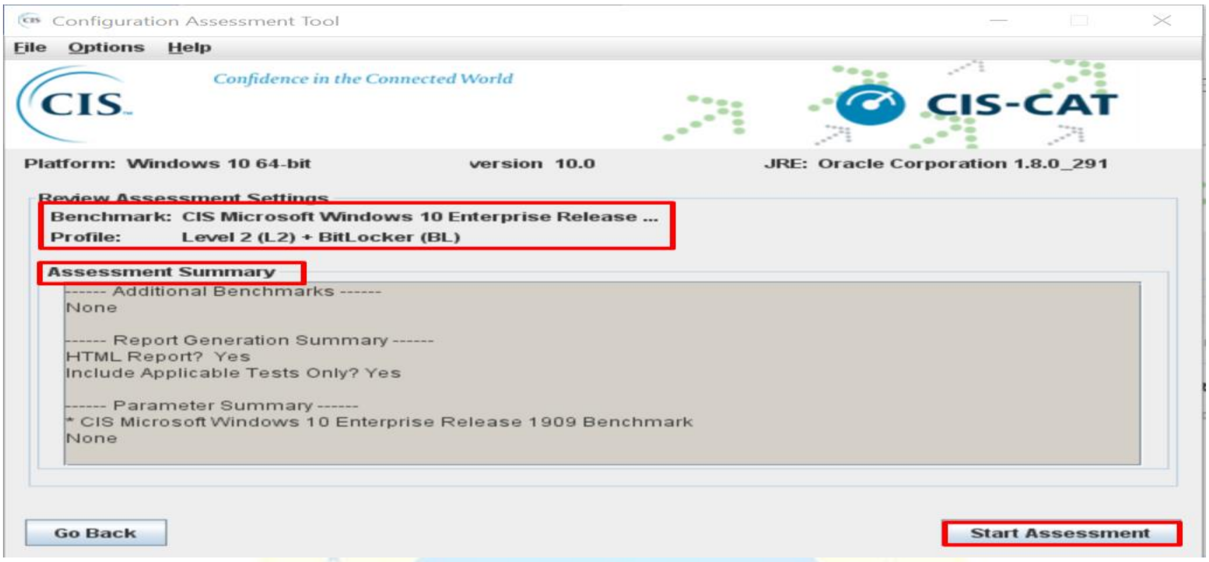
☑ Include Applicable Tests Only □ Asset Reporting Format

Saving To: C:\Users\CDAC\My Documents\CIS-CAT Resul...OP-AQRFUMF-20210622T094149Z

□ Ignore Certificate Warnings?

Here we can see which Benchmark and profile is selected for assessment. And we can see assessment summary also.

Click on Start Assessment.


Configuration Assessment Tool
File Options Help
CIS
Confidence in the Connected World
CIS-CAT

Platform: Windows 10 64-bit   version 10.0   JRE: Oracle Corporation 1.8.0_291

Review Assessment Settings

Benchmark: CIS Microsoft Windows 10 Enterprise Release ...
Profile: Level 2 (L2) + BitLocker (BL)

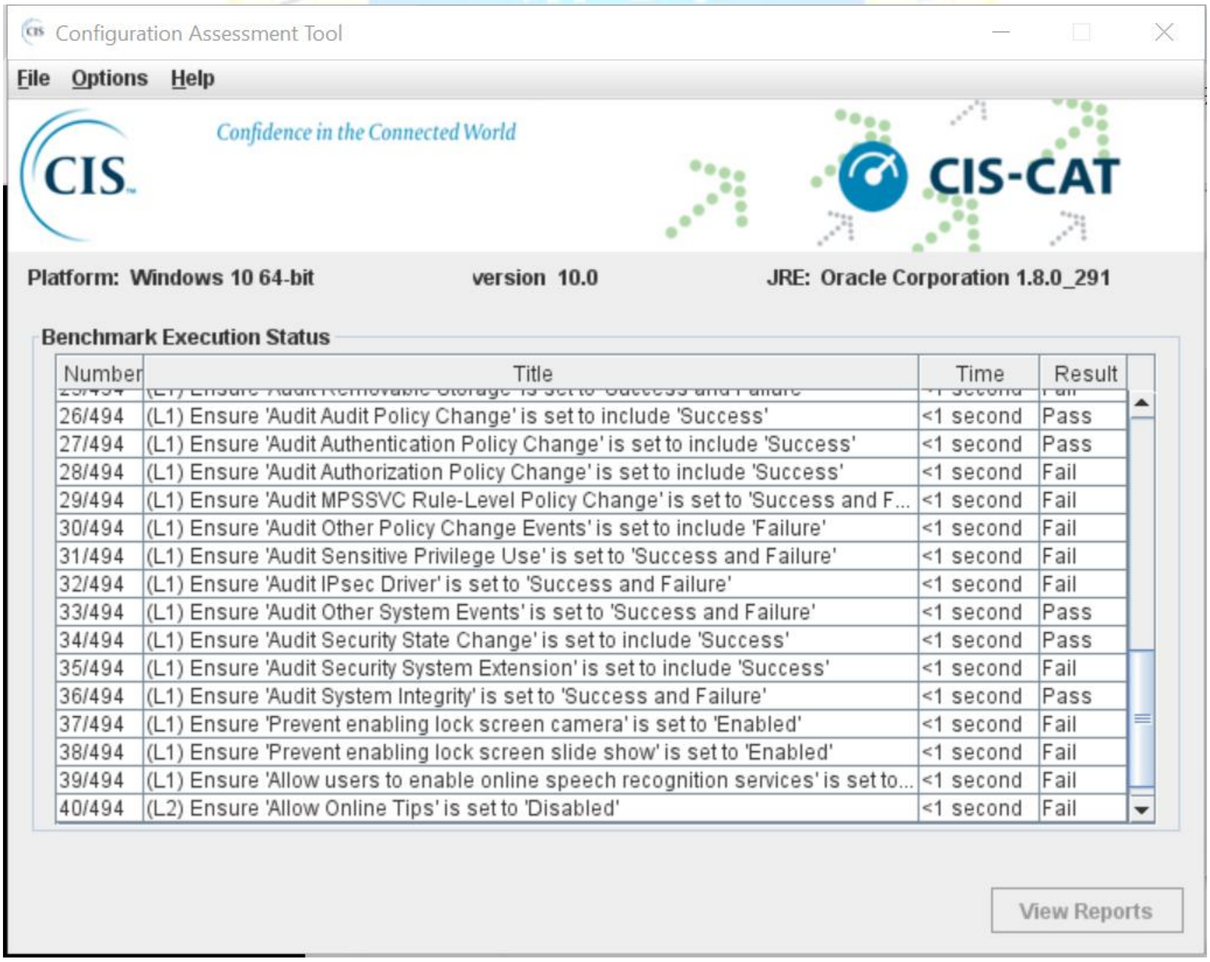
Assessment Summary

```
------ Additional Benchmarks ------
None

------ Report Generation Summary ------
HTML Report?  Yes
Include Applicable Tests Only? Yes

------ Parameter Summary ------
* CIS Microsoft Windows 10 Enterprise Release 1909 Benchmark
None
```

