

# FIS WebScan 2019 Guide

FIS | January 2019

Empowering  
the Financial World

FIS

[www.fisglobal.com](http://www.fisglobal.com)

## Contents

<b>Introduction.....</b>	<b>5</b>
Supported Operating Systems .....	5
Supported Browsers.....	5
Software Requirements.....	5
Hardware Requirements .....	5
Supported Scanners.....	5
Technical Support .....	6
<b>Installation Scenarios.....</b>	<b>7</b>
Standard Installation.....	7
Setting Parameter Values .....	13
Batch File Installation .....	14
<i>Command Line parameters.....</i>	<i>14</i>
<i>Sample Batch File .....</i>	<i>14</i>
<i>Installation Workflow .....</i>	<i>15</i>
<b>Update Scenarios .....</b>	<b>16</b>
Auto Update .....	16
Auto Update Pre-18.0.1018 .....	20
Manual Update.....	23
RDC Client Update.....	28
<b>Uninstallation .....</b>	<b>32</b>
<b>System Tray Menu .....</b>	<b>33</b>
Log Viewer .....	33

Settings .....	35
<i>Panini Settings</i> .....	36
<i>Canon Settings</i> .....	37
<i>SmartSource Settings</i> .....	38
<i>RDM Settings</i> .....	39
<i>Origin Domain Settings</i> .....	39
Add a Domain .....	40
Remove a Domain .....	42
<i>Updater Settings</i> .....	43
Check For Updates .....	44
Install Updates.....	44
View Updater Status.....	44
About .....	45
Exit.....	45
<b>Scanner Test Capture.....</b>	<b>46</b>
<b>Directory Structure .....</b>	<b>48</b>
<b>Post-Install Config .....</b>	<b>49</b>
<b>Code Signing Certificates .....</b>	<b>50</b>
<b>How to... .....</b>	<b>51</b>
Verifying SignalR hub.....	51
Verifying Certificates .....	51
Verifying SSL Certificate Bindings .....	52
Manually Add SSL Certificate Bindings.....	52
Manually Delete SSL Certificate Bindings.....	52

Verifying URL Reservation ..... 52

Manually Add URL Reservation ..... 53

Manually Delete URL Reservation ..... 53

**Troubleshooting ..... 54**

WebScan Load Exception: Exception has been thrown..... 54

Unable to capture with Firefox, but Chrome and IE work ..... 54

Browser(s) has never connected to WebScan..... 58

Edge on Windows 10 won't connect ..... 58

## Introduction

FIS *WebScan* is a software solution that is used by web applications to interface with USB based scanners, without the use of ActiveX or Java. This manual is intended for those who have the responsibility of setting up and managing *WebScan*.

## Supported Operating Systems

- Windows 7 SP1
- Windows 8.1
- Windows 10

## Supported Browsers

- Google Chrome
- Microsoft IE 11
- Microsoft Edge
- Mozilla Firefox

## Software Requirements

- Microsoft .NET Framework 4.5.1 or newer

## Hardware Requirements

- USB 2.0/3.0

## Supported Scanners

The following list is the scanners supported by WebScan. You will need to review the supported scanner list provided with you Remote Deposit Client to verify what scanners it supports.

- Canon® CR-25\*
- Canon CR-55\*
- Canon CR-50
- Canon CR-80
- Canon CR-120
- Canon CR-135i
- Canon CR-150
- Canon CR-180 II\*
- Canon CR-190i
- Digital Check® CX-30
- Digital Check SmartSource Expert
- Digital Check SmartSource Merchant Elite
- Digital Check SmartSource Micro Elite
- Digital Check SmartSource Professional

- Digital Check SmartSource Professional Elite
- Digital Check TS-230\*
- Digital Check TS-240
- Digital Check TS-500
- Epson® S1000 CaptureOne
- Epson S2000
- Epson S9000
- Panini® I:Deal
- Panini Vision next
- Panini Vison X
- Panini wl:Deal
- RDM® EC7000i
- RDM EC7500i
- RDM EC9100i

\*Identifies scanners that have been discontinued by the vendor. FIS will provide help to customers using these scanners but cannot guarantee a resolution of all potential issues.

## Technical Support

FIS customers with a maintenance plan can contact FIS Technical Support in two ways:

Visit <https://my.fisglobal.com> and open a ticket.

For critical issues, call the critical issues hotline at 1-888-41-TOUCH (86824)

If your company does not have a current maintenance contract, you will be billed at an hourly rate for use of these services.

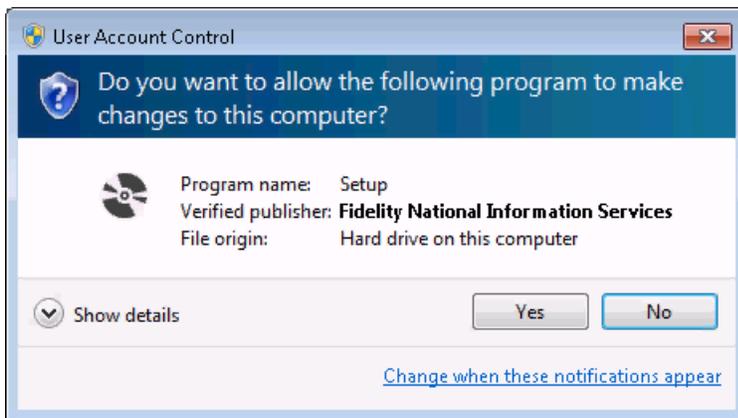
## Installation Scenarios

This section covers the various options available for new WebScan installations.

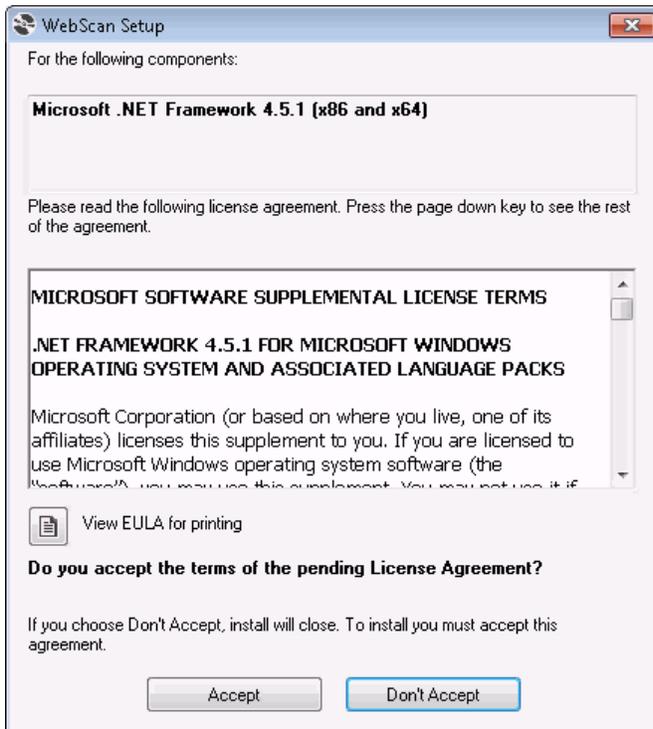
### Standard Installation

This section provides general information on the installation process of the WebScan application. The specific options may change, depending on the installation scenario and what pre-requisites have already been installed.

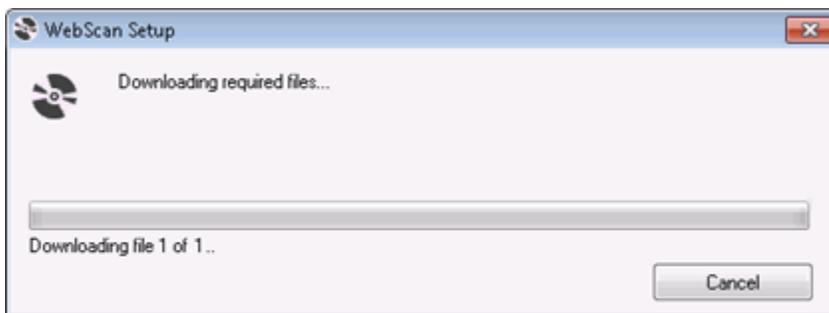
1. Execute the setup.exe to begin the installation process.
2. Depending on the workstation's User Account Control (UAC) setup, you may be prompted with a confirmation dialog. If so, click Yes to continue.



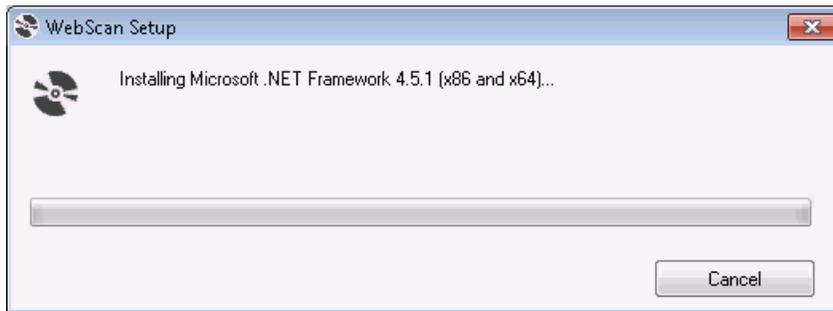
3. If .NET needs to be installed, the .NET 4.5.1 End User Licensing Agreement, click Accept to proceed. Otherwise, proceed to step 5.



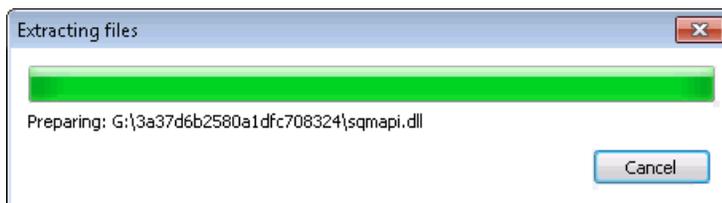
4. After accepting the licensing agreement, .NET will install through a series of dialogs.
  - a) Downloading the .NET installer.



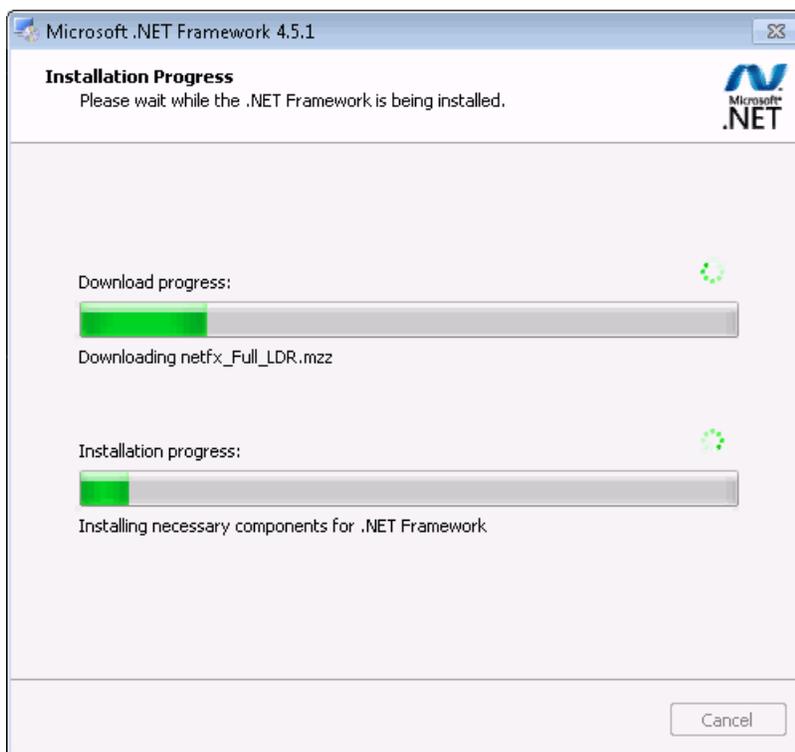
b) Execution of the .NET installer



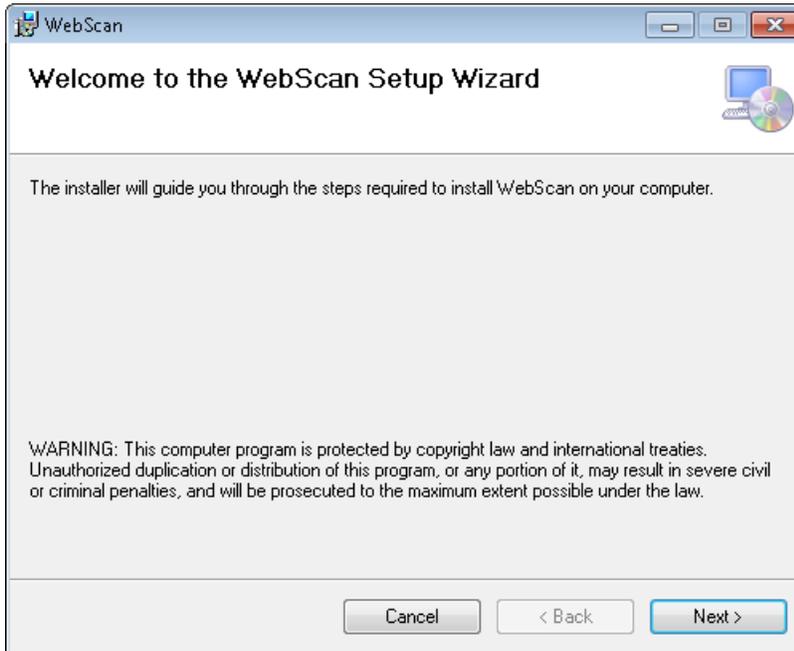
c) Extraction of the installer.



