



Background

Security Technical Implementation Guides (STIGs) are published by the Defense Information Systems Agency (DISA) and provide configuration standards for DoD systems and software, including Operating Systems, Database Management Systems, etc. The Risk Management Framework (RMF) requires DoD information systems to comply with all applicable STIGs.

Training Overview

STIG 101™ is designed to answer core questions and provide guidance on the implementation of STIGs. Students will gain a conceptual understanding of DISA STIGs as well as *hands-on implementation experience* in a virtual “lab” environment. The **STIG 101** curriculum leverages BAI’s extensive experience as a provider of RMF consulting services.

STIG 101 topics include:

- STIG Overview
- Best Practices
- STIG Content
- SCAP Compliance Checker (SCC)
- STIG Viewer
- “How To”
- Resources

Prerequisites

A prerequisite to this course is a strong understanding of technology and system configuration.

Who Should Attend

STIG 101 is open to all students (government and contractors) with an interest in learning about STIGs.

Students who have not yet attended RMF training are encouraged to inquire about discounted pricing for a training “bundle” that includes the **RMF for DoD IT** Full Program (four days) and **STIG 101**.

Delivery Methods

STIG 101 is offered on a regular basis as an online, instructor-led class, using our Online Personal Classroom™ technology.

STIG 101 is also available as a “Friday supplemental class” to organizations wishing to obtain on-site or online RMF training for a “private group” of students.

Learn More

For additional information on **STIG 101** training, or to register for an upcoming class, please call BAI at 1-800-RMF-1903 (763-1903) or visit <https://register.rmf.org>.

STIG 101 – One-Day Course

- Getting Started
- STIG Overview
- Best Practices
- SCC
- STIG Viewer
- Common Pitfalls
- STIG Tools
- Resources & Summary
- Hands-on activities in virtual “Lab” environment



Home | Cybersecurity Training | Topic Map | STIGs | Tools | News | Help | RSS Feeds

STIGs Home

- Control Correlation Identifier (CCI)
- DoD Annex for NIAF Protection Profiles
- DoD Secure Host Baseline Repository *PKI
- FAQs
- Group Policy Objects
- Quarterly Release Schedule and Summary
- SRG/STIG Tools
- SRG-STIG Library Compilations
- STIG Mailing List
- STIGs Master List (A to Z)
- STIGs Technologies
- Vendor Process
- Contact Us

*PKI - DoD PKI Cert Required

Security Technical Implementation Guides (STIGs)

STIGs Updates!

- Router SRG Version 3 - Update 2/12/2018
- Group Policy Objects (GPOs) - January 2018 - Update 2/7/2018
- Backbone Transport Services (BTS) Policy STIG Version 3 *PKI - Update 2/7/2018
- Draft McAfee Endpoint Security (ENS) STIG Version 1, Release 0.1 *PKI - Update 2/7/2018
- Microsoft Windows Privileged Access Workstation (PAW) STIG Version 1 - Update 2/7/2018
- McAfee MOVE AV 4.5 STIG Version 1 Overview - Update 1/17/2018
- McAfee MOVE AV Agentless 4.5 STIG Version 1 - Update 1/17/2018
- McAfee MOVE AV Multi-Platform 4.5 STIG Version 1 - Update 1/17/2018

The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

Questions or comments?
Please contact DISA STIG Customer Support Desk:
disa.stig_spl@mail.mil

DISA STIG Viewer: 2.6

File | Import | Export | Options

STIG Explorer: 2018-02-20 X

▼ Totals

Overall Totals	CAT I	CAT II	CAT III
Open:	67	Not Reviewed: 0	
Not a Finding:	559	Not Applicable: 113	

Not a Finding | Open | Not Applicable | Not Reviewed

▼ Target Data

Computing

Host Name: IP Address: MAC Address: Fully Qualified Domain Name: Get Host Data

Role

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

► STIGs

- Technology Area
- Filter Panel

Status: Vul ID Rule Name

NF	V-2225	WG370
NF	V-2230	WG420
NF	V-2232	WG050
NF	V-2234	WG040
NF	V-2236	WG080
NF	V-2242	WA060
NF	V-2243	WA070
NF	V-2246	WG190
NF	V-2247	WG200
NF	V-2248	WG220
NF	V-2251	WG130
NF	V-2255	WG270
NF	V-2256	WG280
NF	V-2257	WA120
NF	V-2259	WG390
NF	V-2261	WG330
NF	V-2271	WG440
NF	V-6485	WA140
NF	V-6577	WG204
O	V-6724	WG520
NF	V-13613	WA230
NF	V-13620	WG355
NF	V-13621	WG385
NF	V-13672	WG145
NF	V-13724	WA000-WWA0...
NF	V-13725	WA000-WWA0...

Showing rule 1 out of 739

General Information

APACHE SERVER 2.2 for Unix Security Technical Implementation Guide :: Release: 9 Benchmark
Date: 27 Oct 2017

Rule Title: MIME types for csh or sh shell programs must be disabled.

STIG ID: WG370 A22
Rule ID: SV-36309r2_rule
Vuln ID: V-2235

Severity: CAT II
Class: Unclass

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

Vuln Information

Discussion | Check Content | Fix Text

Finding Details

These files do not exist.

Comments