After clicking on start assessment the assessment will be start.

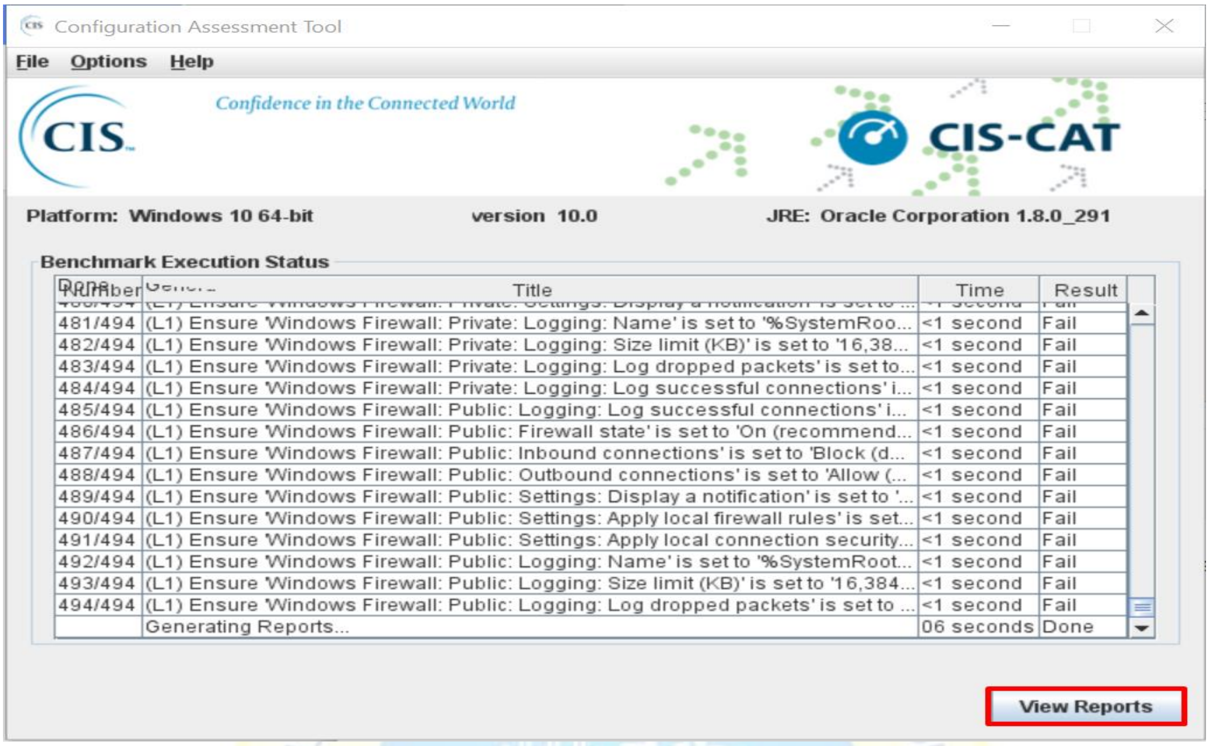

Configuration Assessment Tool
File Options Help
CIS
Confidence in the Connected World
CIS-CAT