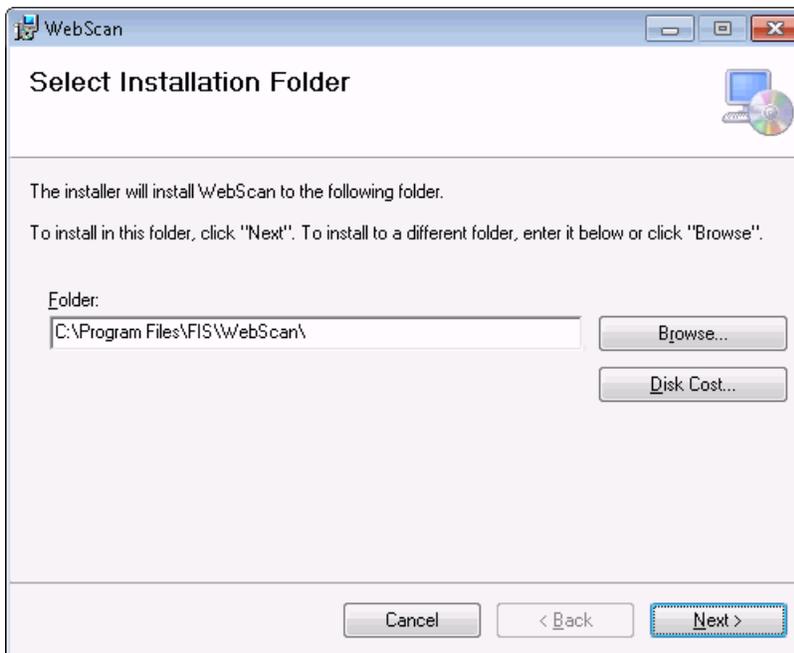
d) Downloading additional files required based on your system and completing the .NET installation.



- The Welcome dialog displays. Click Next to continue.



- The Select Installation Folder dialog displays. If you want to select where to install the software, click Browse and choose the location; otherwise keep the default location. When finished, click Next to install WebScan.

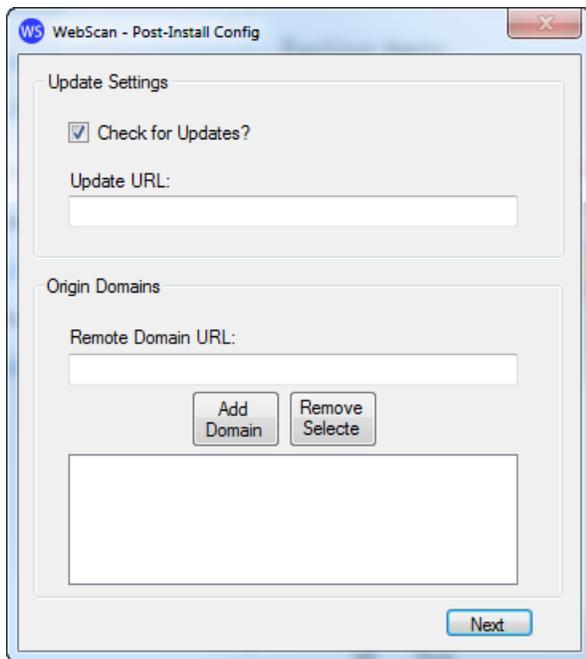


7. Enter the following parameters on the WebScan – Post Install Config dialog and click Next to continue.

---

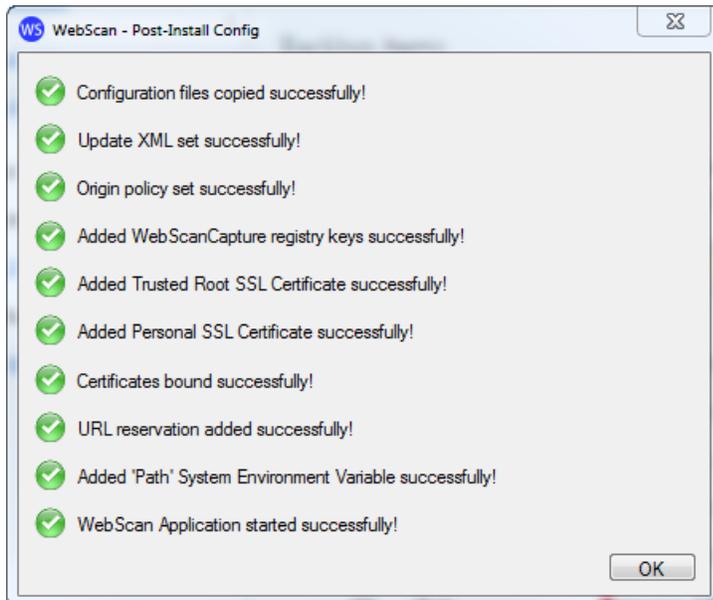
*The WebScan – Post Install Config behavior can be managed using the configuration xml. For more information, see [Setting Parameter Values](#).*

---

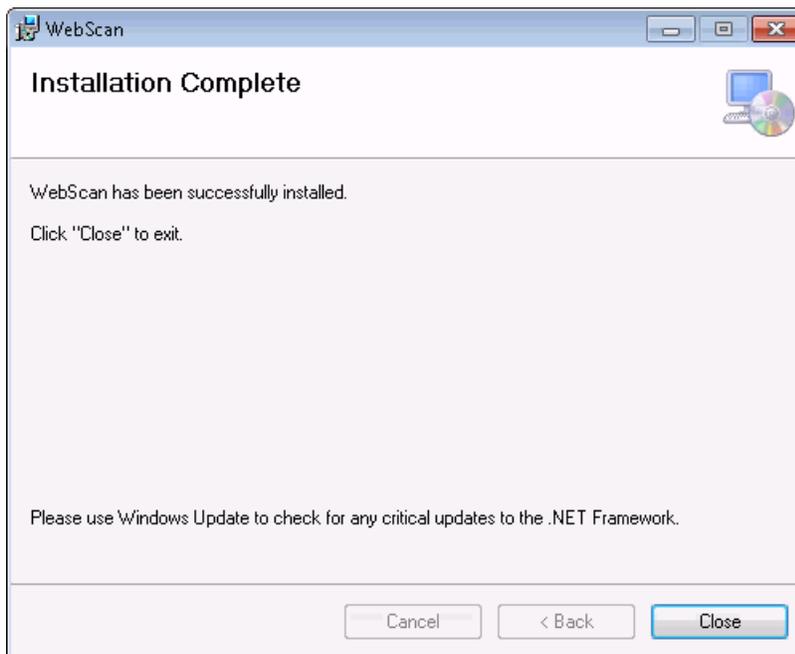


- a) If you want WebScan to automatically check for updates, keep the “Check for Updates?” box checked.
- b) In the Update URL field, specify the URL WebScan will use to check for new updates and to download from when updates are available.
- c) Enter the domain URL of the website(s) allowed to connect to WebScan in the Remote Domain URL field and click Add Domain.
- d) When all configurations are entered, click Next to continue.

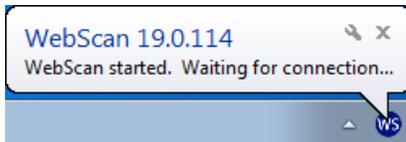
- The WebScan – Post Install Config validation dialog is displayed. Click OK to continue.



- The Installation Complete dialog is displayed. Click Close to complete the installation.



10. When installation has completed, WebScan will automatically start, referencing the current version in the systray.



## Setting Parameter Values

The WebScan msi installer can use an associated configuration xml file to set the values used in the Post-Install steps, like the update URL and origin domains. The file must be named the same as the msi package (WebScanCapture\_Setup.xml). Only the values and behavior of the Post Install Config forms are impacted. This file does not manage any other installer behaviors. The configuration xml can be used when performing a manual or automatic update.

The contents of the file are:

```
<root>
  <CheckUpdate>Y</CheckUpdate>
  <UpdateURL>https://domain.fisglobal.com/webscan</UpdateURL>
  <IsQuiet>Y</IsQuiet>
  <OriginDomains>
    <domain>https://domain.fisglobal.com</domain>
    <domain>https://alternate.fisglobal.com</domain>
  </OriginDomains>
</root>
```

**ChkUpdate** - Sets the bool to determine if WebScan automatically checks the server for updates. Options Y of N

**UpdateUrl** - Sets the URL used to check for updates and downloading new versions of WebScan. This value is provided by your service provider.

**IsQuiet** – Determines if the WebScan Post Install Config dialogs are displayed during installation.

If 'Y', the configuration dialogs are not displayed. Steps 10 and 11 are not shown from the [Standard Installation](#) workflow.

If 'N', the configuration dialogs are displayed, but prepopulated with the values configured in this file.

**OriginDomains** - A list of secure origin domains, each in their own <domain> tag, that can access WebScan.

## Batch File Installation

WebScan can be installed using a batch file. This allows for additional flexibility and scripting during the installation process

This section describes how to create a batch file to install WebScan with the desired input parameters. This can be used with both installers; the WebScan\_CaptureSetup.msi and the setup.exe.

### Command Line parameters

**/quiet** - Sets the installer to run in quiet mode. There is no user interaction. (optional)

**/passive** – Sets the installer to run in unattended mode. The installation shows only a progress bar. (optional)

**/forcerestart** – The machine will be restarted after the installation complete. (optional)

**ChkUpdate** - Sets the bool to determine if WebScan automatically checks the server for updates. Default = Y.

Options Y of N

**UpdateUrl** - Sets the URL used to check for updates and downloading new versions of WebScan. This value must be obtained from your service provider.

**Domains** - A list of secure domains, separated by space then vertical line then space ( | ), that can access WebScan.

### Sample Batch File

```
@ECHO OFF
```

```
SET WSDIRECTORY=%~dp0
```

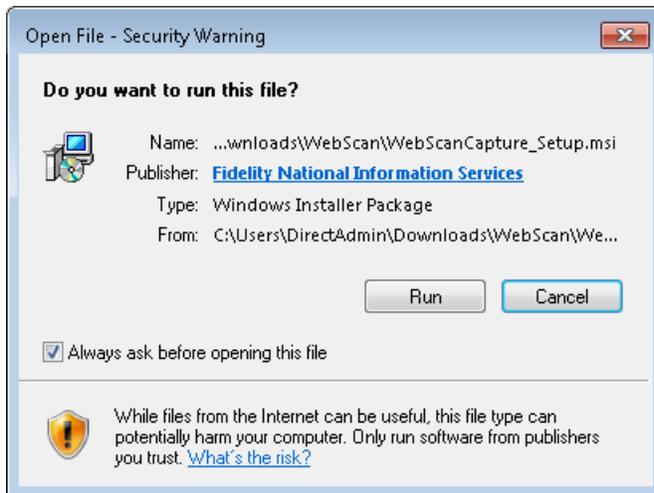
```
cd /d "%WSDIRECTORY%"
```

```
WebScanCapture_Setup.msi /passive ChkUpdate=Y UpdateURL="https://www.domain.com/WebScanUpdate"
```

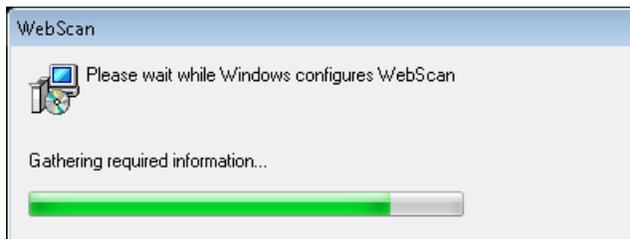
```
Domains="https://www.domain.com | https://www.alternate.com " >> InstallLog.txt
```

## Installation Workflow

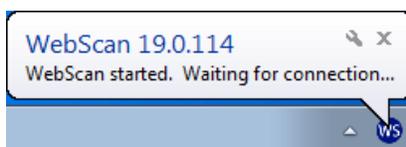
1. Security Warning prompt is presented. Click Run to continue.



2. If running in passive mode, the progress dialog is displayed.



3. When installation has completed, WebScan will automatically start, referencing the new version.



## Update Scenarios

### Auto Update

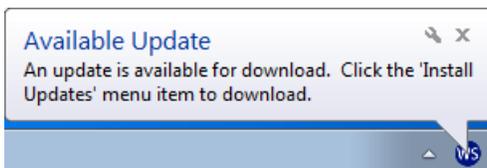
This section covers how WebScan automatically applies updates. If WebScan is configured to check for new updates, it checks at start up and every 6 hours.

---

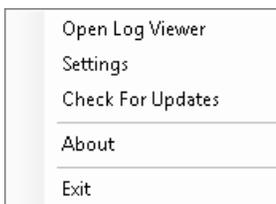
*Version 17.0.1204 or newer is required for auto update to work. Older versions must manually update. See [Manual Update](#) section for steps.*

---

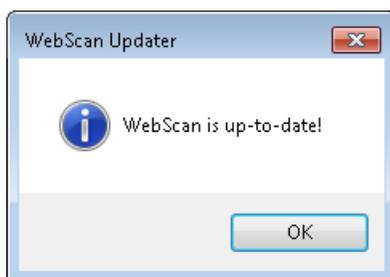
When an update is available, a pop up notification is shown to the user.



To manually check if an update is available, you can select the Check For Updates systray menu option.



If WebScan is on the most current version, an information dialog is display. Click OK to close the message.

