LexisNexis® Upgrade to TLS 1.2

Frequently Asked Questions

Last Updated:

May 8, 2018

LexisNexis® RISK SOLUTIONS

Contents

CONTENTS 2

LEXISNEXIS® UPGRADE TO TLS 1.2 3

FREQUENTLY ASKED QUESTIONS 3

What are the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols? 3

What exactly is changing and how do the changes affect our connection(s) to LexisNexis Risk Solutions URLs and APIs? 3

When is LexisNexis making this change? 3

Why is LexisNexis making this change? 4

How can I test whether or not my LexisNexis Risk Solutions integration supports TLS 1.2? 4

How can clients avoid disruption? 5

What are the TLS 1.2 compatibility requirements? 6

How do I check the TLS version on my browser? 6

Microsoft Internet Explorer 11 7

Google Chrome 8

Mozilla Firefox 9

BRIDGER INSIGHT©XG RELATED FAQ 9

Bridger XG4 EU Environment 9

Bridger XG4 required Smart Client registry change 10

Bridger XG4 SoapUI required configuration change for TLS 1.2 13

CUSTOMER SUPPORT CONTACTS 15

LexisNexis® Upgrade to TLS 1.2

Frequently Asked Questions

QUESTION

What are the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols?

SSL and TLS are widely used protocols designed to transport data securely between a client and a server. The use of SSL during the 1990s enabled the beginning of secure commerce on the Internet. Its successor protocol, TLS, continues to be used by web browsers and servers to protect the privacy of Web communications. When a URL address contains HTTPS, the 'S' stands for secure, and indicates that data is being transmitted securely using one of these protocols.

QUESTION

What exactly is changing and how do the changes affect our connection(s) to LexisNexis Risk Solutions URLs and APIs?

In an effort to provide the highest level of security for our customers, LexisNexis will disable all Transport Layer Security versions less than 1.2. Any server-to-server request that is not using TLS 1.2 will not be able to connect to LexisNexis Risk Solutions product offerings.

QUESTION

When is LexisNexis making this change?

Starting May 13, 2018, LexisNexis Risk Solutions will permanently disable TLS 1.0 and 1.1 in our production environment. **Customers who are not compatible with the latest standards of TLS 1.2 will not be able to access LexisNexis products and systems during those maintenance windows.**

Sunday, May 13, 2018	Tuesday, May 15, 2018
Maintenance Window 12:01am ET - 6:00am ET	Maintenance Window 12:01pm ET - 2:00pm ET
amlinsight.lexisnexis.com	bridger.lexisnexis.com
fastdataweb.lexisnexis.com	bridgerdirect.lexisnexis.com
riskadmin.lexisnexis.com	bridgerinsight.lexisnexis.com
risk.lexis.com	bridgerinsight2.lexisnexis.com
risk.nexis.com	
riskmanagement.lexisnexis.com	
xml.fastdataweb.com	

Sunday, May 20, 2018	Sunday, June 3, 2018
Maintenance Window 12:01am ET - 6:00am ET	Maintenance Window 12:01am ET - 6:00am ET
identitymanagement.lexisnexis.com	riskview.seisint.com
idms.lexisnexis.com/login	secure.accurint.com
mfa.lexisnexis.com	wsonline.seisint.com
mfaweb.lexisnexis.com	
netview.verid.com	
netviewcert.verid.com	
ws.idms.lexisnexis.com	
ws-cert.idms.lexisnexis.com	

If you have not updated your operating system, web browsers, applications and/or framework, we urge you to take action as soon as possible.

QUESTION

Why is LexisNexis making this change?

Due to a series of vulnerabilities in early Transport Layer Security (TLS) that no longer meet minimum standards with industry best practices for security and data integrity, LexisNexis Risk Solutions is disabling support of TLS 1.0 and TLS 1.1.

This is not an action LexisNexis Risk Solutions will take alone. The PCI Security Council sets the rules on which technologies are acceptable for use in transmitting cardholder data. They have explicitly advised TLS 1.0 is no longer a strong form of encryption as it can be easily compromised.

QUESTION

How can I test whether or not my LexisNexis Risk Solutions integration supports TLS 1.2?

