POWERSTRUX™
Suite of Tools

POWERSTRUX | SUITE OF TOOLS

ACAS Validator

Introduction | August 27, 2026

Justin Sylvester · CISO & Lead Cyber Engineer, SecureStrux

SecureStrux Introduction

Cyber Network Defense

Comprehensive cyber network defense addressing compliance frameworks across commercial and defense sectors.

Specialized Consulting

Expert consulting and implementation across CORA, SIPRNet, RMF, and CMMC.

Certified & Accredited

Certified CMMC C3PAO, with ISO 9001:2015 and ISO 27001 certifications.

Who We Are

Premier cybersecurity firm serving Federal Defense and Critical Infrastructure industries.

Headquarters

Lancaster, PA. Registered as a Small Business for federal contracting.

DoD Heritage

Deep roots in DoD cybersecurity, engineering, cloud and support services on SIPR and JWICS networks.

Cleared Personnel

TS facility clearance, with over 80% of personnel cleared.

Past Performance

Multiple prime and sub federal contracts with strong past performance ratings.

About Me

Justin Sylvester

CISO & Lead Cyber Engineer

Certifications

CISSP | CCSP | GPEN | CEH | SEC+

AWS Certified – Security Specialty

Security Interests

Azure Sentinel | Vulnerability Management

Amazon Web Services (AWS) | Microsoft Azure

PowerShell

Introduction to PowerStrux®

PowerStrux is a suite of monitoring tools that track system and user activity on isolated networks.

POWERSTRUX
Suite of Tools

Windows Auditor

Monitors system and user activity across Windows systems.

Linux Auditor

Delivers the same visibility for Linux environments.

Active Directory Auditor

Tracks changes across an Active Directory environment.

ACAS Validator

Automates compliance validation for ACAS deployments against CORA and best-practice requirements.

From Assessment to Automation

Common Problems

Manual ACAS assessments are often:

- Time intensive
- Prone to human error
- Inconsistent between assessors
- Difficult to scale

Assessing Scan Fidelity

Eliminating blind spots relies on ensuring that no plugins applicable to the target system report access failures.

Plugin ID	Plugin Name	Indication
110095	Target Credential Issues by Authentication Protocol - No Issues Found	Good Access
117886	OS Security Patch Assessment Not Available	Good/Bad Access
21745	Authentication Failure - Local Checks Not Run	Bad Access
110723	No Credentials Provided	Bad Access
117885	Authentication Success with Intermittent Failure	Bad Access
110385	Authentication Success Insufficient Access	Bad Access
104410	Authentication Failure(s) for Provided Credentials	Bad Access
102094	SSH Commands Require Privilege Escalation	Bad Access
24786	Nessus Windows Scan Not Performed with Admin Privileges	Bad Access
26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	Bad Access
10428	Microsoft Windows SMB Registry Not Fully Accessible Detection	Bad Access

Lessons Learned from Real-World Deployment

01

Asset Discovery is Not Asset Management

Scanners identify assets.

Asset inventories validate completeness.

02

Credential Success Matters

Authentication success does not equal sufficient access.

Review validation plugins regularly.

03

Simplicity Scales

Standard naming conventions.

Standard policies.

Standard schedules.

04

Measure Quality, Not Quantity

Number of vulnerabilities is not a success metric.