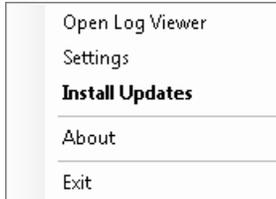


To Install the latest update, you must be logged in as a Windows administrator or manually select WebScan to Run as Administrator:

1. Right click on the WebScan systray icon.

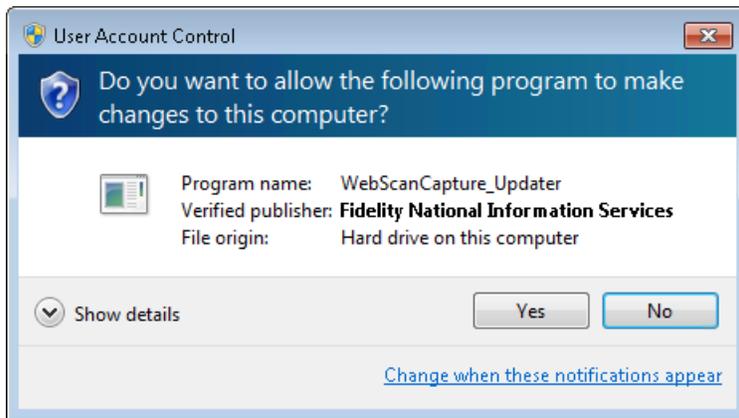


2. Select Install Updates.

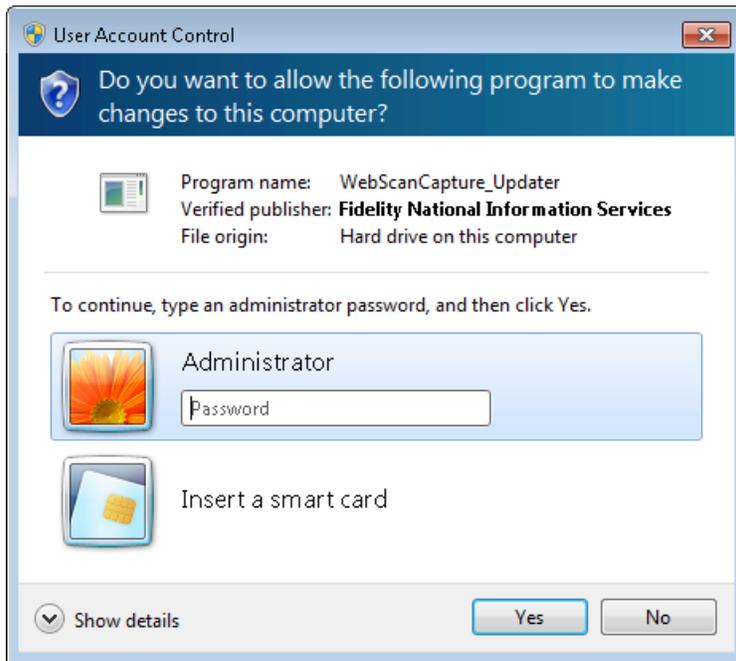


3. Depending on the workstation's User Account Control (UAC) setup, you may be prompted with a confirmation dialog. If the user does not have the required Windows permissions to apply updates, escalated credentials can be provided within the confirmation dialog. Contact your system administrator to apply the update. Once you are ready to proceed, click Yes to continue.

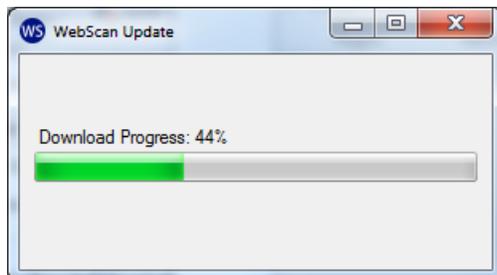
a. UAC confirmation dialog.



- b. UAC confirmation dialog requiring administrative permission.

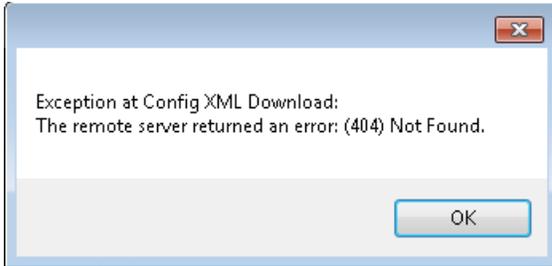


- 4. After selecting Install Updates, WebScan will exit and a download progress dialog is displayed.

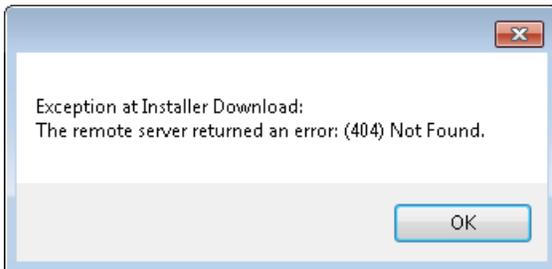


5. If there is an error with the downloaded files, an error message is displayed. Click OK to exit the installation and contact your system administrator.

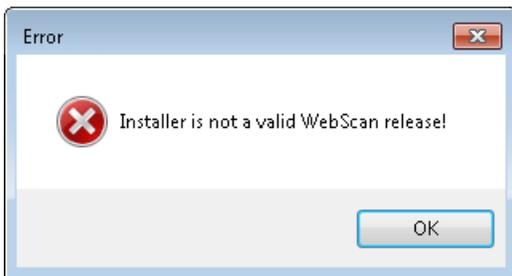
a. If there is an error downloading the configuration file, the following message is displayed:



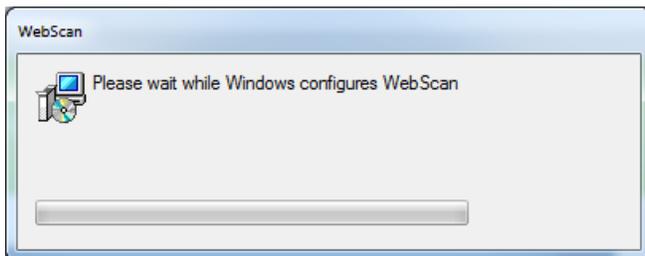
b. If there is an error downloading the WebScan installer, the following message is displayed:



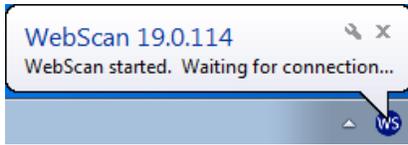
c. If the WebScan installer does not pass code validation, the following message is displayed:



6. Installation will start immediately after the download is complete.



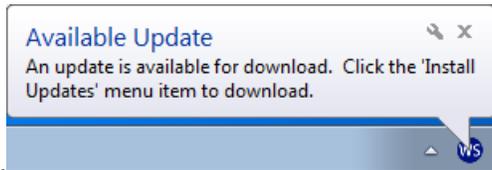
- When installation has completed, WebScan will automatically start, referencing the new version in the systray.



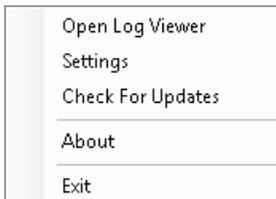
### Auto Update Pre-18.0.1018

Starting with version 18.0.1018, the update process has been modified to improve the user experience. Updating from previous versions is supported, but the user experience is slightly different.

When an update is available, a pop up notification is shown to the user.



If you would like to manually check if an update is available, you can select the Check For Updates sys tray menu option.

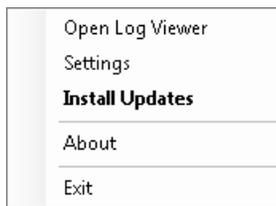


To Install the latest update, you must be logged in as a Windows administrator or manually select WebScan to Run as Administrator:

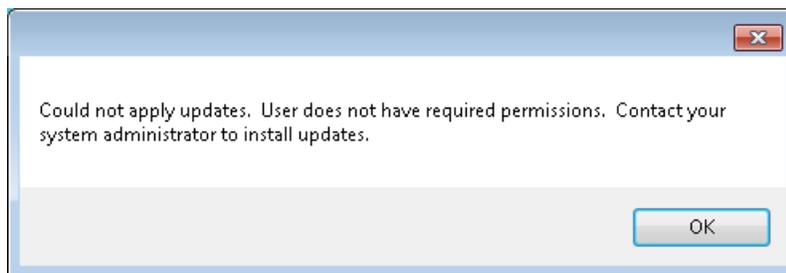
- Right click on the WebScan systray icon.



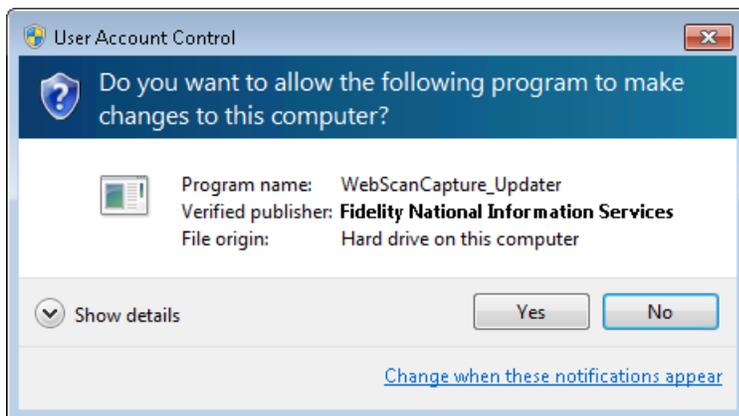
2. Select Install Updates.



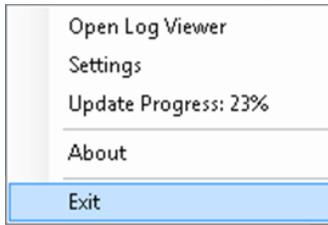
3. If the user does not have the required Windows permissions to apply updates, an information dialog is presented.



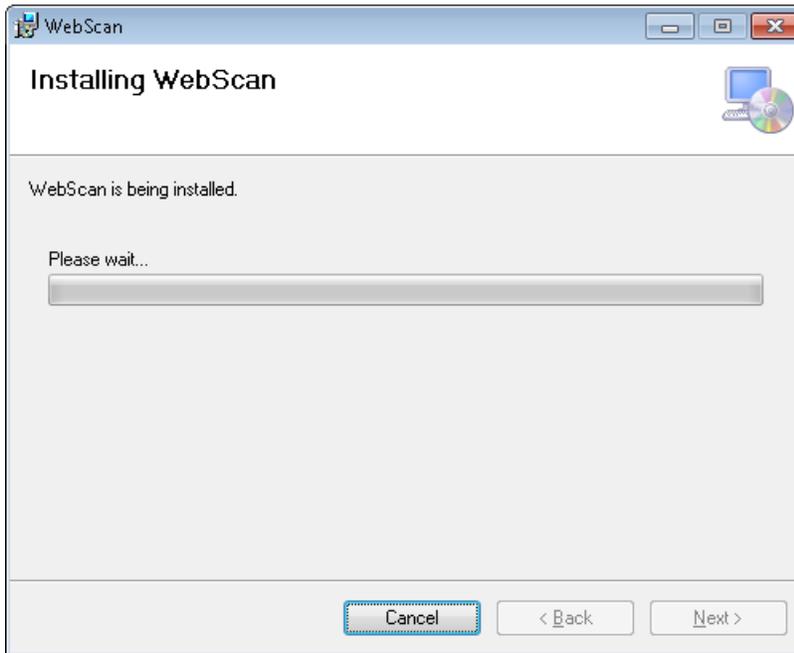
4. Depending on the workstation's User Account Control (UAC) setup, you may be prompted with a confirmation dialog. Click Yes to continue.



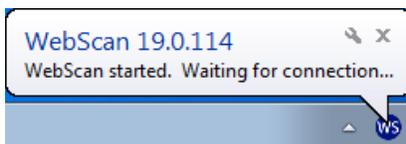
- The update progress (which includes downloading the update) can be viewed by looking at the WebScan systray menu.



- Installation will start immediately after the download is complete.



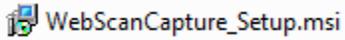
- When installation has completed, WebScan appears to, but does not automatically start. Execute the WebScan shortcut on the Desktop to restart WebScan. The new version is referenced in the systray.



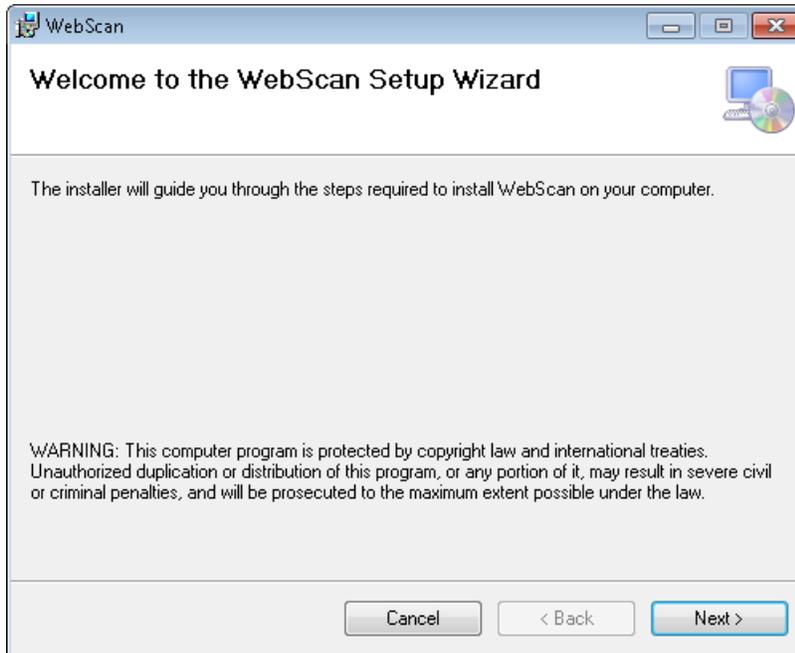
## Manual Update

This process is when the user needs to manually update WebScan.

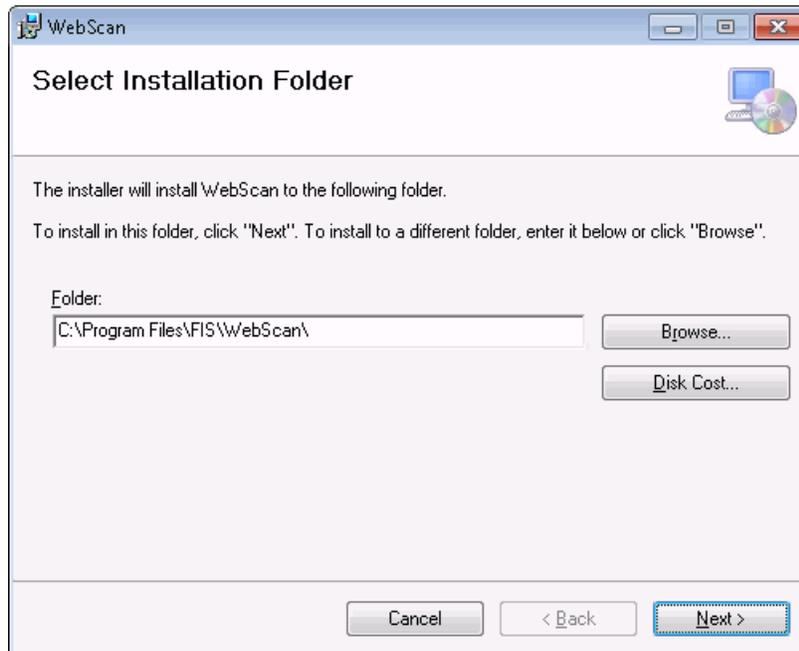
1. Obtain a local copy of WebScanCapture\_Setup.msi and execute.