Platform: Windows 10 64-bit   version 10.0   JRE: Oracle Corporation 1.8.0_291

Benchmark Execution Status

Number	Title	Time	Result
25/494	(L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure'	<1 second	Fail
26/494	(L1) Ensure 'Audit Audit Policy Change' is set to include 'Success'	<1 second	Pass
27/494	(L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success'	<1 second	Pass
28/494	(L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success'	<1 second	Fail
29/494	(L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and F...	<1 second	Fail
30/494	(L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure'	<1 second	Fail
31/494	(L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	<1 second	Fail
32/494	(L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	<1 second	Fail
33/494	(L1) Ensure 'Audit Other System Events' is set to 'Success and Failure'	<1 second	Pass
34/494	(L1) Ensure 'Audit Security State Change' is set to include 'Success'	<1 second	Pass
35/494	(L1) Ensure 'Audit Security System Extension' is set to include 'Success'	<1 second	Fail
36/494	(L1) Ensure 'Audit System Integrity' is set to 'Success and Failure'	<1 second	Pass
37/494	(L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'	<1 second	Fail
38/494	(L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'	<1 second	Fail
39/494	(L1) Ensure 'Allow users to enable online speech recognition services' is set to...	<1 second	Fail
40/494	(L2) Ensure 'Allow Online Tips' is set to 'Disabled'	<1 second	Fail

Once assessment is completed then click on View Reports.


Configuration Assessment Tool
File Options Help
CIS
Confidence in the Connected World
CIS-CAT
View Reports

Platform: Windows 10 64-bit version 10.0 JRE: Oracle Corporation 1.8.0_291

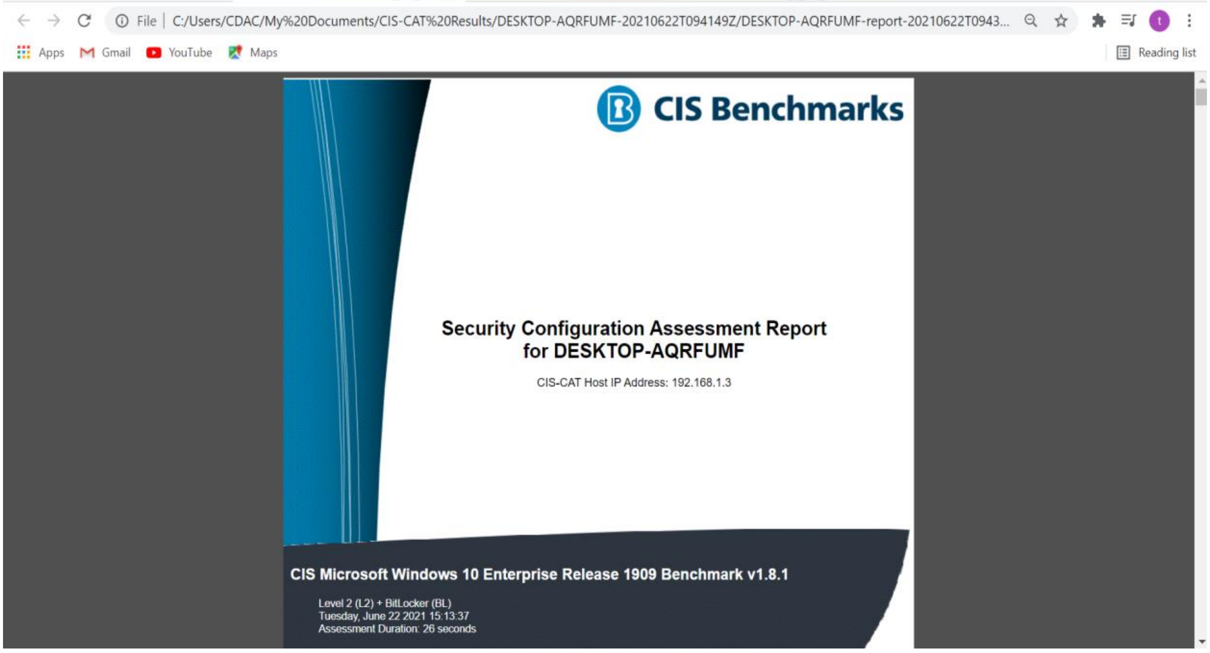
Benchmark Execution Status

Number	Title	Time	Result
481/494	(L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoo...	<1 second	Fail
482/494	(L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,38...	<1 second	Fail
483/494	(L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to...	<1 second	Fail
484/494	(L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' i...	<1 second	Fail
485/494	(L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' i...	<1 second	Fail
486/494	(L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommend...	<1 second	Fail
487/494	(L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (d...	<1 second	Fail
488/494	(L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (...	<1 second	Fail
489/494	(L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to '...	<1 second	Fail
490/494	(L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set...	<1 second	Fail
491/494	(L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security...	<1 second	Fail
492/494	(L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot...	<1 second	Fail
493/494	(L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384...	<1 second	Fail
494/494	(L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to ...	<1 second	Fail
	Generating Reports...	06 seconds	Done

3. CIS-CAT report

The generated report will be open in browser.

This is the compliance report generated by CIS-CAT Lite tool.



File | C:/Users/CDAC/My%20Documents/CIS-CAT%20Results/DESKTOP-AQRFUMF-20210622T094149Z/DESKTOP-AQRFUMF-report-20210622T0943...

