

Configuration Auditing in SecureVue® using DISA Secure Technical Implementation Guides (STIGs)

Solution Brief

DISA STIGs and Information Assurance

As part of its information assurance-focused mission, the Defense Information Systems Agency (DISA) has established a series of Security Technical Implementation Guides (STIGs) to ensure secure configurations across federal systems, including operating systems, network devices such as routers and firewalls, databases, and both enterprise and desktop applications. Based around the information security “triad” – confidentiality, integrity, and availability – and updated frequently to reflect the ever-changing need for information assurance through continuous vigilance, DISA STIGs are mandatory for many federal agencies and military branches.

Today's STIG Audits: Time-Intensive and Resource-Heavy

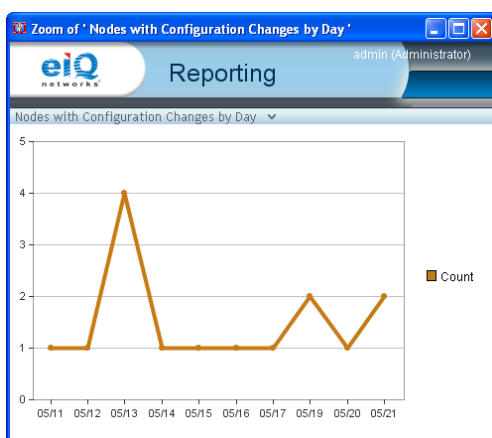
Historically, agencies have had difficulty implementing DISA STIG standards across the enterprise, primarily due to the detailed nature and broad applicability of STIGs. Although DISA's Field Service Office (FSO) provides both STIG content and supporting tools to implement the standard -- such as DISA "Gold Disks" - agencies and branches of the military have struggled with the details of technical implementation of STIGs and spend an inordinate amount of time in the STIG evaluation process using manual auditing tools.

Now, eIQnetworks' SecureVue platform – the first unified situational awareness platform designed specifically for **fast, automated compliance management and auditing** – federal agencies can quickly and easily ensure consistent, continuous compliance with DISA STIGs, achieve rapid certification and accreditation (C&A) and ensure situational awareness across the enterprise.

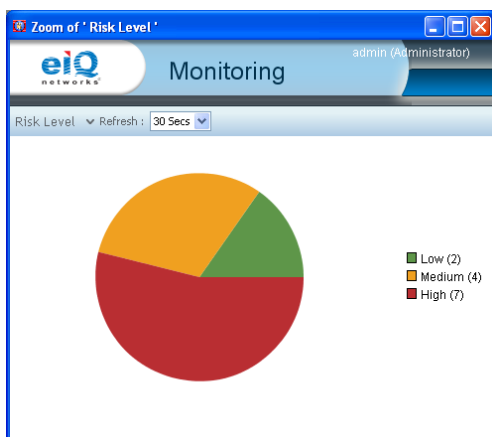
Information Assurance through Situational Awareness

The SecureVue platform provides a complete solution for DISA STIG compliance. As a platform that delivers true unified situational awareness, SecureVue is optimally designed for STIG audits by providing:

- **Single STIG Audit Platform for both Hosts and Devices.** Unlike some STIG audit tools that are limited to only network devices -- such as routers, switches and firewalls - or only hosts like Windows, UNIX and Linux, SecureVue provides a complete library for STIG auditing of both hosts and devices, as well as common applications and database platforms.
- **Secure, Comprehensive STIG Auditing.** SecureVue provides secure, end-to-end and complete STIG auditing, with direct one-to-one correlation against each and every control in each supported STIG -- including non-technical controls!
- **Agentless Technology.** SecureVue is completely agentless, and consequently, can effectively monitor the full range of IT assets.
- **Achieve a Common Operating Picture (COP) of Your Environment.** By providing detailed visualization of STIG controls compliance by operating location, enclave, network and theater, SecureVue ensures that all appropriate personnel -- from information assurance professionals through commanders - have comprehensive visibility of compliance and asset readiness.



SecureVue provides historical context of system changes related to DISA STIG compliance



SecureVue provides real-time visibility of system risk to support situational awareness across the enterprise

SecureVue provides complete DISA STIG audit capabilities through advanced features:

- **Agentless Technology.** No software is required for deployment to any managed systems.
- **Command-and-Control Centralized Management.** All systems are managed on a centralized console with access managed through full role-based access control.
- **Built-In Common Controls Library.** SecureVue ships out-of-box with over 2,500 common technical controls for Windows, UNIX, Linux, Cisco IOS, and other platforms. Users can create additional controls and map them directly to DISA STIGs or any other compliance policy.
- **Scheduled and Ad Hoc Reporting.** Over fifty out-of-box DISA STIG configuration reports are available, and can be run on-the-fly or scheduled for delivery via e-mail. Supported report formats include PDF, XLS, CVS, and others.

- **Regular STIG Updates and SCAP-Based Content.** eIQnetworks continuously monitors and updates DISA STIGs benchmarks as they are released, ensuring that federal customers can conduct C&A activities based on the most up-to-date security requirements. STIG content is also available through SCAP-based sources, including DISA.

