InstallShield 2018 Express Edition
Release Notes

Originally released January 2018; updated to include R2 (September 2018) and SP1 (May 2018)

Introduction

InstallShield is the industry standard for authoring high-quality Windows Installer–based installations. InstallShield 2018 Express Edition helps you mitigate the risks of OSS code with a quick and easy scan of your daily build. You'll uncover OSS and IP compliance vulnerabilities before you ship, so your build becomes the first line of defense against future OSS data breaches.

InstallShield 2018 Express Edition also offers new features and enhancements that make it easy to use the latest technologies.

For the latest information about InstallShield 2018 Express Edition, including updates to these release notes, see the online version of the InstallShield 2018 Express Edition release notes.

Changes in R2

In InstallShield 2018 R2 Express Edition, several issues were resolved. For descriptions of these resolved issues, refer to InstallShield 2018 R2 Express Edition.

Changes in SP1

InstallShield 2018 Express Edition includes the following new feature:

- Support Dual Signing Using SHA1 and SHA256 Digest
- Resolved Issues in SP1

Support Dual Signing Using SHA1 and SHA256 Digest

In previous releases, you could choose the signature digest hashing algorithm only based on:

- Certificate Hash
- SHA-1
- SHA-256

In InstallShield 2018 SP1 Express Edition, along with the above signature digest hashing algorithm, you can now choose

- Dual Signing - (SHA-1 and SHA-256) digest

Resolved Issues in SP1

For descriptions of resolved issues in InstallShield 2018 SP1 Express Edition, refer to InstallShield 2018 SP1 Express Edition.

New Features

InstallShield 2018 Express Edition includes the following new features:

- Perform Open Source Risk Assessment with FlexNet Code Aware
- Set Forms Authentication on Web Applications

Perform Open Source Risk Assessment with FlexNet Code Aware

InstallShield now includes full integration with FlexNet Code Aware, an automated open source risk assessment and package discovery solution that enables you to quickly scan your products for security and intellectual property (IP) compliance risk.

- Supported File Types
- Running FlexNet Code Aware
- Reading the FlexNet Code Aware Report
- More Information

Supported File Types

FlexNet Code Aware supports analysis of the following files:

- Java Packages
- Node Packages
- Nuget Packages
- RPM Packages
- Ruby Packages
- EXE & DLL Files

Security vulnerabilities are looked up against the National Vulnerability Database (NVD).

Running FlexNet Code Aware

FlexNet Code Aware is part of InstallShield and no activation ID is required to activate it.

To run FlexNet Code Aware from within InstallShield, click **Scan Project using FlexNet Code Aware** on the InstallShield **Project** menu or click the FlexNet Code Aware icon on the standard toolbar.

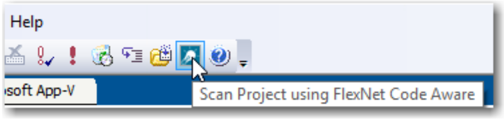


Figure 1: FlexNet Code Aware Icon on InstallShield Toolbar

***Note** • This FlexNet Code Aware menu options are disabled out if you are not currently in an open InstallShield project.*

When FlexNet Code Aware completes the scan of your project, the Results Summary view opens, displaying the number of files scanned, and the number of open-source packages and vulnerabilities found.

