

QUALYS DEMO - PART 3

Monitoring Profile CreationTurn help tips: On | Off Launch help

Step 1 of 3

- Hosts** ✓
- Ruleset
- Notifications

Configure a profile for continuous monitoring of your hosts.

Profile for Continuous Monitoring (*) REQUIRED FIELDS

Title*

Choose Target Hosts

Tell us which hosts (IP addresses) you would like to monitor.

☐ Select Tags ☒ Select IPs/Ranges

IPs/Ranges

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

PROFILE CREATION

QUALYS DEMO - PART 3

Monitoring Profile CreationTurn help tips: On | Off Launch help

Step 2 of 3

- 1 Hosts
- 2 Ruleset
- 3 Notifications

Choose a set of alert rules to be used for this profile.

Choose Ruleset (*) REQUIRED FIELDS

Your ruleset tells us the events you would like to be alerted on. For example: new host found, host changed, SSL certificate expired, vulnerability detected and more.

Alert Ruleset*

WEBSITE CHANGES

▼

Create New

WEBSITE CHANGES [Edit](#)

Description:
DETECT CHANGES TO WEBSITE

Cancel

Previous

Continue

CHOOSE RULESET

QUALYS DEMO - PART 3

Monitoring Profile CreationTurn help tips: On | Off Launch help

Step 3 of 3

- 1 Hosts ✓
- 2 Ruleset ✓
- 3 Notifications ✓

You have the option to set up alert notifications for you and other users.

Frequency (*) REQUIRED FIELDS

Tell us how often you want to receive notifications.

Send email alerts

Users

Tell us who should receive alerts. Select from your distribution groups.

Distribution Groups

[Remove All](#)

TECHNICAL (1 email)

[View](#) | [Remove](#)

[Cancel](#)

[Previous](#) [Finish](#)

NOTIFICATIONS

QUALYS DEMO - PART 3

Continuous Monitoring ▾

Alerts Configuration

Configuration Monitoring Profiles Rulesets License Details

Search...

Actions (0) ▾ New Profile

☐	Title	Ruleset	Notifications	Created by
☐	☒ WEBSITE	WEBSITE CHANGES	daily	detat-nm1

MONITORING PROFILE ACTIVE

QUALYS DEMO - PART 3

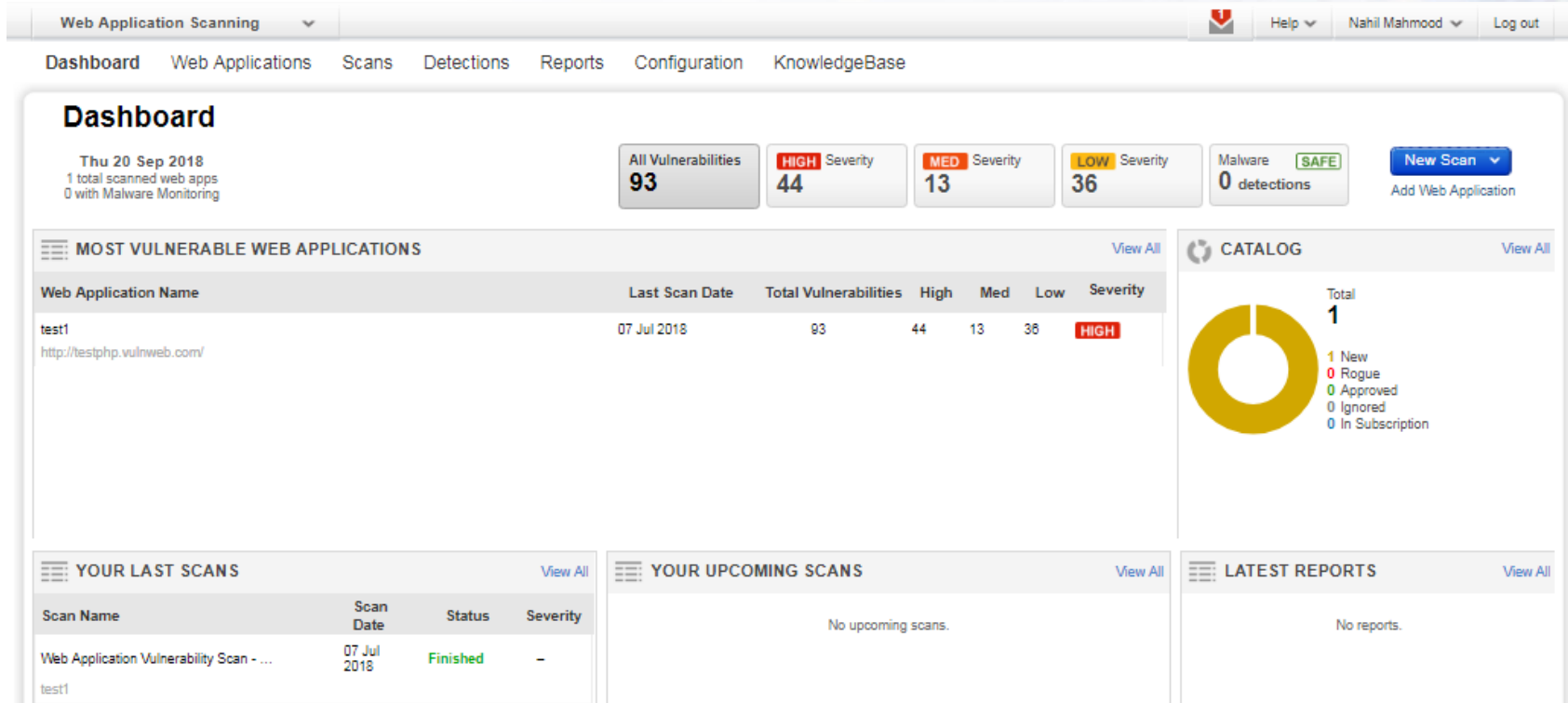
- Qualys Continuous Monitoring is very useful for watching critical changes that may impact security

END

QUALYS WEB APPLICATION SCANNING

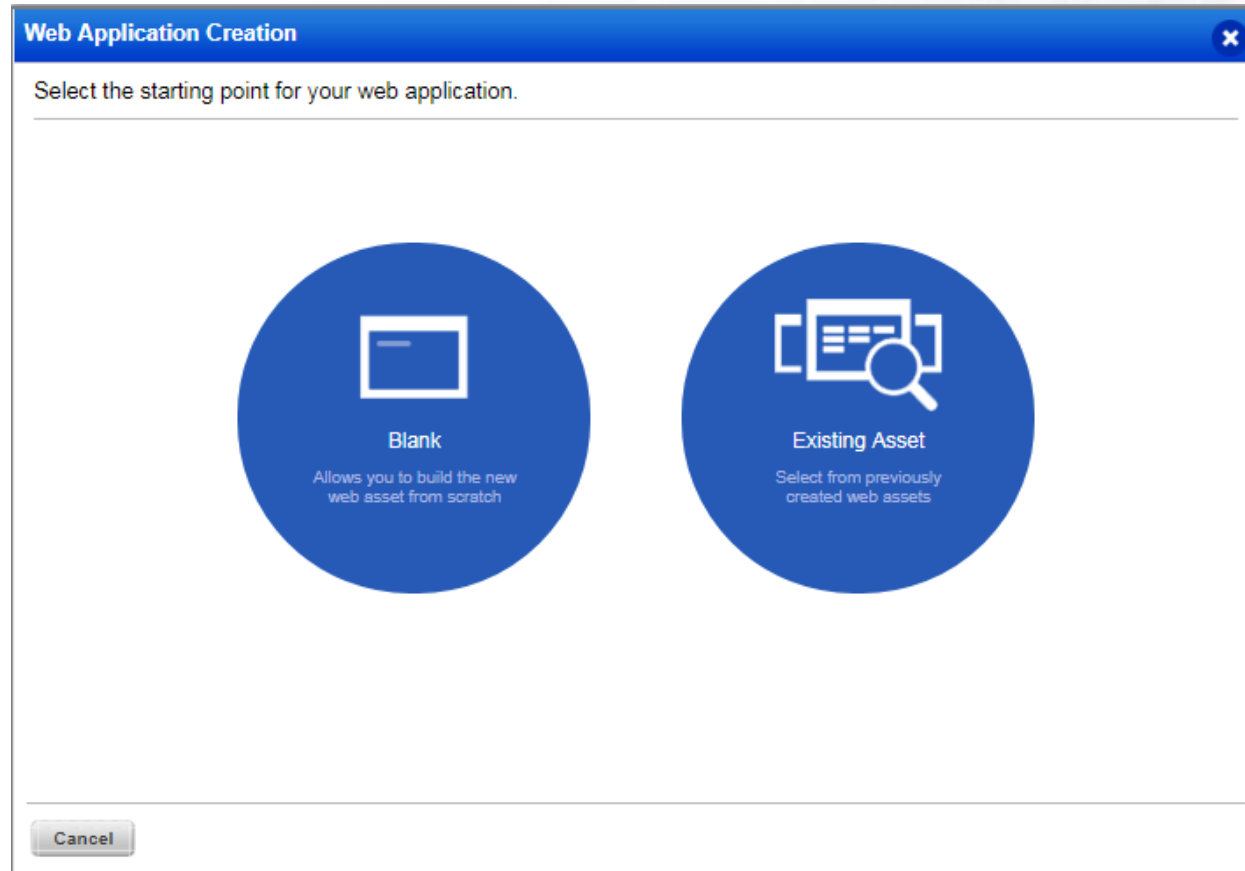
- Lets have a look at Qualys Web Application Scanning

QUALYS WEB APPLICATION SCANNING



DASHBOARD

QUALYS WEB APPLICATION SCANNING



CREATION – BLANK OR EXISTING ASSET

QUALYS WEB APPLICATION SCANNING

Web Application CreationTurn help tips: On | Off Launch help

Step 1 of 11

- Asset Details** ✓
- Application Details
- Scan Settings
- Crawl Settings
- Redundant Links
- Authentication
- Exclusions
- Advanced Options
- Malware Monitoring
- Comments
- Review And Confirm

Tell us about the asset you want to scan

Definition (*) REQUIRED FIELDS

Let's start with some basic information.

Name*

Target Definition

Web Application URL*

For scanning Swagger-based REST APIs, the Web Application URL should point to the Swagger file. It is your responsibility to verify that you have permission to scan all web applications that you specify as scan targets.

Custom Attributes

Provide attribute information that will help you categorize this web application within your subscription.

Name	Value

Add

Tags

Select tags to apply to the web application

Select | Create | Remove All

Cancel

Continue

ASSET DETAILS

QUALYS WEB APPLICATION SCANNING

Web Application Creation

Turn help

Step 2 of 11

- 1 Asset Details
- 2 Application Details
- 3 Scan Settings
- 4 Crawl Settings
- 5 Redundant Links
- 6 Authentication
- 7 Exclusions

Tell us about the web application you want to scan

Target Definition

Web Application URL

Crawl Scope*

Limit to content located at or below URL subdirectory

Limit at or below URL hostname (www.i' .com)

Limit to content located at or below URL subdirectory

Limit to URL hostname and specified sub-domain

Limit to URL hostname and specified domains

CRAWL SCOPE

QUALYS WEB APPLICATION SCANNING

Web Application CreationTurn help tips: On | Off Launch help

Step 3 of 11

- Asset Details
- Application Details
- Scan Settings**
- Crawl Settings
- Redundant Links
- Authentication
- Exclusions
- Advanced Options
- Malware Monitoring
- Comments
- Review And Confirm

Tell us the scan settings you'd like to use

Default Scan Options(*) REQUIRED FIELDS

Choose the default scan settings for your web application. You can change the defaults for each scan.

Option Profile

WEB SCANNING PROFILE (Default) View Create

Scanner Appliance

Choose the default scanner appliance for your web application. You can change the defaults for each scan

☒ External ☐ Individual ☐ Tags (Scanner pool)

☒ Lock this scanner appliance for this web application.

Duration

Cancel the scan after N hours or at a certain time. By default the scan will run until it completes, or the maximum scan time is reached.

When selecting Cancel After, the scan will cancel after the time period set once it begins running and may not reflect the time the scan was submitted. This may be due to scan queues or scanner availability. To end scan at a precise time, please use the option Cancel At and select the desired time the scan should end regardless of queues, scanner availability or submittal/run time.

Cancel Option

Cancel Scan After 1 hour

Cancel

PreviousContinue

SCAN SETTINGS

QUALYS WEB APPLICATION SCANNING

Web Application CreationTurn help tips: On | Off Launch the

Step 9 of 11

- Asset Details
- Application Details
- Scan Settings
- Crawl Settings
- Redundant Links
- Authentication
- Exclusions
- Advanced Options
- Malware Monitoring**
- Comments
- Review And Confirm

Malware Monitoring

By enabling Malware Monitoring on this web application, you will allow QualysGuard to perform a regular scan for malware on your external web site. The application owner will receive an email notification when malicious software is detected. Note Malware Monitoring is available for external sites only.

Status

☒ Enable Malware Monitoring for this web application

Recurrence

Mode*

Launch Information

Start Date

Time*

Time Zone*

Notification

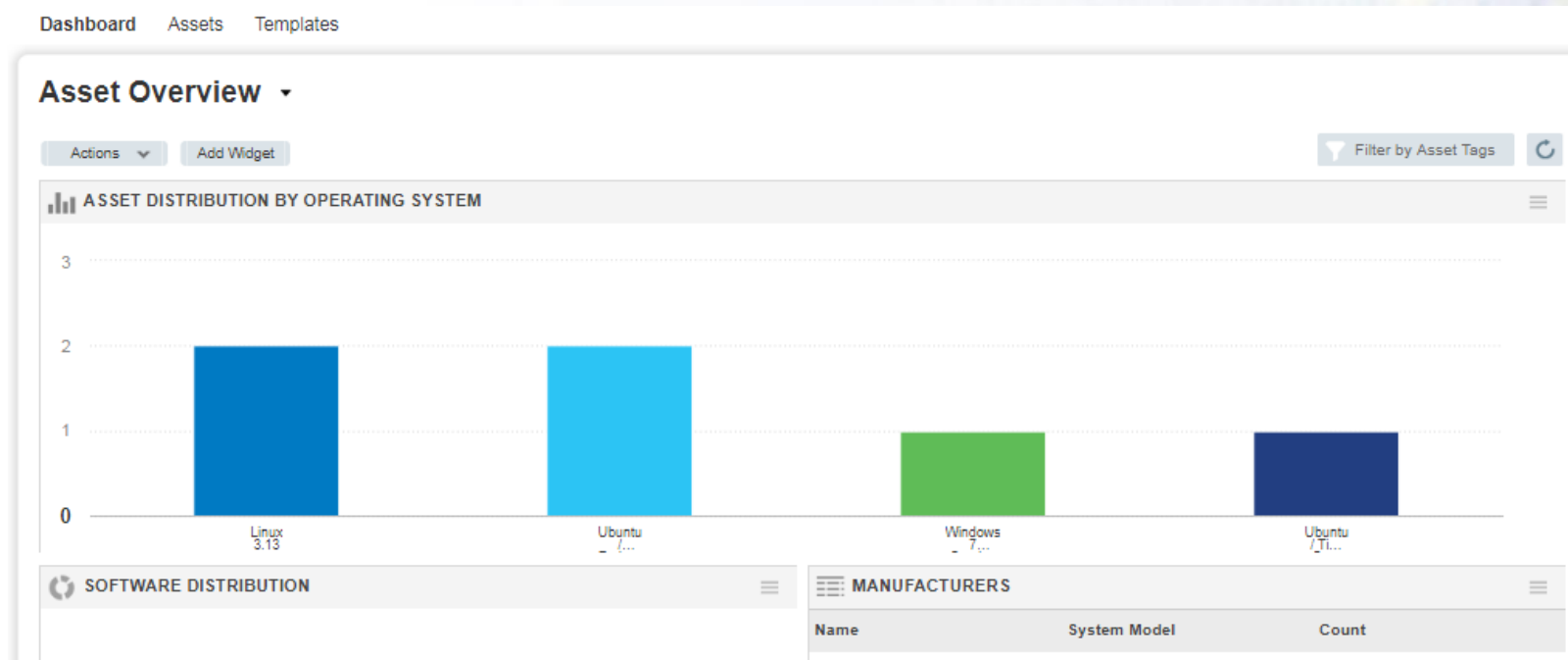
Choose to send notifications about malware scans to the web application owner.

MALWARE MONITORING

ASSET MANAGEMENT THROUGH QUALYS

- Lets have a look at Qualys asset management capabilities

ASSET MANAGEMENT THROUGH QUALYS



QUALYS ASSET OVERVIEW DASHBOARD

ASSET MANAGEMENT THROUGH QUALYS

AssetView							
Assets		Tags					
Saved Searches ▾		create widget save save as undo				Search Actions ▾	
Search...						Search	
Actions (0) ▾		Group assets by... ▾				Assets	
						9	
☐	Asset Name	OS	Modules	Last Logged-In User	Activity	Sources	Tags
☐	WEB	OS Not Identified	WAS	N/A	New 46 minutes ago		
☐	WEB	Not Applicable		N/A	New 46 minutes ago		
☐	firewall	Windows 7 Service Pack 1	VM	—	Scanned September 9, 2018		INACTIVE
☐		Ubuntu / Tiny Core Linux / Linux 2.6.x		—	Scanned August 15, 2018		INACTIVE
☐	www	Linux 3.13		—	Scanned August 15, 2018		INACTIVE
☐	www	Linux 3.13		—	Scanned August 15, 2018		INACTIVE
☐		Ubuntu / Fedora / Tiny Core Linux / Linux 3.x	VM	—	Scanned June 28, 2018		INACTIVE ssh

ASSETS LIST

ASSET MANAGEMENT THROUGH QUALYS

Add a new widget to your dashboard

Templates

Search

All22

Threat13

Assets5

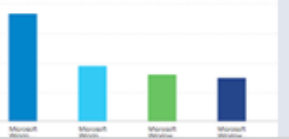
Shared0

Pick a preconfigured widget to add to your dashboard or [create a custom widget](#)

You can also create and customize your own widgets.