- **Major Certification & Accreditation Standards.** SecureVue has been validated under a number of stringent federal standards, including NIST FIPS 140-2, Level 2, NIAP Common Criteria, and SCAP (*pending*). Additionally, SecureVue is listed on the DISA Unified Capability (UC) Approved Product List (APL) and maintains a current US Army Certificate of Networthiness (CON).
- **Flexible Output Options.** SecureVue can output reports, raw data and summary data in a broad range of human- and machine-readable formats. Without programming, reports can be generated in PDF, HTML, CSV, TXT, XLS and DOC formats. Using a simple, straightforward XML API, SecureVue can output raw data and summary data in machine-readable XML streams.

Section	Control	Rule	Status
3.7.1.3 Internet Communication Management and I...	(3.083) V0003471 (A) Error Reporting - Report Errors	Report Errors	OK
3.7.1.4 Logon	(3.067) V0003470 (A) Logon - Always Wait for the Network at Computer Startup and Logon	Wait for Network at Logon and Startup	VIOLATION
3.7.1.5 Remote Assistance	(3.068) V0003443 (A) Remote Assistance - Offer Remote Assistance	Allow Unsolicited Help	OK
3.7.1.6 Windows Time Service	(3.084) V0003472 (A) Windows Time Service - Configure Windows NTP Client	Windows NTP Service Time Server	OK
3.7.1.7 Internet Explorer	(5.032) V0003431 (A) IE - Disable Automatic Install of Internet Explorer Components	Disable Automatic Install of IE Components	OK
	(5.033) V0003432 (A) IE - Disable Periodic Check for Internet Explorer Software Updates	Disable Periodic Check of IE Updates	OK
	(5.034) V0003433 (A) IE - Disable Software Update Shell Notifications on Program Launch	Disable Software Update Shell Notifications on Program Launch	OK
	(5.031) V0003430 (A) IE - Make Proxy Settings Per Machine	Make Proxy Settings Per Machine	OK
	(5.030) V0003429 (A) IE - Security Zones - Do Not Allow Users to Add/Delete Sites	Do Not Allow Users to Add or Delete Sites	OK
	(5.029) V0003428 (A) IE - Security Zones - Do Not Allow Users to Change Policies	Do Not Allow Users to Change Policies	OK
	(5.028) V0003427 (A) IE - Security Zones - Use Only Machine Settings	Use Only Machine Settings	OK
3.7.1.8 NetMeeting	(5.027) V0003426 (A) NetMeeting - Disable Remote Desktop Sharing	Disable Remote Desktop Sharing for NetMeeting	OK
3.7.1.9 Terminal Services	(5.041) V0003452 (A) Terminal Services - Do Not Allow Local Administrators to Customize P...	Do Not Allow Local Administrators to Customize Permissions	OK
	(5.039) V0003450 (A) Terminal Services - Limit Number of Connections	Limit Number of Connections	OK
	(5.038) V0003449 (A) Terminal Services - Limit Users to One Remote Session	Limit Users to One Remote Session	OK
	(3.066) V0003341 (A) Terminal Services - Remote Control Settings	Remote Control Settings	OK
	(5.042) V0003453 (A) Terminal Services - Always Prompt Client for Password Upon Connec...	Always Prompt Client for Password Upon Connection	OK
	(5.043) V0003454 (A) Terminal Services - Set Client Connection Encryption Level	Set Client Connection Encryption Level	OK
	(5.103) V0004447 (A) Terminal Services - Secure Server	Secure Server	OK
	(5.048) V0003459 (A) Terminal Services - Allow Reconnection from Original Client Only	Allow Reconnection from Original Client Only	VIOLATION
	(5.047) V0003458 (A) Terminal Services - Set Time Limit for Idle Sessions	Maximum Time for Idle Sessions	OK
	(5.046) V0003457 (A) Terminal Services - Set Time Limit for Disconnected Sessions	Maximum Time for Disconnected Sessions to Reconnect	OK
	(5.049) V0003460 (A) Terminal Services - Terminate Session When Time Limits are Reached	Terminate Sessions When Time Limit Reached	VIOLATION

SecureVue comes with complete DISA STIG policy maps and provides automatic identification of compliance with individual sections and standards within each STIG

Save Up to 90% in STIG Audit Costs with SecureVue

eIQnetworks maintains a comprehensive, fully-tested library of DISA STIG content across network and security devices, host operating systems, applications and databases. Currently supported STIGs include:

- Microsoft Windows® XP and Windows 7
- Microsoft Windows Server 2003 and 2008
- Sun (now Oracle) Solaris®
- Red Hat® Enterprise Linux®
- IBM AIX®
- VMware ESX Server®
- Cisco® Firewalls & Routers
- CheckPoint® Firewalls
- Microsoft® SQL Server (multiple versions)
- Oracle® Database Server (multiple versions)

In addition, SecureVue can read any SCAP-based content file and create a policy from the data.

Discover how SecureVue dramatically lowers DISA STIG compliance costs, while increasing compliance and minimizing the impact on personnel. Contact us at +1 877.564.7787 or email sales@eIQnetworks.com to learn more.



eIQnetworks
 31 Nagog Park
 Acton, MA 01720
 t. +1 978.266.9933
 f. +1 978.266.0004
www.eIQnetworks.com

© 2012, eIQnetworks, Inc. eIQnetworks, the eIQnetworks logo and SecureVue are registered trademarks of eIQnetworks, Inc. All other trademarks, servicemarks, registered trademarks or registered servicemarks are the property of their respective owners. All rights reserved.