All LexisNexis Risk Solutions sites and systems are currently TLS 1.2 compatible. To test whether your LexisNexis Risk Solutions integration supports TLS 1.2, you must have your TLS 1.2 enabled when communicating to LNRS sites and systems. In order to assure that your LNRS integration supports TLS 1.2, TLS 1.0 and 1.1 should be disabled while testing on TLS 1.2. Please see below the versions and communication channels to consider when testing.

Below are the communications channels to consider when determining whether your LexisNexis Risk Solution integration supports TLS 1.2:

- **.NET**
  .NET 4.6 uses TLS 1.2 automatically.
  .NET 4.5 may be configured to use TLS 1.2.
  .NET 3 and below do not support TLS 1.2.

- **Java**
  Java 8 supports TLS 1.2 and enables its use by default.
  Java 7 supports TLS 1.2, but does not enable its use by default for clients.
  Java 6 does not support TLS 1.2 natively. Support for TLS 1.2 in Java 6 is provided by third parties.

- **OpenSSL (PHP, Ruby, Python)**
  Most dynamic languages such as Ruby, PHP, and Python rely on the underlying operating system's OpenSSL version. You can check it by running the command 'openssl version'. The minimum required is 1.0.1.

QUESTION

How can clients avoid disruption?

To avoid disruption, please ensure your internal systems meet the minimum TLS 1.2 requirements. If you cannot meet TLS 1.2 protocol requirements, your access to LexisNexis systems will be impacted. Please view the requirements for required actions.

QUESTION

What are the TLS 1.2 compatibility requirements?

Following is a reference compatibility chart for TLS 1.2 standards:

Operating System Version	Web Browser	Applications and Frameworks
Windows 7*	Internet Explorer v11+	OpenSSL 1.01 +
Windows Server 2008 R2*	Internet Explorer Edge	JDK 8 +
Windows 8*	Google Chrome v30+	.NET 4.6 +
Windows Server 2012	Mozilla Firefox v27+	Apache 2.2.23
Windows 8.1	Apple Safari v7+	
Windows Server 2012 R2	Opera v17+	
Windows 10		
Windows Server 2016		
CentOS 6+ / RHEL 6+		
Mac OS X 10.9 +		
iOS 5.x +		
Android 5.x +		

*TLS 1.2 not enabled by default

NOTE: The operating systems will require the minimum version of web browser or application, as listed above, to be compatible.

QUESTION

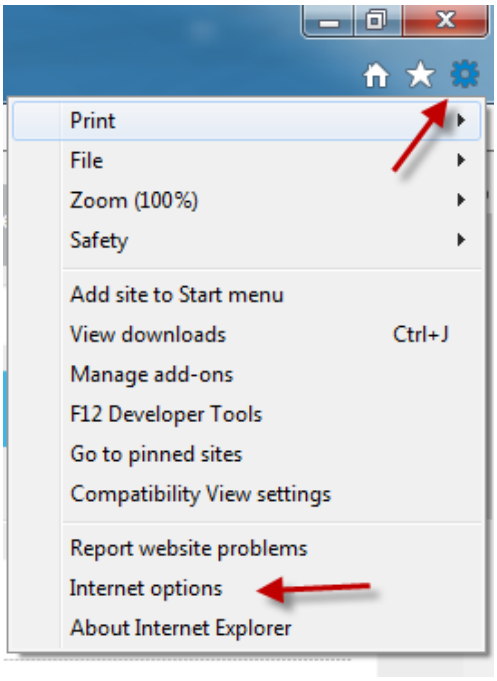
How do I check the TLS version on my browser?

To check your version and enable TLS 1.2 protocols on your web browser ONLY, see below, you may need to contact your IT department or Administrator to make this security change on your browser. If you have other connections to LN products, API Calls, XML calls, SFTP servers, and/or Batch Servers, please use the about minimum requirements to check your current environments.