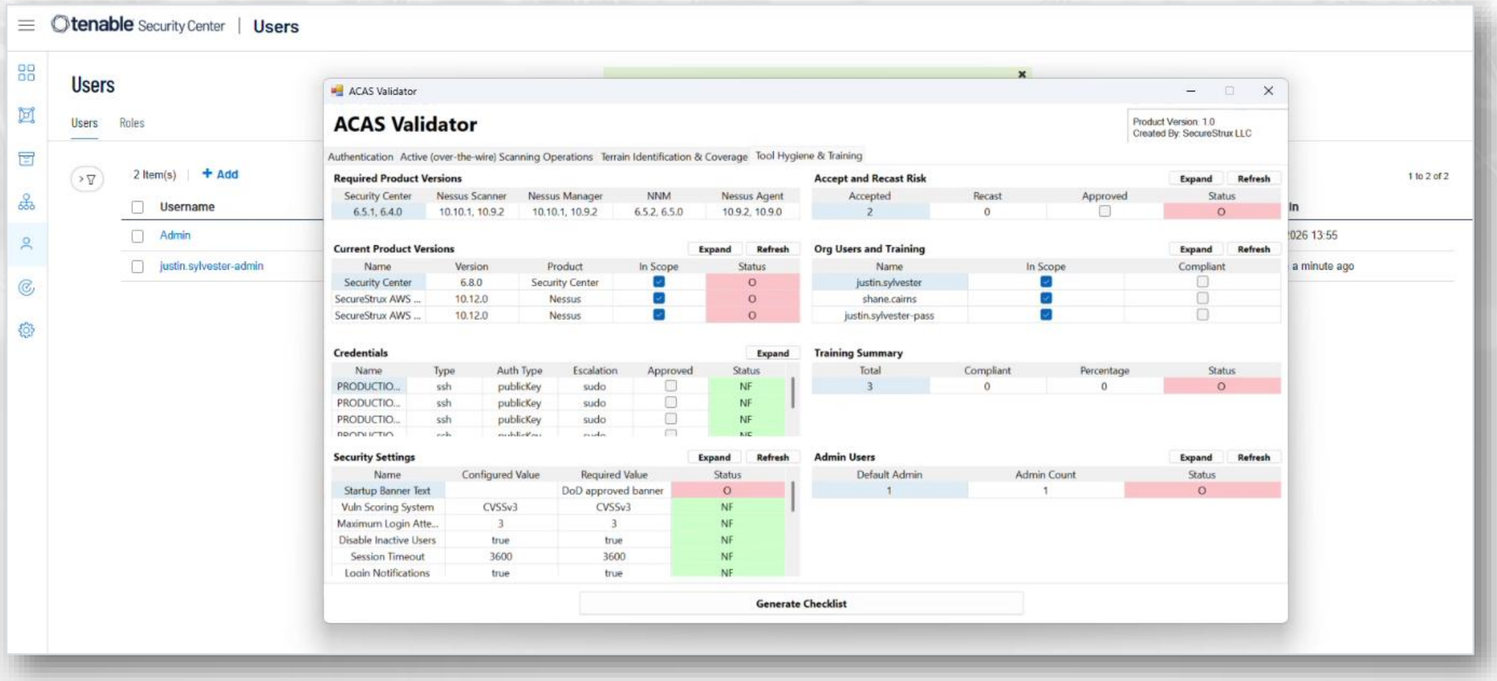
Scan fidelity is a success metric.

Introducing PowerStrux ACAS Validator

Purpose

Automate the collection and validation of ACAS configuration data against TASKORD requirements.

- Faster assessments
- Consistent results
- Reduced manual effort
- Repeatable methodology



Assessment Areas Evaluated

Active (Over-the-Wire) Scanning Operations

- Authentication Success & Scan Fidelity
- Scan Policy Compliance
- Vulnerability Assessments
- Configuration Audits
- Discovery Operations

Terrain Identification & Coverage

- Repository Coverage Validation
- Scan Zone Alignment
- Scan Scope & Asset Coverage

Scanning Tool Hygiene & Operator Training

- Product Version Compliance
- Credential Management & Validation
- Security Center Configuration Review
- Risk Acceptance & Recast Rule Governance
- Administrative Access Review
- ACAS Training & Certification Compliance

Lessons Learned While Building the Tool

1

Consistency Matters

Organizations struggle more with configuration consistency than with vulnerability detection.

2

Validation Beats Assumptions

Many environments appear compliant until schedules, repositories, credentials, and policies are validated.

3

Automation Enables Scale

Assessment automation lets engineers focus on remediation rather than evidence collection.

Key Takeaways

1

Coverage

You cannot secure assets you do not know exist.

2

Accuracy

Credentialed scans provide the most reliable results.

3

Consistency

Standardized policies and schedules improve repeatability.

4

Validation

Review access validation plugins before reviewing findings.

5

Prioritization

CVSS is important, but risk extends beyond severity.

6

Automation

Automate evidence collection so engineers can focus on reducing risk.

Before we jump into Q&A…

The next webinar in our webinar series will be Thursday, October 8th

SIPRNet

1PM EDT

Q&A

Justin Sylvester

CISO & Lead Cyber Engineer, SecureStrux

justin.sylvester@securestrux.com