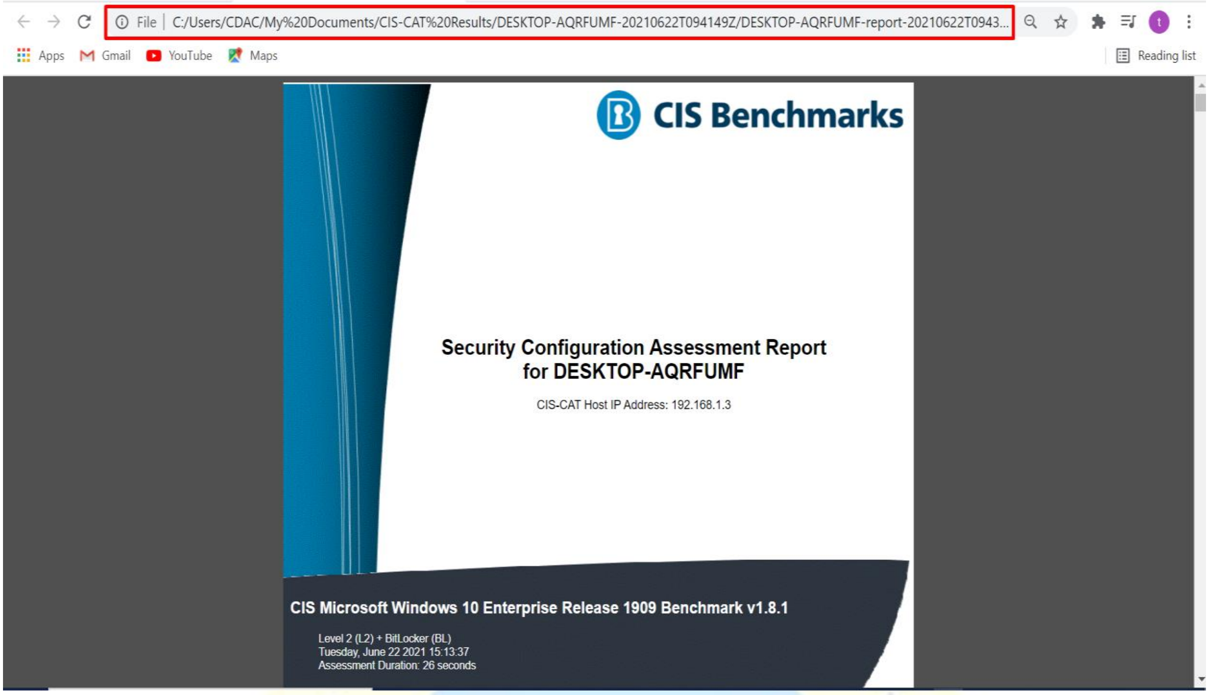
Security Configuration Assessment Report
for DESKTOP-AQRFUMF

CIS-CAT Host IP Address: 192.168.1.3

CIS Microsoft Windows 10 Enterprise Release 1909 Benchmark v1.8.1

Level 2 (L2) + BitLocker (BL)
Tuesday, June 22 2021 15:13:37
Assessment Duration: 26 seconds

As we can see the path of the generated report.


File | C:/Users/CDAC/My%20Documents/CIS-CAT%20Results/DESKTOP-AQRFUMF-20210622T094149Z/DESKTOP-AQRFUMF-report-20210622T0943...
Apps
Gmail
YouTube
Maps
Reading list

CIS Benchmarks

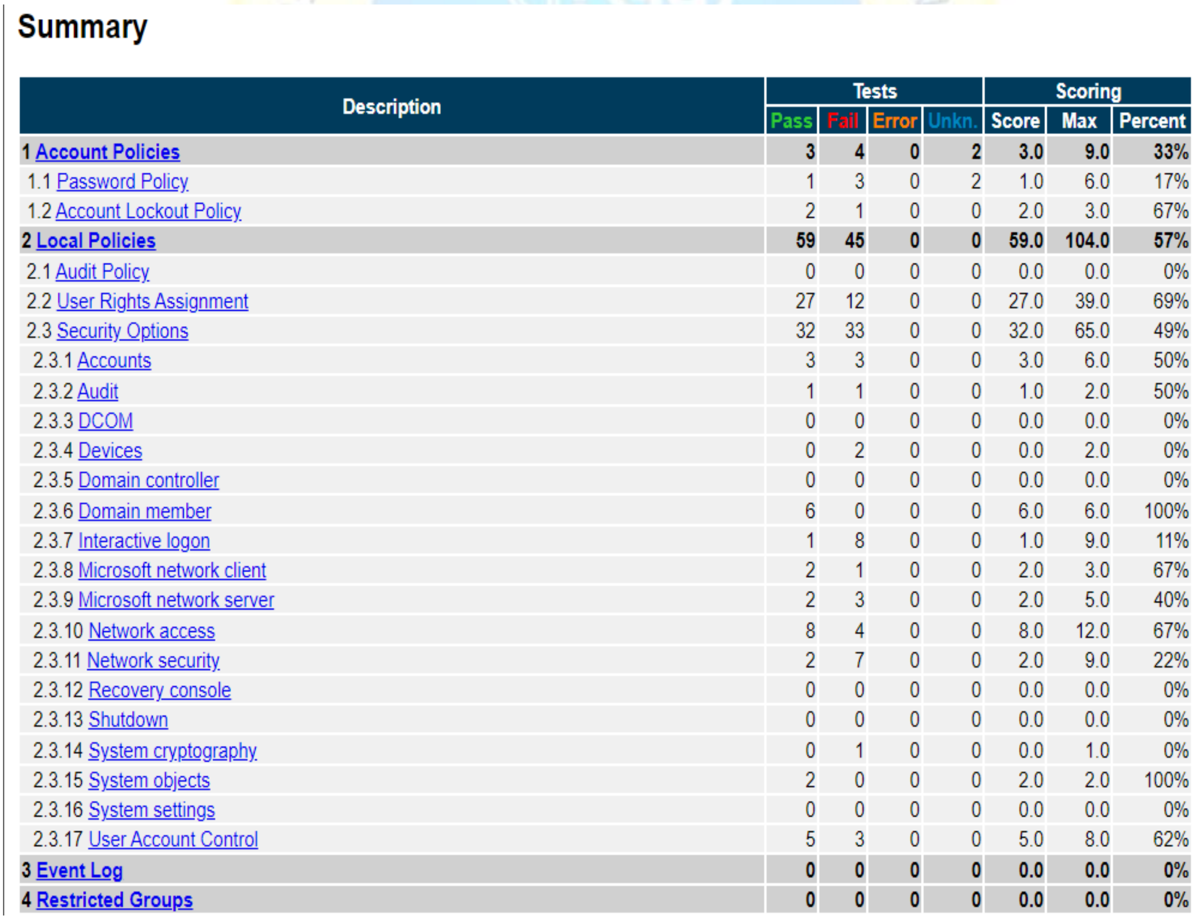
Security Configuration Assessment Report
for DESKTOP-AQRFUMF