Assets with exploits available

A column chart displaying your assets which have an exploit available, broken down by operating system.



Assets with Qualys TOP-10 external vulnerabilities

See how many assets contain vulnerabilities listed amongst Qualys TOP-10 external vulns.

ASSETS WITH QUALYS TOP 10 EXTERNAL VULNERABILITIES
116

Assets with Qualys TOP-10 internal vulnerabilities

See how many assets contain vulnerabilities listed amongst Qualys TOP-10 internal vulns.

ASSETS WITH QUALYS TOP 10 INTERNAL VULNERABILITIES
69

Latest Threat Feeds

View the Latest Threats as provided by the Qualys threat intelligence feed. Get correlation data with your existing assets and measure the threat severity.

LATEST THREATS FROM LIVE FEED

Title	Impa...	Seve...	Publi...
Adobe Flash Player under ne...	101	HIGH	4/5/2018
Latest Adobe 0-day now in An...	101	HIGH	3/28/20...
Oracle patches 0-day in Java	118	HIGH	3/24/20...

Custom Count

ASSETS WITH BINDATMARE

Cancel

Add to Dashboard

ADD NEW ASSET WIDGET TO DASHBOARD

4

ASSET MANAGEMENT THROUGH QUALYS

Create a new dashboard

Templates

Search

All8

Threat2

Assets5

Shared0

Create a new dashboard from an existing template

Start by picking the desired template and click Next to customize it.

Stack Clash

This dashboard provides details on systems that have not been patched for the Stack Clash vulnerability. A widget is also included to track a related privilege escalation vulnerability in sudo. The checks against this vulnerability require authenticated scanning or the Qualys Cloud Agent.



WannaCry and Shadow Brokers

This dashboard provides details on systems that have not been patched for vulnerabilities exploited by EternalBlue, such as WannaCry and other malware. It also contains widgets for tracking exploited systems that have WannaCry or the DoublePulsar backdoor as well as widgets to track other Shadow Brokers vulnerabilities.



Asset Overview

This dashboard provides a general overview of your assets.

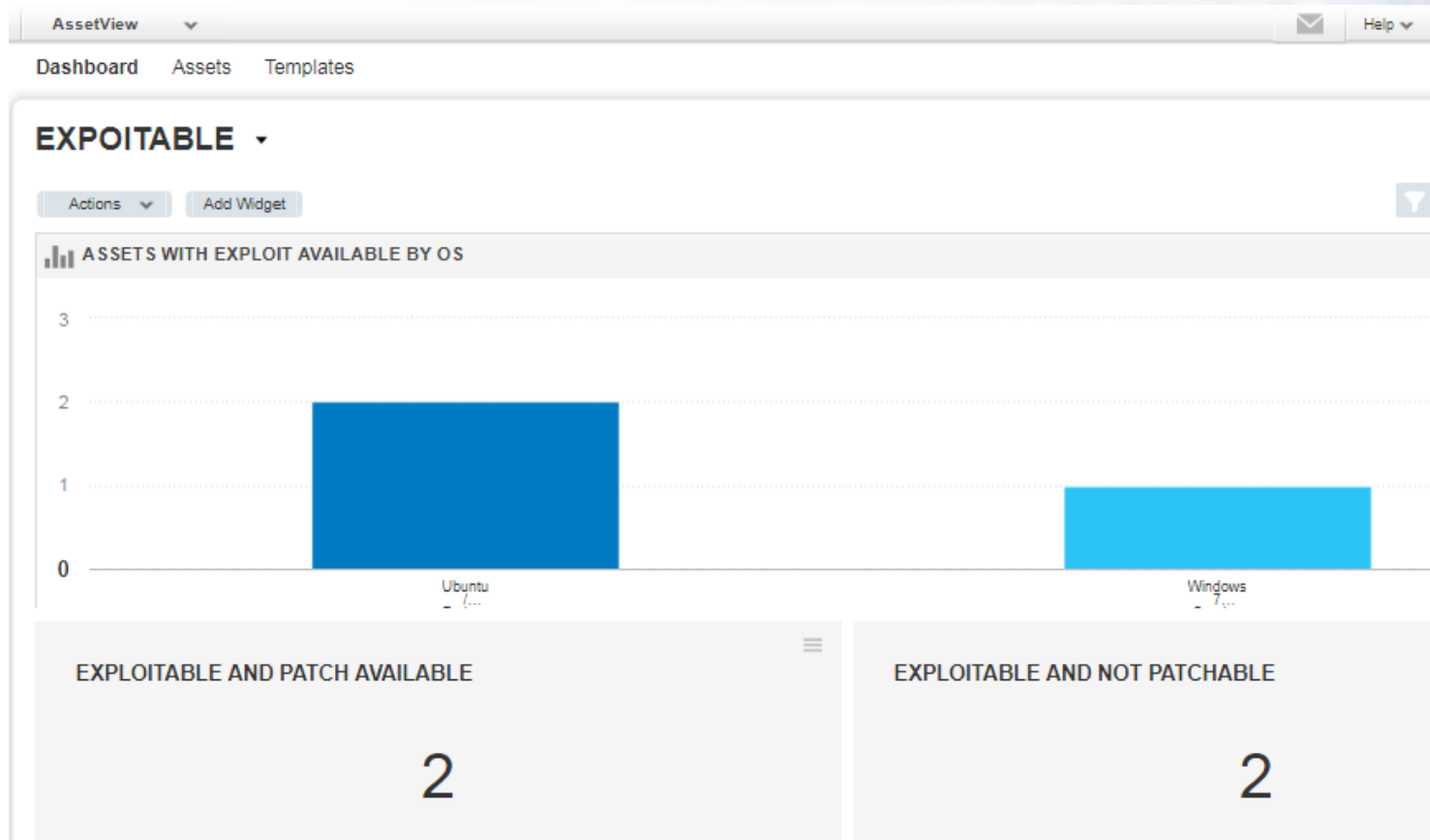


Cancel

Next

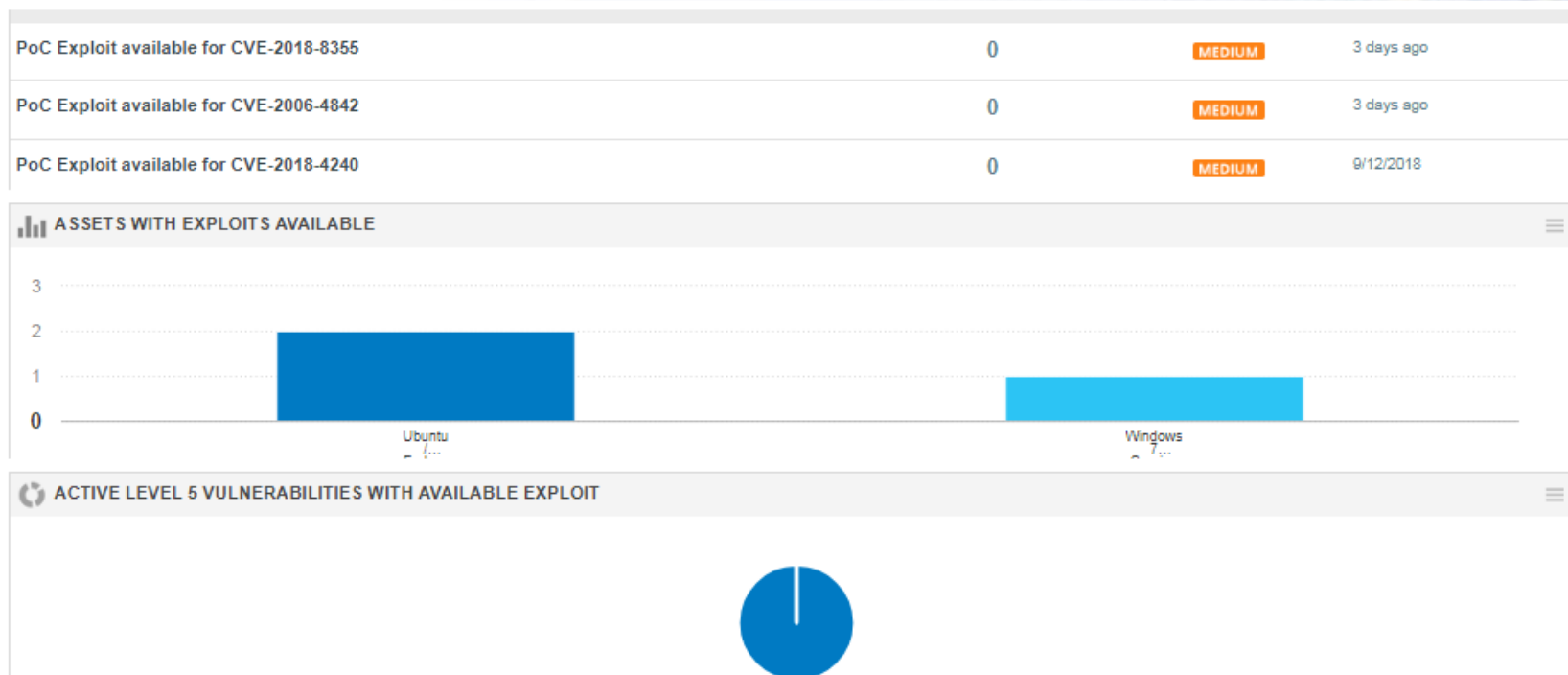
CREATE A NEW DASHBOARD

ASSET MANAGEMENT THROUGH QUALYS



NEW DASHBOARD CREATED

ASSET MANAGEMENT THROUGH QUALYS



ASSETS WITH EXPLOITS AVAILABLE

ASSET MANAGEMENT THROUGH QUALYS

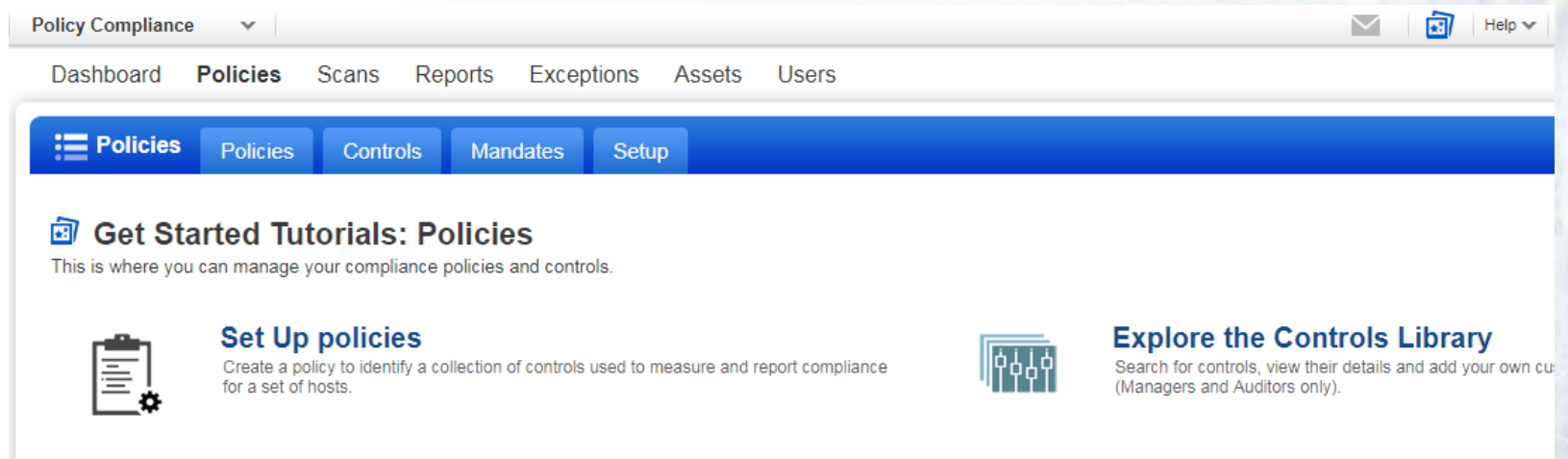
- Qualys allows various reporting and views on assets and their characteristics

END

QUALYS POLICY LIBRARIES

- Lets have a detailed look at Qualys built-in libraries for creating scanning policies
- CIS
- QUALYS
- MANDATE
- DISA
- VENDOR

QUALYS POLICY LIBRARIES



The screenshot displays the Qualys Policy Compliance web interface. At the top, there is a navigation bar with a 'Policy Compliance' dropdown menu, an email icon, a help icon, and a 'Help' dropdown. Below this is a secondary navigation bar with links for 'Dashboard', 'Policies', 'Scans', 'Reports', 'Exceptions', 'Assets', and 'Users'. The main content area features a blue header with tabs for 'Policies', 'Controls', 'Mandates', and 'Setup'. Under the 'Policies' tab, there is a section titled 'Get Started Tutorials: Policies' with the text 'This is where you can manage your compliance policies and controls.' Below this, there are two main cards. The first card, 'Set Up policies', includes a clipboard icon and the text 'Create a policy to identify a collection of controls used to measure and report compliance for a set of hosts.' The second card, 'Explore the Controls Library', includes a server rack icon and the text 'Search for controls, view their details and add your own controls (Managers and Auditors only).'

Policy Compliance

Dashboard **Policies** Scans Reports Exceptions Assets Users

Policies Policies Controls Mandates Setup

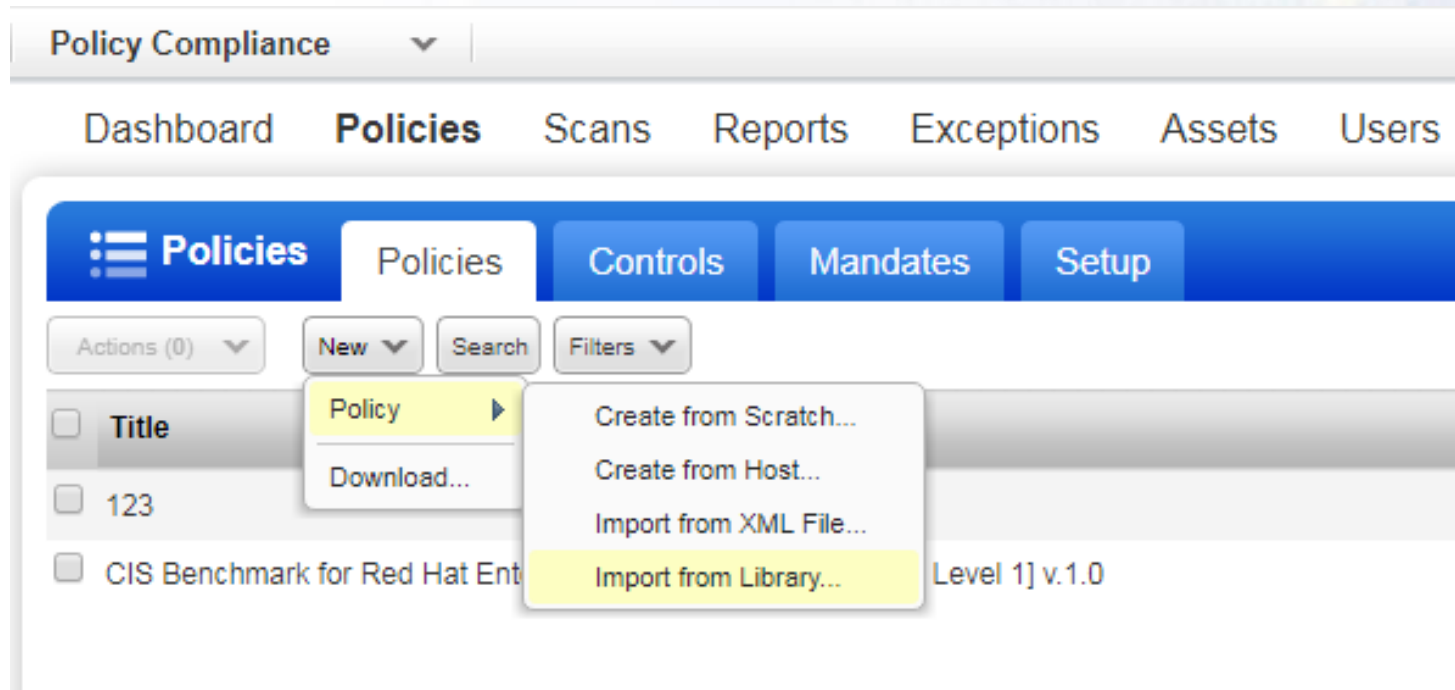
 **Get Started Tutorials: Policies**
This is where you can manage your compliance policies and controls.