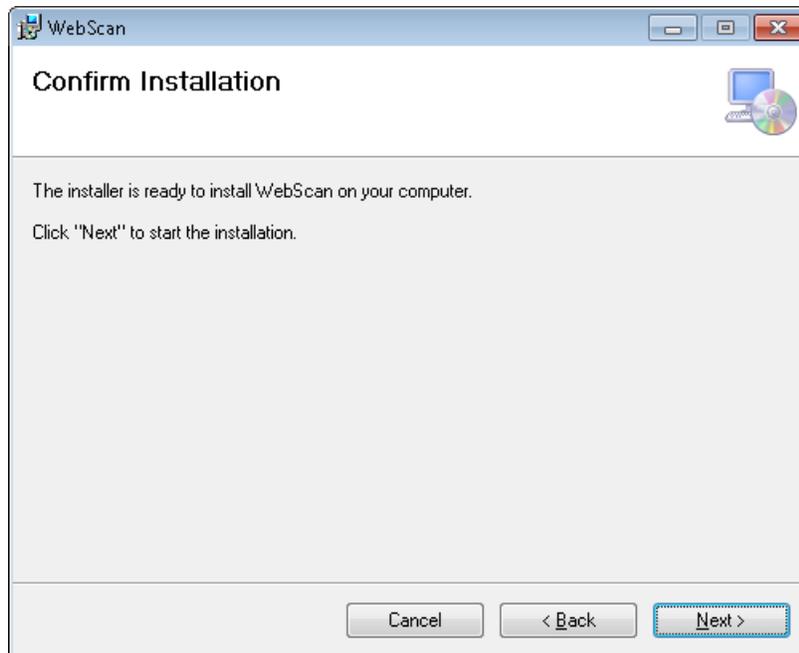
2. Presented with the Welcome dialog. Click Next.



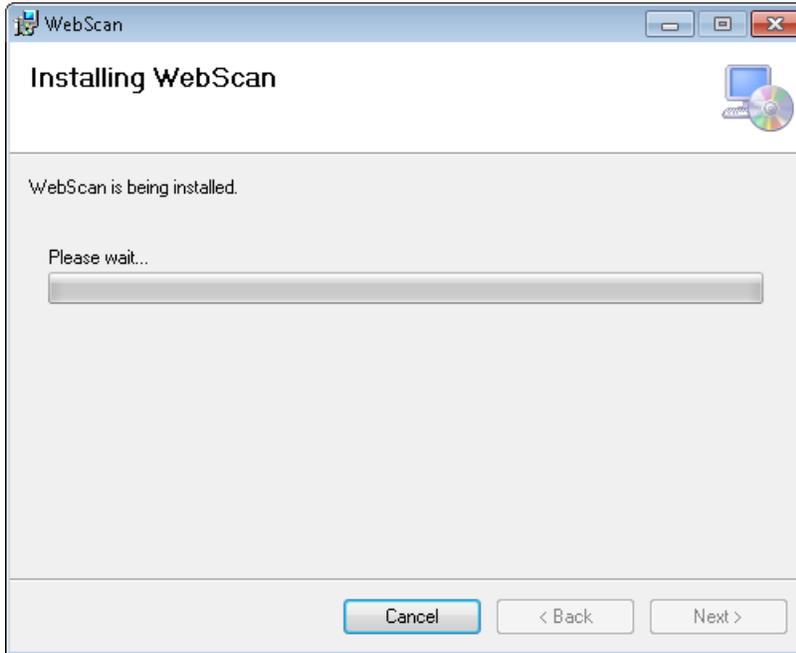
- Presented with the Installation Folder dialog. Click Next.



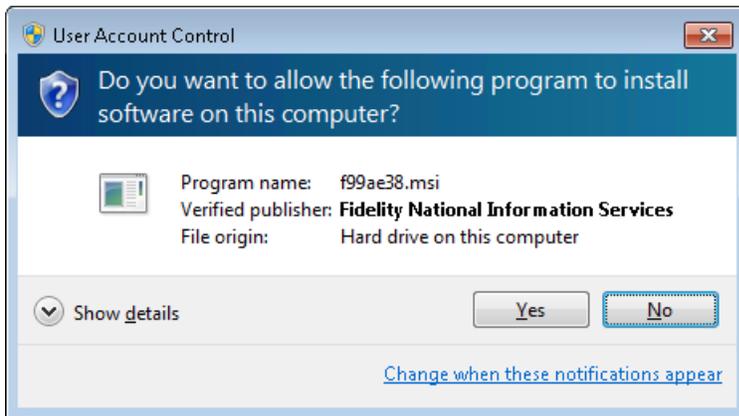
- Presented with the Confirm Installation dialog. Click Next to continue.



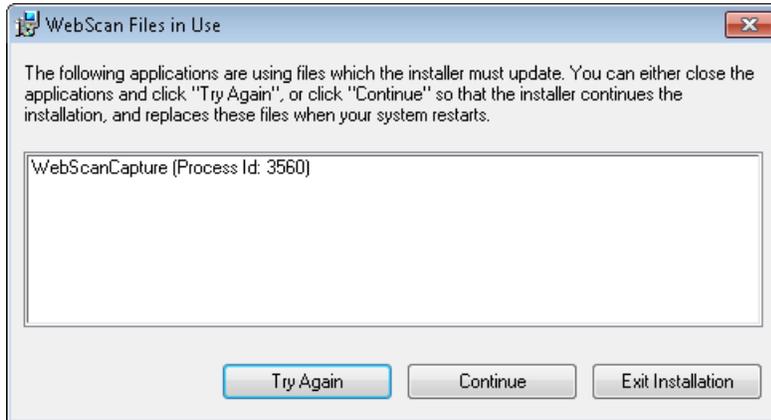
- Presented with the Installing WebScan dialog.



- Depending on your system's User Account Control (UAC) setup, you may be presented with confirmation dialog. Click Yes to continue.



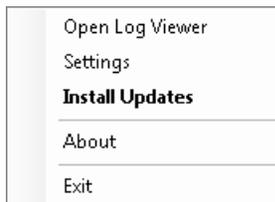
7. If WebScan is still running, you are presented with the Files in Use dialog. By clicking Continue, you can skip the rest of this step, but a system restart will be required after installation completes.



- a. Right click on the WebScan systray icon.

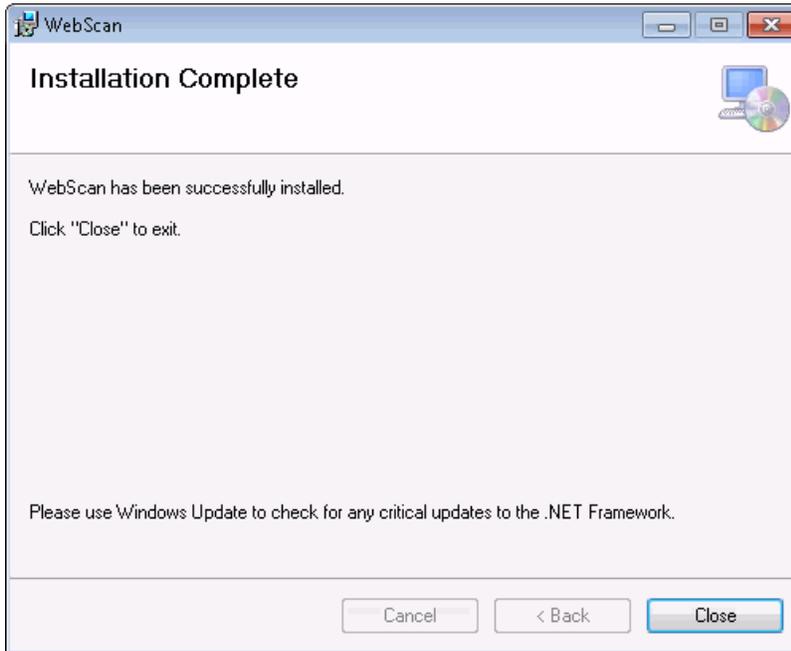


- b. Select Exit

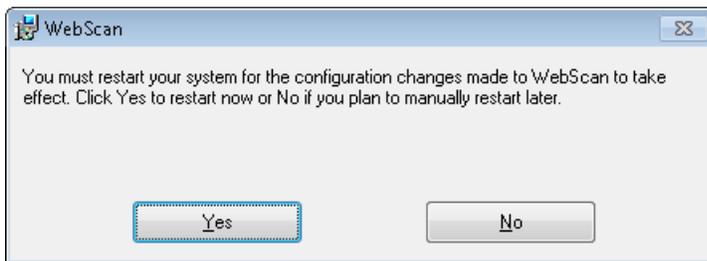


- c. Click Try Again.

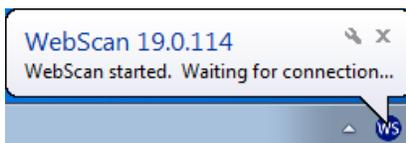
- The Installation Complete dialog is presented. Click Close to continue.



- If you choose Continue on step 7, you are presented with a dialog prompting a system restart. Click Yes to complete the installation now, or No to manually restart later to complete installation.



- When installation has completed, WebScan will automatically start, referencing the new version. If updating from version 18.0.706 or older, you will need to manually launch WebScan by executing the WebScan desktop shortcut.



## RDC Client Update

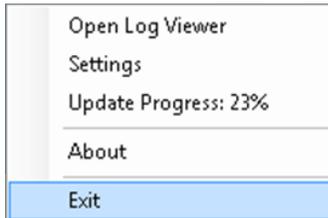
WebScan's update process can be managed entirely by the RDC client. In this scenario, the RDC client determines when WebScan checks for and applies the update. While the notification and execution of the update experience will be different by RDC client, the WebScan update steps will be the same. Please refer to your RDC client provider for detailed information of this process.

---

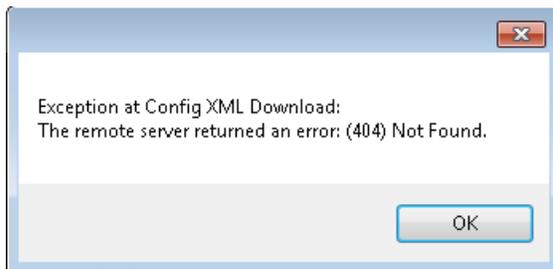
*WebScan must be on a minimum of 18.0.1018 to be managed by a RDC client.*

---

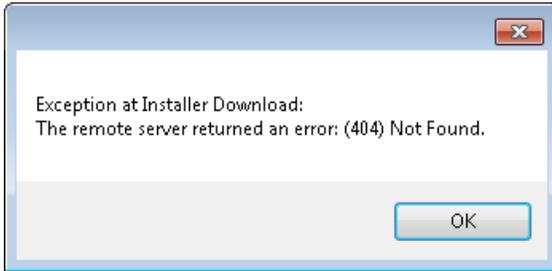
1. The update progress (which includes downloading the update) can be viewed by looking at the WebScan systray menu.



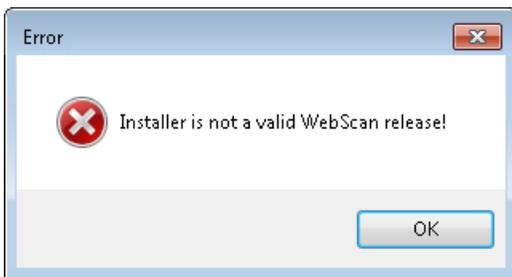
2. If there is an error with the downloaded files, and error message is displayed. Click OK to exit the installation and contact your system administrator.
  - a. If there is an error downloading the configuration file, the following message is displayed:



- b. If there is an error downloading the WebScan installer, the following message is displayed:

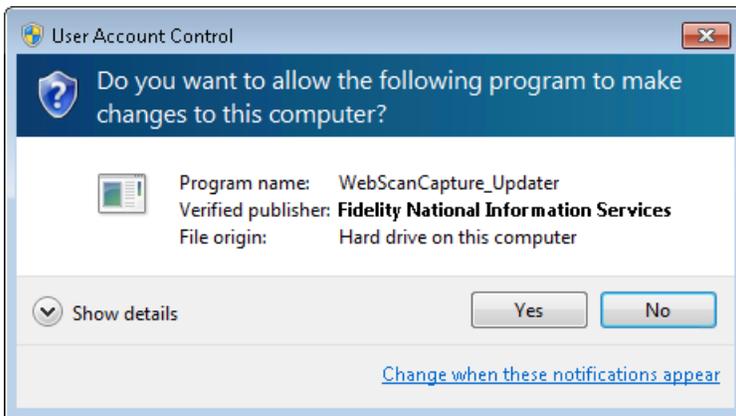


- c. If the WebScan installer does not pass code validation, the following message is displayed:

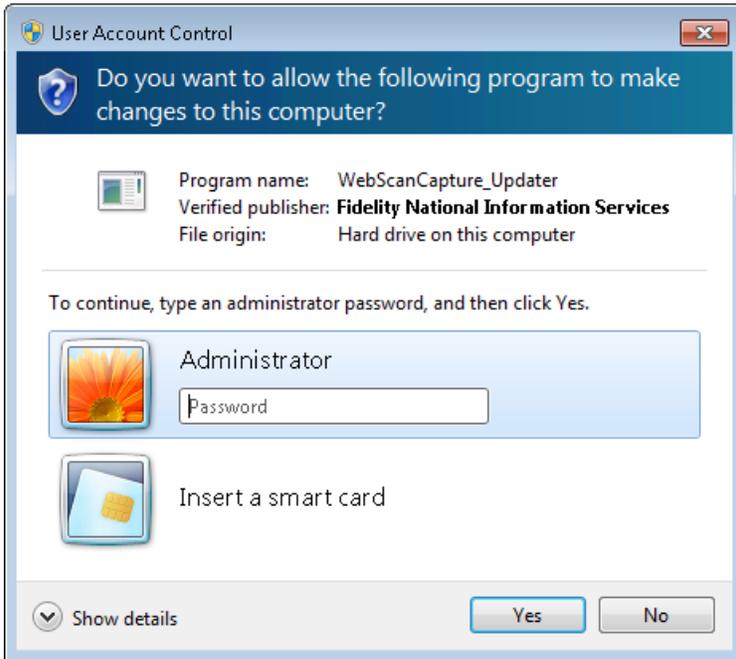


- 3. Depending on the workstation's User Account Control (UAC) setup, you may be prompted with a confirmation dialog. If the user does not have the required Windows permissions to apply updates, escalated credentials can be provided within the confirmation dialog. Contact your system administrator to apply the update. Once you are ready to proceed, click Yes to continue.