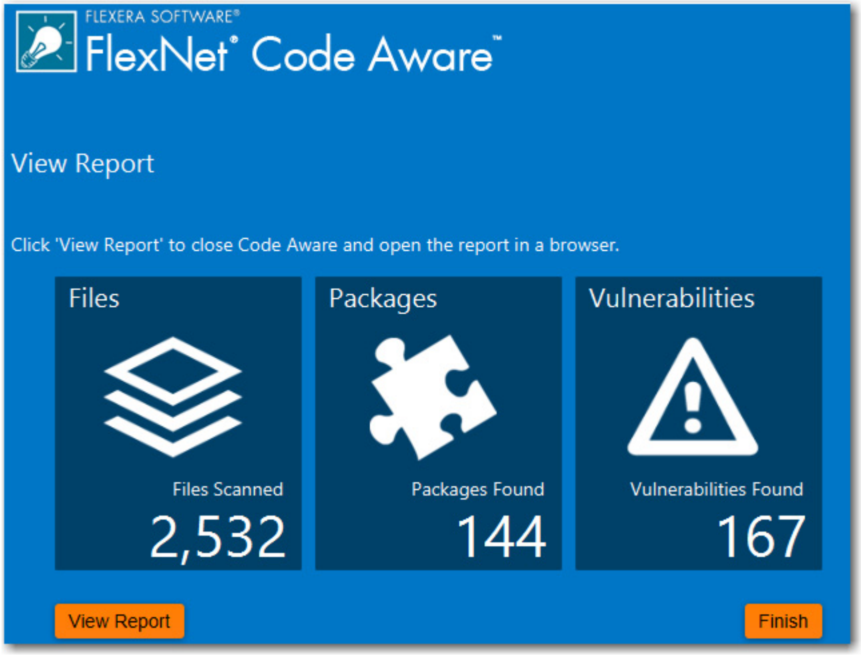


Figure 2: FlexNet Code Aware Results Summary

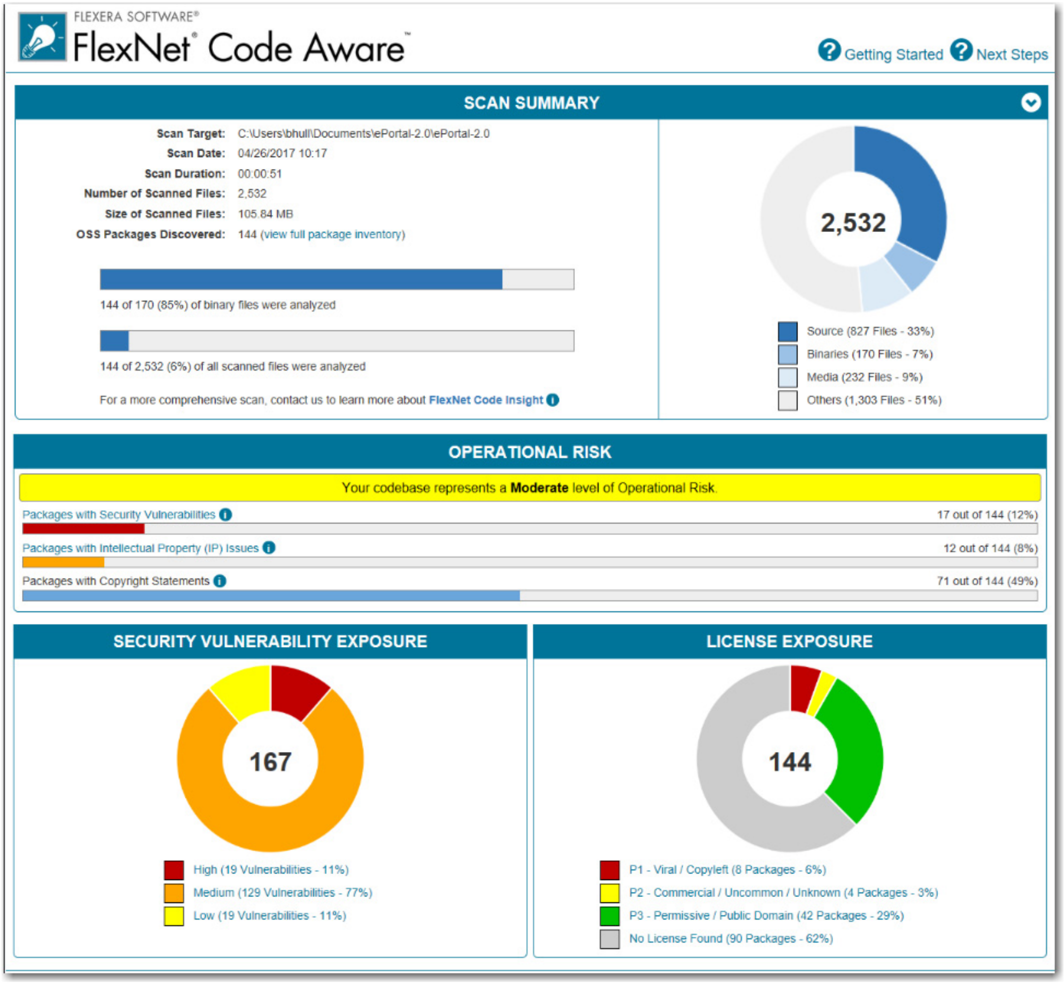
When you click the **View Report** button, a full report is displayed.

Reading the FlexNet Code Aware Report

When you click **View Report** on the Results Summary screen, the full FlexNet Code Aware report opens, consisting of an **Initial Summary** view and a **Package Inventory** view.

Initial Summary View

The **Initial Summary** view presents the user with a scan summary, and assessments of operational risk, security vulnerability exposure, and license exposure.



SCAN SUMMARY

Scan Target: C:\Users\bhull\Documents\ePortal-2.0\ePortal-2.0
Scan Date: 04/26/2017 10:17
Scan Duration: 00:00:51
Number of Scanned Files: 2,532
Size of Scanned Files: 105.84 MB
OSS Packages Discovered: 144 (view full package inventory)

144 of 170 (85%) of binary files were analyzed

144 of 2,532 (6%) of all scanned files were analyzed

For a more comprehensive scan, contact us to learn more about **FlexNet Code Insight**

- Source (827 Files - 33%)
- Binaries (170 Files - 7%)
- Media (232 Files - 9%)
- Others (1,303 Files - 51%)

OPERATIONAL RISK

Your codebase represents a **Moderate** level of Operational Risk.

Packages with Security Vulnerabilities	17 out of 144 (12%)
Packages with Intellectual Property (IP) Issues	12 out of 144 (8%)
Packages with Copyright Statements	71 out of 144 (49%)

SECURITY VULNERABILITY EXPOSURE

- High (19 Vulnerabilities - 11%)
- Medium (129 Vulnerabilities - 77%)
- Low (19 Vulnerabilities - 11%)

LICENSE EXPOSURE

- P1 - Viral / Copyleft (8 Packages - 6%)
- P2 - Commercial / Uncommon / Unknown (4 Packages - 3%)
- P3 - Permissive / Public Domain (42 Packages - 29%)
- No License Found (90 Packages - 62%)