 **Set Up policies**
Create a policy to identify a collection of controls used to measure and report compliance for a set of hosts.

 **Explore the Controls Library**
Search for controls, view their details and add your own controls (Managers and Auditors only).

EXPLORE THE CONTROLS LIBRARY

QUALYS POLICY LIBRARIES



CREATE NEW POLICY > IMPORT FROM LIBRARY

QUALYS POLICY LIBRARIES

Create a New Policy

 **Policy from Library:** Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels

- All
- New
- Updated
- CIS
- Qualys
- Mandate
- DISA STIG
- Vendor

Technologies

- ☐ AIX 6.x
- ☐ AIX 7.x
- ☐ Amazon Linux 2 AMI
- ☐ Amazon Linux AMI
- ☐ Apache HTTP Server 2.2.x
- ☐ Apache HTTP Server 2.4.x
- ☐ Apache Tomcat 6.x
- ☐ Apache Tomcat 7.x
- ☐ Apache Tomcat 8.x
- ☐ CentOS 6.x
- ☐ CentOS 7.x
- ☐ Checkpoint Firewall
- ☐ Cisco ASA 8.x
- ☐ Cisco ASA 9.x

Policies (260)

-  CIS Benchmark for SuSE Enterprise Linux Server 10.x v2.0 [Scored]
Version 2.0 02/10/2016 [View Description](#) | [View Policy](#)
-  CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored and Not Scored, Level 1]
Version 2.0 12/01/2017 [View Description](#) | [View Policy](#)
-  CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored and Not Scored, Level 1 and Level 2]
Version 2.0 12/01/2017 [View Description](#) | [View Policy](#)
-  CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored, Level 1 and Level 2]

[Back](#)

Choose Source

[Next](#)

CREATE A NEW POLICY

QUALYS POLICY LIBRARIES

The screenshot displays the Qualys Policy Libraries interface. On the left, there are two columns: 'Labels' and 'Technologies'. The 'Labels' column includes 'All', 'New', 'Updated', 'CIS' (highlighted), 'Qualys', 'Mandate', 'DISA STIG', and 'Vendor'. The 'Technologies' column lists various operating systems and versions, with 'Red Hat Enterprise Linux 7.x' selected. The main area shows a list of policies under the heading 'Policies (3)'. The policies are:

- CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1]
Version 1.0 06/20/2018 [View Description](#) | [View Policy](#)
- CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2]
Version 1.0 06/20/2018 [View Description](#) | [View Policy](#)
- CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 2]
Version 1.0 06/20/2018 [View Description](#) | [View Policy](#)

The entire policy list is enclosed in a blue dashed border. Each policy entry includes a document icon, a lock icon, and a Red Hat logo.

CIS > RED HAT ENT. LINUX 7.X

QUALYS POLICY LIBRARIES

Policy Compliance ▾

Dashboard **Policies** Scans Reports Exceptions Assets Users

Policies Policies Controls Mandates Setup

Actions (1) ▾ New ▾ Search Filters ▾

☐ Title

120

☒ CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2] v.1.0

☐ CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1] v.1.0

CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2] v.1.0

ID: 372295

Policy Title: CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2] v.1.0

Lock Status: Locked at Import

Active: Active

Evaluate Now: No

Created By: Nahil Mahmood (detat-nm1)

POLICIES DASHBOARD

QUALYS POLICY LIBRARIES

Create a New Policy



Policy from Library: Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels	Technologies	Policies (18)
All	☐ MS IIS 10.x	 DISA Security Technical Implementation Guide (STIG) for Internet Explorer 10, V1R15 Version 4.0 07/24/2018 View Description View Policy
New	☐ MS IIS 7.x	
Updated	☐ MS IIS 8.x	
CIS	☐ Red Hat Enterprise Linux 5.x	
Qualys	☐ Red Hat Enterprise Linux 6.x	 DISA Security Technical Implementation Guide (STIG) for Windows 8.1, V1R20 Version 1.0 08/02/2018 View Description View Policy
Mandate	☐ Red Hat Enterprise Linux 7.x	
DISA STIG	☐ Windows 10	 DISA Security Technical Implementation Guide (STIG) for Windows Server 2008 (non-R2) DC, V6R39 Version 1.0 08/02/2018 View Description View Policy
Vendor	☐ Windows 2008 Active Directory	
	☐ Windows 2008 Server	
	☐ Windows 2012 R1/R2 Active Directory	
	☐ Windows 2012 Server	
	☐ Windows 2016 Active Directory	 DISA Security Technical Implementation Guide (STIG) for Windows Server 2012 (non-R2) DC, V6R39

Back

Choose Source

Next

DISA STIG

QUALYS POLICY LIBRARIES

Create a New Policy



Policy from Library: Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels

All

New

Updated

CIS

Qualys

Mandate

DISA STIG

Vendor

Technologies

- ☐ Oracle Enterprise Linux 6.x
- ☐ Oracle Enterprise Linux 7.x
- ☐ Oracle WebLogic Server 11g
- ☐ Oracle WebLogic Server 12c
- ☐ Pivotal tc Server 3.x
- ☐ PostgreSQL 9.x
- ☐ Red Hat Enterprise Linux 6.x
- ☐ Red Hat Enterprise Linux 7.x
- ☒ SAP Adaptive Server Enterprise 16
- ☐ vFabric tc Server 2.9.x
- ☐ Windows 10
- ☐ Windows 2000
- ☐ Windows 2000 Active Directory

Policies (1)



Qualys - Security Configuration and Compliance Policy for SAP Adaptive Server Enterprise 16.0



Version 2.0 07/24/2018 [Hide Description](#) | [View Policy](#)

This policy for 'Security Configuration and Compliance Policy for SAP Adaptive Server Enterprise 16.0' is based on the 'CIS benchmark for Sybase ASE 15.0, v.1.1.0'. The Policy contains Level 1 and Level 2 'Scored' types of checks from the benchmark. The controls within the policy are configured on the basis of values specified by CIS benchmark.

[Back](#)

[Choose Source](#)

[Next](#)

QUALYS SAP ADAPTIVE SERVER ENT 16

QUALYS POLICY LIBRARIES

Create a New Policy

 **Policy from Library:** Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels

- All
- New
- Updated
- CIS
- Qualys
- Mandate
- DISA STIG
- Vendor**

Technologies

- ☐ VMware ESX/ESXi 4.x
- ☐ VMware ESXi 5.x
- ☐ VMware ESXi 6.x
- ☐ Windows 10
- ☐ Windows 2008 Active Directory
- ☐ Windows 2008 Server
- ☐ Windows 2012 Server
- ☐ Windows 2016 Server
- ☐ Windows 7
- ☐ Windows 8
- ☐ Windows 8.1
- ☐ Windows Server 2012 R2

Policies (17)



VMWare vSphere Security Hardening Guide for ESXi 6.x

 Version 3.0 03/01/2018 [View Description](#) | [View Policy](#)

VMware



Microsoft Security Compliance Manager (SCM) Baseline for Windows Server 2012 R2 [Member Server]

 Version 2.0 09/20/2016 [View Description](#) | [View Policy](#)





Microsoft Security Compliance Manager (SCM) Baseline for Windows 8.1

 Version 3.0 09/20/2016 [View Description](#) | [View Policy](#)





Microsoft Security Compliance Manager (SCM) Baseline for Windows 10 version 1511

Back

Choose Source

Next

VENDOR POLICIES

QUALYS POLICY LIBRARIES

- Qualys has a vast number of options for Compliance Scans, and these should be fully explored through the Qualys trial

END

A Look At CIS Security Benchmarks (1)

- Center for Internet Security (CIS)
 - <https://www.cisecurity.org/cis-benchmarks/>
 - Fill out your details and will receive an email with link

A Look At CIS Security Benchmarks (1)



CIS Benchmarks

You now have access to all of our CIS Benchmark PDFs. Feel free to download as many as you like!

If you have any issues accessing the files, please let us know at learn@cisecurity.org.

Looking for a previous version of a CIS Benchmark? See our [archive](#).

Operating Systems

Distribution Independent Linux Linux

CIS Distribution Independent Linux Benchmark v1.0.1

[Download PDF](#)

Microsoft Windows Desktop Microsoft Windows

CIS Microsoft Windows 10 Enterprise Release 1607 Benchmark v1.2.0

[Download PDF](#)

A Look At CIS Security Benchmarks (2)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	107

A Look At CIS Security Benchmarks (1)

#	OPERATING SYSTEMS	TOTAL
1	DISTRIBUTION INDEPENDENT LINUX	1
2	MICROSOFT WINDOWS DESKTOP	5
3	DEBIAN LINUX	2
4	UBUNTU LINUX	3
5	AMAZON LINUX	1
6	CENTOS LINUX	2
7	ORACLE LINUX	2

A Look At CIS Security Benchmarks (1)

#	OPERATING SYSTEMS (CONTD)...	TOTAL
8	REDHAT LINUX	3
9	SUSE LINUX	2
10	APPLE OS (UNIX)	5
11	IBM AIX (UNIX)	1
12	ORACLE SOLARIS (UNIX)	3
13	MS WINDOWS SERVER	6
	TOTAL BENCH MARKS OPERATING SYSTEMS	36

A Look At CIS Security Benchmarks (1)

Microsoft Windows Desktop

Microsoft Windows

CIS Microsoft Windows 10 Enterprise Release 1607 Benchmark v1.2.0

CIS Microsoft Windows 8.1 Workstation Benchmark v2.2.1

CIS Microsoft Windows 7 Workstation Benchmark v3.0.1

CIS Microsoft Windows XP Benchmark v3.1.0

CIS Microsoft Windows 8 Benchmark v1.0.0

A Look At CIS Security Benchmarks (1)

Microsoft Windows Server

Microsoft Windows

CIS Microsoft Windows Server 2016 RTM (Release 1607) Benchmark v1.0.0

CIS Microsoft Windows Server 2008 (non-R2) Benchmark v3.0.1

CIS Microsoft Windows Server 2008 R2 Benchmark v3.0.1

CIS Microsoft Windows Server 2012 R2 Benchmark v2.2.1

CIS Microsoft Windows Server 2012 (non-R2) Benchmark v2.0.1

CIS Microsoft Windows Server 2003 Benchmark v3.1.0

A Look At CIS Security Benchmarks (1)

#	SERVER SOFTWARE	TOTAL
1	MICROSOFT IIS (WEB SERVER)	3
2	VMWARE (VIRTUALIZATION)	2
3	MONGODB (DATABASE SERVER)	3
4	IBM DB2 (DATABASE SERVER)	3
5	BIND (DNS SERVER)	1
6	APACHE TOMCAT (WEB SERVER)	2
7	MICROSOFT SQL SERVER (DB SERVER)	3

A Look At CIS Security Benchmarks (1)

#	SERVER SOFTWARE (CONTD)...	TOTAL
8	APACHE (HTTP SERVER)	2
9	DOCKER (VIRTUALIZATION)	5
10	ORACLE (DATABASE SERVER)	3
11	KUBERNETES (VIRTUALIZATION)	1
12	MIT KERBEROS (AUTHENTICATION)	1
13	ORACLE MySQL (DB SERVER)	4
	TOTAL BENCH MARKS SERVER SOFTWARE	33

A Look At CIS Security Benchmarks (1)

Microsoft SQL Server Database Server

CIS Microsoft SQL Server 2008 R2 Benchmark v1.4.0

CIS Microsoft SQL Server 2012 Benchmark v1.3.0

CIS Microsoft SQL Server 2014 Benchmark v1.2.0

A Look At CIS Security Benchmarks (1)

#	CLOUD PROVIDERS	TOTAL
1	AMAZON WEB SERVICES	2
	TOTAL CLOUD PROVIDERS	2

A Look At CIS Security Benchmarks (1)

- Next module...remaining categories

END

A Look At CIS Security Benchmarks (2)

- Mobile devices, network devices, desktop software, multifunction print devices

A Look At CIS Security Benchmarks (2)

#	MOBILE DEVICES	TOTAL
1	APPLE IOS	5
2	GOOGLE ANDROID	3
	TOTAL BENCH MARKS MOBILE DEVICES	8

A Look At CIS Security Benchmarks (2)

#	NETWORK DEVICES	TOTAL
1	CISCO	4
2	PALO ALTO NETWORKS	2
	TOTAL BENCH MARKS NETWORK DEVICES	6

A Look At CIS Security Benchmarks (2)

#	DESKTOP SOFTWARE	TOTAL
1	MICROSOFT OFFICE	13
2	GOOGLE CHROME (WEB BROWSER)	1
3	MS EXCHANGE SERVER	3
4	MS INTERNET EXPLORER	2
5	MOZILLA FIREFOX	2
	TOTAL BENCH MARKS DESKTOP SOFTWARE	21

A Look At CIS Security Benchmarks (2)

#	MULTIFUNCTION PRINT DEVICES	TOTAL
1	MULTIFUNCTION DEVICE	1
	TOTAL BENCH MARKS MULTIFUNCTION PRINT DEVICES	1

A Look At CIS Security Benchmarks (2)

Apple iOS

CIS Apple iOS 10 Benchmark v2.0.0

CIS Apple iOS 9 Benchmark v1.0.0

CIS Apple iOS 8 Benchmark v1.0.0

CIS Apple iOS 7 Benchmark v1.1.0

CIS Apple iOS 6 Benchmark v1.0.0

A Look At CIS Security Benchmarks (2)

Google Android

CIS Google Android 7 Benchmark v1.0.0

CIS Google Android 4 Benchmark v1.0.0

CIS Google Android 2.3 Benchmark v1.1.0

A Look At CIS Security Benchmarks (2)

Cisco

CIS Cisco Firewall Benchmark v4.0.0

CIS Cisco IOS 12 Benchmark v4.0.0

CIS Cisco IOS 15 Benchmark v4.0.0

CIS Cisco Wireless LAN Controller 7 Benchmark v1.1.0

A Look At CIS Security Benchmarks (2)

Microsoft Office

Productivity Software

CIS Microsoft Office 2016 Benchmark v1.1.0

CIS Microsoft Office PowerPoint 2016 Benchmark v1.0.1

CIS Microsoft Office PowerPoint 2013 Benchmark v1.0.1

CIS Microsoft Office Excel 2016 Benchmark v1.0.1

CIS Microsoft Office Excel 2013 Benchmark v1.0.1

CIS Microsoft Office Access 2016 Benchmark v1.0.1

CIS Microsoft Office Access 2013 Benchmark v1.0.1

A Look At CIS Security Benchmarks (2)

CIS Microsoft Office 2013 Benchmark v1.1.0

CIS Microsoft Office Word 2016 Benchmark v1.1.0

CIS Microsoft Office Word 2013 Benchmark v1.1.0

CIS Microsoft Office Outlook 2016 Benchmark v1.1.0

CIS Microsoft Office Outlook 2013 Benchmark v1.1.0

CIS Microsoft Outlook 2010 Benchmark v1.0.0

A Look At CIS Security Benchmarks (3)

- CIS Benchmarks example (Network Devices)

A Look At CIS Security Benchmarks (3)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	107

CIS Benchmarks

- The CIS Benchmarks are prescriptive **configuration recommendations** for more than **25+ vendor product families**. They represent the **consensus-based effort of cybersecurity experts** globally to help you protect your systems against threats more confidently.

CIS Benchmarks

CIS Benchmarks from the Center of Internet Security (CIS)

- a set of **globally recognized and consensus-driven** best practices to help security practitioners implement and manage their cybersecurity defenses.
- Developed with a **global community of security experts**, the guidelines help organizations **proactively safeguard against emerging risks**.
- Companies implement the CIS Benchmark **guidelines to limit configuration-based security vulnerabilities** in their digital assets.

CIS Benchmarks

When you implement CIS Benchmarks, you can better secure your legacy systems against common and emerging risks by taking steps such as these:

- Disabling unused ports
- Removing unnecessary app permissions
- Limiting administrative privileges

CIS levels

- **Level 1:** Basic easily implementable configurations designed to lower the attack surface without impacting performance.
- **Level 2:** Configuration recommendations that may create system conflicts and are intended to provide “defense in depth” for environments that need enhanced security

Domain Controller& Memeber Server

- A computer with a **server OS and Active Directory installed** is a **Domain Controller**.
- Any other computer with a **server OS or for example with SQL Server installed**, which works as a server and is joined to the domain can be called a **member server**. A member server does not have Active Directory installed.
- If a computer has DHCP or DNS, but not Active Directory, it's a **member server**.

Scored and Unscored

- Each recommendation is either 'scored' or 'not scored'.
- '**Scored**' recommendations are **mandatory** to achieve CIS compliance, and if not met, they lower the total benchmark score.
- Recommendations that are '**not scored**' have **no impact** on the overall score of the benchmark.



[Home](#) > [CIS Benchmarks](#)

CIS Benchmarks List

The CIS Benchmarks are prescriptive configuration recommendations for more than 25+ vendor product families. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.

[ACCESS ALL BENCHMARKS](#) →

Are you new to the CIS Benchmarks? [Learn More](#)

Find the CIS Benchmark you're looking for



STEP 3

Download your CIS Benchmark.

Download the latest version or learn what other resources are available for this CIS Benchmark.

