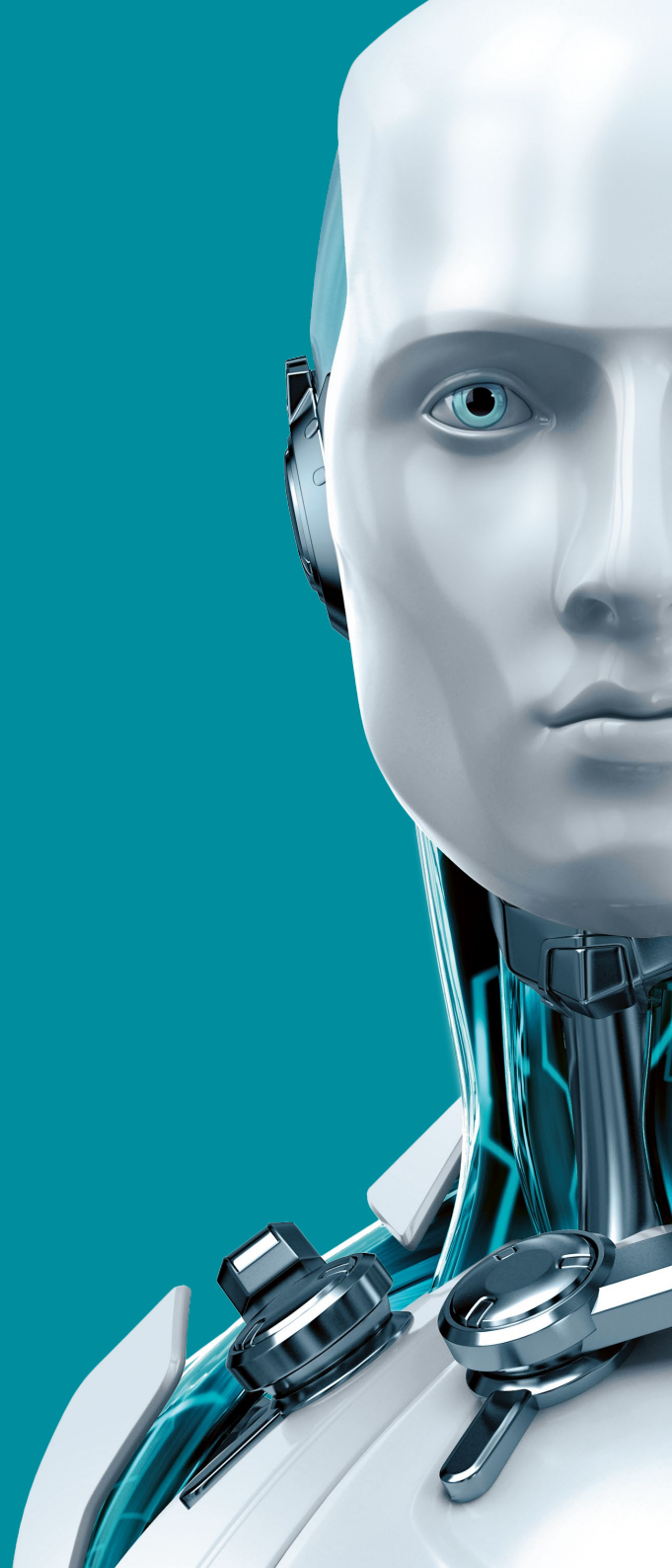
FLEXERA SOFTWARE

Patch Management

Corporate Software Inspector
System Requirements

BUSINESS

ESET TECHNOLOGY ALLIANCE



FLEXERA SOFTWARE

Patch management with Corporate Software Inspector

Corporate Software Inspector gives you the when, where, what and how of security patching. It tells you when a software vulnerability with an available patch is threatening your infrastructure, where it will have the most critical impact, what the right remediation strategy is and how to deploy it.

Secunia Research continuously verifies vulnerabilities and the effectiveness of the patches published by the vendors. This intelligence is then matched to your infrastructure, making it possible to prioritize, plan and execute workflows, and document your risk reduction efforts.

Requirements

Corporate Software Inspector (CSI) 7.0 System Requirements

CSI 7.0 is a web based solution. It is fully functional from the latest version of Internet Explorer. Scan results can also be viewed from other browsers.