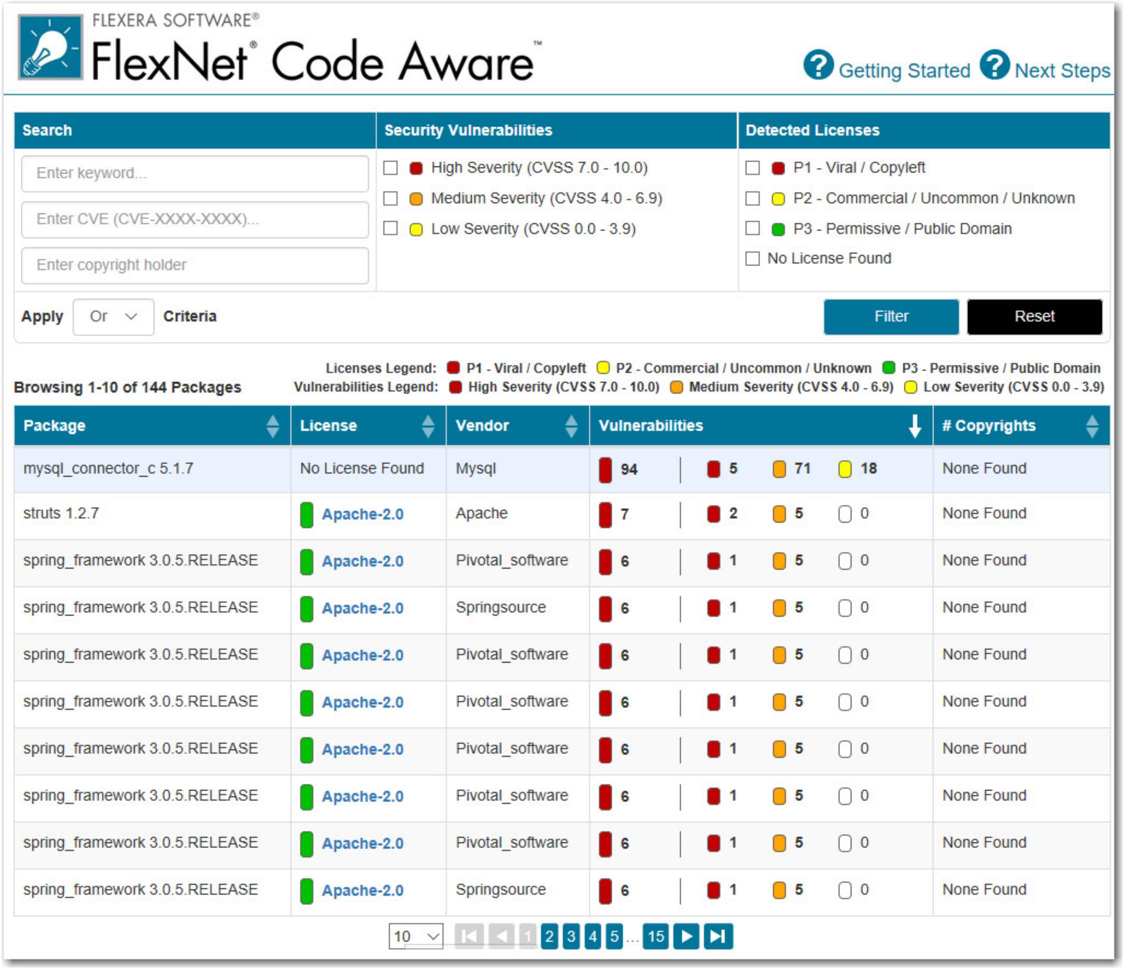
Figure 3: FlexNet Code Aware Initial Summary View

The FlexNet Code Aware Initial Summary View displays the following information:

- **Scan Summary**—This section provides details regarding the codebase that was scanned, including a breakdown of file types, percent of files analyzed, and number of findings.
- **Operational Risk**—This section provides a composite risk rating based on the combination of packages with Intellectual Property (IP) issues and packages with Security Vulnerabilities.
- **Security Vulnerability Exposure and License Exposure**—These sections provide a breakdown of the types and categories of identified issues.

Package Inventory View

The **Package Inventory** view, available by clicking **View full package inventory** in the **Scan Summary** section, provides a complete list of discovered open source and third-party packages with associated licenses, security vulnerabilities, dependencies, and detected copyright statements.



Search

Enter keyword...

Enter CVE (CVE-XXXX-XXXX)...

Enter copyright holder

Security Vulnerabilities

- □ 🟥 High Severity (CVSS 7.0 - 10.0)
- □ 🟧 Medium Severity (CVSS 4.0 - 6.9)
- □ 🟨 Low Severity (CVSS 0.0 - 3.9)

Detected Licenses

- □ 🟥 P1 - Viral / Copyleft
- □ 🟨 P2 - Commercial / Uncommon / Unknown
- □ 🟩 P3 - Permissive / Public Domain
- □ No License Found

Apply Or ▾ **Criteria** Filter Reset

Licenses Legend: 🟥 P1 - Viral / Copyleft 🟨 P2 - Commercial / Uncommon / Unknown 🟩 P3 - Permissive / Public Domain

Vulnerabilities Legend: 🟥 High Severity (CVSS 7.0 - 10.0) 🟧 Medium Severity (CVSS 4.0 - 6.9) 🟨 Low Severity (CVSS 0.0 - 3.9)

Browsing 1-10 of 144 Packages

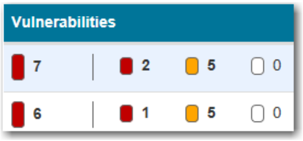
Package	License	Vendor	Vulnerabilities	# Copyrights
mysql_connector_c 5.1.7	No License Found	Mysql	🟥 94 🟥 5 🟧 71 🟨 18	None Found
struts 1.2.7	🟩 Apache-2.0	Apache	🟥 7 🟥 2 🟧 5 ▢ 0	None Found
spring_framework 3.0.5.RELEASE	🟩 Apache-2.0	Pivotal_software	🟥 6 🟥 1 🟧 5 ▢ 0	None Found
spring_framework 3.0.5.RELEASE	🟩 Apache-2.0	Springsource	🟥 6 🟥 1 🟧 5 ▢ 0	None Found
spring_framework 3.0.5.RELEASE	🟩 Apache-2.0	Pivotal_software	🟥 6 🟥 1 🟧 5 ▢ 0	None Found
spring_framework 3.0.5.RELEASE	🟩 Apache-2.0	Pivotal_software	🟥 6 🟥 1 🟧 5 ▢ 0	None Found
spring_framework 3.0.5.RELEASE	🟩 Apache-2.0	Pivotal_software	🟥 6 🟥 1 🟧 5 ▢ 0	None Found
spring_framework 3.0.5.RELEASE	🟩 Apache-2.0	Pivotal_software	🟥 6 🟥 1 🟧 5 ▢ 0	None Found
spring_framework 3.0.5.RELEASE	🟩 Apache-2.0	Pivotal_software	🟥 6 🟥 1 🟧 5 ▢ 0	None Found
spring_framework 3.0.5.RELEASE	🟩 Apache-2.0	Springsource	🟥 6 🟥 1 🟧 5 ▢ 0	None Found

10 ▾ |◀ ◀ 1 2 3 4 5 ... 15 ▶ ▶|

Figure 4: FlexNet Code Aware Package Inventory View

The **Package Inventory** view provides filters that you can use to execute targeted queries to refine the list to various package types of interest.