1 2 3 4

[CLOUD PROVIDERS](#) [DESKTOP SOFTWARE](#) [DEVSECOPS TOOLS](#) [MOBILE DEVICES](#) [MULTI FUNCTION PRINT DEVICES](#) [NETWORK DEVICES](#) [OPERATING SYSTEMS](#) [SERVER SOFTWARE](#)

Alibaba Cloud

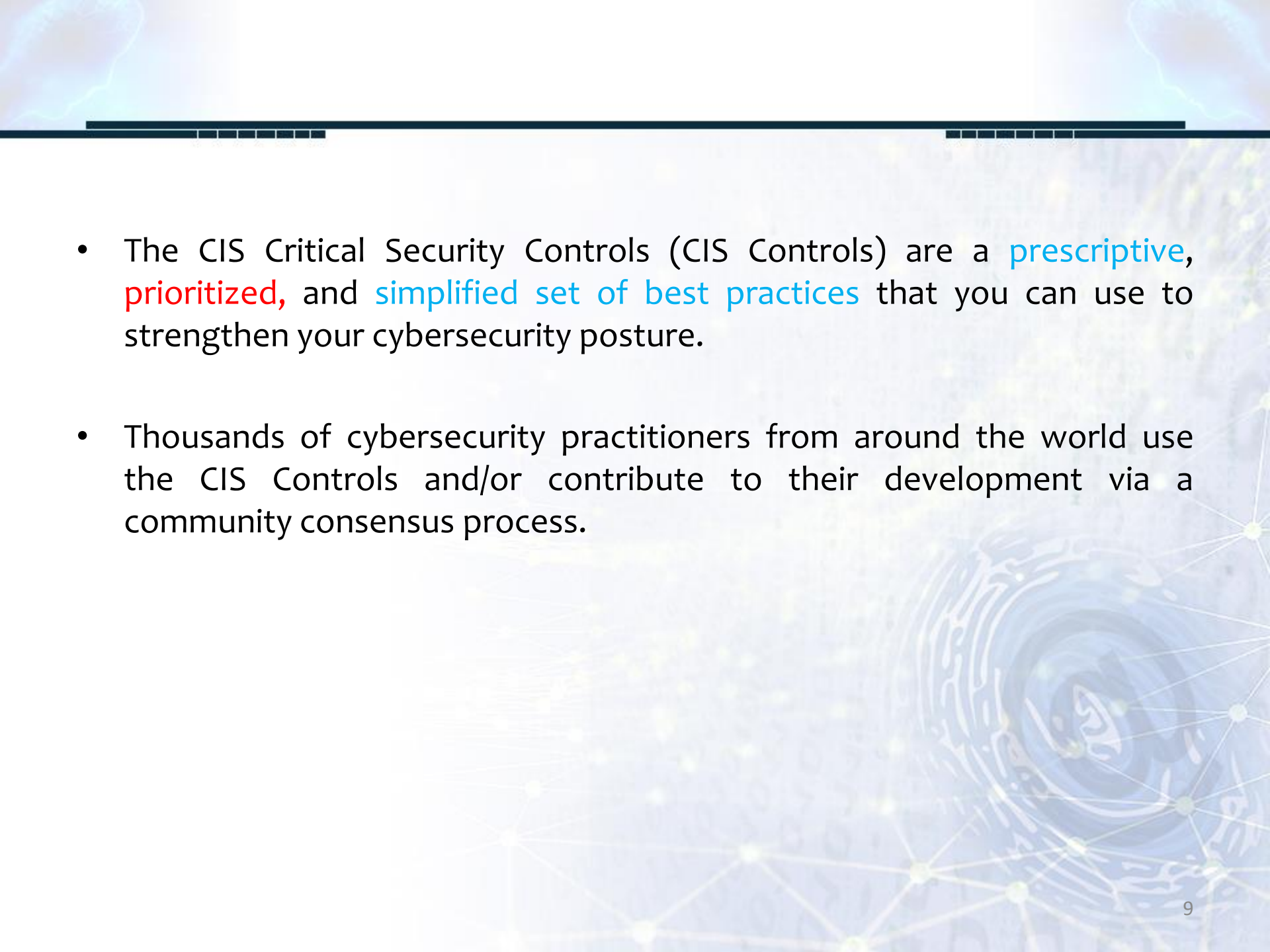
[| DOWNLOAD THE BENCHMARK](#) →



<https://www.cisecurity.org/cis-benchmarks>

CIS Critical Security Controls

- Formerly the SANS Critical Security Controls (**SANS Top 20**) these are now officially called the **CIS Critical Security Controls** (CIS Controls).
- CIS Top 20 Critical Security Controls are a **prioritized set of cybersecurity best practices** that can help **protect enterprises** from the **most pervasive and dangerous attacks**.
- <https://www.cisecurity.org/controls>

- 
- The CIS Critical Security Controls (CIS Controls) are a **prescriptive, prioritized, and simplified set of best practices** that you can use to strengthen your cybersecurity posture.
 - Thousands of cybersecurity practitioners from around the world use the CIS Controls and/or contribute to their development via a community consensus process.

CIS-CAT

- CIS-CAT Pro Assessor **evaluates the cybersecurity posture** of a system **against recommended policy settings**. The tool helps organizations save time and resources by employing automated content with policy setting recommendations based on 100+ globally recognized CIS Benchmarks.
- The CIS Controls Self Assessment Tool (CSAT) is a companion tool that helps IT security teams **track their implementation of every CIS Control** and Sub-Control
- <https://www.cisecurity.org/insights/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls>



There are two versions of CIS CSAT.

- The **CIS-hosted CSAT** is free to every organization for use in a non-commercial capacity.
- **CIS CSAT Pro** is an on-premises version that offers additional features and benefits and is only available to CIS SecureSuite Members.

A Look At CIS Security Benchmarks (4)

- CIS Benchmarks
example (Operating
Systems)
 - MS Windows Server
2012-R2

A Look At CIS Security Benchmarks (4)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	107

A Look At CIS Security Benchmarks (4)

CIS Microsoft Windows Server 2012 R2 Benchmark

v2.2.1 - 01-31-2017

- January 31, 2017
- 760 pages PDF doc

A Look At CIS Security Benchmarks (4)

- Profile applicability:
 - Level 1 domain controller
 - Level 1 member server
 - **Level 2 domain controller**
 - **Level 2 member server**

A Look At CIS Security Benchmarks (4)

- Level 1: Items in this profile intend to:
 - be practical and prudent;
 - provide a clear security benefit; and
 - not inhibit the utility of the technology beyond acceptable means

A Look At CIS Security Benchmarks (4)

- Level 2: extends the Level 1 - profile
 - intended for environments or use cases where security is paramount
 - acts as defense in depth measure
 - may negatively inhibit the utility or performance of the technology

A Look At CIS Security Benchmarks (4)

- Control content:
 - Profile applicability (ASA 8.X, ASA 9.X)
 - Description
 - Rationale
 - Audit
 - Remediation
 - **Impact**
 - Default value
 - References

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1]: *Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (Scored)*
 - *Profile applicability:
Level 1 Domain
Controller, Level 1
Member Server*

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1] Description:
 - This policy setting defines how long a user can use their password before it expires.
 - Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire.

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1] Audit:
 - Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

A Look At CIS Security Benchmarks (4)

Remediation:

To establish the recommended configuration via GP, set the following UI path to 60 or fewer days, but not 0:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
```

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1] Default Value: 42 days
- 1.1.2 [L1] Reference: CCE-37167-4
 - Common Configuration Enumeration (Unique identifiers for common system config issues)

END

A Look At CIS Security Benchmarks (3)

CIS Cisco Firewall Benchmark

v4.0.0 - 06-29-2016

- June 29, 2016
- 174 pages PDF doc

A Look At CIS Security Benchmarks (3)

- Control content:
 - Profile applicability (ASA 8.X, ASA 9.X)
 - Description
 - Rationale
 - Audit
 - Remediation
 - Default value
 - References

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
 - Profile applicability: Level 1, Cisco ASA9.X
 - Description: Sets the idle timeout for a console session before the security appliance terminates it.

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
 - Rationale: Limiting session timeout prevents unauthorized users from using abandoned sessions to perform malicious activities.

A Look At CIS Security Benchmarks (3)

Audit:

- Step 1: Run the following command to show what the console timeout is set to

```
hostname#sh run console | in timeout.5
```

The output should look like

```
console timeout 5
```

Example:

```
Asa-fw#sh run console | in timeout.5  
console timeout 5
```

Here the session timeout is 5 minutes

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

A Look At CIS Security Benchmarks (3)

Remediation:

- Step 1: Run the following command to set the console timeout to less than or equal to 5 minutes