CIS-CAT Host IP Address: 192.168.1.3

CIS Microsoft Windows 10 Enterprise Release 1909 Benchmark v1.8.1

Level 2 (L2) + BitLocker (BL)
Tuesday, June 22 2021 15:13:37
Assessment Duration: 26 seconds

In summary section we can see Description, Tests and scoring.

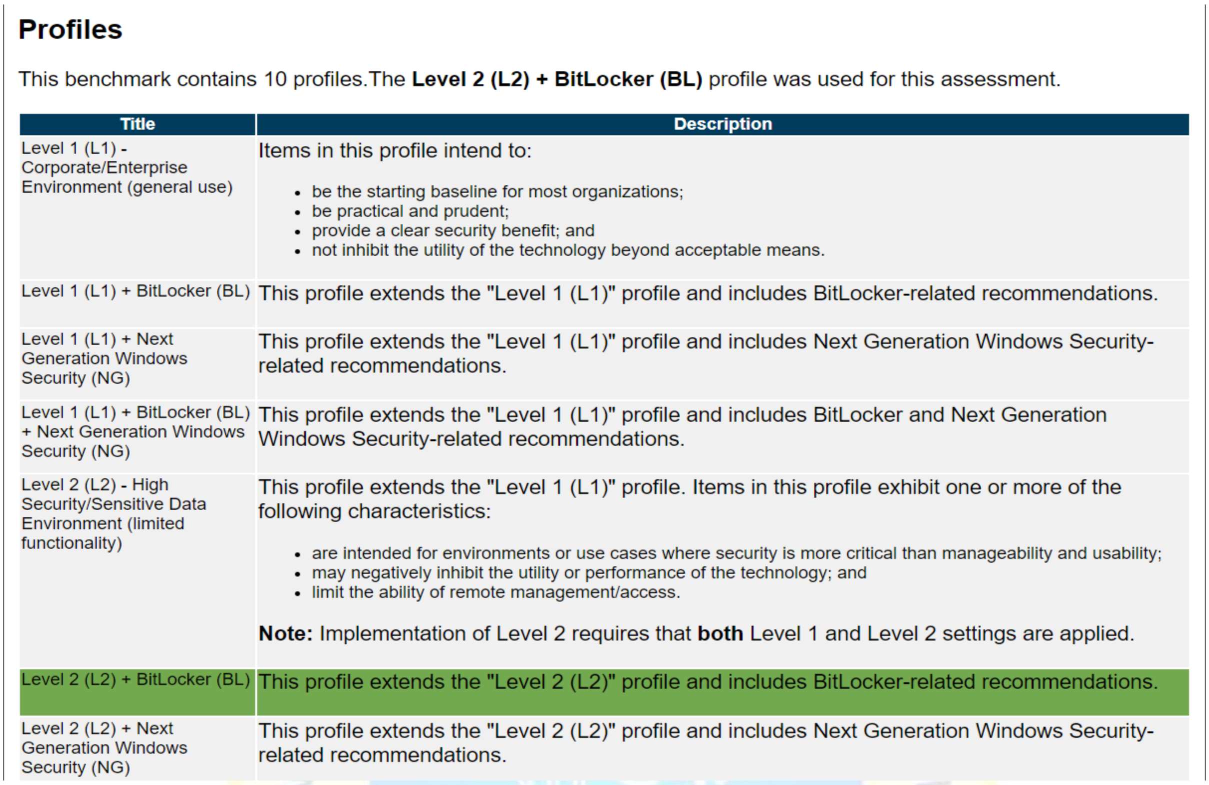


Summary

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
1 Account Policies	**3**	**4**	**0**	**2**	**3.0**	**9.0**	**33%**
1.1 Password Policy	1	3	0	2	1.0	6.0	17%
1.2 Account Lockout Policy	2	1	0	0	2.0	3.0	67%
2 Local Policies	**59**	**45**	**0**	**0**	**59.0**	**104.0**	**57%**
2.1 Audit Policy	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	27	12	0	0	27.0	39.0	69%
2.3 Security Options	32	33	0	0	32.0	65.0	49%
2.3.1 Accounts	3	3	0	0	3.0	6.0	50%
2.3.2 Audit	1	1	0	0	1.0	2.0	50%
2.3.3 DCOM	0	0	0	0	0.0	0.0	0%
2.3.4 Devices	0	2	0	0	0.0	2.0	0%
2.3.5 Domain controller	0	0	0	0	0.0	0.0	0%
2.3.6 Domain member	6	0	0	0	6.0	6.0	100%