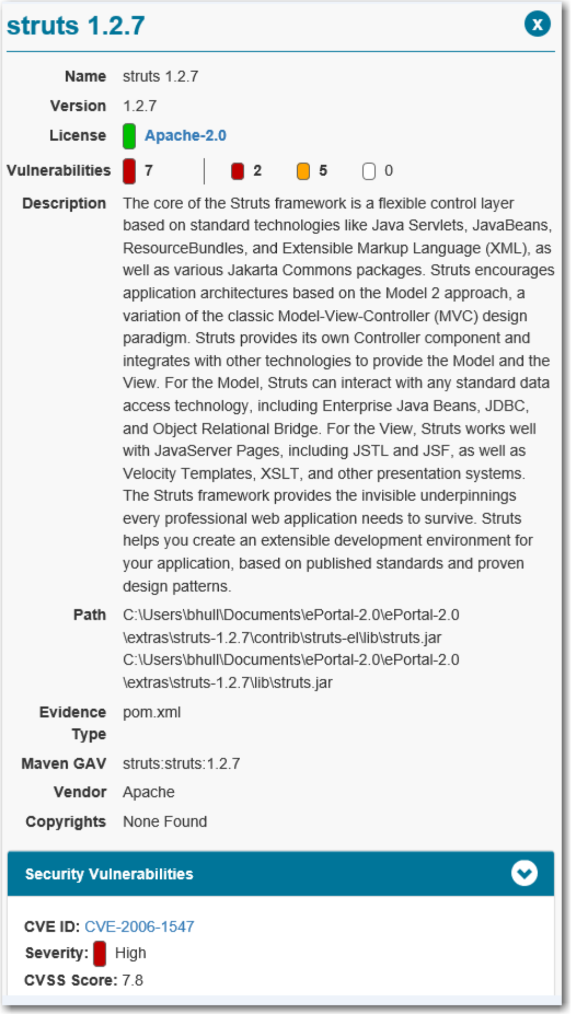
To view additional package details, click a vulnerability count listed in the **Vulnerabilities** column of the package you want to review:



Vulnerabilities
🟥 7 🟥 2 🟧 5 ▢ 0
🟥 6 🟥 1 🟧 5 ▢ 0

Figure 5: Vulnerabilities Column

The **Vulnerabilities Detail** page opens (covering a portion of the Package Inventory view), and displays detailed information on the selected package.



struts 1.2.7

Name struts 1.2.7

Version 1.2.7

License 🟩 Apache-2.0

Vulnerabilities 🟥 7 | 🟥 2 🟧 5 □ 0

Description The core of the Struts framework is a flexible control layer based on standard technologies like Java Servlets, JavaBeans, ResourceBundles, and Extensible Markup Language (XML), as well as various Jakarta Commons packages. Struts encourages application architectures based on the Model 2 approach, a variation of the classic Model-View-Controller (MVC) design paradigm. Struts provides its own Controller component and integrates with other technologies to provide the Model and the View. For the Model, Struts can interact with any standard data access technology, including Enterprise Java Beans, JDBC, and Object Relational Bridge. For the View, Struts works well with JavaServer Pages, including JSTL and JSF, as well as Velocity Templates, XSLT, and other presentation systems. The Struts framework provides the invisible underpinnings every professional web application needs to survive. Struts helps you create an extensible development environment for your application, based on published standards and proven design patterns.

Path C:\Users\bhull\Documents\ePortal-2.0\ePortal-2.0\extras\struts-1.2.7\contrib\struts-el\lib\struts.jar
C:\Users\bhull\Documents\ePortal-2.0\ePortal-2.0\extras\struts-1.2.7\lib\struts.jar