```
hostname(config)# console timeout 5
```

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
 - Default Value: The default timeout is 0, which means the console session will not time out

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
 - Reference: CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.1

A Look At DISA STIGs (1)

- Defense Information Systems Agency (DISA) provides technical guides referred to as Security Technical Implementation Guides (STIGs).

A Look At DISA STIGs (1)

- USA DoD
- Security Technical Implementation Guides (STIGs)
- Most expansive security benchmarks available
- Most regularly updated
- 425 STIGs available

A Look At DISA STIGs (1)

- **STIGs master list (A-Z):**
 - <https://public.cyber.mil/stigs/downloads/>
 - **STIG viewer:**
 - <https://public.cyber.mil/stigs/srg-stig-tools/>

A Look At DISA STIGs (1)

STIGs HOME



[Topics](#) [Training](#) [PKI/PKE](#) [SRGs/STIGs](#) [Resources](#) [Help](#)

SECURITY TECHNICAL IMPLEMENTATION GUIDES (STIGs)

[SRG/STIGs Home](#)

[Automation](#)

[Control Correlation Identifier \(CCI\)](#)

[Document Library](#)

[DoD Annex for NIAP Protection Profiles](#)

[DoD Cloud Computing Security](#)

[Frequently Asked Questions - FAQs](#)

[Group Policy Objects](#)

[Quarterly Release Schedule and
Summary](#)

[SRG / STIG Library Compilations](#)

[SRG / STIG Mailing List](#)

[SRG/STIG Tools and Viewing Guidance](#)



STIGs

CRITICAL UPDATES

To provide increased flexibility for the future, DISA has updated the systems that produce STIGs and SRGs. This has resulted in a modification to Group and Rule IDs (Vul and Subvul IDs).

Test STIGs and test benchmarks were published from March through October 2020 to invite feedback. New and updated STIGs are now being published with the modified content.

New releases of STIGs published prior to this change will include the "legacy" Group and Rule IDs as XCCDF ident elements.

For all questions related to STIG content, please contact the DISA STIG Customer Support Desk at disa.stig_spt@mail.mil.

STIG UPDATES

DISA releases the Red Hat Ansible
Automation Controller Security
Technical Implementation Guide

Request for comments - DISA
releases draft Kubernetes STIG SCAP
benchmark for review

DISA releases the VMware vSphere
7.0 Security Technical
Implementation Guide

The SCC Development Team is
pleased to announce the release of
SCC 5.7.1.

<https://public.cyber.mil/stigs/>

A Look At DISA STIGs (1)

STIGs Master List



[STIGS]

- SRG/STIGs Home
- Automation
- Control Correlation Identifier (CCI)
- Document Library
- DoD Annex for NIAP Protection Profiles
- DoD Cloud Computing Security
- Frequently Asked Questions – FAQs
- Group Policy Objects
- Quarterly Release Schedule and Summary
- SRG / STIG Library Compilations
- SRG / STIG Mailing List
- SRG/STIG Tools and Viewing Guidance
- Sunset Products
- Vendor STIG Development Process
- Help

Topics Training PKI/PKE SRGs/STIGs Resources Help

Search:

Show 10 entries

	TITLE	SIZE	UPDATED
	2016-04-21 DoD CIO Memo - Use of Wearable Devices DoD Accredited Spaces with FAQ	541.89 KB	30 Nov 2018
	A10 Networks ADC ALG - Ver 2, Rel 1	523.3 KB	27 Apr 2021
	A10 Networks Application Delivery Controller (ADC) NDM STIG Ver 1	269.56 KB	30 Nov 2018
	A10 Networks Application Delivery Controller (ADC) Overview, Ver 1	86.24 KB	30 Nov 2018
	A10 Networks Application Delivery Controller (ADC) STIG Ver 1 Release Memo	70.89 KB	30 Nov 2018
	AAA SRG - Ver 1, Rel 2	665.83 KB	16 Jan 2020
	Active Directory Domain STIG - Ver 3, Rel 2	668.75 KB	09 Nov 2022
	Active Directory Forest STIG - Ver 2, Rel 8	433.92 KB	30 Nov 2018
	Adobe Acrobat Pro DC STIGs - Release Memo	707.86 KB	30 Nov 2018
	Adobe Acrobat Professional DC Continuous Track STIG - Ver 2, Rel 1	1.33 MB	26 Jul 2021

Showing 1 to 10 of 549 entries

Previous 1 2 3 4 5 ... 55 Next

STIG TOPICS

- ☐ Application Security (137) [+]
- ☐ Cloud Security (4)
- ☐ Control Correlation Identifier (CCI) (4)
- ☐ DoD Cloud Computing Security (DCCS) (5)
- ☐ Draft STIGs/SRGs (2)
- ☐ Group Policy Objects (GPO) (1)
- ☐ Host-Based Security Systems (HBSS) (3) [+]
- ☐ Mobility (28) [+]
- ☐ Network/Perimeter/Wireless (96) [+]
- ☐ NIAP Protection Profiles (5)
- ☐ Operating Systems (52) [+]
- ☐ Security Content Application Protocols (SCAP) (52) [+]
- ☐ STIG Compilations (2)
- ☐ STIG Policy (1)
- ☐ STIG Tools (5)
- ☐ STIG Viewing (11)
- ☐ Sunset (132) [+]
- ☐ Supplemental Automation Content (19) [+]
- ☐ Vendor Process (1)

<https://public.cyber.mil/stigs/downloads/>

A Look At DISA STIGs (1)

STIGs Viewer



Topics Training PKI/PKE SRGs/STIGs Resources Help

[STIGS]

SRG/STIGs Home

Automation

Control Correlation Identifier (CCI)

Document Library

DoD Annex for NIAP Protection Profiles

DoD Cloud Computing Security

Frequently Asked Questions - FAQs

Group Policy Objects

Quarterly Release Schedule and Summary

SRG / STIG Library Compilations

SRG / STIG Mailing List

SRG/STIG Tools and Viewing Guidance

Sunset Products

Vendor STIG Development Process

Help

STIG Viewing Tools

XCCDF formatted SRGs and STIGs are intended be ingested into an SCAP validated tool for use in validating compliance of a Target of Evaluation (TOE). As such, getting to the content of a XCCDF formatted STIG to read and understand the content is not as easy as opening a .doc or .pdf file and reading it. The process can be a little confusing and trying. Below are tools which can be used to view the STIGs and a Whitepaper describing the STIG Viewing processes.

DISA has produced standalone versions of STIG Viewer for the Windows and Linux platforms on 64-bit x86 processors. With the end of free support for Java 8 in early 2019, Oracle Corporation changed the licensing and distribution model for Java software. Users without supported Java 8 SE environments should use the standalone versions of STIG Viewer. Users with supported Java 8 SE environments may still use the current JAR file. DISA will base future STIG Viewer development on open-source software developed by the OpenJDK and OpenJFX projects.

Show 10 entries

Search:

TITLE	SIZE	UPDATED
 How to Create and SRG-STIG ID Mapping Spreadsheet	298.21 KB	03 Feb 2021
 STIG Sorted by STIG ID	103.46 KB	30 Mar 2015
 STIG Sorted by Vulnerability ID	101.59 KB	30 Mar 2015
 STIG Viewer 2.17	1.14 MB	21 Sep 2022
 STIG Viewer 2.17 Hashes	1.36 KB	21 Sep 2022
 STIG Viewer 2.17-Linux	73.38 MB	21 Sep 2022
 STIG Viewer 2.17-Win64	54.03 MB	21 Sep 2022
 STIG Viewer 2.17-Win64 msi	54.26 MB	21 Sep 2022

<https://public.cyber.mil/stigs/srg-stig-tools/>

A Look At DISA STIGs (1)

STIG Viewer Download



Topics Training PKI/PKE SRGs/STIGs Resources Help

Automation

Control Correlation Identifier (CCI)

Document Library

DoD Annex for NIAP Protection Profiles

DoD Cloud Computing Security

Frequently Asked Questions – FAQs

Group Policy Objects

Quarterly Release Schedule and Summary

SRG / STIG Library Compilations

SRG / STIG Mailing List

SRG/STIG Tools and Viewing Guidance

Sunset Products

Vendor STIG Development Process

Help

STIG Viewing Tools

XCCDF formatted SRGs and STIGs are intended be ingested into an SCAP validated tool for use in validating compliance of a Target of Evaluation (TOE). As such, getting to the content of a XCCDF formatted STIG to read and understand the content is not as easy as opening a .doc or .pdf file and reading it. The process can be a little confusing and trying. Below are tools which can be used to view the STIGs and a Whitepaper describing the STIG Viewing processes.

DISA has produced standalone versions of STIG Viewer for the Windows and Linux platforms on 64-bit x86 processors. With the end of free support for Java 8 in early 2019, Oracle Corporation changed the licensing and distribution model for Java software. Users without supported Java 8 SE environments should use the standalone versions of STIG Viewer. Users with supported Java 8 SE environments may still use the current JAR file. DISA will base future STIG Viewer development on open-source software developed by the OpenJDK and OpenJFX projects.

Show 10 entries

Search:

	TITLE	SIZE	UPDATED
	How to Create and SRG-STIG ID Mapping Spreadsheet	298.21 KB	03 Feb 2021
	STIG Sorted by STIG ID	103.46 KB	30 Mar 2015
	STIG Sorted by Vulnerability ID	101.59 KB	30 Mar 2015
	STIG Viewer 2.17	1.14 MB	21 Sep 2022
	STIG Viewer 2.17 Hashes	1.36 KB	21 Sep 2022
	STIG Viewer 2.17-Linux	73.38 MB	21 Sep 2022
	STIG Viewer 2.17-Win64	54.03 MB	21 Sep 2022
	STIG Viewer 2.17-Win64 msi	54.26 MB	21 Sep 2022
	STIG Viewer User Guide (Sep 2022)	1.77 MB	21 Sep 2022

A Look At DISA STIGs (1)

STIG Library Compilation



Topics Training PKI/PKE SRGs/STIGs Resources Help

(STIGs)

SRG/STIGs Home

Automation

Control Correlation Identifier (CCI)

Document Library

DoD Annex for NIAP Protection Profiles

DoD Cloud Computing Security

Frequently Asked Questions – FAQs

Group Policy Objects

Quarterly Release Schedule and Summary

SRG / STIG Library Compilations

SRG / STIG Mailing List

SRG/STIG Tools and Viewing Guidance

Sunset Products

Vendor STIG Development Process

The SRG-STIG Library Compilation .zip files are compilations of DoD Security Requirements Guides (SRGs) and DoD Security Technical Implementation Guides (STIGs), as well as some other content that may be available through the Cyber Exchange web site's STIG pages. Specifically excluded are Security Readiness Review (SRR) Tools (scripts and OVAL Benchmarks), Group policy objects, and draft SRGs and STIGs.

The Library Compilation .zip files will be updated and released during each SRG-STIG Update Release Cycle to capture all newly updated or released SRGs, STIGs, and Tools. New SRG-STIG content released mid cycle will be individually downloadable from IASE as released. These SRGs-STIGs will appear in the subsequent release of the Library Compilation.

See **SRG-STIG Library Compilation READ ME** for more information to include download / extraction instructions and a FAQ.

NOTE: While every attempt will be made to provide a complete set of **currently in force** SRGs, STIGs, and related tools, DISA makes no guarantee as to the completeness of the compilation or the **currently in force** status of the contents.

NOTE: While every attempt will be made to publish updated compilation files on the SRG-STIG Quarterly Update Release date, publication may lag due to competing workloads. Updated Compilation files will be published on or as soon as possible the published date. We apologize for any inconvenience this may impose.

Concerns or questions related to the contents or format of these compilation files should be directed to the DISA STIG Customer Support Desk at disa.stig_spt@mail.mil

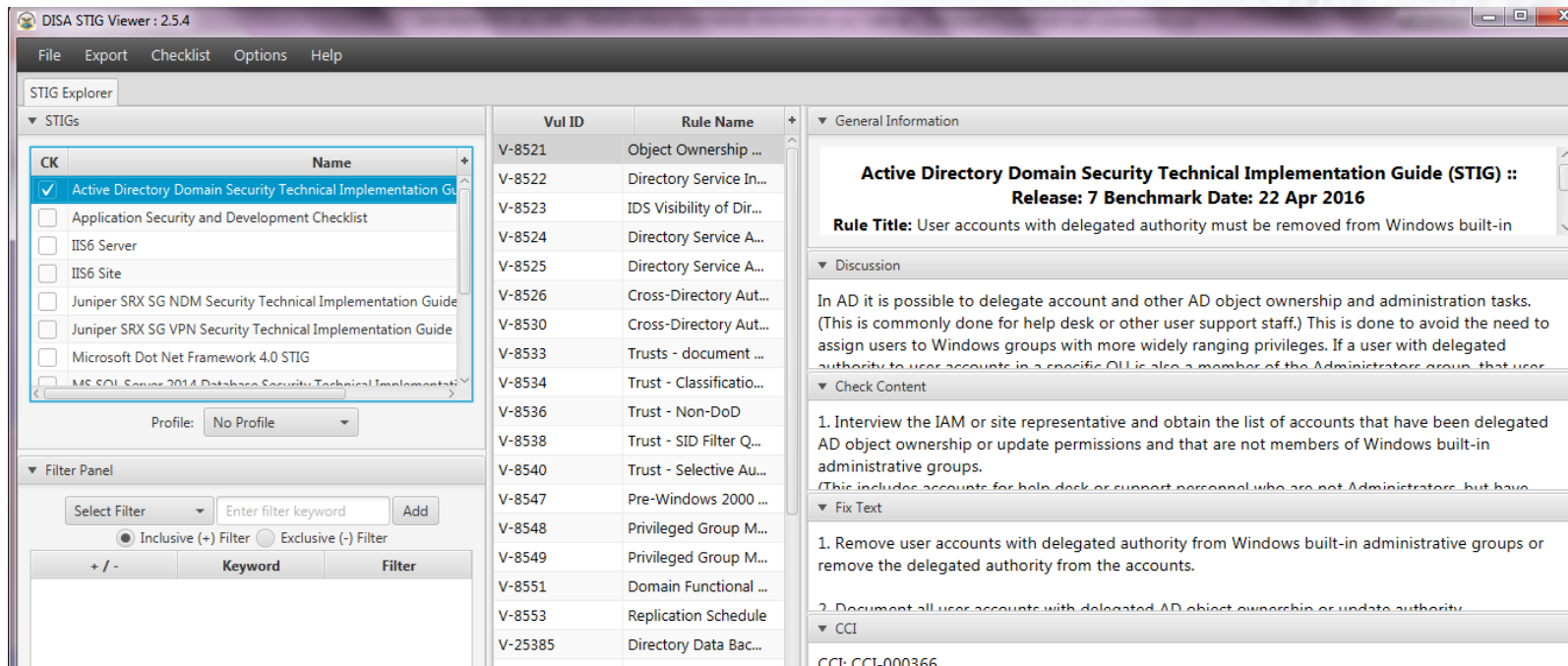
SRG/STIG Compilations

	TITLE	SIZE	UPDATED
	Compilation - SRG-STIG Library	260.47 MB	24 Jan 2023
	Compilation - SRG-STIG Library - READ ME	122.17 KB	19 Jun 2019

- There are three categories of severity, ranked on level of risk or vulnerability.
- These are known as Severity Category Codes (CAT), with CAT 1, CAT 2 and CAT 3 levels of risk.
- CAT 1 controls cover the most severe vulnerabilities and risks.
- CAT I weaknesses should receive the highest priority for correction or mitigation.

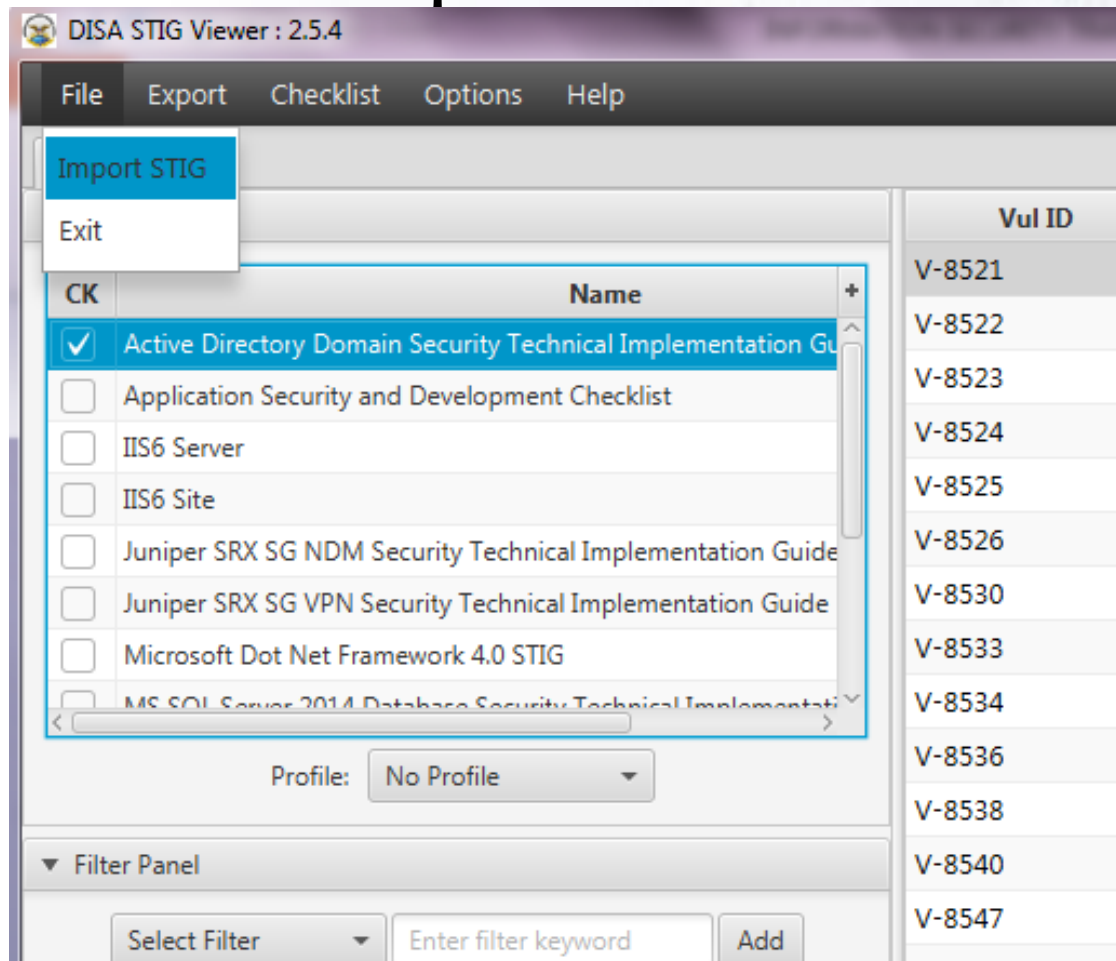
A Look At DISA STIGs (1)

STIG Viewer Window



A Look At DISA STIGs (1)

Import STIG





[HOME](#) [STIGS](#) [DOD 8500](#) [NIST 800-53](#) [COMMON CONTROLS HUB](#) [ABOUT](#)



[Microsoft Windows 11](#)
[Microsoft Windows 2008 Server Domain Name System](#)
[Microsoft Windows 2012 Server Domain Name System](#)