Microsoft Internet Explorer 11

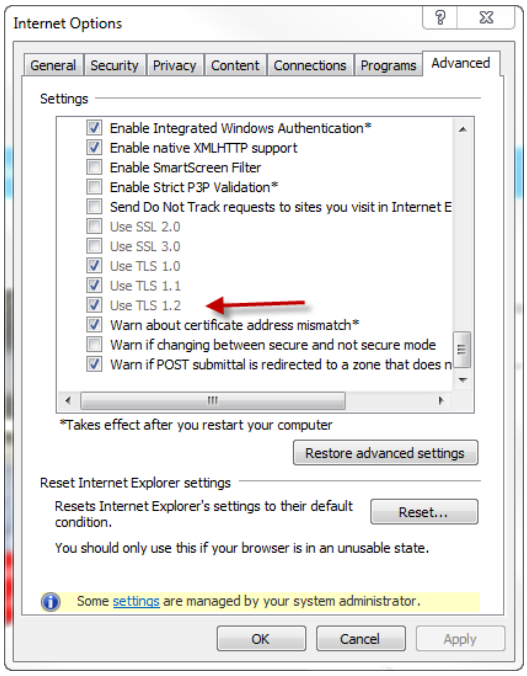
1. Open Internet Explorer

    a. From the menu bar, click **Tools>Internet Options**



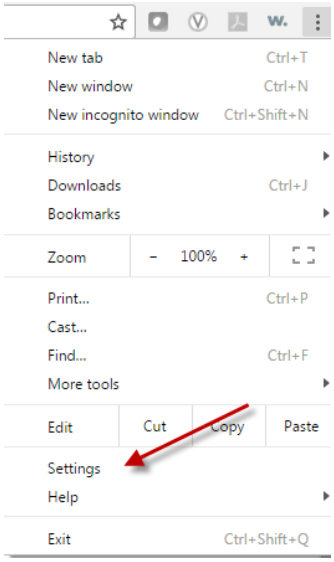
2. Click on the **Advanced** Tab

3. Scroll down to the **Security** section where you can see the TLS versions selected.

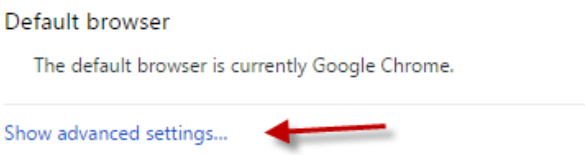


Google Chrome

1. Open Google Chrome
2. Click the options menu in the top right



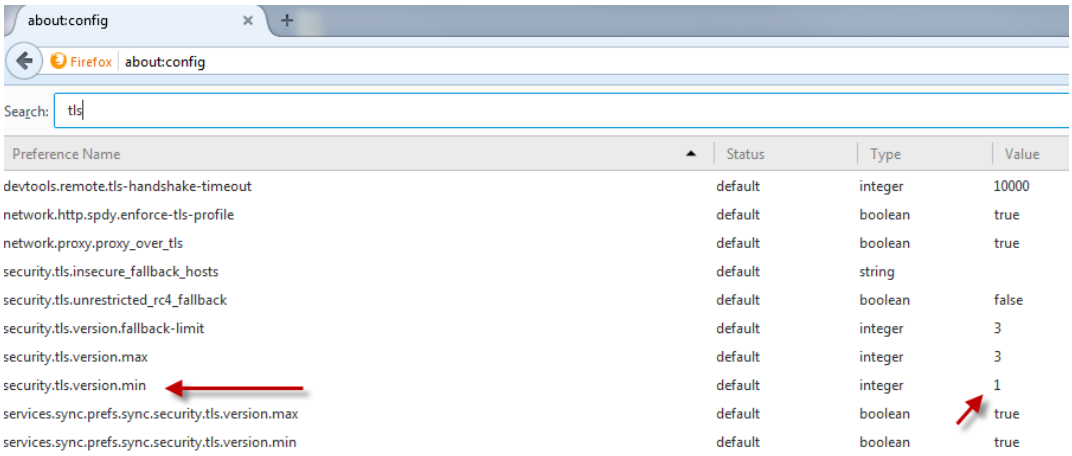
3. Click the **Settings** option
4. Click the **Show Advanced Settings** at the bottom of the page