Evidence Type pom.xml

Maven GAV struts:struts:1.2.7

Vendor Apache

Copyrights None Found

Security Vulnerabilities

CVE ID: CVE-2006-1547
Severity: 🟥 High
CVSS Score: 7.8

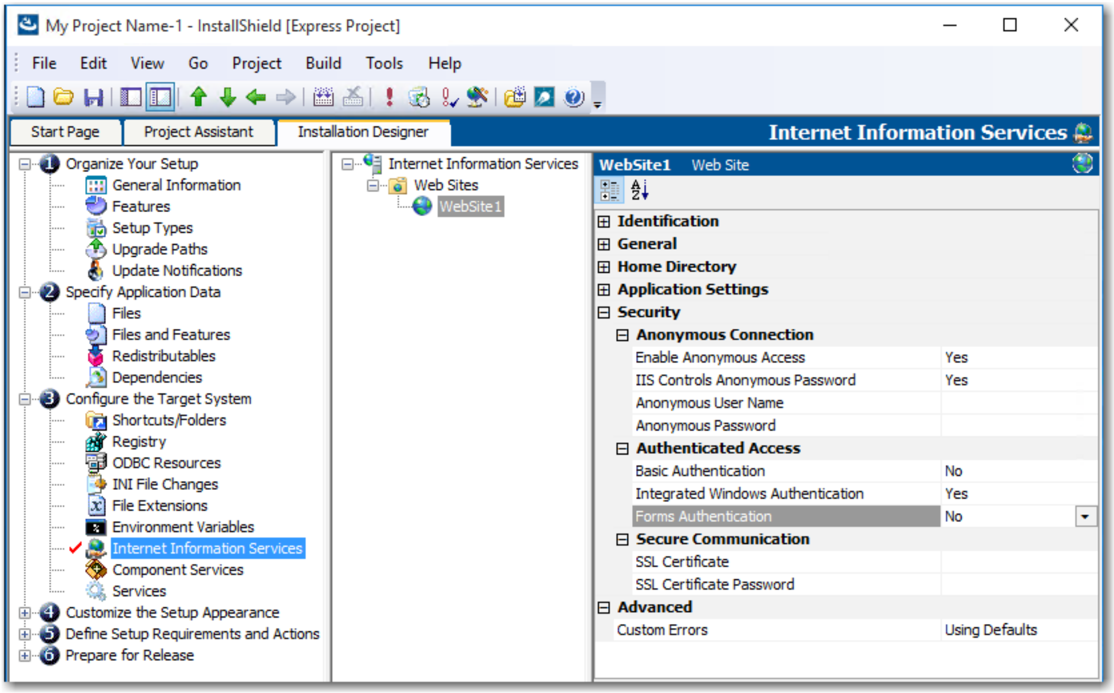
Figure 6: Vulnerabilities Detail

More Information

For detailed information on using FlexNet Code Aware, see *Using FlexNet Code Aware to Perform Open Source Risk Assessment* in the InstallShield Help Library.

Set Forms Authentication on Web Applications

InstallShield 2018 Express Edition includes a new option to set forms authentication on web applications. This new option, **Forms Authentication**, is displayed under the **Authenticated Access** section of the **Internet Information Services** view for a website.



⊞ Identification	
⊞ General	
⊞ Home Directory	
⊞ Application Settings	
⊟ Security	
⊟ Anonymous Connection	
Enable Anonymous Access	Yes
IIS Controls Anonymous Password	Yes
Anonymous User Name	
Anonymous Password	
⊟ Authenticated Access	
Basic Authentication	No
Integrated Windows Authentication	Yes
Forms Authentication	No
⊟ Secure Communication	
SSL Certificate	
SSL Certificate Password	
⊟ Advanced	
Custom Errors	Using Defaults

Figure 7: Forms Authentication Option on Internet Information Services View

Set the **Forms Authentication** option to **Yes** to enable forms authentication. ASP.NET forms-based authentication works well for sites or applications on public Web servers that receive many requests. This authentication mode lets you manage client registration and authentication at the application level, instead of relying on the authentication mechanisms provided by the operating system.

Important • *Forms authentication sends the user name and password to the Web server as plain text. You should use Secure Sockets Layer (SSL) encryption for the Log On page and for all other pages in your application except the Home page.*

Note • *This change was tracked in issue IOJ-1625840.*

Enhancements

InstallShield 2018 releases include the following enhancements:

- InstallShield 2018 R2 Express Edition
- InstallShield 2018 SP1 Express Edition
- InstallShield 2018 Express Edition

InstallShield 2018 R2 Express Edition

InstallShield 2018 R2 Express Edition includes the following enhancements:

- Add Pre-Defined Install Conditions
- Shortcut to Run As Administrator

Add Pre-Defined Install Conditions

In InstallShield 2018 R2, you can now add pre-defined install conditions for .net 4.7:

- 4.7
- 4.7.1
- 4.7.2

Shortcut to Run As Administrator

In InstallShield 2018 R2, you can now enable the shortcut to ‘Run As Administrator’.

Available options are:

- **Yes**—Enables the shortcut to Run As Administrator.
- **No**—To not to set the shortcut to Run As Administrator.

InstallShield 2018 SP1 Express Edition

InstallShield 2018 SP1 Express Edition includes the following enhancements:

- Customize Update Launcher Name
- Specify Predefined Public Folder

Customize Update Launcher Name

In InstallShield 2018 SP1 Express Edition, a new setting is introduced to customize the name of the Update Launcher. By default, InstallShield uses Update.exe in the name for the Update Launcher. Now, you can create an Update Launcher with a specified name.

Specify Predefined Public Folder

In InstallShield, a new predefined folder is introduced to hold the full path to the Users Public folder.

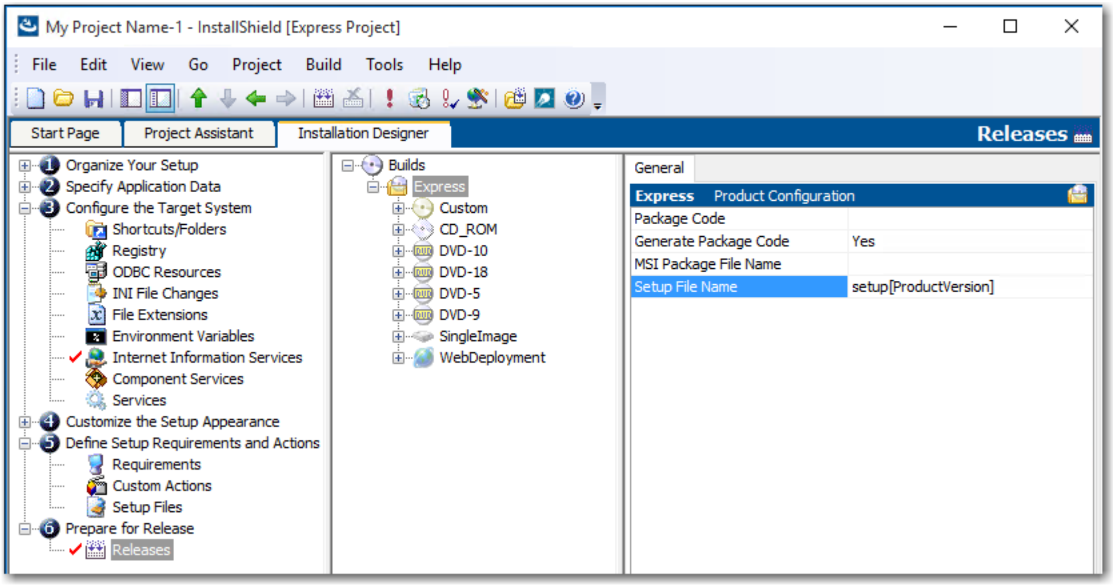
InstallShield 2018 Express Edition

InstallShield 2018 Express Edition includes the following enhancements:

- Include the Value of a Property in a Product Configuration’s Setup File Name
- New MSBuild Parameters to Set Summary Information Stream Comments and to Set Package File Name
- Additional Prerequisites Included

Include the Value of a Property in a Product Configuration’s Setup File Name

In InstallShield 2018 Express Edition, you can now include the value of a property from the Property Table in product release setup and package file names.



Package Code	
Generate Package Code	Yes
MSI Package File Name	
Setup File Name	setup[ProductVersion]

Figure 8: Entering a Property in the Setup File Name Field on the Releases View

For example, you could enter any of the following properties in the **Setup File Name** or **MSI Package File Name** field on the **General** tab of the **Releases > Express** view:

```
setup[ProductVersion]
setup[CustomVersion]
setup[ProductCode]
setup[ProductCode][ProductVersion]
```

If you entered **`setup[ProductVersion]`** in the **Setup File Name** field, it would result in a setup named `setup14.10.1234.exe`, for example.

***Note** • This change was tracked in issue IOJ-1764179.*

New MSBuild Parameters to Set Summary Information Stream Comments and to Set Package File Name

In InstallShield 2018 Express Edition, new MSBuild parameters were added to enable you to set add comments to an installer and to set the package file name of an installer.

- New Parameter to Set Summary Information Stream Comments
- New Parameter to Set Package File Name

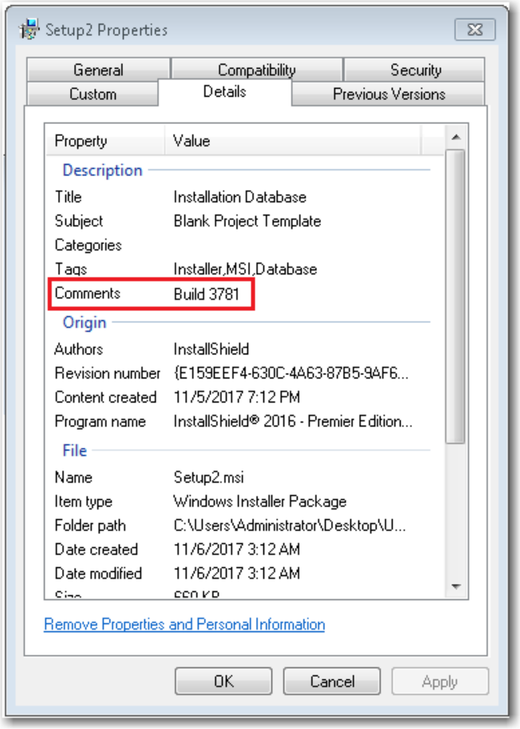
New Parameter to Set Summary Information Stream Comments

You can add comments to an installer in the **Summary Information Stream Comments** field on the **General Information** view.

In InstallShield 2018 Express Edition, you also have the option of entering comments at build time. A new parameter has been added to the `MSBuild.exe` task, named `SummaryInfoComments`, to set the **Summary Information Stream** comments at build time, such as including the build number, as shown in the following example:

```
MSBuild.exe c:\installers\Setup.sln /Property:SummaryInfoComments="Insert Comments Here"
```

The comments that are added using the `SummaryInfoComments` property can be viewed on the **Properties** dialog box of the built installer.



Property	Value
Description	
Title	Installation Database
Subject	Blank Project Template
Categories	
Tags	Installer,MSI,Database
Comments	Build 3781
Origin	
Authors	InstallShield
Revision number	{E159EEF4-630C-4A63-87B5-9AF6...
Content created	11/5/2017 7:12 PM
Program name	InstallShield® 2016 - Premier Edition...
File	
Name	Setup2.msi
Item type	Windows Installer Package
Folder path	C:\Users\Administrator\Desktop\U...
Date created	11/6/2017 3:12 AM
Date modified	11/6/2017 3:12 AM
Size	560 KB

Figure 9: Comments on Properties Dialog Box

***Note** • This change was tracked in issue IOJ-1735932.*

New Parameter to Set Package File Name

You can specify the package file name of an installer in the **MSI Package File Name** field on the **General** tab on the **Releases > Express** view.

In InstallShield 2018 Express Edition, you also have the option of setting the package file name at build time. A new parameter has been added to the `MSBuild.exe` task, named `MSIPackageFileName`, to set the package file name of the built installer at build time, as shown in the following example:

```
MSBuild.exe c:\installers\Setup.isproj /Property:MSIPackageFileName="MySetup"
```

When entering the value for the `MSIPackageFileName` parameter, you need to enter the file name—without the period or the file extension—that InstallShield should use for the `.msi` file.

***Note** • This change was tracked in issue IOJ-1735520.*

Additional Prerequisites Included

InstallShield 2018 Express Edition includes the following additional prerequisites:

- Visual C++ 2017 x86 and x64 Prerequisites
- Microsoft SQL Server 2014 SP1 and SP2 Prerequisites
- Microsoft .NET Framework 4.7 Prerequisite

Visual C++ 2017 x86 and x64 Prerequisites

Because Microsoft Visual Studio 2017 has been released, InstallShield now includes the prerequisites for Visual C++ 2017 x86 and x64.