[Microsoft Windows Defender Antivirus](#)
[Microsoft Windows Firewall with Advanced Security](#)
[Microsoft Windows PAW](#)
[Microsoft Windows Phone 8.1](#)
[Microsoft Windows Server 2012 Domain Controller](#)
[Microsoft Windows Server 2012 Member Server](#)
[Microsoft Windows Server 2012/2012 R2 Domain Controller](#)
[Microsoft Windows Server 2012/2012 R2 Member Server](#)
[Microsoft Windows Server 2016](#)
[Microsoft Windows Server 2019](#)
[Microsoft Windows Server 2022](#)
[Microsoft Word 2003](#)
[Microsoft Word 2007](#)
[Microsoft Word 2010](#)

<https://www.stigviewer.com/stigs>



HOME STIGS DOD 8500 NIST 800-53 COMMON CONTROLS HUB ABOUT

Search...



Microsoft Windows Server 2012/2012 R2 Member Server Security Technical Implementation Guide

Overview

Version	Date	Finding Count (330)			Downloads		
3	2022-09-06	CAT I (High): 33	CAT II (Med): 238	CAT III (Low): 59	Excel	JSON	XML

STIG Description

This Security Technical Implementation Guide is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements are derived from the National Institute of Standards and Technology (NIST) 800-53 and related documents. Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil.

Available Profiles



Findings (MAC III - Administrative Sensitive)

Finding ID	Severity	Title	Description
V-225447	High	Anonymous access to the registry must be restricted.	The registry is integral to the function, security, and stability of the Windows system. Some processes may require anonymous access to the registry. This must be limited to properly protect the system.
V-225244	High	Administrative accounts must not be used with applications that access the Internet, such as web browser s, or with potential Internet sources, such as email.	Using applications that access the Internet or have potential Internet sources using administrative privileges exposes a system to compromise. If a flaw in an application is exploited while...
V-225258	High	The Windows 2012 / 2012 R2 system must use an anti-virus program.	Malicious software can establish a base on individual desktops and servers. Employing an automated mechanism to detect this type of software will aid in elimination of the software from the...
V-225547	High	The Act as part of the operating system user right must not be assigned to any groups or accounts.	Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the "Act as part of the operating system" user right can assume the...
V-225438	High	File Transfer Protocol (FTP) servers must be configured to prevent access to the system drive.	The FTP service allows remote users to access shared files and directories. Access outside of the specific directories of shared data could provide access to system resources and compromise the system.
V-225449	High	Local accounts with blank passwords must be restricted to prevent access from the network.	An account without a password can allow unauthorized access to a system as only the username would be required. Password policies should require...

A Look At DISA STIGs (1)

- Completely different mechanism for DISA STIGs

END

A Look At DISA STIGs (2)

- STIG content:
 - General information (title)
 - Discussion
 - Check content
 - Fix text
 - CCI (References)

A Look At DISA STIGs (2)

SEVERITY	DISA CATEGORY CODE GUIDELINES
CAT 1	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT 2	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT 3	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity

A Look At DISA STIGs (2)

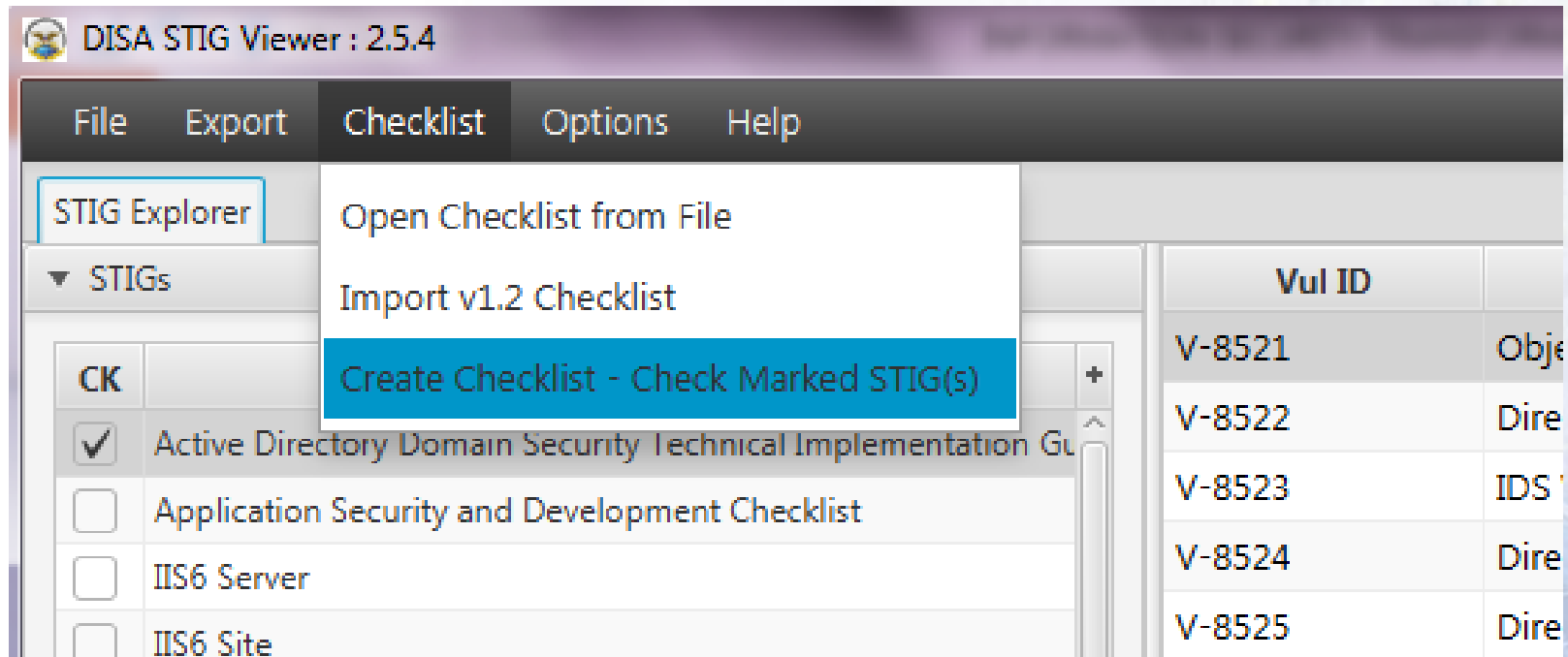
FILTER PANEL

The screenshot shows a 'Filter Panel' window. At the top, there is a dropdown menu currently set to 'CAT I'. A list of filter options is displayed below it: Keyword, Rule Title, STIG ID, Vulnerability ID, Rule ID, IA Control, CAT I (highlighted), CAT II, CAT III, and CCI. To the right of the dropdown, the text 'CAT I' is displayed, followed by an 'Add' button. Below this, there are two radio buttons: 'Filter' (selected) and 'Exclusive (-) Filter'. A table with two columns, 'Keyword' and 'Filter', is shown below the radio buttons. The table is currently empty, with the text 'content in table' visible. At the bottom of the panel, there are two buttons: 'Remove Filter(s)' and 'Remove All Filters'.

Keyword	Filter
content in table	

A Look At DISA STIGs (2)

CREATE CHECKLIST



A Look At DISA STIGs (2)

CHECKLIST

The screenshot displays the DISA STIG Viewer 2.5.4 application interface. The window is titled "DISA STIG Viewer : 2.5.4" and has a menu bar with "File", "Import", and "Export". The "Checklist X" tab is selected in the "STIG Explorer" section. The "Totals" section shows "Overall Totals" with "Open: 0", "Not Reviewed: 42", "Not a Finding: 0", and "Not Applicable: 0". The "Target Data" section includes fields for "Host Name", "IP Address", "MAC Address", and "Fully Qualified Domain Name", along with a "Get Host Data" button. The "Role" section has radio buttons for "None", "Workstation", "Member Server", and "Domain Controller", and a checkbox for "Web or Database STIG". The "STIGs" section shows a list of STIGs, with "Active Directory Domain Security Technical Implementation Guide (STIG)" selected. The "General Information" section displays the "Active Directory Domain Security Technical Implementation Guide (STIG) :: Release: 7 Benchmark Date: 22 Apr 2016" and the "Rule Title: User accounts with delegated authority must be removed from Windows built-in administrative groups or remove the delegated authority from the accounts." The "Status" section shows "Not Reviewed" selected. The "Vuln Information" section includes tabs for "Discussion", "Check Content", "Fix Text", "CCI", and "Misc", with the "Discussion" tab selected. The "Finding Details" section is empty. The "Comments" section is also empty. The bottom status bar shows "Showing rule 1 out of 42".

Status	Vul ID	Rule Name
NR	V-8521	Object Owners...
NR	V-8522	Directory Servic...
NR	V-8523	IDS Visibility of ...
NR	V-8524	Directory Servic...
NR	V-8525	Directory Servic...
NR	V-8526	Cross-Directory...
NR	V-8530	Cross-Directory...
NR	V-8533	Trusts - docum...
NR	V-8534	Trust - Classific...
NR	V-8536	Trust - Non-DoD
NR	V-8538	Trust - SID Filte...
NR	V-8540	Trust - Selective...
NR	V-8547	Pre-Windows 2...
NR	V-8548	Privileged Grou...
NR	V-8549	Privileged Grou...
NR	V-8551	Domain Functio...
NR	V-8553	Replication Sch...
NR	V-25385	Directory Data ...
NR	V-25840	DSRM Passwor...
NR	V-25841	Review of Hosti...
NR	V-25997	Replication in t...
NR	V-36431	Enterprise Admi...
NR	V-36432	Domain Admin...
NR	V-36433	Domain Memb...

A Look At DISA STIGs (2)

- Checklist screens:
 - Overall totals
 - Target data
 - Role
 - Finding details
 - Comments

A Look At DISA STIGs (2)

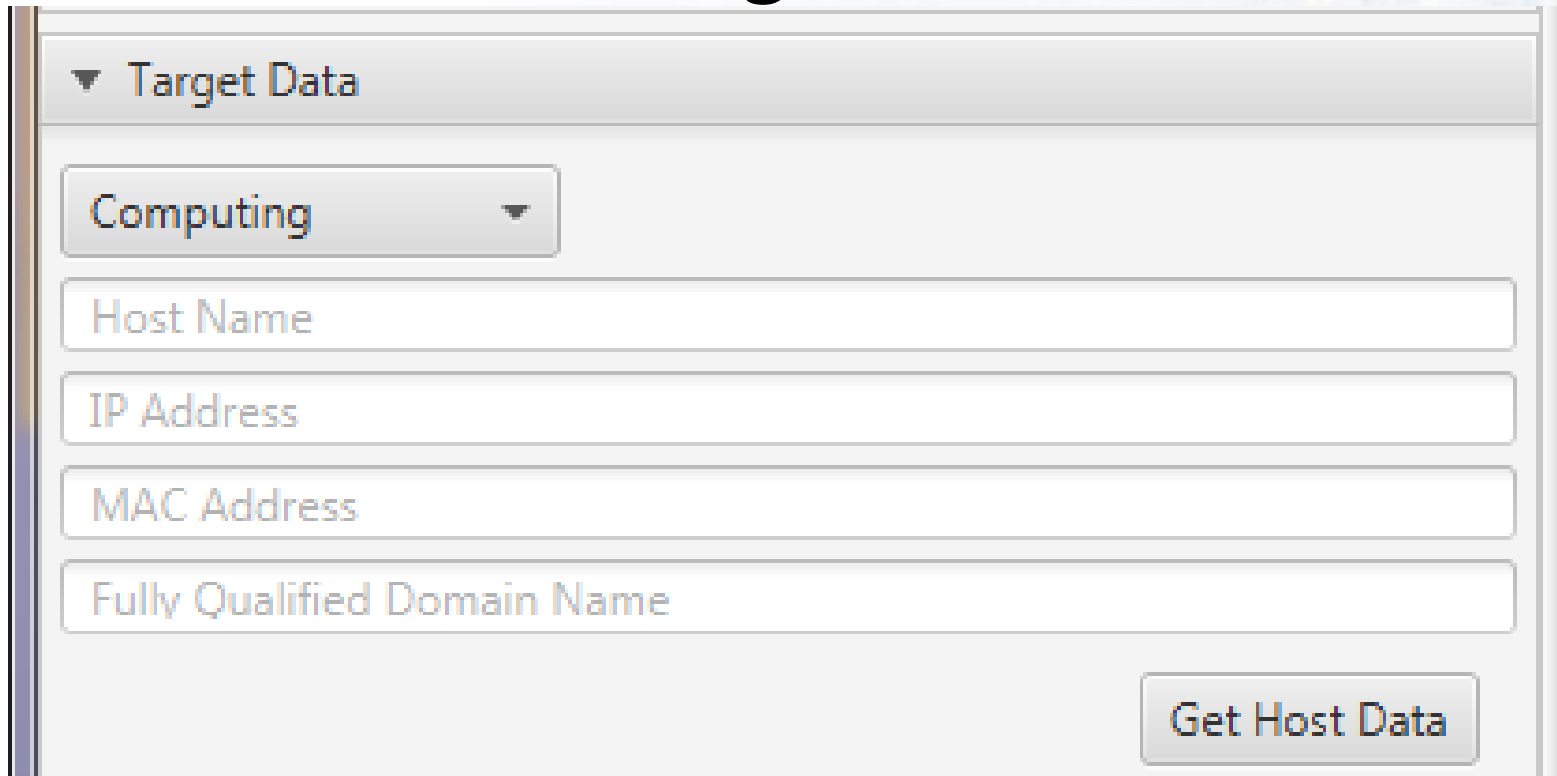
- Checklist screens (STATUS):
 - Not reviewed
 - Open
 - Not a finding
 - Not applicable

Totals

3

A Look At DISA STIGs (2)

Target Data



The screenshot shows a software interface for entering target data. It features a header bar with a dropdown arrow and the text "Target Data". Below this is a category dropdown menu currently set to "Computing". There are four text input fields stacked vertically, labeled "Host Name", "IP Address", "MAC Address", and "Fully Qualified Domain Name". A "Get Host Data" button is located at the bottom right of the form.

▼ Target Data

Computing ▼

Host Name

IP Address

MAC Address

Fully Qualified Domain Name

Get Host Data

A Look At DISA STIGs (2)

Status

▼ General Information

**Active Directory Domain Security Technical Implementation Guide (STIG) ::
Release: 7 Benchmark Date: 22 Apr 2016**

Rule Title: User accounts with delegated authority must be removed from Windows built-in administrative groups or remove the delegated authority from the accounts.

Status: ☐ Not Reviewed ☒ Open ☐ Not a Finding ☐ Not Applicable

Severity Override ▼

A Look At DISA STIGs (2)

Vuln Information

Review of Hostin...

Status: ☐ Not Reviewed ☒ Open ☐ Not a Finding ☐ Not Applicable Severity Override ▾

▼ Vuln Information

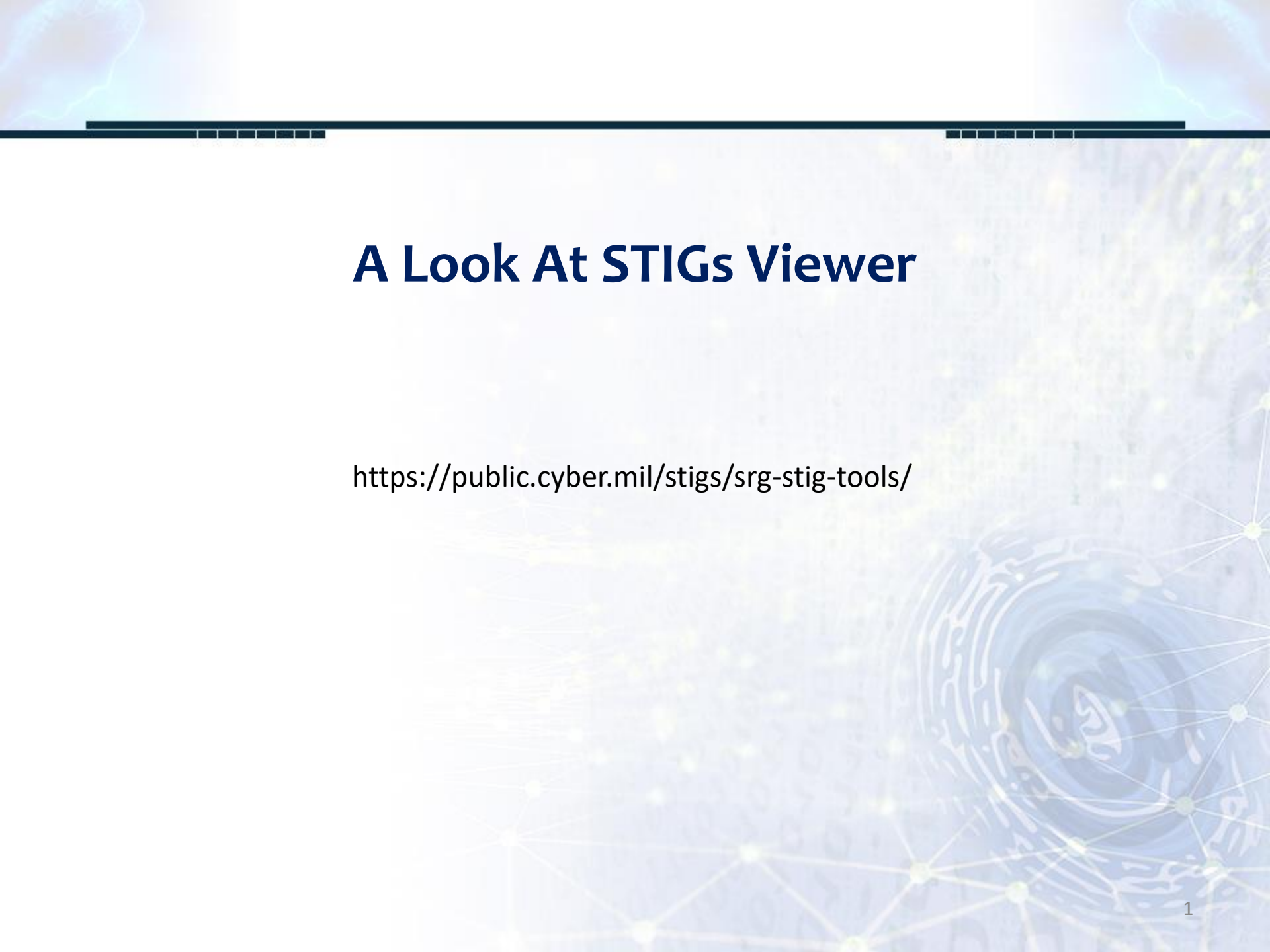
Discussion Check Content Fix Text CCI Misc

In AD it is possible to delegate account and other AD object ownership and administration tasks. (This is commonly done for help desk or other user support staff.) This is done to avoid the need to assign users to Windows groups with more widely ranging privileges. If a user with delegated authority to user accounts in a specific OU is also a member of the Administrators group, that user

A Look At DISA STIGs (2)

- In the next module lets look at further details

END



A Look At STIGs Viewer

<https://public.cyber.mil/stigs/srg-stig-tools/>

Frequently Asked Questions – FAQs

Group Policy Objects

Quarterly Release Schedule and
Summary

SRG / STIG Library Compilations

SRG / STIG Mailing List

SRG/STIG Tools and Viewing Guidance

Sunset Products

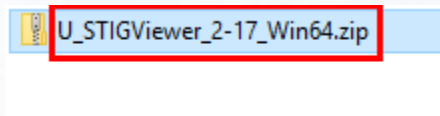
Vendor STIG Development Process

Help

Show 10 |  entries

	TITLE
	How to Create and SRG-STIG ID Mapping Spreadsheet
	STIG Sorted by STIG ID
	STIG Sorted by Vulnerability ID
	STIG Viewer 2.17
	STIG Viewer 2.17 Hashes
	STIG Viewer 2.17-Linux
	STIG Viewer 2.17-Win64
	STIG Viewer 2.17-Win64 msi
	STIG Viewer User Guide (Sep 2022)
	STIG Viewer Video

Showing 1 to 10 of 11 entries



<https://public.cyber.mil/stigs/srg-stig-tools/>

Name	Date modified	Type	Size
 app	27/07/2022 2:54 pm	File folder	
 runtime	27/07/2022 2:54 pm	File folder	
 SWIDTAG	27/07/2022 2:54 pm	File folder	
 STIG Viewer	27/07/2022 2:56 pm	Application	592 KB
 STIG Viewer	27/07/2022 2:54 pm	Icon	175 KB
 ActionLog	11/04/2023 1:04 pm	Text Document	1 KB

DISA STIG Viewer : 2.17 : STIG Explorer

FileExportChecklistOptionsHelp

STIG Explorer

STIGs

Filter on STIG name...

CK	Name
No content in table	

Profile: No Profile

Filter Panel

Must match: ☒ All ☐ Any

Keyword

Enter filter keyword

Add

☒ Inclusive (+) Filter ☐ Exclusive (-) Filter

+ / -	Keyword	Filter
No content in table		

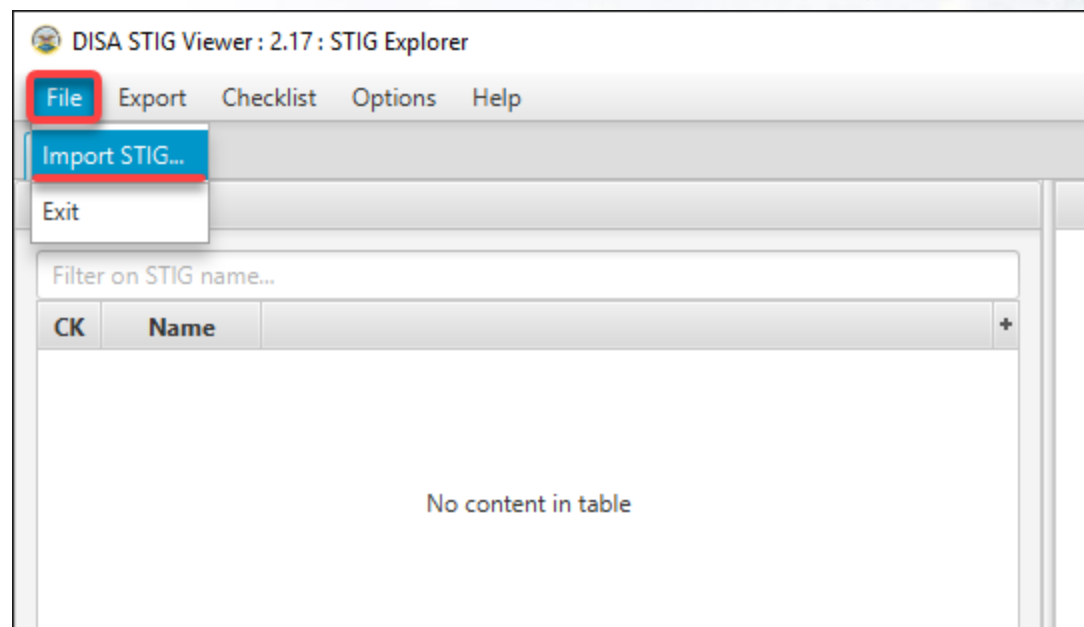
Remove Filter(s)

Remove All Filters

Vul ID	Rule ID	Rule Name
No content in table		

No Rules Selected

5



A Look At STIGs Viewer



Topics Training PKI/PKE SRGs/STIGs Resources Help

[STIGS]

SRG/STIGs Home

Automation

Control Correlation Identifier (CCI)

Document Library

DoD Annex for NIAP Protection Profiles

DoD Cloud Computing Security

Frequently Asked Questions – FAQs

Group Policy Objects

Quarterly Release Schedule and Summary

SRG /STIG Library Compilations

SRG /STIG Mailing List

SRG/STIG Tools and Viewing Guidance

Sunset Products

Vendor STIG Development Process

Help

Show 10 entries

Search:

TITLE	SIZE	UPDATED
 Microsoft Sharepoint Designer 2013 STIG - Ver 1, Rel 3	442.79 KB	01 Dec 2018
 Microsoft Skype for Business 2016 STIG - Ver 1, Rel 1	352.2 KB	01 Dec 2018
 Microsoft Visio 2013 STIG - Ver 1, Rel 4	427.91 KB	01 Dec 2018
 Microsoft Visio 2016 STIG - Ver 1, Rel 1	355.78 KB	01 Dec 2018
 Microsoft Windows 10 STIG - Ver 2, Rel 5	966.35 KB	09 Nov 2022
 Microsoft Windows 10 STIG Benchmark - Ver 2, Rel 7	100.42 KB	13 Jan 2023
 Microsoft Windows 11 STIG - Ver 1 Rel 2	948.64 KB	09 Nov 2022
 Microsoft Windows 11 STIG Benchmark - Ver 1, Rel 1	94.76 KB	17 Nov 2022
 Microsoft Windows 2012 and 2012 R2 DC STIG- Ver 3, Rel 5	905.58 KB	09 Nov 2022
 Microsoft Windows 2012 and 2012 R2 MS STIG - Ver 3, Rel 5	852.32 KB	09 Nov 2022

Showing 231 to 240 of 549 entries

Previous

1

...

23

24

25

...

55

Next

STIG TOPICS

- ☐ Application Security (137) [+]
- ☐ Cloud Security (4)