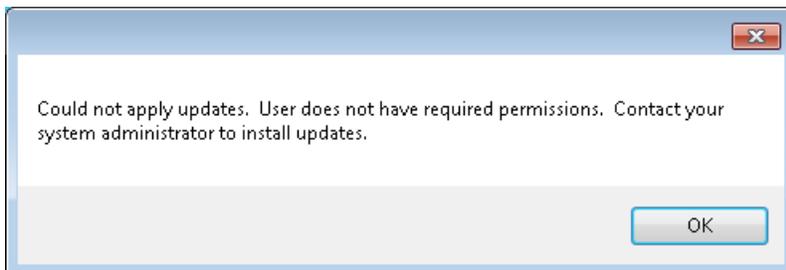
- a. UAC confirmation dialog.



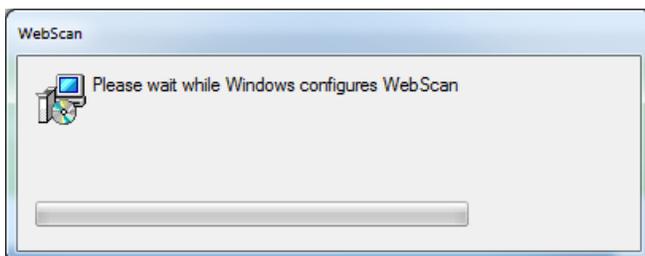
- b. UAC confirmation dialog requiring administrative permission.



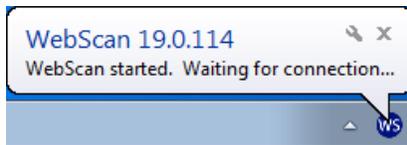
- 4. If the user does not have the required Windows permissions to apply updates, an information dialog is presented. Click OK to exit the installation and contact your system administrator to apply the update.



- 5. Installation will start immediately after the download is complete.



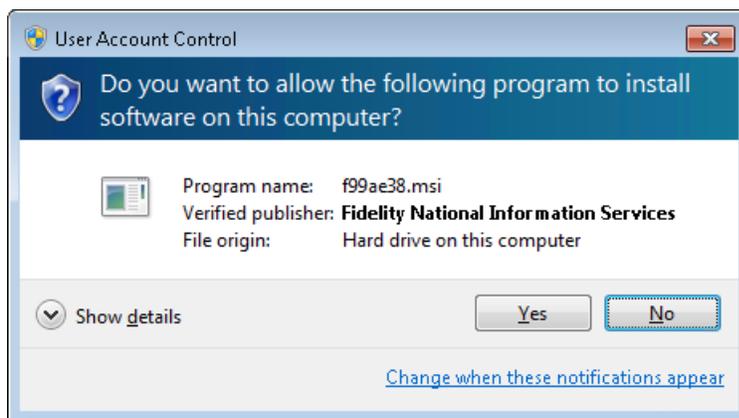
- When installation has completed, WebScan will automatically start, referencing the new version. If upgrading from a version older than 18.0.1018, you will need to manually launch WebScan using the Desktop shortcut.



## Uninstallation

Steps may vary slightly based on your operating system.

1. Select Start Menu.
2. Select Control Panel.
3. Select Programs and Features.
4. Select WebScan from the list of Programs.
5. Select Uninstall.
6. Depending on your system's User Account Control (UAC) setup, you may be presented with confirmation dialog. Click Yes to continue.



## System Tray Menu

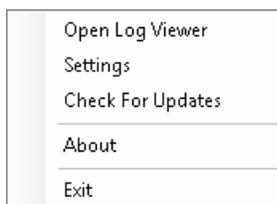
This section reviews configuration and menu options available from WebScan's system tray (systray) menu.

To get to the menu and configuration options.

1. Right click on the WebScan systray icon.



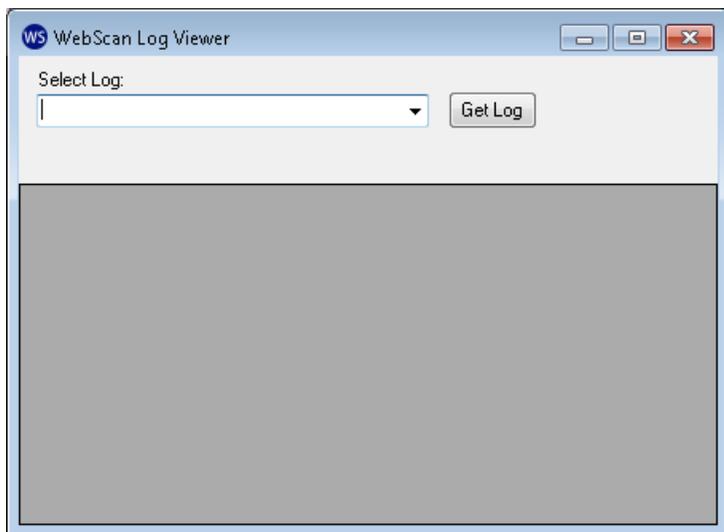
2. The systray menu displays



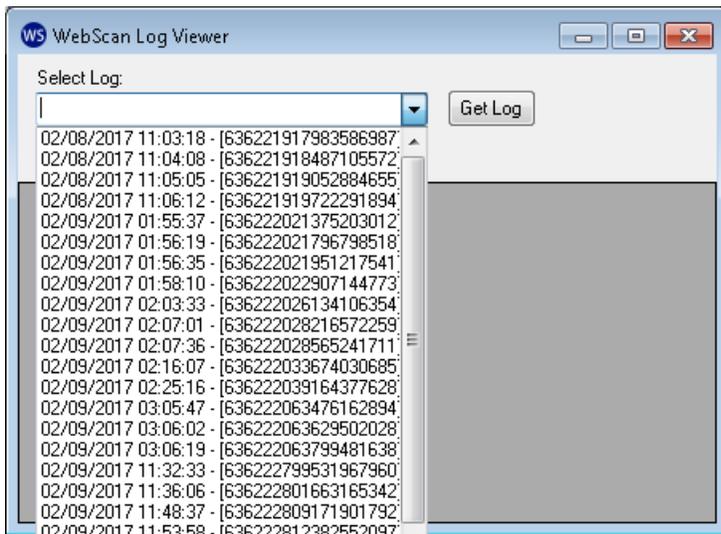
## Log Viewer

The log viewer can be used to review logs from the last 7 days.

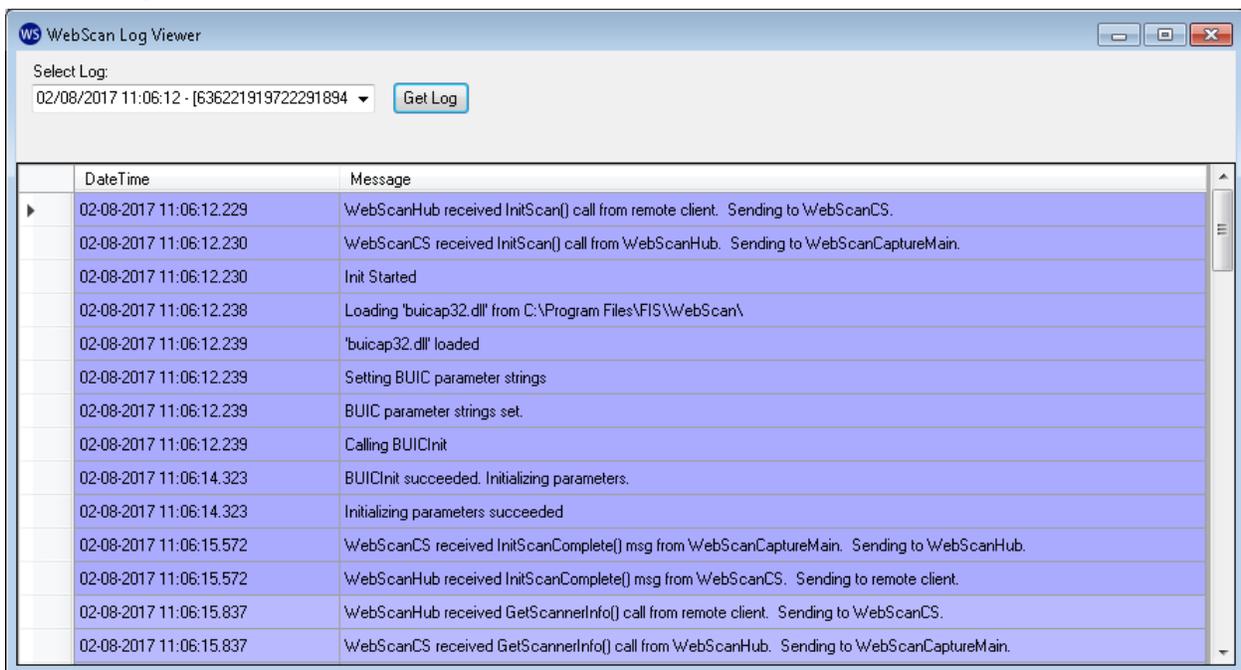
1. Select Open Log Viewer.



- Select the log entry for the desired session from the dropdown list.



- Click Get Log to view the selected entry.

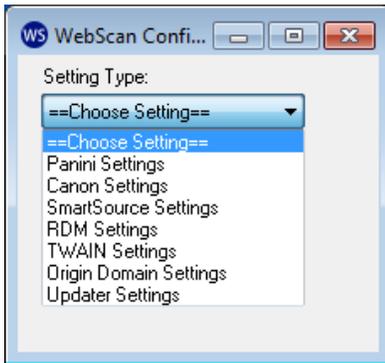
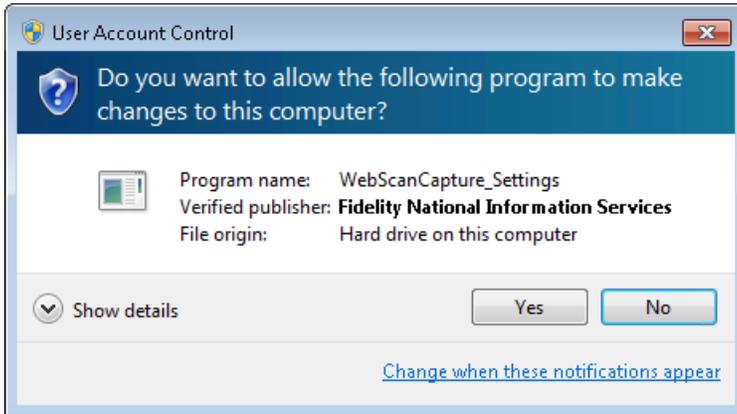


- When finished, close the dialog using clicking the red x button in the upper right hand corner.

## Settings

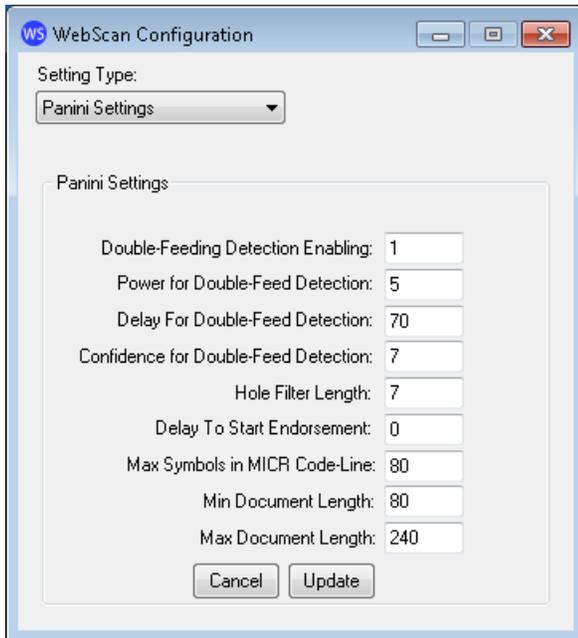
Use the settings section to configure WebScan and specific scanner settings.

Depending on your user's privileges and the system's User Account Control (UAC) setup, you may be presented with a confirmation dialog. Click Yes to continue.



## Panini Settings

This provides the Panini scanner settings that are available to access within WebScan. To access, select Panini Settings from the Setting Type list.



**Double-Feeding Detection Enabling** – Determines if double feed detection is enable or not (0 -1, default is 1 enabled).

**Power for Double-Feed Detection** – Sets the power value of the photocell detecting the Double Feeding. A higher value means fewer double feeds will be detected (2 – n, default is 5).

**Delay for Double-Feed Detection** – The Delay is the distance from the lead edge of the document where the test sampling of the sensors begins (10 mm – 150 mm from leading edge, default is 70mm). If a frequent false double feed is being detected due to a heavily printed signature. Increasing the Delay may resolve the problem.

**Confidence for Double-Feed Detection** – The sensor reading is sampled many times while the document passes in front of it. The Confidence setting allows you to set the percentage of times the sensor must detect a double feed to report the double feed condition (2 – 10, default is 7). For example, if set at 7, then the sensor must be blocked in 70% or more of the samples to report a double feed. A higher value means fewer double feeds will be reported. The range for this setting is 2 to 10, representing 20% to 100% of samples reporting a double feed are required for the device to report a double feed.

**Hole Filter Length** – To avoid holes in the paper indicating document end (5 mm – 10 mm, default is 7 mm).

**Delay To Start Endorsement** – Set the delay in print starting, referred to the leading edge of the document (0 mm – 220 mm, default is 0 mm).