***Note** • This change was tracked in issue IOJ-1832110.*

Microsoft SQL Server 2014 SP1 and SP2 Prerequisites

Because Microsoft SQL Server 2014 has had 2 Service Packs released, InstallShield now includes the prerequisites for both Microsoft SQL Server 2014 SP1 and SP2.

***Note** • This change was tracked in issue IOJ-1832297.*

Microsoft .NET Framework 4.7 Prerequisite

InstallShield now includes a prerequisite for Microsoft .NET Framework 4.7.

***Note** • This change was tracked in issue IOJ-1834933.*

Important Information

Note the following important information regarding the InstallShield 2018 Express Edition release:

- Evaluating InstallShield
- Obtaining the Installations for InstallShield, InstallShield Add-Ons, and the Redistributable Files
- Installing More than One Edition of InstallShield
- Installing More than One Version of InstallShield
- Removal of .NET/J# Tab from the Releases View

Evaluating InstallShield

If you have not purchased a license for InstallShield, you can install it and use it for a limited number of days without activating it or connecting it to a license server. When you use InstallShield before activating it or connecting it to a license server, it operates in evaluation mode, and some of its functionality is not available. For details, see Functionality Notes for the Evaluation Version of InstallShield. Note that the evaluation limitations are removed when you activate InstallShield or when you connect it to a license server and check out a license for it.

Obtaining the Installations for InstallShield, InstallShield Add-Ons, and the Redistributable Files

The following installations are available for download from the Flexera Software Product and License Center as documented in the InstallShield download and licensing instructions:

- InstallShield
- Redistributable files (for example, InstallShield prerequisites and InstallScript objects)
- Add-ons (if you are entitled to them) such as the Standalone Build and the InstallShield MSI Tools
- FlexNet Licensing Server software (if you purchased concurrent licenses and you need to set up your organization's license server)
- Skin Customization Kit
- InstallScript Object templates
- InstallShield service packs (if available)

Installing More than One Edition of InstallShield

Only one edition of InstallShield 2018—Premier, Professional, or Express—can be installed on a system at a time. In addition, the InstallShield 2018 DIM Editor cannot be installed on the same machine with any edition of InstallShield 2018.

Microsoft Visual Studio can be integrated with only one version of InstallShield at a time. The last version of InstallShield that is installed or repaired on a system is the one that is used for Visual Studio integration.

Installing More than One Version of InstallShield

InstallShield 2018 Express Edition can coexist on the same machine with other versions of InstallShield.

The InstallShield 2018 Express Edition Standalone Build can coexist on the same machine with other versions of the Standalone Build. In most cases, the Standalone Build is not installed on the same machine where InstallShield is installed. If you do install both on the same machine and you want to use the automation interface, review the *Installing the Standalone Build and InstallShield on the Same Machine* topic in the InstallShield Help Library to learn about special registration and uninstallation considerations.

Removal of .NET/J# Tab from the Releases View

The **.NET./J#** tab in the **Releases** view of the Installation Designer was originally provided to support .NET 1.1/2.0 and J# redistributables. Those technologies have become obsolete and no longer supported by Microsoft. Therefore, in InstallShield 2018 Express Edition, the **.NET/J#** tab of the **Releases** view has been removed (as well as the associated .NET 1.1/2.0 Core Language and .NET 1.1/2.0 Language Packs dialog boxes).

Project Upgrade Alerts

The following information describes possible upgrade issues that may occur when you upgrade projects that were created with InstallShield 2016 and earlier to InstallShield 2018. It also alerts you to possible changes in behavior that you may notice between new InstallShield 2018 projects and projects that are upgraded from InstallShield 2016 or earlier to InstallShield 2018.

- General Information about Upgrading Projects that Were Created in Earlier Versions of InstallShield
- Changes to the List of Supported Versions of Windows for Target Systems
- Localized String Considerations

General Information about Upgrading Projects that Were Created in Earlier Versions of InstallShield

If you use InstallShield 2018 to open an project that was created with an earlier version, InstallShield 2018 displays a message box that asks you if you want to convert the project to the new version. If you reply that you do want to convert it, InstallShield creates a backup copy of the project with a file extension such as .777 (for an .ism project) or .2016 (for an .issuite project) before converting it. Delete the .777 or .2016 part from the original project's file name if you want to reopen the project in the earlier version of InstallShield. Note that you cannot open InstallShield 2018 projects in earlier versions of InstallShield.

You can upgrade projects that were created with the following versions of InstallShield to InstallShield 2018: InstallShield 2016 and earlier, InstallShield 12 and earlier, InstallShield DevStudio, InstallShield Professional 7 and earlier, and InstallShield Developer 8 and earlier. Note that projects that were created with InstallShield MultiPlatform or InstallShield Universal cannot be upgraded to InstallShield 2018.

Changes to the List of Supported Versions of Windows for Target Systems

For all project types except for Suites, Windows XP SP3 and Windows Server 2003 SP2 are the minimum versions of Windows that are required for target systems that run the installations that are created in InstallShield. For suites (Advanced UI, and Suite/Advanced UI project types), Windows Vista and Windows Server 2008 are the minimum versions of Windows that are required for target systems.

Localized String Considerations

Changes to the handing and detection of localized strings were introduced starting in InstallShield 2016. For example, localized string content that includes square brackets around invalid characters can now trigger a build time warning or error. Accordingly, the following new warning and errors might occur when you are working with your installation.

Error or Warning Number	Message	Troubleshooting Information
-7355	The %4 value for string %2 does not meet validation criteria for table %1 column %3.	This warning occurs if a localized string value does not meet validation criteria for a column in the String Editor table. To resolve this warning, update the flagged value in the String Editor.
-7354	The %4 value for string %2 does not contain a legitimate value for table %1 column %3.	This error occurs if a localized string value does not contain a legitimate value in the named column of the String Editor table. To resolve this error, update the flagged value in the String Editor.