- ☐ Control Correlation Identifier (CCI) (4)
- ☐ DoD Cloud Computing Security (DCCS) (5)
- ☐ Draft STIGs/SRGs (2)
- ☐ Group Policy Objects (GPO) (1)
- ☐ Host-Based Security Systems (HBSS) (3) [+]
- ☐ Mobility (28) [+]
- ☐ Network/Perimeter/Wireless (96) [+]
- ☐ NIAP Protection Profiles (5)
- ☐ Operating Systems (52) [+]
- ☐ Security Content Application Protocols (SCAP) (52) [+]
- ☐ STIG Compilations (2)
- ☐ STIG Policy (1)
- ☐ STIG Tools (5)
- ☐ STIG Viewing (11)
- ☐ Sunset (132) [+]
- ☐ Supplemental Automation Content (19) [+]
- ☐ Vendor Process (1)

[STIGs]

SRG/STIGs Home

Automation ▸

Control Correlation Identifier (CCI)

Document Library

DoD Annex for NIAP Protection Profiles

DoD Cloud Computing Security

Frequently Asked Questions – FAQs

Group Policy Objects

Quarterly Release Schedule and
Summary

SRG / STIG Library Compilations

SRG / STIG Mailing List

SRG/STIG Tools and Viewing Guidance

Sunset Products

Vendor STIG Development Process

Help

Show 10 ▾ entries

Search:

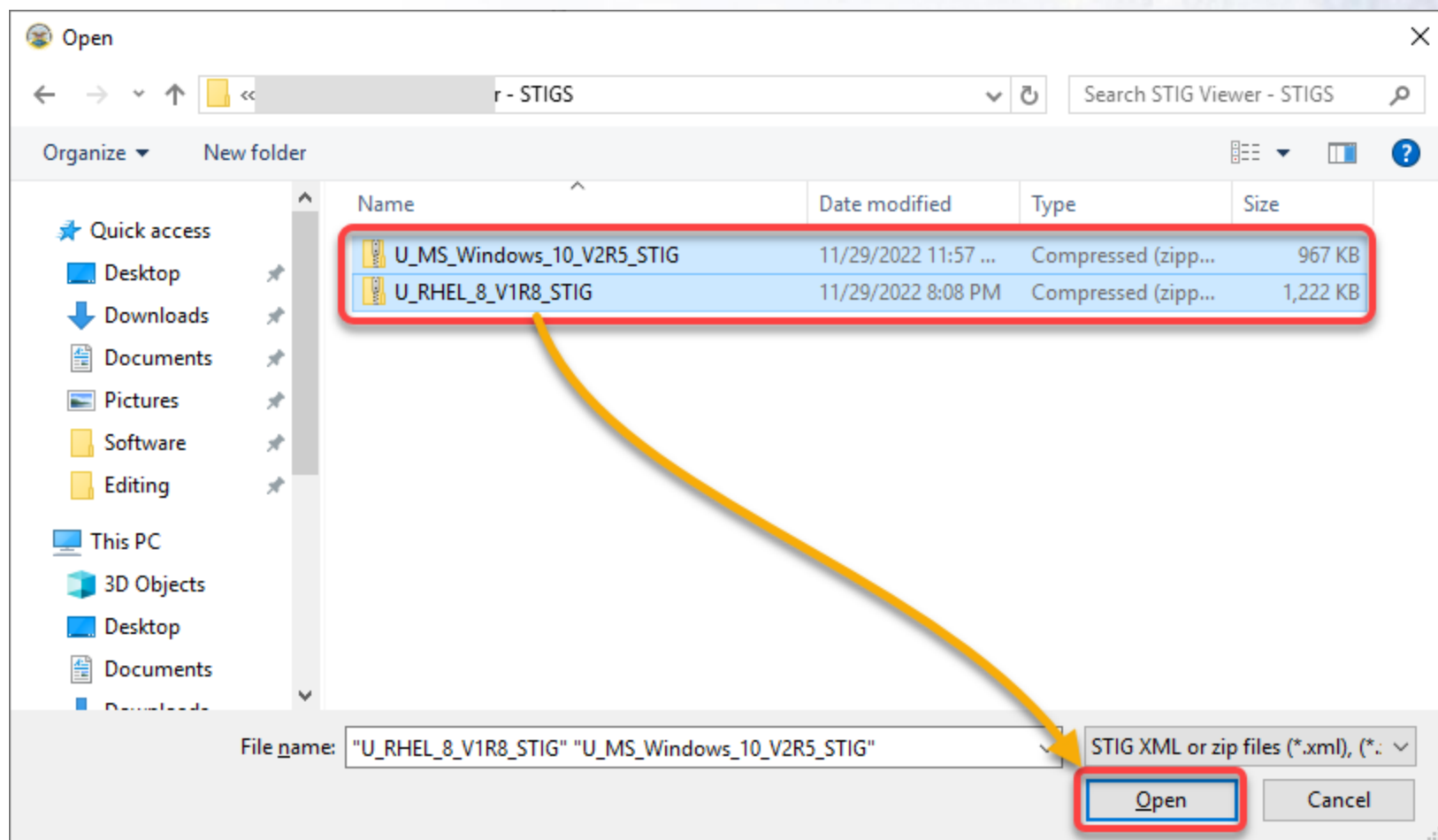
	TITLE ▲	SIZE ▴	UPDATED ▴
	Microsoft Word 2013 STIG - Ver 1, Rel 6	462.31 KB	01 Dec 2018
	Microsoft Word 2016 STIG - Ver 1, Rel 1	361.84 KB	01 Dec 2018
	Mobile Iron Core v9.x Release Memo	65.5 KB	11 Mar 2019
	MobileIron Core v10.x MDM STIG Ver 1 Rel 1	1 MB	06 Jun 2019
	MongoDB Enterprise Advanced 3.x STIG - Ver 2, Rel 1	609.61 KB	19 Apr 2022
	MongoDB Enterprise Advanced 4.x STIG - Ver 1, Rel 2	1.56 MB	21 Oct 2022
	Motorola Android 9.x STIG	2.95 MB	10 Nov 2020
	Motorola Solutions Android 11 - Ver 1, Rel 2	1.68 MB	07 Sep 2022
	Mozilla Firefox for Linux STIG Benchmark - Ver 6, Rel 3	17.52 KB	21 Oct 2022
	Mozilla Firefox for Windows STIG Benchmark - Ver 6, Rel 3	14.8 KB	21 Oct 2022

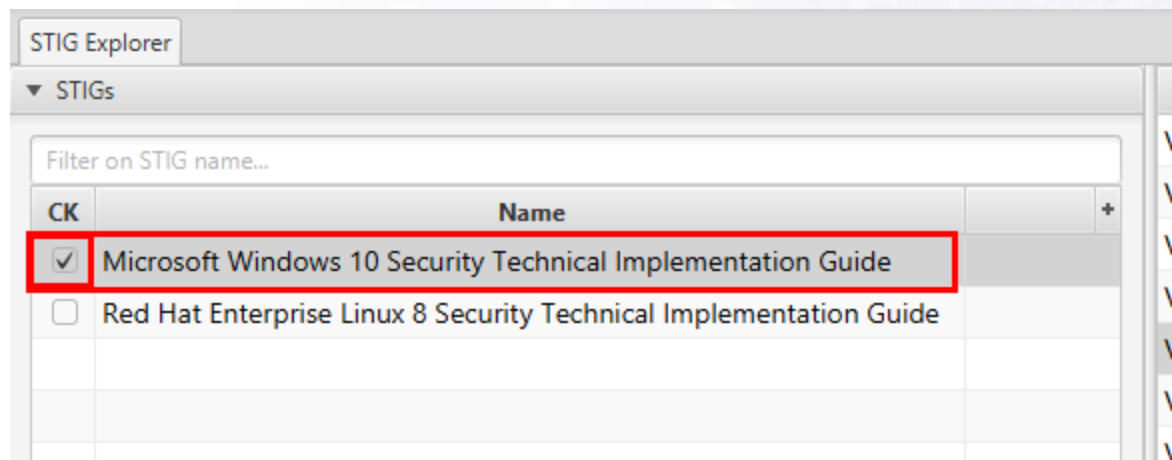
Showing 261 to 270 of 549 entries

Previous 1 ... 26 **27** 28 ... 55 Next

STIG TOPICS

- ☐ Application Security (137) [⊕]
- ☐ Cloud Security (4)
- ☐ Control Correlation Identifier (CCI) (4)
- ☐ DoD Cloud Computing Security (DCCS) (5)
- ☐ Draft STIGs/SRGs (2)
- ☐ Group Policy Objects (GPO) (1)
- ☐ Host-Based Security Systems (HBSS) (3) [⊕]
- ☐ Mobility (28) [⊕]
- ☐ Network/Perimeter/Wireless (96) [⊕]
- ☐ NIAP Protection Profiles (5)
- ☐ Operating Systems (52) [⊕]
- ☐ Security Content Application Protocols (SCAP) (52) [⊕]
- ☐ STIG Compilations (2)
- ☐ STIG Policy (1)
- ☐ STIG Tools (5)
- ☐ STIG Viewing (11)
- ☐ Sunset (132) [⊕]
- ☐ Supplemental Automation Content (19) [⊕]
- ☐ Vendor Process (1)





Vul ID	Rule ID	Rule Name	+	M
V-220697	SV-220697r8571...	SRG-OS-000480-...		
V-220698	SV-220698r8571...	SRG-OS-000480-...		
V-220699	SV-220699r5691...	SRG-OS-000480-...		
V-220700	SV-220700r5691...	SRG-OS-000480-...		
V-220701	SV-220701r7931...	SRG-OS-000191-...		
V-220702	SV-220702r8592...	SRG-OS-000185-...		
V-220703	SV-220703r8591...	SRG-OS-000185-...		
V-220704	SV-220704r8592...	SRG-OS-000185-...		
V-220705	SV-220705r8519...	SRG-OS-000370-...		
-----	-----	-----		

Group Title: S

Rule Title: Wi
the following
external scans

Vul ID	Rule ID	Rule Name
V-220697	SV-220697r85...	SRG-OS-00048...
V-220698	SV-220698r85...	SRG-OS-00048...
V-220699	SV-220699r56...	SRG-OS-00048...
V-220700	SV-220700r56...	SRG-OS-00048...
V-220701	SV-220701r79...	SRG-OS-00019...
V-220702	SV-220702r85...	SRG-OS-00018...
V-220703	SV-220703r85...	SRG-OS-00018...
V-220704	SV-220704r85...	SRG-OS-00018...
V-220705	SV-220705r85...	SRG-OS-00037...
V-220706	SV-220706r85...	SRG-OS-00048...
V-220707	SV-220707r79...	SRG-OS-00048...
V-220708	SV-220708r56...	SRG-OS-00008...
V-220709	SV-220709r56...	SRG-OS-00048...
V-220710	SV-220710r56...	SRG-OS-00013...
V-220711	SV-220711r56...	SRG-OS-00011...
V-220712	SV-220712r85...	SRG-OS-00032...
V-220713	SV-220713r56...	SRG-OS-00048...
V-220714	SV-220714r56...	SRG-OS-00009...
V-220715	SV-220715r56...	SRG-OS-00048...
V-220716	SV-220716r56...	SRG-OS-00007...
V-220717	SV-220717r85...	SRG-OS-00031...
V-220718	SV-220718r56...	SRG-OS-00009...
V-220719	SV-220719r56...	SRG-OS-00009...
V-220720	SV-220720r56...	SRG-OS-00009...
V-220721	SV-220721r56...	SRG-OS-00009...
V-220722	SV-220722r56...	SRG-OS-00009...
V-220723	SV-220723r56...	SRG-OS-00048...
V-220724	SV-220724r56...	SRG-OS-00048...
V-220725	SV-220725r56...	SRG-OS-00048...

Showing rule 5 out of 257

Microsoft Windows 10 Security Technical Implementation Guide :: Version 2, Release: 5 Benchmark Date: 14 Nov 2022

Vul ID: V-220701 **Rule ID:** SV-220701r793197_rule **STIG ID:** WN10-00-000025
Severity: CAT II **Classification:** Unclass **Legacy IDs:** V-63343; SV-77833

Group Title: SRG-OS-000191-GPOS-00080

Rule Title: Windows 10 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously, where ESS is used; 30 days, for any additional internal network scans not covered by ESS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP).

Discussion: An approved tool for continuous network scanning must be installed and configured to run.

Without the use of automated mechanisms to scan for security flaws on a continuous and/or periodic basis, the operating system or other system components may remain vulnerable to the exploits presented by undetected software flaws.

To support this requirement, the operating system may have an integrated solution incorporating continuous scanning using ESS and periodic scanning using other tools, as specified in the requirement.

Check Text: Verify DoD-approved ESS software is installed and properly operating. Ask the site ISSM for documentation of the ESS software installation and configuration.

If the ISSM is not able to provide a documented configuration for an installed ESS or if the ESS software is not properly maintained or used, this is a finding.

Note: Example of documentation can be a copy of the site's CCB approved Software Baseline with version of software noted or a memo from the ISSM stating current ESS software and version.

Fix Text: Install DoD-approved ESS software and ensure it is operating continuously.

References

CCI: CCI-001233: The organization employs automated mechanisms on an organization-defined frequency to determine the state of information system components with regard to flaw remediation.
NIST SP 800-53 :: SI-2 (2)
NIST SP 800-53A :: SI-2 (2).1 (ii)
NIST SP 800-53 Revision 4 :: SI-2 (2)

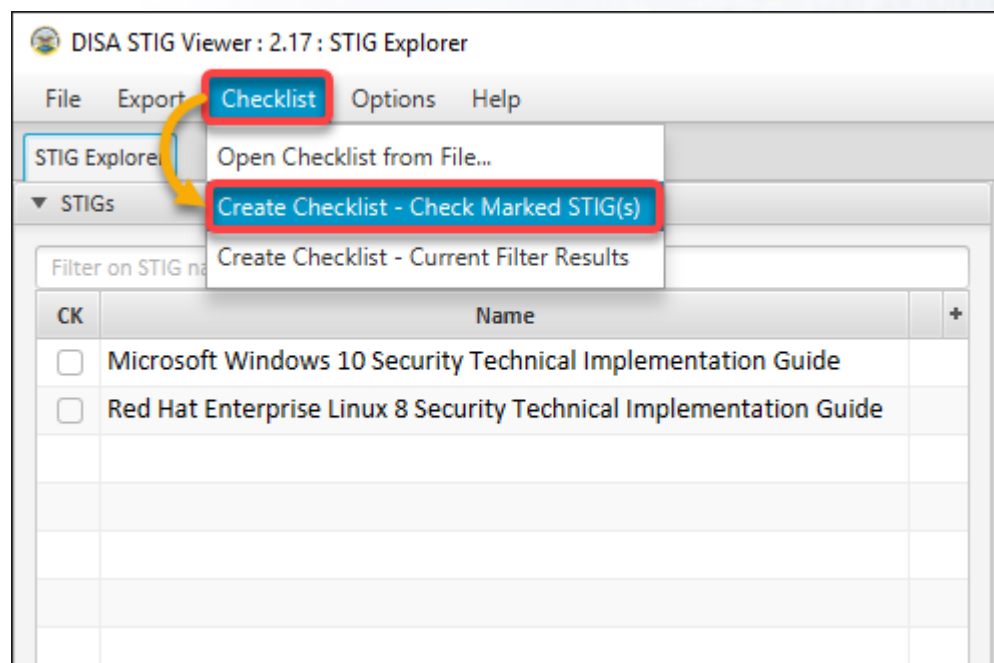
Microsoft Windows 10 Security Technical Implementation Guide :: Version 2. Release: 5 Benchmark Date: 14 Nov 2022

Vul ID: V-220701 **Rule ID:** SV-220701r793197_rule **STIG ID:** WN10-00-000025
Severity: CAT II **Classification:** Unclass **Legacy IDs:** V-63343; SV-77833

Group Title: SRG-OS-000191-GPOS-00080

Rule Title: Windows 10 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously, where ESS is used; 30 days, for any additional internal network scans not covered by ESS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP).

Discussion: An approved tool for continuous network scanning must be installed and configured to run.



DISA STIG Viewer : 2.17 : *New Checklist

File Import Export Options

STIG Explorer *New Checklist X

▼ Totals

Overall Totals CAT I CAT II CAT III

Open: 0 Not Reviewed: 257
Not a Finding: 0 Not Applicable: 0



▼ Target Data

Computing ▼

CUI

Host Name

IP Address

MAC Address

Fully Qualified Domain Name

Target Comments

Get Host Data

Role

- ☒ None
☐ Workstation
☐ Member Server
☐ Domain Controller
☐ Web or Database STIG

Status	Vul ID	Rule ID	Rule Name
NR	V-220697	SV-220697r857...	SRG-OS-000480...
NR	V-220698	SV-220698r857...	SRG-OS-000480...
NR	V-220699	SV-220699r569...	SRG-OS-000480...
NR	V-220700	SV-220700r569...	SRG-OS-000480...
NR	V-220701	SV-220701r793...	SRG-OS-000191...
NR	V-220702	SV-220702r859...	SRG-OS-000185...
NR	V-220703	SV-220703r859...	SRG-OS-000185...
NR	V-220704	SV-220704r859...	SRG-OS-000185...
NR	V-220705	SV-220705r851...	SRG-OS-000370...
NR	V-220706	SV-220706r857...	SRG-OS-000480...
NR	V-220707	SV-220707r793...	SRG-OS-000480...
NR	V-220708	SV-220708r569...	SRG-OS-000080...
NR	V-220709	SV-220709r569...	SRG-OS-000480...
NR	V-220710	SV-220710r569...	SRG-OS-000138...
NR	V-220711	SV-220711r569...	SRG-OS-000118...
NR	V-220712	SV-220712r851...	SRG-OS-000324...
NR	V-220713	SV-220713r569...	SRG-OS-000480...
NR	V-220714	SV-220714r569...	SRG-OS-000095...
NR	V-220715	SV-220715r569...	SRG-OS-000480...
NR	V-220716	SV-220716r569...	SRG-OS-000076...
NR	V-220717	SV-220717r851...	SRG-OS-000312...
NR	V-220718	SV-220718r569...	SRG-OS-000095...
NR	V-220719	SV-220719r569...	SRG-OS-000096...
NR	V-220720	SV-220720r569...	SRG-OS-000095...
NR	V-220721	SV-220721r569...	SRG-OS-000096...

A Look At DISA STIGs (4)

- Firewall Security
Technical
Implementation Guide
- Vulnerability ID: V-3967
- Rule name: The console
port does not timeout
after 10 mins

A Look At DISA STIGs (4)

The screenshot displays the STIG Explorer application interface. The main window is titled "STIG Explorer" and contains several panes:

- STIGs:** A list of STIGs with checkboxes. The "Firewall Security Technical Implementation Guide - Cisco" is selected.
- Filter Panel:** A section for filtering rules. It includes a "Select Filter" dropdown, an "Enter filter keyword" text box, and buttons for "Add", "Inclusive (+) Filter", and "Exclusive (-) Filter". Below this is a table with columns for "+ / -", "Keyword", and "Filter". The table is currently empty, showing "No content in table".
- Rule List:** A table listing rules with columns "Vul ID" and "Rule Name". The rule "V-3967 The console port does not timeout after 10 minutes." is highlighted.
- General Information:** A pane on the right showing details for the selected rule. It includes the title "Firewall Security Technical Implementation Guide :: Release: 22 Benchmark Date: 28 Apr 2017", the rule title "Rule Title: The network devices must time out access to the console port at 10 minutes or less of inactivity.", and the STIG ID "STIG ID: NET1624".
- Discussion:** A section containing text about terminating an idle session within a short time period to reduce the window of opportunity for unauthorized personnel.
- Check Content:** A section with the text "Review the configuration and verify a session using the console port will time out after 10 minutes or less of inactivity." and a note "If console access is not configured to timeout at 10 minutes or less, this is a finding."
- Fix Text:** A section with the text "Configure the timeout for idle console connection to 10 minutes or less."

The rule list table contains the following data:

Vul ID	Rule Name
V-3966	More than one local account is defined.
V-3967	The console port does not timeout after 10 minutes.
V-3969	Network element must only allow SNMP read access.
V-3982	L2TP is terminated in the private network.
V-4382	Authentication required for console access.
V-4619	Firewall is not operating on a STIG'd OS
V-5611	Management connections are not restricted.
V-5612	SSH session timeout is not 60 seconds or less.
V-5613	SSH login attempts value is greater than 3.
V-5646	Devices not configured to filter and drop half-open conn..
V-5731	Perimeter is not compliant with DOD Instr. 8551.1
V-7011	The auxiliary port is not disabled.
V-14637	IPv6 Router Advertisements must be suppressed.
V-14643	Firewall inspection is not performed adequately
V-14644	Firewall must block loopback address
V-14646	Alerts generated at 75% log storage capacity.
V-14647	No FW log dump procedures
V-14648	FA is not informed of critical alerts.
V-14649	FW alert not written to remote console.
V-14653	Audit record must display violation
V-14655	Alerts must remain until acknowledged.