2.3.7 Interactive logon	1	8	0	0	1.0	9.0	11%
2.3.8 Microsoft network client	2	1	0	0	2.0	3.0	67%
2.3.9 Microsoft network server	2	3	0	0	2.0	5.0	40%
2.3.10 Network access	8	4	0	0	8.0	12.0	67%
2.3.11 Network security	2	7	0	0	2.0	9.0	22%
2.3.12 Recovery console	0	0	0	0	0.0	0.0	0%
2.3.13 Shutdown	0	0	0	0	0.0	0.0	0%
2.3.14 System cryptography	0	1	0	0	0.0	1.0	0%
2.3.15 System objects	2	0	0	0	2.0	2.0	100%
2.3.16 System settings	0	0	0	0	0.0	0.0	0%
2.3.17 User Account Control	5	3	0	0	5.0	8.0	62%
3 Event Log	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
4 Restricted Groups	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**

Here in profile section we can see the profiles and description about it.

The selected profile will be highlighted as shown in screenshot below.

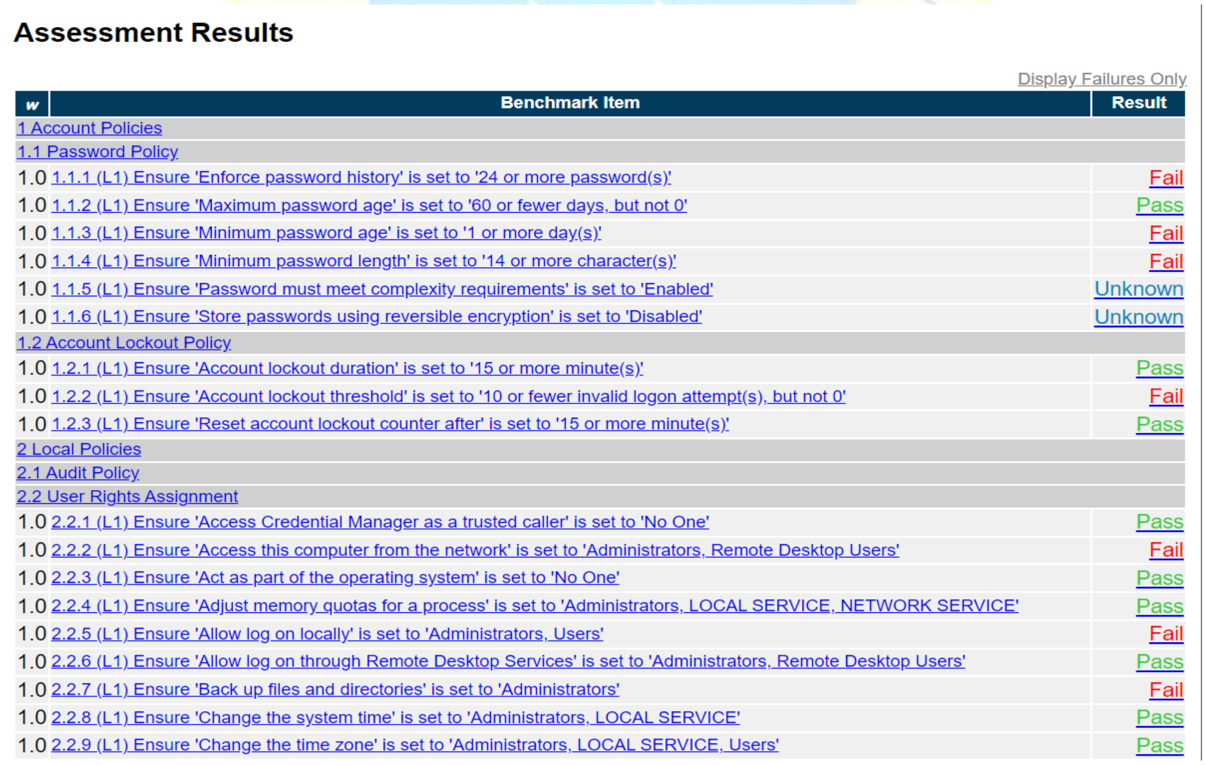


Profiles

This benchmark contains 10 profiles.The **Level 2 (L2) + BitLocker (BL)** profile was used for this assessment.