Resolved Issues

This section lists the customer issues that were resolved in the following versions of InstallShield:

- InstallShield 2018 R2 Express Edition
- InstallShield 2018 SP1 Express Edition
- InstallShield 2018 Express Edition

InstallShield 2018 R2 Express Edition

This section lists the customer issues that were resolved in InstallShield 2018 R2 Express Edition.

Issue Number	Issue Summary
IOJ-1875224	The InstallShield IDE exits with an c0000005 exception when deselected the “Ready to Install” dialog from the dialog view.
IOJ-1875922	In InstallShield 2018 SP1, any information which is being displayed in parentheses is corrupted while clicking on a main view (ex Organization, Application Data, System Configuration) for the second time.
IOJ-1872837	Short File Name not generated for String Entries that Contain the characters * or ?
IOJ-1883924	Patch Design does not Uncompress a Compressed Setup.exe.
IOJ-1877004	COM extraction from a 64-bit out-of-process .NET server freezes build and RegSpyUi.exe

InstallShield 2018 SP1 Express Edition

This section lists the customer issues that were resolved in InstallShield 2018 SP1 Express Edition.

Issue Number	Issue Summary
IOJ-1853555	Using a Store Certificate to sign swidtag ends in a build error.
IOJ-1862582	Unable to change the fonWt (color, style, or size) in InstallShield 2018 Express. The ability to change the font (color, style, or size) of the Setup window does not work as expected.
IOJ-1860906	With or without a project open, if selected Tools > Options > Prerequisites tab, and then tries to add a new folder to the list to be searched for prerequisites, the field is blank.
IOJ-1860620	Adding an InstallShield project to a VS solution, receives an error when trying to build the solution with MSBuild.
IOJ-1842874	While the setup is completed, all the files are cleaned in TEMP folder; Except for a single media with feature prerequisite leaves two setup.exe in the temp.
IOJ-1731438	The registry view in the InstallShield IDE has a limit on what it will display as the value for a DWORD. Entering anything over 2147483647, hexadecimal 0x7FFFFFFF is displayed as 0x7FFFFFFF in the IDE.
IOJ-1665230	Setting INSTALLDIR from the Registry does not search 64-bit portion of registry and needs to be read from x64 location.

InstallShield 2018 Express Edition

This section lists the customer issues that were resolved in InstallShield 2018 Express Edition.

Issue Number	Issue Summary
IOJ-1627091	Dependent files are not being included in the InstallShield package when building an InstallShield project with MSBUILD. However, dependent files are included when building the same project using the Visual Studio interface.
IOJ-1749409	When you attempt to use COM extraction in InstallShield on a poorly written DLL, it will get stuck in an infinite loop during registration. InstallShield will hang indefinitely instead of stopping the process and displaying an error message after a certain amount of time has elapsed.
IOJ-1813258	Microsoft SQL Server 2016 Express prerequisites fail to download.
IOJ-1830045	Checking for updates in InstallShield 2016 SP2 causes Software Manager to display “The product version is not registered on the server” instead of displaying the message that no updates are available.

Issue Number	Issue Summary
IOJ-1842270	SETUPEXEDIR does not resolve to the expected value when passed to an InstallShield prerequisite.

IOJ-1846227	Request that a registry convention be used as a condition for the Microsoft Visual C++ 2015 Update 3 redistributable instead of the msvcp140.dll file, which could be unreliable.
	The currently installed version is stored in this key:
	`HKEY_LOCAL_MACHINE\SOFTWARE[\Wow6432Node]\Microsoft\VisualStudio\vs-version\VC\Runtimes{x86|x64|ARM}`
	For example, C++ 2015 Update 3 x86 is stored in:
	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\NodeMicrosoft\VisualStudio\14.0\VC\Runtimes\x86\Version=v14.0.24212.00`
	For more information, see Redistributing Visual C++ Files.

System Requirements

This section contains the minimum requirements for systems that run InstallShield (the authoring environment), as well as for target systems that run the installations created with InstallShield (the run-time environment).

- For Systems Running InstallShield
- For Target Systems

For Systems Running InstallShield

InstallShield runs on the latest versions of these operating systems, fully updated with the most recent patches and service packs.

Item	Description
Processor	Pentium III-class PC (500 MHz or higher recommended)
RAM	256 MB of RAM (512 MB preferred)
Hard Disk	750 MB free space
Display	Designed for XGA resolution at 1024 × 768 or higher

Item	Description
Operating System	● Windows Vista ● Windows Server 2008 ● Windows 7 ● Windows Server 2008 R2 ● Windows 8 ● Windows Server 2012 ● Windows 8.1 ● Windows Server 2012 R2 ● Windows 10 ● Windows Server 2016
Privileges	Administrative privileges on the system
Mouse	Microsoft IntelliMouse or other compatible pointing device
Optional Integration with Visual Studio	The following versions of Microsoft Visual Studio can be integrated with InstallShield Premier or Professional Editions: ● Visual Studio 2008 ● Visual Studio 2010 ● Visual Studio 2012 ● Visual Studio 2013 ● Visual Studio 2015 ● Visual Studio 2017 The following editions of these versions of Visual Studio can be integrated with InstallShield Premier or Professional Editions: ● Community ● Professional ● Premium ● Ultimate

For Target Systems

Target systems must meet the following minimum operating system requirement:

- Windows XP SP3
- Windows Server 2003 SP2
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2
- Windows 8
- Windows Server 2012
- Windows 8.1
- Windows Server 2012 R2
- Windows 10
- Windows Server 2016

Target systems must also support the SSE2 instruction set.

Known Issues

For a list of known issues, see https://flexeracommunity.force.com/customer/articles/en_US/INFO/InstallShield-2018-Express-Edition-Known-Issues.

Legal Information

Copyright Notice

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexera.com/producer/company/about/intellectual-property/. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.