CSI 7.0 is a Vulnerability and Patch Management Software Solution that completes and targets the Patch Management process. It combines Vulnerability Intelligence, Vulnerability Scanning, and Patch Creation with Patch Deployment Tool Integration to enable targeted, reliable, and cost-efficient Patch Management.

To use CSI 7.0 console your system should meet the following requirements:

- Min resolution: 1024x768
- The latest version of Internet Explorer (Scan results can also be viewed from other browsers) Internet connection capable of connecting to https://csi7.secunia.com
- First-Party cookie settings at least to Prompt (in Internet Explorer) Allow session cookies
- A PDF reader (for example, Adobe Reader) – optional

CSI 7.0 with Scanning and Patching Capabilities

To successfully scan and create updates the following should also be present when using CSI:

- Internet Explorer 8 or later with the CSI Plugin WSUS installer (Administration console only) Visual C runtime
- Microsoft .NET Framework runtime 4 or later
- If the WSUS Self-Signed Certificate is going to be used, and the user wishes to provision the certificate through the Patching > WSUS/SCCM > Deployment function, Remote Registry service must be enabled on the clients
- Select the target hosts where the certificate is to be installed (CTRL+ mouse click for multiple selection), right-click and select Verify and Install Certificate

The Dashboard provides an overview of your hosts with the help of various „portlets". Portlets are a collection of components that graphically display key data and allow you to create profiles which can display a unique combination of portlets.

Download and Install CSI Plugin

The first time you login to CSI, click the link on the bottom of the page and follow the on-screen instructions to download and install the CSI Plugin to enable scanning and patching. Please note that the plugin is compatible with, and should be run using, the latest version of Internet Explorer.

The CSI Plugin is installed locally and must be installed on the machine you are running CSI console from. Once the CSI Plugin has been installed the download link is removed from the page.

Download and Install the Secunia Daemon

The Secunia Daemon is a stand-alone executable that executes the scanning and import schedules configured in CSI console. It runs as a background service with no user interaction. You can download the Secunia Daemon here.

The Secunia Daemon integrates a number of local data sources in your network with the Secunia Cloud. It should be deployed to a node in the network that has high availability (for example, the server running the SCCM or SQL server). Once deployed, the Daemon will regularly scan the data sources, based on the configuration created in CSI, for:

- Active Directory scanning
- SCCM import (SQL + WSUS)
- Scheduled exports
- WSUS state change

Agent-based Scan Requirements (Windows)

The flexibility offered by CSI ensures that it can be easily adapted to your environment.

If you choose to scan using the installable Agent (Agent-based scans), the following requirements should be present in the target hosts:

- Administrative privileges (to install the CSI Agent – csia.exe) Microsoft Windows XP, 2003, 2008, Vista, 7 or 8
- Internet Connection – SSL 443/TCP to https://*.secunia.com/ Windows Update Agent 2.0 or later

Agent-based Scan Requirements (Mac OS X)

The following requirements should be met before installing the Single Host Agent on an Intel-based Mac OS X machine:

- Supported Systems:
  10.5 Leopard/10.6 Snow Leopard/10.6 Snow Leopard Server/10.7 Lion/10.8 Mountain Lion Administrator privileges at minimum ('root' privileges required for the installation)
- Internet Connection – SSL 443/TCP to https://*.secunia.com
- The user installing the agent must have ‚execute' permissions on the file (chmod +x)

Remote/Agent-less Scan Requirements (Windows)

If you prefer to scan without installing the CSI Agent (Agent-less scans), the following requirements should be present in the target hosts:

- Ports 139/TCP and 445/TCP open inbound (on hosts)
- File sharing enabled on hosts
- Easy/simple file sharing disabled
- Windows Update Agent 2.0 or later

Required Windows services started on hosts:

- Workstation service
- Server service
- Remote Registry service (by default is disabled on Win7/ Vista)
- COM+ services (COM+ System Application: Set to Automatic)

Scanning Red Hat Enterprise Linux (RHEL)

The scan agent for RHEL uses the inventory which is already present (RPM) and displays this in CSI after being processed by Secunia Detection/Version Rules. To download CSI Agent for Red Hat Linux, go to Scanning > Scanning via Local Agents > Download Local Agents.

TECHNOLOGY ALLIANCE

ESET Technology Alliance aims to better protect businesses with a range of complementary IT security solutions. We provide customers with a better option when staying protected in the ever-changing security environment by combining our proven and trusted technology with other best-of-breed products.