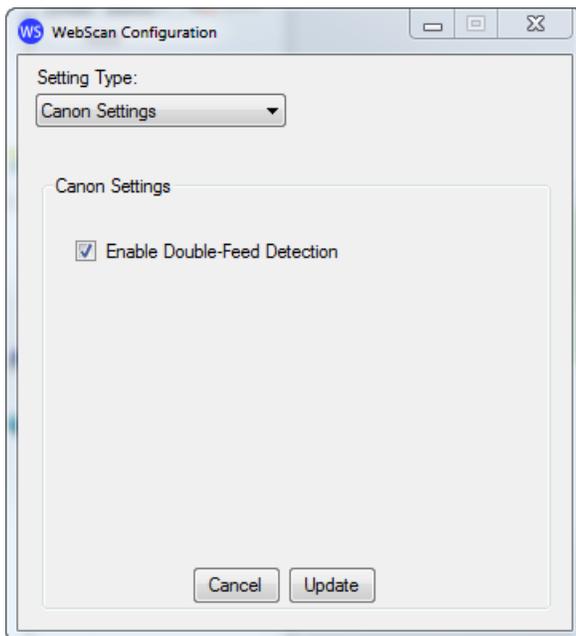
**Max Symbols in MICR Code-Line** – This parameter can reduce the MICR reading length. The value represents the maximum number of MICR symbols accepted (10 – 80, default is 80).

**Min Document Length** – This value is the minimum document length accepted (80 – 240 mm, default is 80).

**Max Document Length** – This value is the maximum document length accepted (80 – 240 mm, default is 240).

## Canon Settings

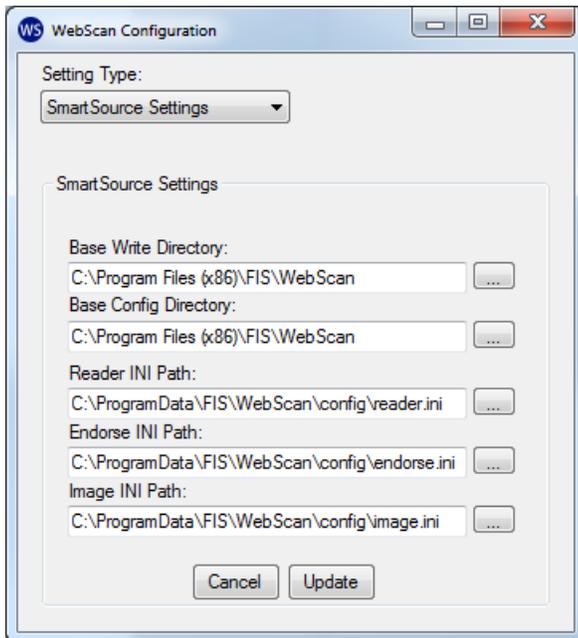
This provides the Canon scanner settings that are available to configure within WebScan. To access, select Canon Settings from the Setting Type list.



**Enable Double-Feed Detection** – Check box that enables/disables double feed detection for Canon scanners. This is enabled by default.

## SmartSource Settings

This provides the SmartSource scanner settings that are available to configure within WebScan. To access, select SmartSource Settings from the Setting Type list.



**Base Write Directory** – This path must be a writable folder to extract temporary resources and save trace logs. All files created here are overwritten on every SmartSource initialization. Default path is 'C:\Program Files (x86)\FIS\WebScan'.

**Base Config Directory** – This path is used for user-customized .ini files, or Digital Check provided patches, which will be copied at initialization time to the Base Write Directory. Default path is 'C:\Program Files (x86)\FIS\WebScan'.

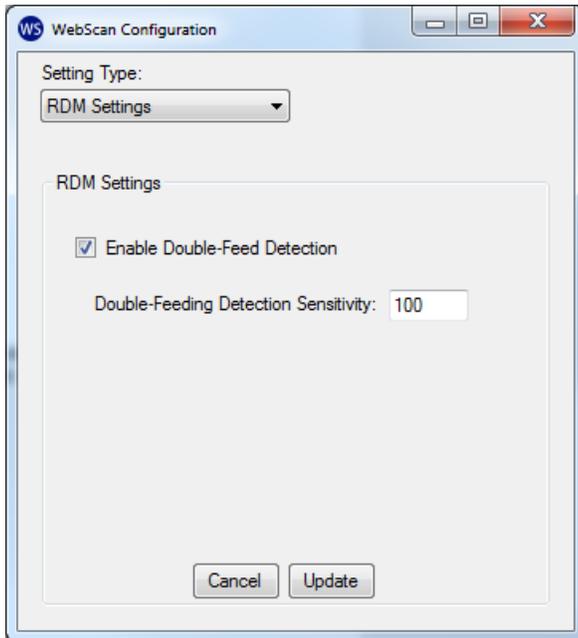
**Reader INI Path** – The path to read the reader.ini file. Default path is 'C:\ProgramData\FIS\WebScan\config\reader.ini'.

**Endorse INI Path** – The path to read the endorse.ini file. Default path is 'C:\ProgramData\FIS\WebScan\config\endorse.ini'.

**Image INI Path** – The path to read the image.ini file. Default path is 'C:\ProgramData\FIS\WebScan\config\image.ini'.

## RDM Settings

This provides the Canon scanner settings that are available to configure within WebScan. To access, select RDM Settings from the Setting Type list.



**Enable Double-Feed Detection** – Check box that enables/disables double feed detection for RDM scanners. This is enabled by default

**Double-Feeding Detection Sensitivity** – Determines how sensitive is the double feed detection (1 – 100, default is 100).

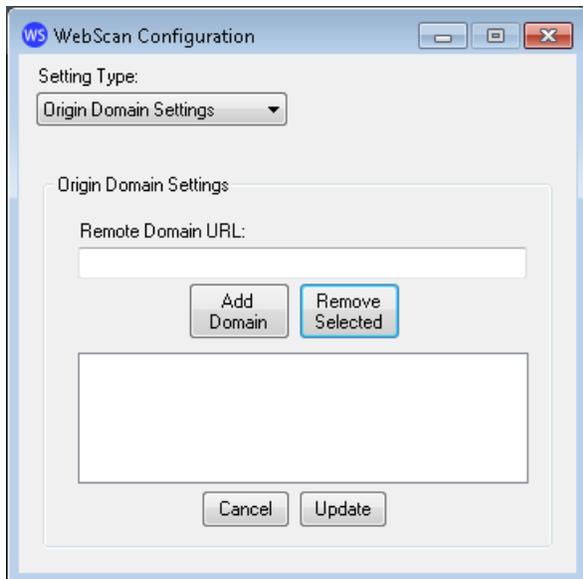
## Origin Domain Settings

WebScan requires cross-domain access to allow the RDC client access. To prevent any website access to WebScan, origin domain settings configure a white list of domains. If the RDC hosted domain is not configured within the origin domain settings, it will be prevented from communicating with WebScan. More than one domain can be configured.

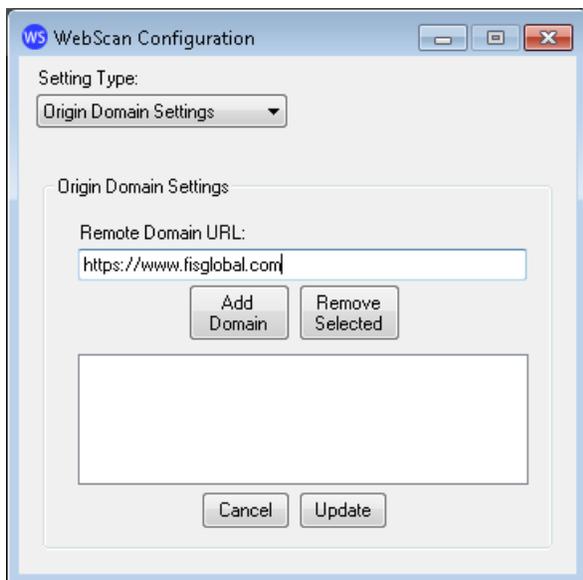
This configuration requires a user with admin rights to edit. Basic users are limited to a read-only view.

## Add a Domain

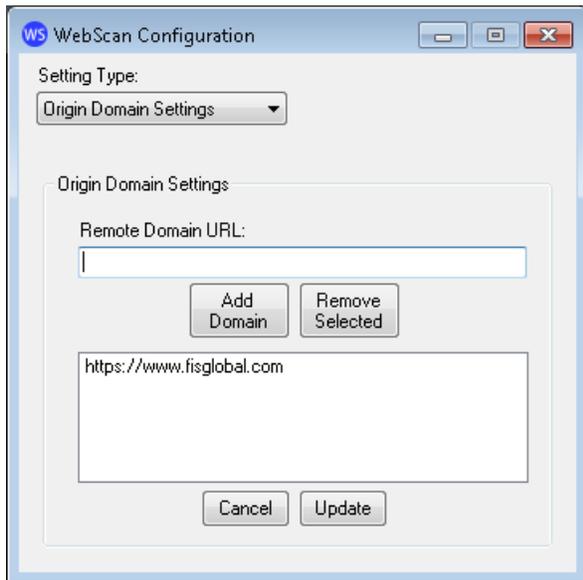
1. Select Origin Domain Settings.



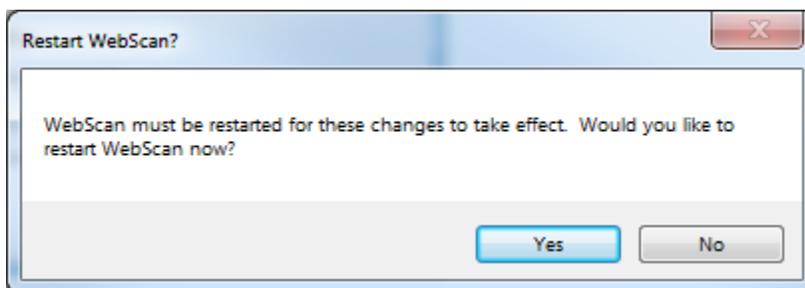
2. Insert the domain URL to allow access to WebScan. (i.e. if the RDC website is <https://www.fisglobal.com/RDC/Login.html>, the domain to add would be <https://www.fisglobal.com>).



3. Click Add Domain.



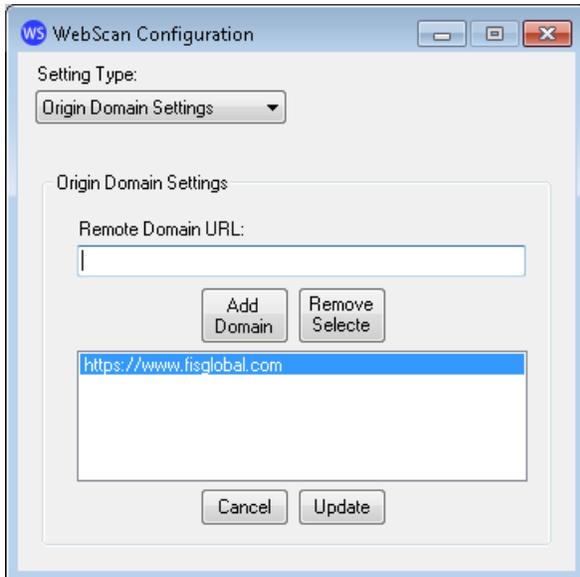
4. Click Update.



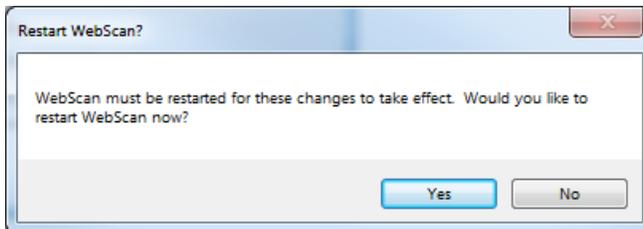
5. Clicking Yes will restart WebScan and apply the changes. Clicking No, saves the changes, but does not restart WebScan to apply the changes.
6. Close WebScan Configuration.

## Remove a Domain

1. Select Origin Domain Settings.



2. Select the desired domain from the list.
3. Click Remove Selected.
4. Click Update.

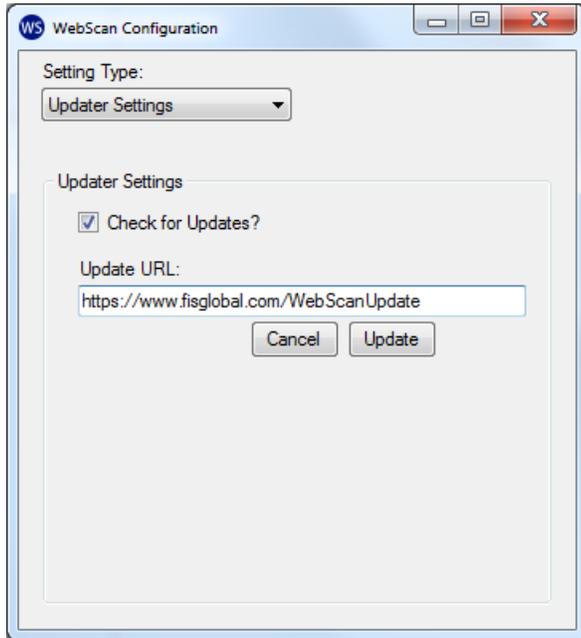


5. Clicking Yes will restart WebScan and apply the changes. Clicking No, saves the changes, but does not restart WebScan to apply the changes.
6. Close WebScan Configuration.

## Updater Settings

This section determines if WebScan checks for updates automatically, and where the update is available. Changes will not take effect until after WebScan is restarted.

This configuration requires a user with admin rights to edit. Basic users are limited to a read-only view.

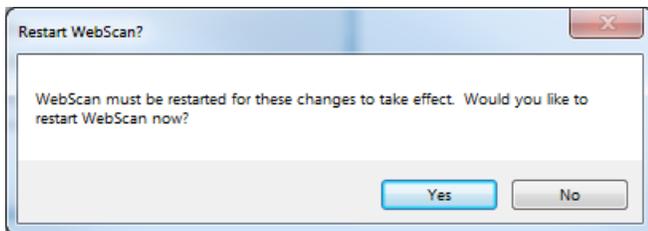


**Check for Updates?** – Enables the auto update functionality.

**Update URL:** - The URL where the most current version is maintained.

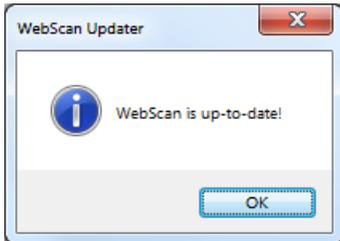
If changes are made, click Update.

Clicking Yes will restart WebScan and apply the changes. Clicking No, saves the changes, but does not restart WebScan to apply the changes.