Title	Description
Level 1 (L1) - Corporate/Enterprise Environment (general use)	Items in this profile intend to: • be the starting baseline for most organizations; • be practical and prudent; • provide a clear security benefit; and • not inhibit the utility of the technology beyond acceptable means.
Level 1 (L1) + BitLocker (BL)	This profile extends the "Level 1 (L1)" profile and includes BitLocker-related recommendations.
Level 1 (L1) + Next Generation Windows Security (NG)	This profile extends the "Level 1 (L1)" profile and includes Next Generation Windows Security-related recommendations.
Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)	This profile extends the "Level 1 (L1)" profile and includes BitLocker and Next Generation Windows Security-related recommendations.
Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)	This profile extends the "Level 1 (L1)" profile. Items in this profile exhibit one or more of the following characteristics: • are intended for environments or use cases where security is more critical than manageability and usability; • may negatively inhibit the utility or performance of the technology; and • limit the ability of remote management/access. **Note:** Implementation of Level 2 requires that **both** Level 1 and Level 2 settings are applied.
Level 2 (L2) + BitLocker (BL)	This profile extends the "Level 2 (L2)" profile and includes BitLocker-related recommendations.
Level 2 (L2) + Next Generation Windows Security (NG)	This profile extends the "Level 2 (L2)" profile and includes Next Generation Windows Security-related recommendations.

In Assessment Results section we can see the the Benchmark Item which are pass or fail.

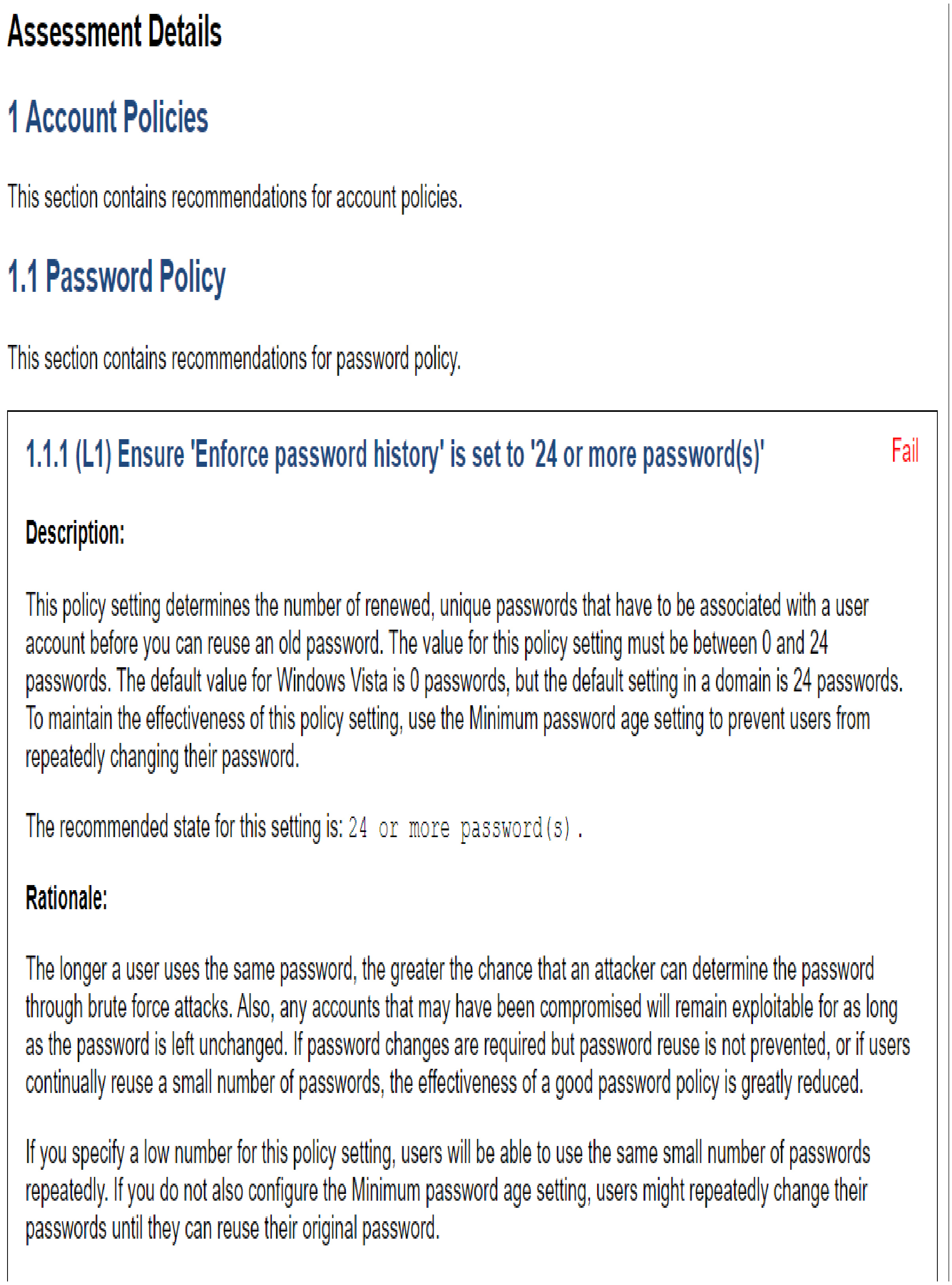


Assessment Results

Display Failures Only

w	Benchmark Item	Result
1 Account Policies		
1.1 Password Policy		
1.0	1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	Fail
1.0	1.1.2 (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'	Pass
1.0	1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	Fail
1.0	1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	Fail
1.0	1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'	Unknown
1.0	1.1.6 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'	Unknown
1.2 Account Lockout Policy		
1.0	1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'	Pass
1.0	1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'	Fail
1.0	1.2.3 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'	Pass
2 Local Policies		
2.1 Audit Policy		
2.2 User Rights Assignment		
1.0	2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'	Pass
1.0	2.2.2 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'	Fail
1.0	2.2.3 (L1) Ensure 'Act as part of the operating system' is set to 'No One'	Pass
1.0	2.2.4 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	Pass
1.0	2.2.5 (L1) Ensure 'Allow log on locally' is set to 'Administrators, Users'	Fail
1.0	2.2.6 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'	Pass
1.0	2.2.7 (L1) Ensure 'Back up files and directories' is set to 'Administrators'	Fail
1.0	2.2.8 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'	Pass
1.0	2.2.9 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users'	Pass

In Assessment Details section we will get all the detail information about the finding. Like Finding number, name, description, rationale, remediation, impact, assessment and references.



