# SecureGap Scanning Guide

## SecureGap Standard User Guide for STIG Policy Audits, Windows Log Audits, and Vulnerability Assessment

V1.5

August 5, 2024

**Prepared by:**

Alejandra Del Valle, Sako Sahakian, Karthik Sundaram, and Nikola Popovic

# Document Revision History

| Release Date | Version | Modifier Name | Description |
|---|---|---|---|
| 12 July 2024 | V 1.0 | Nikola Popovic | Initial Draft - created the outline for the user guide and major section structure. |
| 20 July 2024 | V 1.1 | Sako Sahakian | Updated scanning guidelines to include detailed information on STIG procedures. |
| 23 July 2024 | V 1.2 | Nikola Popovic | Updated the software logo and created more detailed information on vulnerability and compliance. |
| 1 August 2024 | V 1.3 | Karthik Sundaram | Adjusted Installation Instructions to provide clarity and dependency instructions. |
| 4 August 2024 | V 1.4 | Alejandra Del Valle | Updated the Setup and Scheduling Scans sections to improve clarity and readability. Reformatted steps into numbered lists for easier navigation. Enhanced detail in scan setup instructions and simplified language for user accessibility. |
| 5 August 2024 | V 1.5 | Nikola Popovic | Added support contact information and common troubleshooting steps for end-points. |

# Document Properties

**Owner:** SecureGap

**Document Owner:** Nikola Popovic

**Approval:** Alejandra Del Valle, Sako Sahakian, Karthik Sundaram

**Discrepancies**: Please report any corrections to support@securegap.us

# Table of Contents

# 1 Introduction

## 1.1 Purpose

This document is intended to provide basic user guide instructions for cybersecurity professionals and systems administrators responsible for auditing and securing air-gapped enclaves and systems of various classification levels, in accordance with established industry standards and government policies.

## 1.2 System Requirements

1. SecureGap variants affected by this guide:
   a. SecureGap 1.0
2. Minimum recommended hardware requirements for SecureGap:
   a. **CPU:** At least one 2 GHz core
   b. **Memory:** 4GB of RAM
   c. **Disk space:** 1 GB, not including any space used by the host operating system
3. System requirements before the beginning the installation process:
   a. C++ installation
   b. Windows Server 2019 or later; Windows 10 or later

# 2 First Time Installation of SecureGap

## 2.1 Preparing the Endpoint and Installing SecureGap

To prepare the targeted endpoint for SecureGap installation, ensure you have top-level administrator access, which will allow you to install the software. Follow these steps to install the software:

1. Obtain the necessary access and associated credentials for the endpoint.
2. Obtain the SecureGap installation file (SecureGap.zip) on your preferred and authorized media storage.
3. Log into the Windows environment with privileged credentials.
4. Verify C++ is available on the endpoint.
5. Place the SecureGap.zip installation file in any directory on the targeted endpoint.
6. Unzip the package.
7. Run installer.exe in administrator mode.

## 2.2 Preparing SecureGap for Compliance Scans

### 2.2.1 Dashboard Function

The dashboard serves as a top-level information tool that displays several critical application elements of the application:

1. **Last Compliance Scan:** Displays the time and date of the previous time the compliance scan successfully ran and produced a system administrator report.
2. **Next Scheduled Scan:** Displays the time and date for the upcoming scheduled scan.
3. **Refresh Button:** Used to update the display information for the last successful scan and the next scheduled scan.
4. **Run Compliance Scan Button:** Directs users to the Compliance Scan section of the application to configure and initiate scans.
5. **Application Status:** Displayed in the bottom left corner of the application window. A “Ready” status indicates that the application is prepared to conduct scans.
    a. **Note:** The application status will change as the scans are conducted and the application performs critical tasks.

### 2.2.2 Compliance Scan Function Description

This section of the application is dedicated to configuring the following types of scans: STIG (Security Technical Implementation Guide) Policy Audit, Vulnerability Scan, and Windows Log Audit.

1. **STIG Policy Audit:** This process involves reviewing and assessing the compliance of systems, software, and configurations against the Security Technical Implementation Guides (STIGs). STIGs are a set of policies and best practices developed by the DISA (Defense Information Systems Agency) to enhance the security of information systems utilized by the DoD (Department of Defense), subordinate agencies, and contracting partners.
   Main objectives of the STIG policy audit:
    a. Compliance Verification
    b. Risk Assessment
    c. Remediation
    d. Documentation and Reporting

2. **Vulnerability Scan:** Identifies, assesses, and reports on potential security vulnerabilities within systems, networks, or applications.
   Main objectives of the vulnerability scans:
   a. Detection of vulnerabilities, including outdated software, missing patches, and insecure protocols
   b. Risk Assessment
   c. Intrusion Prevention
   d. Compliance and Reporting
   e. Security Monitoring
   f. Incident Response
3. **Windows Log Audit:** Records and stores various events related to security, system, application, and setup within Windows environments.
   Main objectives of the Windows log audit:
   a. Security Auditing
   b. System Monitoring
   c. Compliance
   d. Forensic Investigation
   e. User Activity Tracking (Insider Threat Mitigation)

## 2.3 Setting Up Scans

This section details how to configure the application to conduct the three types of scans, store report files and enter the required credentials.