## Check For Updates

This option manually checks for a new version of WebScan. If an update is required, the user can select the Install Updates option. If the installed version is up to date, the current version dialog displays. Click OK to close this dialog.

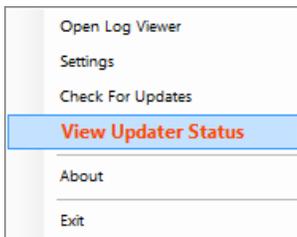


## Install Updates

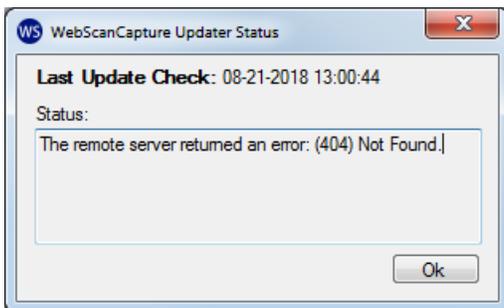
This option initiates the download and applies the newest version of WebScan. See the [Auto Update](#) section for more information.

## View Updater Status

This option only displays if there was a failure connecting to the Update URL when checking for an update.

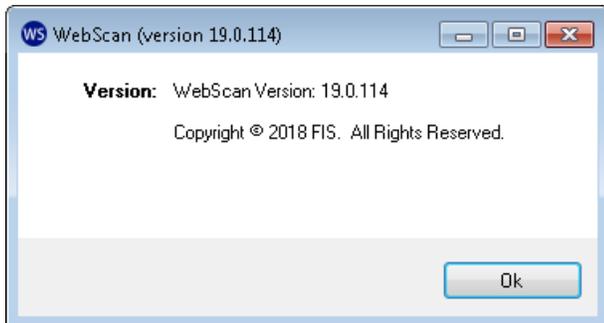


If selected, it opens the WebScan Updater Status dialog to display what error occurred.



## About

This option shows the current version and copyright information.



## Exit

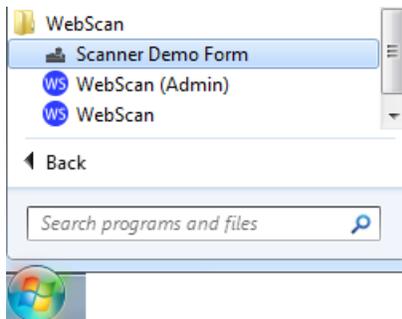
This option will close WebScan.

## Scanner Test Capture

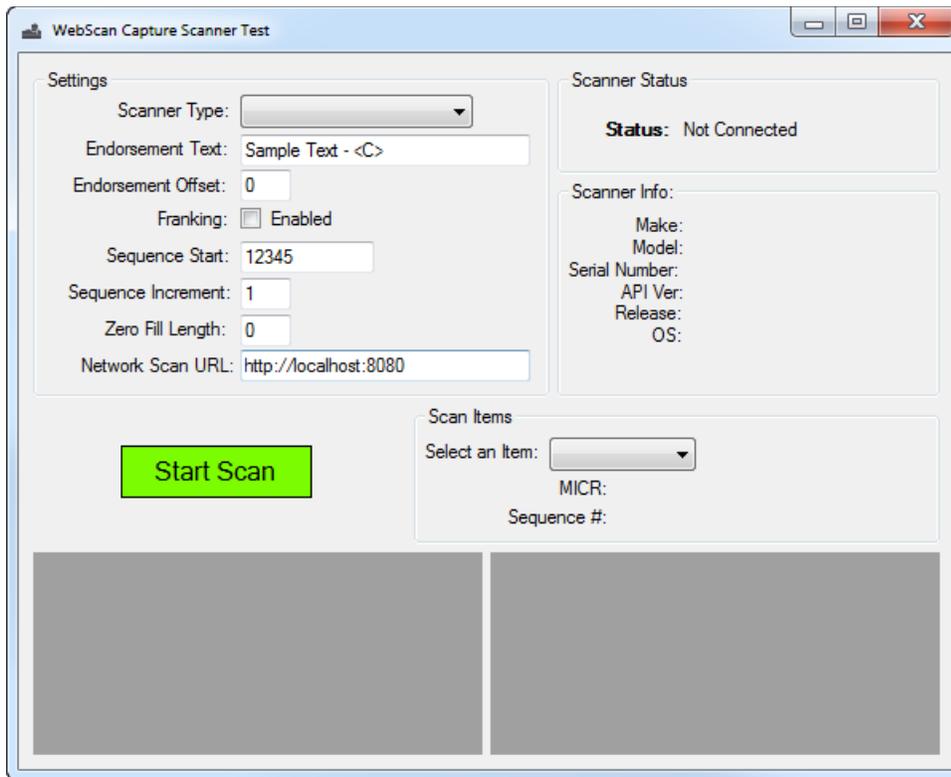
WebScan is installed with a scanner test application that can be used to test the integration to the scanner API. The does not utilize the signalr hub to access the scanner through WebScan, but to use the same code as WebScan to connect to the scanner.

To use the test application,

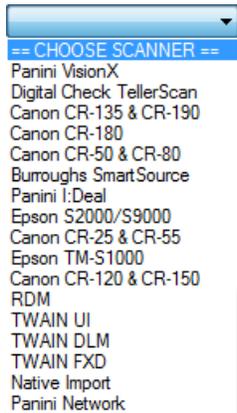
1. Open the Start Menu and select WebScan | Scanner Demo Form.



2. The test form opens.



3. Select the desired Scanner Type:



4. If the scanner does not use an ink cartridge or you wish to not test the physical endorser, delete the contents in the Endorsement Text field.
5. Select the Start Scan button to begin.

## Directory Structure

This section goes over the folder paths and files used by WebScan.

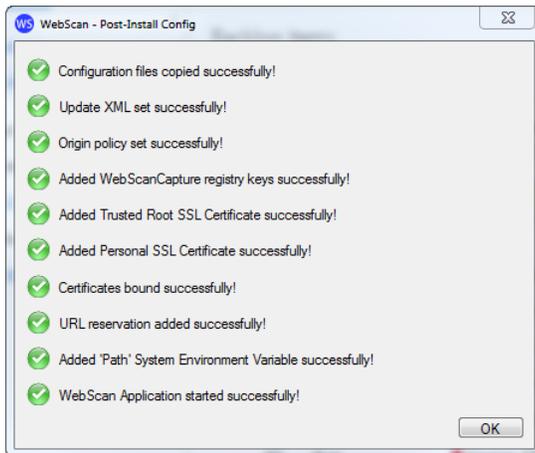
**C:\Program Files (x86)\FIS\WebScan** – the default installation path where the WebScan code, application executables and certificates are located.

### **C:\ProgramData\**

- a) **config** – Where the configuration files used by the scanners and WebScan are stored. The Origin Domain (domain.xml) and Updates (update.xml) configuration files are encrypted and can only be modified through the configuration interface.
- b) **log** – Where session log files are retained. WebScan keeps the last 10 days' worth of logs.
- c) **PostInstall** – Path where the post installation log is created.
- d) **Update** – Path where WebScan downloads the latest version and creates a log file during the update process.
- e) **UpdateCheck** – Path where WebScan creates a log file during the check for update process.

## Post-Install Config

During installation, there are custom configuration actions performed to setup WebScan to run on the workstation. If the `IsQuiet` is set to 'Y', this dialog is not displayed.



**Configuration files copied successfully!** – Files were successfully copied to the configuration path.

**Update XML set successfully!** – The `update.xml` file was successfully updated with the update URL.

**Origin policy set successfully!** – The `domain.xml` file was successfully updated with the configured domain(s).

**Added WebScanCapture registry keys successfully!** – WebScan components were registered with Windows.

**Added Trusted Root SSL Certificate successfully!** – Added FIS Certificate Authority certificate to the Trusted Root store.

**Added Personal SSL Certificate successfully!** – Added localhost certificate to the Trusted Root store.

**Certificates bound successfully!** – SSL certificates were bound to IP 127.0.0.1:58080.

**URL reservation added successfully!** – URL `https://127.0.0.1:58080` was reserved for Everyone.

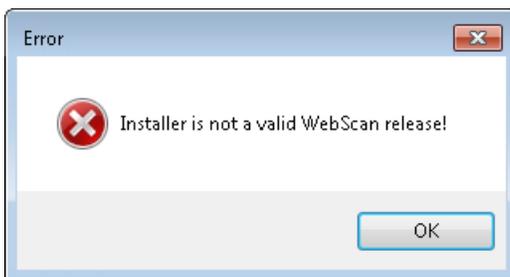
**Added 'Path' System Environment Variable successfully!** – The path to WebScan code ("`C:\Program Files (x86)\FIS\WebScan`") was added to the environment variable 'path'.

**WebScan Application started successfully!** – WebScan started without any recorded issues.

## Code Signing Certificates

Code signing is the process of digitally signing executables and scripts to confirm the software author, and guarantee that the code has not been altered or corrupted since it was signed. FIS updates their certificate every 2 years. As a security measure, the WebScan auto update feature verifies that the code was signed by a certificate issued by FIS. When a new certificate is issued, there is a transition period where a version of WebScan is signed with the old certificate, but now recognizes the new certificate. The minimum version of WebScan for the auto update feature to recognize the new code certificate is 17.0.1204.

If WebScan does not recognize the installer package attempting to perform the upgrade, the user is presented with an error message.



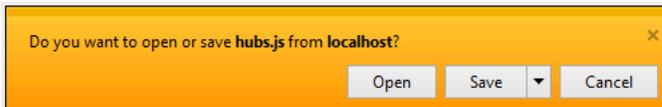
If this occurs, the customer will need to contact support and have WebScan upgraded manually. For more information, see the [Manual Update](#) section.

## How to...

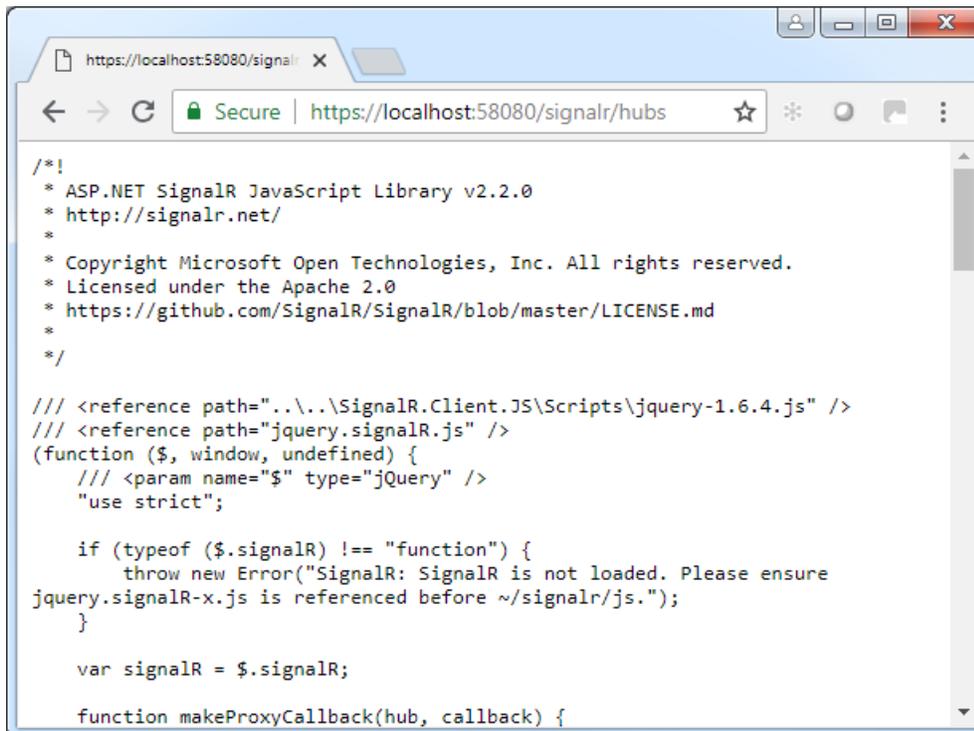
This section covers some processes used to validate or repair WebScan configurations.

### Verifying SignalR hub

1. Open any browser
2. Browse to 'https://localhost:58080/signalr/hubs'
3. If IE 11 or Edge, you are prompted to open or save hubs.js from localhost:



4. If another browser, you are displayed our hubs.js file:



```

/!*
 * ASP.NET SignalR JavaScript Library v2.2.0
 * http://signalr.net/
 *
 * Copyright Microsoft Open Technologies, Inc. All rights reserved.
 * Licensed under the Apache 2.0
 * https://github.com/SignalR/SignalR/blob/master/LICENSE.md
 *
 */

/// <reference path="../../SignalR.Client.JS/Scripts/jquery-1.6.4.js" />
/// <reference path="jquery.signalR.js" />
(function ($, window, undefined) {
    /// <param name="$" type="jQuery" />
    "use strict";

    if (typeof ($.signalR) !== "function") {
        throw new Error("SignalR: SignalR is not loaded. Please ensure
        jquery.signalR-x.js is referenced before ~/signalr/js.");
    }

    var signalR = $.signalR;

    function makeProxyCallback(hub, callback) {

```

### Verifying Certificates

1. Open Microsoft Management Console (MMC.exe)
2. Under File, Select Add/Remove Snap-in...
3. Select Certificate

4. Select Computer account
5. Select Local computer: (the computer this console is running on)
6. Click OK.
7. Verify Certificate | Personal | Certificate | Issued To: localhost, Issued By: FIS Certificate Authority

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
localhost	FIS Certificate Authority	4/29/2027	Server Authentication	<None>

8. Verify Certificate | Trusted Root Certification Authorities | Certificate | Issued To: FIS Certificate Authority.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
FIS Certificate Authority	FIS Certificate Authority	4/24/2047	Server Authentication, Client ...	<None>