V-14656	FW acknowledge messages must be recorded
V-14667	Key expiration exceeds 180 days.

Showing rule 26 out of 73

A Look At DISA STIGs (4)

- General Information:
 - **Rule Title:** The network devices must time out access to the console port at 10 minutes or less of inactivity
 - **STIG ID:** NET1624
 - **Severity:** CAT II

A Look At DISA STIGs (4)

- Discussion:
 - Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console...

A Look At DISA STIGs (4)

- Discussion...:
 - port that has been left unattended. In addition quickly terminating an idle session will also free up resources committed by the managed network device. Setting the timeout of the session to 10 minutes

A Look At DISA STIGs (4)

- Discussion...:
 - or less increases the level of protection afforded critical network components

A Look At DISA STIGs (4)

- Check Content:
 - Review the configuration and verify a session using the console port will time out after 10 mins or less of inactivity.
 - If console access is not configured to timeout at 10 minutes or less, this is a finding.

A Look At DISA STIGs (4)

- Fix Text:
 - Configure the timeout for idle console connection to 10 minutes or less.

END

A Look At DISA STIGs (3)

- Windows Server 2012 R2 Member Server
 - Import STIG
 - V1099 (Lockout duration)

A Look At DISA STIGs (2)

STIG Explorer

File Export Checklist Options Help

▼ STIGs

CK	Name
☐	MS SQL Server 2014 Database Security Technical Implementation Guide
☐	Firewall Security Technical Implementation Guide - Cisco
☐	Firewall Security Technical Implementation Guide
☐	SharePoint 2010 Security Technical Implementation Guide (STIG)
☐	Windows Server 2008 R2 Member Server Security Technical Implementation Guide
☐	Layer 2 Switch Security Technical Implementation Guide - Cisco
☐	Layer 2 Switch Security Technical Implementation Guide
☒	Windows Server 2012/2012 R2 Member Server Security Technical Implementation Guide

Profile: No Profile

▼ Filter Panel

CAT I CAT I Add

☒ Inclusive (+) Filter ☐ Exclusive (-) Filter

+ / - Keyword Filter

Vul ID ▲	Rule Name
V-1070	Physical security
V-1072	Shared User Accounts
V-1073	Unsupported Service Packs
V-1074	WIN00-000100
V-1075	Display Shutdown Button
V-1076	System Recovery Backups
V-1081	NTFS Requirement
V-1089	Legal Notice Display
V-1090	Caching of logon credentials
V-1093	Anonymous shares are not restricted
V-1097	Bad Logon Attempts
V-1098	Bad Logon Counter Reset
V-1099	Lockout Duration
V-1102	User Right - Act as part of OS
V-1104	Maximum Password Age

A Look At DISA STIGs (2)

Vul ID ▲	Rule Name	+	▼ General Information
V-1070	Physical security		
V-1072	Shared User Accounts		
V-1073	Unsupported Service Packs		
V-1074	WIN00-000100		
V-1075	Display Shutdown Button		
V-1076	System Recovery Backups		
V-1081	NTFS Requirement		
V-1089	Legal Notice Display		
V-1090	Caching of logon credentials		
V-1093	Anonymous shares are not restricted		
V-1097	Bad Logon Attempts		
V-1098	Bad Logon Counter Reset		
V-1099	Lockout Duration		Windows Server 2012/2012 R2 Member Server Security Technical Implementation Guide :: Release: 8 Benchmark Date: 28 Apr 2017 Rule Title: The lockout duration must be configured to require an
V-1102	User Right - Act as part of OS		▼ Discussion The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that an account will remain locked after the specified number of failed logon attempts. A value of 0 will require an administrator to unlock the account.
V-1104	Maximum Password Age		▼ Check Content Verify the effective setting in Local Group Policy Editor. Run "gpedit.msc".
V-1105	Minimum Password Age		Navigate to Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account
V-1107	Password Uniqueness		▼ Fix Text Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy -> "Account lockout duration" to "0" minutes, "Account is locked out until administrator unlocks it".
V-1112	Dormant Accounts		▼ CCI
V-1113	Disable Guest Account		
V-1114	Rename Built-in Guest Account		
V-1115	Rename Built-in Administrator Account		

A Look At DISA STIGs (3)

- Rule Title:
 - The lockout duration must be configured to require an administrator to unlock an account
 - Severity: CAT II

A Look At DISA STIGs (3)

- Discussion:
 - The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that an account will remain locked after the specified number

A Look At DISA STIGs (3)

- Discussion...:
 - of failed logon attempts. A value of 0 will require an administrator to unlock the account.

A Look At DISA STIGs (3)

- Check Content:
 - Verify the effective setting in Local Group Policy Editor.
Run "gpedit.msc".

A Look At DISA STIGs (3)

- Check Content:
 - Navigate to Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy.

A Look At DISA STIGs (3)

- Check Content...:
 - If the "Account lockout duration" is not set to "0", requiring an administrator to unlock the account, this is a finding.

A Look At DISA STIGs (3)

- Fix Text:
 - Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy -> "Account lockout duration" to "0" minutes,

A Look At DISA STIGs (3)

- Fix Text...:
 - "Account is locked out until administrator unlocks it".
- CCI: NIST SP 800-53
Revision 4 :: AC-7 b

END

Security Hardening – Case Study – Win 10

- Windows 10
- DISA, Release 9
 - 28 April 2017

Security Hardening – Case Study – Win 10

STIGVIEWER WINDOW

The screenshot shows the DISA STIG Viewer 2.5.4 application. The interface includes a menu bar (File, Export, Checklist, Options, Help), a STIG Explorer pane on the left, a central table of STIGs, and a right-hand pane for detailed information.

STIG Explorer:

- ☐ Windows Server 2012/2012 R2 Member Server Security Technical Implementation Guide
- ☐ Firewall Security Technical Implementation Guide - Cisco
- ☐ Firewall Security Technical Implementation Guide
- ☐ Windows Server 2012/2012 R2 Domain Controller Security Technical Implementation Guide
- ☐ SOLARIS 10 X86 SECURITY TECHNICAL IMPLEMENTATION GUIDE
- ☐ Oracle Database 11.2g Security Technical Implementation Guide
- ☒ Windows 10 Security Technical Implementation Guide

Profile: No Profile

Filter Panel:

- CATI (selected)
- Inclusive (+) Filter (selected)
- Exclude (-) Filter
- + / -
- Keyword
- Filter

STIG Table:

Vul ID	Rule Name
V-63325	WN10-CC-000315
V-63335	WN10-CC-000330
V-63337	WN10-00-000030
V-63347	WN10-CC-000345
V-63349	WN10-00-000040
V-63351	WN10-00-000045
V-63353	WN10-00-000050
V-63361	WN10-00-000070
V-63377	WN10-00-000100
V-63379	WN10-EM-000005
V-63429	WN10-AC-000045
V-63651	WN10-CC-000155
V-63667	WN10-CC-000180
V-63671	WN10-CC-000185
V-63673	WN10-CC-000190

General Information:

Windows 10 Security Technical Implementation Guide ::
Release: 9 Benchmark Date: 28 Apr 2017

Rule Title: The Windows Installer Always install with elevated privileges must be disabled.

Discussion:

Standard user accounts must not be granted elevated privileges. Enable Windows Installer to elevate privileges when installing applications can allow malicious persons and applications to gain full control of a system.

Check Content:

If the following registry value does not exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Installer\

Security Hardening – Case Study – Win 10

- General Information:
 - **Rule Title:** The antivirus program must be configured to update signature files on a daily basis.
 - **STIG ID:** WN10-00-000046
 - **Severity:** CAT I

Security Hardening – Case Study – Win 10

- Discussion:
 - Virus scan programs are a primary line of defense against the introduction of viruses and malicious code that can destroy data and even render a computer inoperable. Using a virus scan program provides the ability to...

Security Hardening – Case Study – Win 10

- Discussion...:
 - ...detect malicious code before extensive damage occurs. Updated virus scan data files help protect a system, as constantly changing malware is identified by the antivirus software vendors

Security Hardening – Case Study – Win 10

- Check Content:
 - This requirement is NA if McAfee VirusScan Enterprise (VSE) is used. It will be addressed with the corresponding McAfee VSE STIG.
 - Configurations will vary depending on the product.

Security Hardening – Case Study – Win 10

- Fix Text:
 - Configure the antivirus program to update signature files at least daily. Ensure the updates are occurring on timely basis and are not more than a week old.

Security Hardening – Case Study – Win 10

- CCI (Control Correlation Identifier):

- CCI: 000366

The org implements the security config settings.

NIST SP 800-53 :: CM-6 b

NIST SP 800-53A :: CM-6.1 (iv)

NIST SP 800-53

Revision 4 :: CM-6

END

Comparison of CIS Vs DISA

Comparison of CIS Vs DISA

- Many controls are common
- Approaches are different
- Organization styles are different

Comparison of CIS Vs DISA

FEATURE	CIS	DISA
CONTROL COVERAGE	GOOD	EXCELLENT
ORG SUITABILITY	SMALL AND MEDIUM ORGS	LARGE ORGS
USER FRIENDLINESS	GOOD	SATISFACTORY
UNUSABLE TERMINOLOGY	NO	YES
CONTROL DETAIL	GOOD	SATISFACTORY
TOOLS	CAT (COMMERCIAL)	SCAP (MILITARY USE)

Comparison of CIS Vs DISA

FEATURE	CIS	DISA
CONTROL PRIORITIZATION	LEVEL 1, LEVEL 2	CAT I - CAT III
TRACKING EASE	CAT TOOL (COMMERCIAL)	FREE STIG VIEWER (CHECKLIST)
FREQUENCY OF UPDATES	FAIR	QUARTERLY
INDUSTRY CREDIBILITY	HIGH	VERY HIGH
INDUSTRY ADOPTION	HIGH	MODERATE

Comparison of CIS Vs DISA

- How to select CIS/DISA:
 - Size of organization
 - IT infrastructure extent
 - Nature of business
 - Security program goals
 - Maturity of IT & security staff

Comparison of CIS Vs DISA

- Rule of thumb:
 - Smaller orgs use CIS
 - Larger orgs use DISA
 - CIS is part of Homeland Security, DISA is part of US Military
 - DISA more frequently updated and maintained with wider coverage

END

ISMS:Leading InfoSec Governance Framework

- ISO27001:2013 (ISMS)
 - Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system
 - Ten short clauses
 - Long annex

ISMS:Leading InfoSec Governance Framework



ISO27001:2013 MANDATORY CLAUSES

Reference		Description
Mandatory	Clause 4	Context of the organization
	Clause 5	Leadership
	Clause 6	Planning
	Clause 7	Support
	Clause 8	Operation
	Clause 9	Performance evaluation
	Clause 10	Improvement

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISMS:Leading InfoSec Governance Framework



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 113

ISMS:Leading InfoSec Governance Framework

- Merits of ISO27001:2013 (ISMS):
 - Exceptional framework with comprehensive coverage of mandatory requirements (clauses 4-10) and discretionary controls (annex)

ISMS:Leading InfoSec Governance Framework

- Merits of ISO27001:2013 (ISMS):
 - Highly beneficial as a framework for security program
 - Covers all domain areas
 - Provides a structure and organized sequence for security controls

ISMS:Leading InfoSec Governance Framework

- Merits of ISO27001:2013 (ISMS):
 - Complements security transformation model as serves as a reference and guideline for activities and controls

ISMS:Leading InfoSec Governance Framework

- **De-merits of ISO27001:2013 (ISMS):**
 - Very broad
 - Generic framework – leaves it to organization how to implement the measures and controls
 - Not suited for orgs that are new to security program

ISMS:Leading InfoSec Governance Framework

- How to best use advantages of ISO27001:2013 (ISMS):
 - Implement security transformational model
 - Cap off security transformation project with ISO27001:2013 (ISMS) certification

ISMS:Leading InfoSec Governance Framework

- How to best use advantages of ISO27001:2013 (ISMS):
 - ISMS as a complementary reference and checklist rather than main framework