Assessment Details

1 Account Policies

This section contains recommendations for account policies.

1.1 Password Policy

This section contains recommendations for password policy.

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'

Fail

Description:

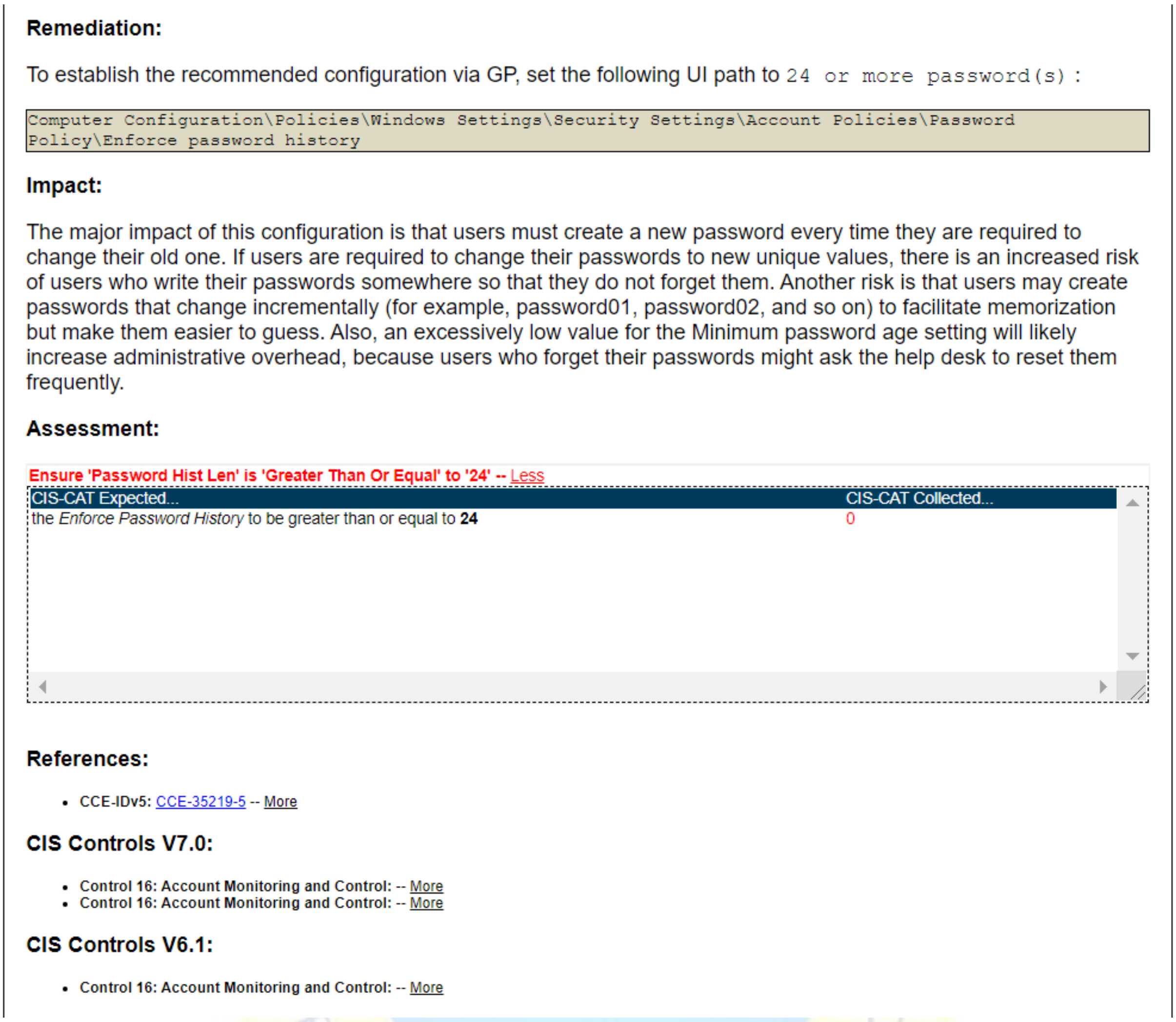
This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password.

The recommended state for this setting is: `24 or more password(s)`.

Rationale:

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.

If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.



Remediation:

To establish the recommended configuration via GP, set the following UI path to `24 or more password(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password
Policy\Enforce password history
```

Impact:

The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

Assessment:

Ensure 'Password Hist Len' is 'Greater Than Or Equal' to '24' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the *Enforce Password History* to be greater than or equal to **24**	0

References:

- **CCE-IDv5:** CCE-35219-5 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More
- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

5. References

- https://www.cisecurity.org/