## Verifying SSL Certificate Bindings

1. Open CMD.exe Run as administrator
2. Type 'netsh http show sslcert' to verify the SSL Certificate bindings

```
SSL Certificate bindings:
-----
IP:port           : 127.0.0.1:58080
Certificate Hash   : 4dbc405fdbbfc721f91818221340ab99f884f19e
Application ID    : {12345678-db90-4b66-8b01-88f7af2e36bf}
Certificate Store Name : <null>
Verify Client Certificate Revocation      : Enabled
Verify Revocation Using Cached Client Certificate Only : Disabled
Usage Check           : Enabled
Revocation Freshness Time : 0
URL Retrieval Timeout : 0
Ctl Identifier        : <null>
Ctl Store Name       : <null>
DS Mapper Usage      : Disabled
Negotiate Client Certificate : Disabled
```

## Manually Add SSL Certificate Bindings

1. Open CMD.exe Run as administrator
2. Type 'netsh http add sslcert ipport=127.0.0.1:58080 certhash=4dbc405fdbbfc721f91818221340ab99f884f19eappid={12345678-db90-4b66-8b01-88f7af2e36bf}'

## Manually Delete SSL Certificate Bindings

1. Open CMD.exe Run as administrator
2. Type 'netsh http delete sslcert ipport=127.0.0.1:58080'

## Verifying URL Reservation

1. Open CMD.exe Run as administrator
2. Type 'netsh http show urlacl'
3. Search through the list for the following entry:

```
Reserved URL           : https://127.0.0.1:58080/  
User: \Everyone  
Listen: Yes  
Delegate: No  
SDDL: D:(A;;GX;;;WD)
```

### Manually Add URL Reservation

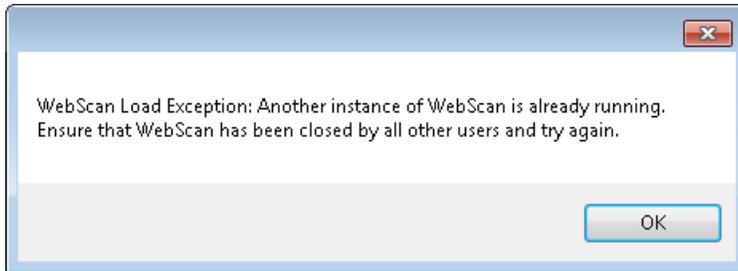
1. Open CMD.exe, Run as administrator
2. Type 'netsh http add urlacl url=https://127.0.0.1:58080/ user=Everyone'

### Manually Delete URL Reservation

1. Open CMD.exe Run as administrator
2. Type 'netsh http delete urlacl url=https://127.0.0.1:58080/'

## Troubleshooting

### WebScan Load Exception: Exception has been thrown...



**SOLUTION 1:** This can be thrown when there is already an instance of WebScan running, generally caused by the previous instance not existing correctly, or another user logged into Windows and already has an instance of WebScan running. Using Task Manager, go to the Processes tab and End Process any instance of WebScan. You will need to select “Show processes from all users” to see if another user is running WebScan.

**SOLUTION 2:** This has been seen when a file was not applied correctly during installation. Uninstall WebScan, delete the WebScan folders under “Program Files” and “ProgramData” and reinstall.

### Unable to capture with Firefox, but Chrome and IE work

**SOLUTION:** Firefox manages their own certificate stores. The FIS Certificate Authority must be added to the browser’s list of trusted authorities. To add the FIS certificate to the list of trusted authorities, use the following steps:

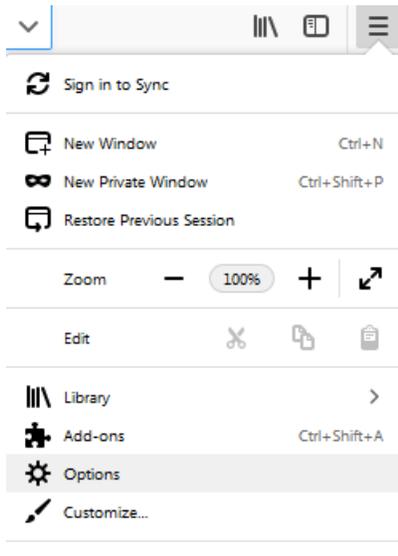
---

Firefox menus and options may differ depending on the version you are using.

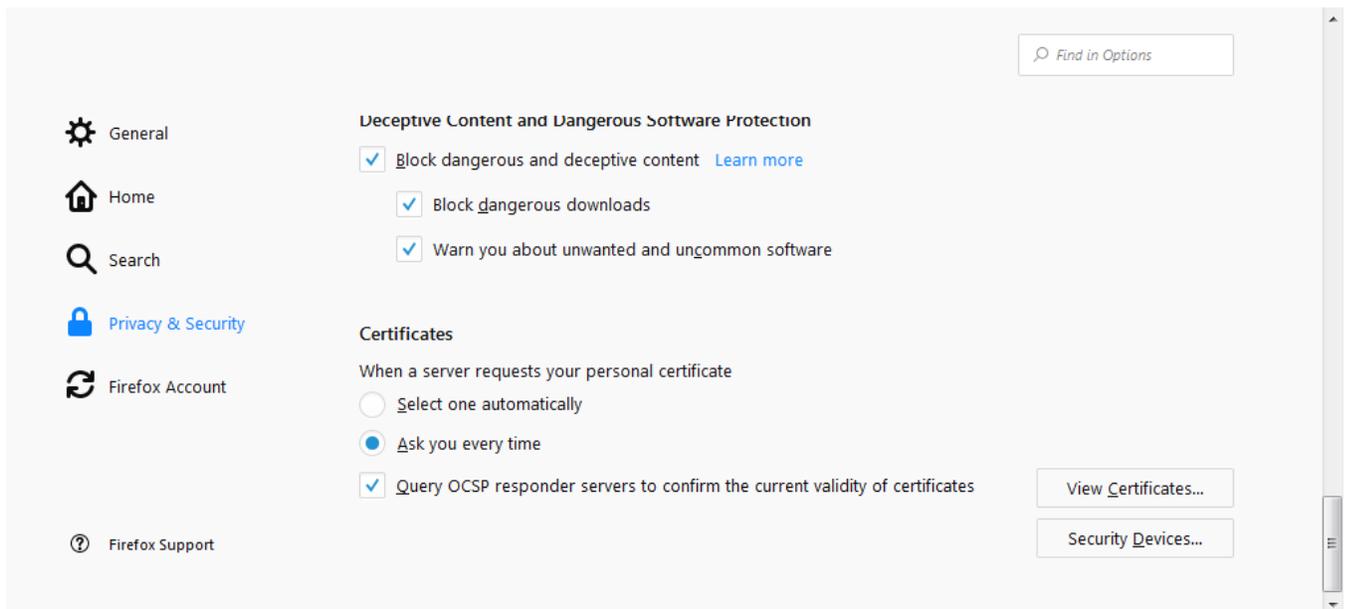
---

1. Open Firefox.

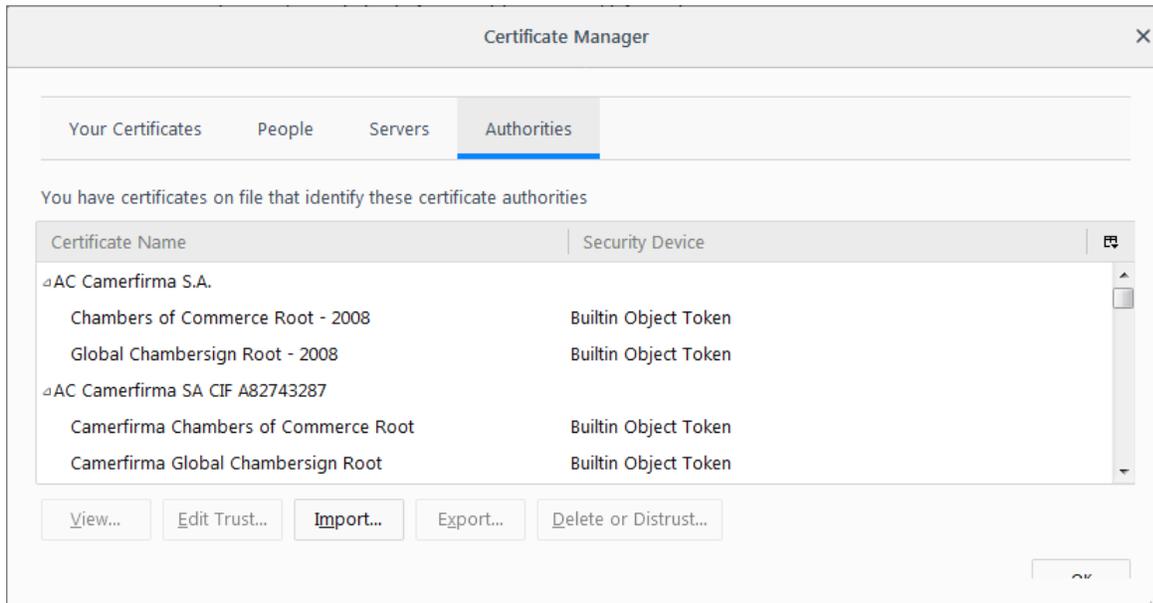
2. Open the Options menu:



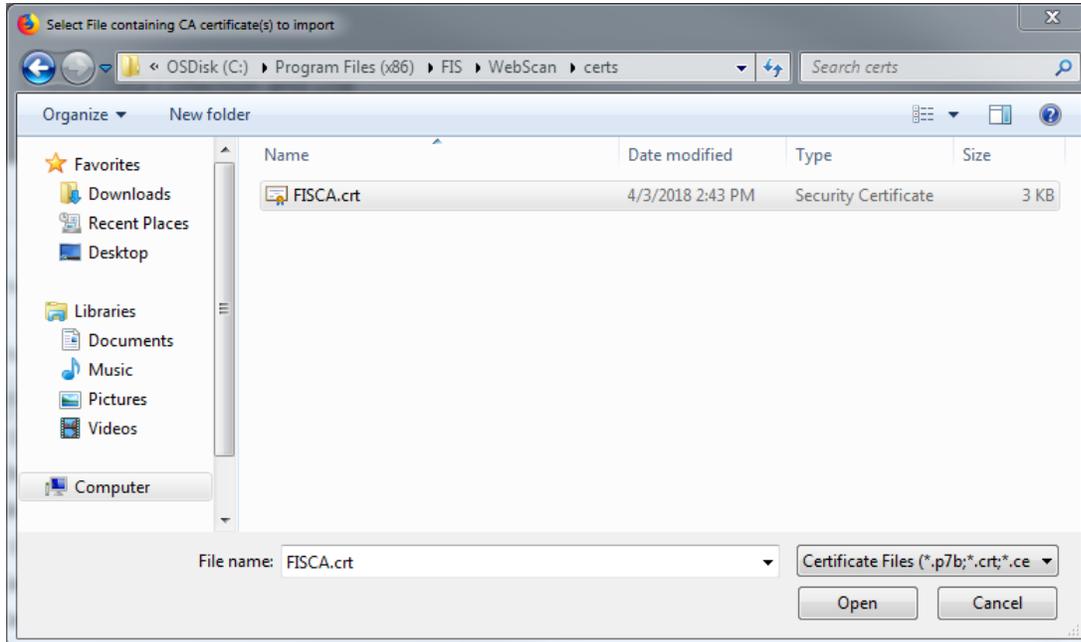
3. Select Privacy & Security, scroll to the bottom of the page, and select View Certificates.



4. Within the “Certificate Manager” panel, go to Authorities | Import.

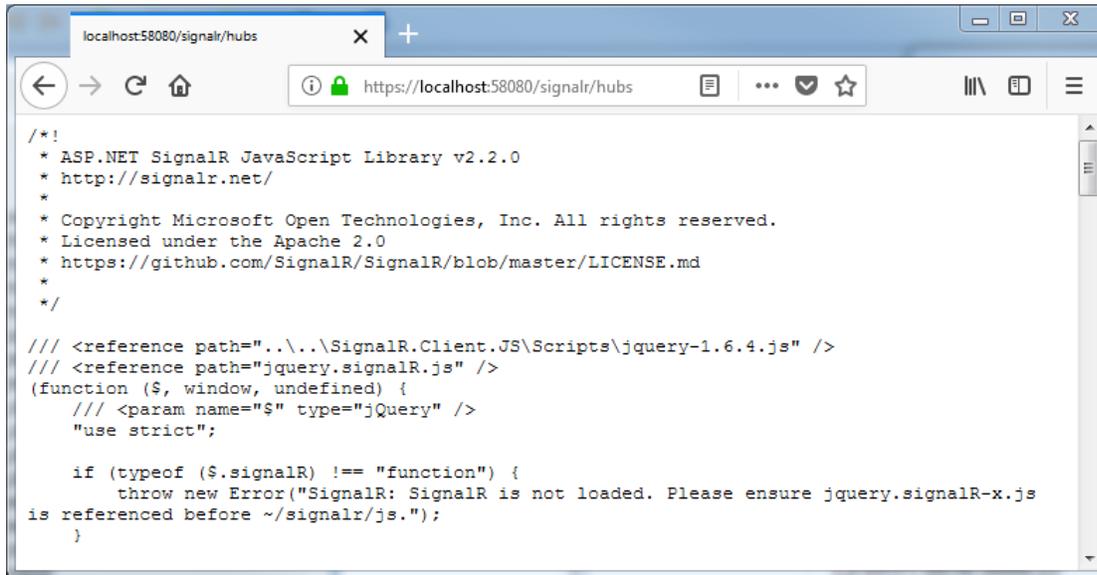


5. Browse to the directory where WebScan is installed and open the “certs” folder. Select the “FISCA.crt” file and click the Open button.





8. You can further verify, by browsing to <https://localhost:58080/signalr/hubs> and receive a trusted page.



## Browser(s) has never connected to WebScan

**SOLUTION 1:** Verify the correct domain is configured in Origin Domain Settings.

**SOLUTION 2:** Verify that you can browse to `https://localhost:58080/signalr/hubs`.

**SOLUTION 3:** Add the RDC client domain to the 'Trusted sites' browser security zone.

**SOLUTION 4:** Verify cross domain access is granted to the 'Trusted sites' browser security zone.

## Edge on Windows 10 won't connect

Depending on how Windows 10 is configured, it's possible that loopback is disabled for Edge. For Edge to communicate with WebScan correctly, the loopback needs to be enabled.

To enable loopback for Edge, use this command:

```
CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"
```

If needed, to disable loopback for Edge use this command:

```
CheckNetIsolation.exe LoopbackExempt -d -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"
```