

|  |
| --- |
| Microsoft BinScope 2014Getting Started Guide |
| Microsoft Trustworthy Computing |  |

Contents

[Overview 2](#_Toc431315287)

[Installation 2](#_Toc431315288)

[For Previous Users of BinScope 2](#_Toc431315289)

[System Requirements 2](#_Toc431315290)

[Download Link 3](#_Toc431315291)

[Uninstall 3](#_Toc431315292)

[How to Run BinScope 3](#_Toc431315293)

[Starting BinScope 3](#_Toc431315294)

[Perform a Scan 3](#_Toc431315295)

[Navigating the BinScope HTML Report 3](#_Toc431315296)

[Open the BinScope HTML Report in Internet Explorer 4](#_Toc431315297)

[Support 4](#_Toc431315298)

# Overview

Microsoft BinScope 2014 was designed in order to detect potential vulnerabilities that can be introduced into Binary files. The tests implemented in BinScope examine application binary files to identify coding and building practices that can potentially render the application vulnerable to attack or to being used as an attack vector. The tests include:

* Validating compiler and linker flags
* Ensuring the use of “known good” ATL headers
* Verifying that current compiler versions are used
* Identifying specific coding constructs that are deemed "dangerous"

By default, all checks required by the Security Development Lifecycle policy (SDL) are enabled. However, users can enable and disable checks selectively. BinScope supports a command-line interface to fit the needs of your environment.

Typical Information Technology users of BinScope:

* **Developers** use BinScope to verify compliance with coding and building best practices.
* **IT Security Auditors,** during reviews, can evaluate the risk presented by a particular piece of software installed on the Windows platform.

By reading this document and performing the sample exercise you can expect to gain the following skills:

* To have a general understanding of what BinScope does and the value it can add to your security strategy.
* Understand the software requirements for BinScope.
* Understand the installation procedure.
* Perform a basic scan using BinScope.
* Be familiar with some of the terminology used in BinScope.

# Installation

## For Previous Users of BinScope

It is recommended that you remove any previous versions of BinScope from your machine.

## System Requirements

BinScope requires .NET Framework 4 or higher to be installed on the machine performing the analysis. .NET is not required to be installed on the development machine that builds the binary file under analysis.

**Note:** Before beginning the installation process, download all Windows updates that are available for the machine on which you are installing.

## Download Link

Microsoft BinScope 2014 and supporting documentation can be downloaded from <http://microsoft.com/security/sdl>.

## Uninstall

1. Go to **Control Panel > Programs and Features**.
2. Right-click **Microsoft BinScope 2014** and select **Uninstall**.

# How to Run BinScope

## Starting BinScope

Open an elevated (Administrator) Command Prompt and navigate to the BinScope installation directory:

**%ProgramFiles%\Microsoft BinScope 2014\**

Or

**%ProgramFiles (x86)%\Microsoft BinScope 2014\**

Various arguments are available when starting BinScope from the Command Prompt. To see the list of arguments enter the following string:

**“%Program Files%\Microsoft\ Microsoft BinScope 2014\BinScope.exe /?”**

Or

**“%Program File s(x86)%\Microsoft\ Microsoft BinScope 2014\BinScope.exe /?”**

## Perform a Scan

**Note:** Before beginning a scan, make sure private symbols are available to BinScope.

Take the following steps to perform a scan:

1. Open a Command Prompt window and navigate to the BinScope [installation directory](#_Starting_BinScope).
2. For scans where the private symbols are in the same location as the binary, provide the following command: **binscope.exe /target “<path to binary>”**.

 ***Note****: BinScope is unable to run against files located in a system-protected directory.*

1. For scans where the private symbols are not in the same location as the binary, provide the following command: **binscope.exe /target “<path to binary”> /SymPath “<path to symbols>”**

## Navigating the BinScope HTML Report

By default, BinScope will save an HTML report file at **\users\<username>\BinScope\** which can be viewed in a browser such as Internet Explorer.

BinScope has a total of three categories that may be output into a log file**: Failed checks [Fail]**, **Checks that didn’t complete** **[Error]**, and **Passed checks [Pass]**. It is important to note that passed checks are not written to the log by default and must be enabled by using the **/verbose** switch.

## Open the BinScope HTML Report in Internet Explorer

1. Select **Allow** **Blocked** **Content** when prompt to enable ActiveX controls.



*Figure 1 ActiveX Prompt in Internet Explorer*

1. When viewing the report, you can obtain details on failed and incomplete checks by clicking the entry, as shown here:



*Figure 2 BinScope HTML Report*

As the example shows, Compiled2003.exe failed the DBCheck because binary is not marked as being compatible with DYNAMICBASE.

# Support

For support, please visit the following links:

* [Microsoft Security Development Lifecycle](http://www.microsoft.com/security/sdl/default.aspx)
* [Microsoft Cyber Trust Blog](http://blogs.microsoft.com/cybertrust/category/cloud-computing/)
* [MSDN Forums for SDL](http://social.msdn.microsoft.com/Forums/en-US/home?forum=sdlprocess)

Copyright © 2015 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.