### 2.3.1 STIG Policy Audit Setup

1. In the menu bar, click on **Compliance Scan.**
2. Select **STIG Policy Audit** from the list of scans.
3. Under **Select files to import**, click on **STIG Policy Audit.**
4. Windows Explorer will open, allowing you to browse to the location of the latest STIG audit file.
5. Select the desired XCCDF STIG file in XML format.
6. Under **Select a profile**, choose the audit profile based on the system classification and audit requirements as outlined by your organization's cybersecurity management guidelines, approved by the security management staff
7. Under **Select where to save your report**, click on **Browse** and choose the directory to save the report.
8. Click on **Start Scan** to initiate the STIG Policy Audit.

### 2.3.2 Vulnerability Scan Setup

1. In the menu bar, click on **Compliance Scan.**
2. Select **Vulnerability Scan***.*
3. Under **Select files to import***,* click on **Vulnerability Scan.**
4. Windows Explorer will open, allowing you to browse to the location of the desired opal files.
5. Select the desired opal audit file.
6. Under **Select where to save your report,** click on **Browse** and choose the directory to save the report.
7. Click on **Start Scan** to initiate the Vulnerability Scan.

### 2.3.3 Windows Log Audit Setup

1. On the menu bar, click on **Compliance Scan.**
2. Select **Windows Log Audit***.*
3. A window will prompt you to enter:
    a. **Target IP:** Enter localhost or the IP address of the endpoint you want to scan.
    b. **Admin Username:** Enter the admin username required for conducting scans (privileged Kernel access required).
    c. **Admin Password:** Enter the admin password.
    d. Under **Select where to save your report***,* click on **Browse** and choose the directory to save the report.
    e. Click on **Start Scan** to initiate the Windows Log Audit scan.

## 2.4 Schedule Scan Function

This section explains how to set the periodicity of scans and adjust it as necessary.

### 2.4.1 Schedule Compliance Scans

1. Navigate to **Schedule Scan** on the menu.
2. You will have three options for scheduling:
    a. **Add New Schedule:**
        i. Enter the Scan Type, Frequency, and Next Run Date.
        ii. Once all fields are populated, click **OK***.*
        iii. The newly scheduled scan will appear in the **Scheduled Compliance Scans** field.

   b. **Edit Selected:**
      i. Click on a previously scheduled scan instance. Once selected, the instance will turn blue to indicate the selection.
      ii. Click on **Edit Selected.**
      iii. Adjust Scan Type, Frequency, Next Run Date fields.
      iv. Once all fields are adjusted, select **OK.**
   c. **Delete Selected:**
      i. Click on a previously scheduled scan instance. Once selected, the instance will turn blue to indicate the selection.
      ii. Click on **Delete Selected.**
      iii. Confirm the deletion by clicking ***Yes*** when prompted by the application.
3. The following scheduled scan in sequence will appear on the dashboard

# 3 Help Function

This section will describe help function menu options.

## 3.1 User Guide

This section contains this document itself, designed to provide users with a comprehensive overview of how to utilize all the features of the software effectively.

## 3.2 Tutorial

The tutorial is available on our website and includes detailed, step-by-step instructions on how to set up and perform essential scan functions. It is designed to help both new and experienced users maximize the capabilities of the software. Access the tutorial at **www.securegap.us**.

## 3.3 Support

This section provides essential contact information for technical support, enabling users to resolve issues efficiently. To reach the customer support please email us at: support@securegap.us

### 3.3.1 Remote Endpoints Troubleshooting Steps

1. Enable PS Remoting
2. Enable-PSRemoting - Force

3. Please ensure the firewall allows the following connections to ensure the scanner can access the remote machine
    a. Configure the firewall to allow WinRM traffic, WinRM typically operates on the following ports:
        i. HTTP: Port 5985 (default for unencrypted communication)
        ii. HTTPS: Port 5986 (default for encrypted communication)

## 3.4 About

This section contains basic information about the product, helping users understand the software’s background and purpose. Users should review the EULA carefully to understand their rights and responsibilities when using the software.

# 4 Reporting

This section will describe the report function and interpretation.

## 4.1 STIG Scan Report

STIG Report contains information on the system configuration and evaluates the severity of exposure by assigning criticality value. Administrators and security professionals can prioritize which configuration settings should be mitigated in order of severity.

## 4.2 Vulnerability Report

Future capability that will assign the risk score and mitigation instructions for both STIG assessment and software vulnerability assessment.

## 4.3 Windows Log Report

This report contains Windows security, session, and event logs. It is used for informational purposes and user tracking. An auditor must evaluate findings and take appropriate action. The report is produced in PDF format for easy storage and archiving for future audits.