5. Scroll down to **Network** section and click **Change Proxy Settings. (You may need to contact your IT department)**
6. Select **Advanced** tab
7. Scroll down to **Security** category, manually check the option box for TLS 1.2

Mozilla Firefox

1. Open **Firefox**
2. In the address bar, type **about:config** and press Enter
3. In the **Search** field, enter **tls**. Find and double-click the entry for **security.tls.version.min**



4. Set the integer value to "3" to force a minimum protocol of TLS 1.2.

Bridger Insight©XG Related FAQ

Bridger XG4 EU Environment

The Bridger Insight™ XG4 EU Environment will be disabling TLS 1.0 and 1.1 on May 1st, 2018. That is the following URLs:

Bridger Insight XG EU Service WebServices https://bridgerinsighteu.lexisnexis.com/webservices/{version}/{apname}

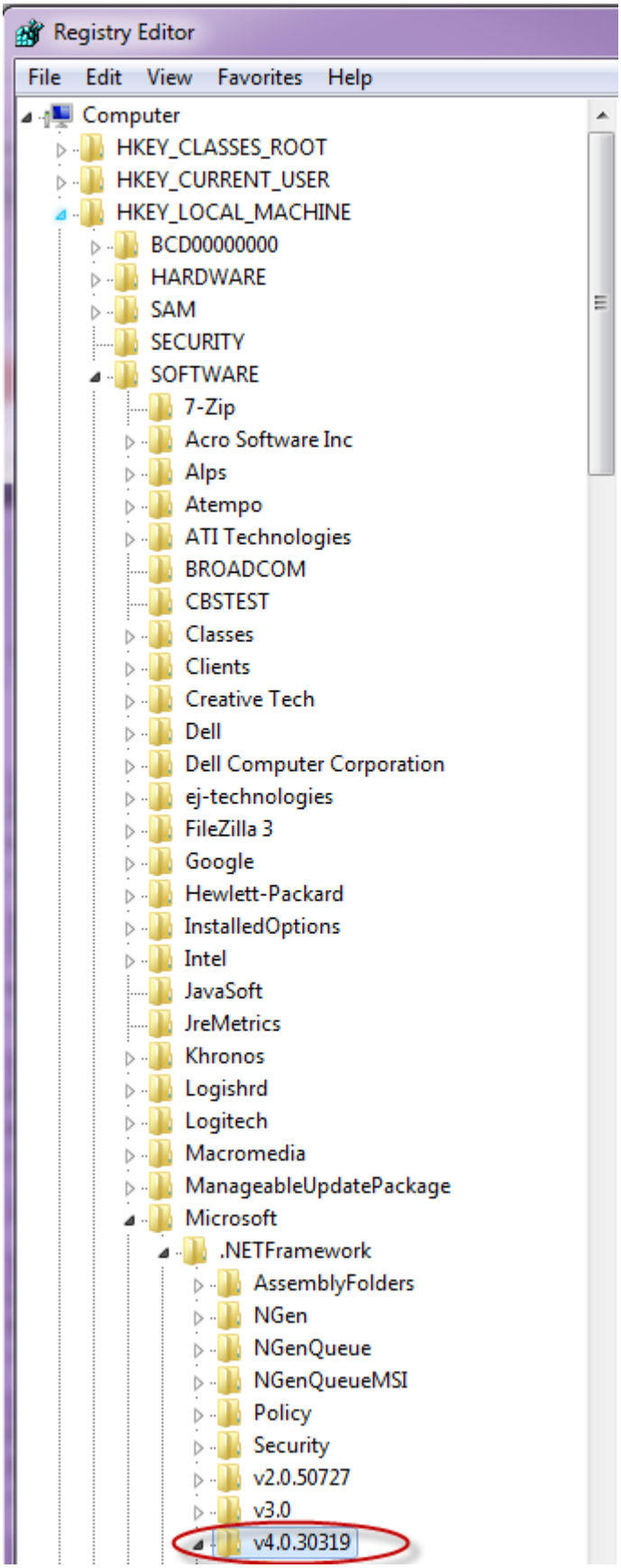
Bridger Insight XG EU WebClient	https://bridgerinsighteu.lexisnexis.com

Bridger XG4 required Smart Client registry change

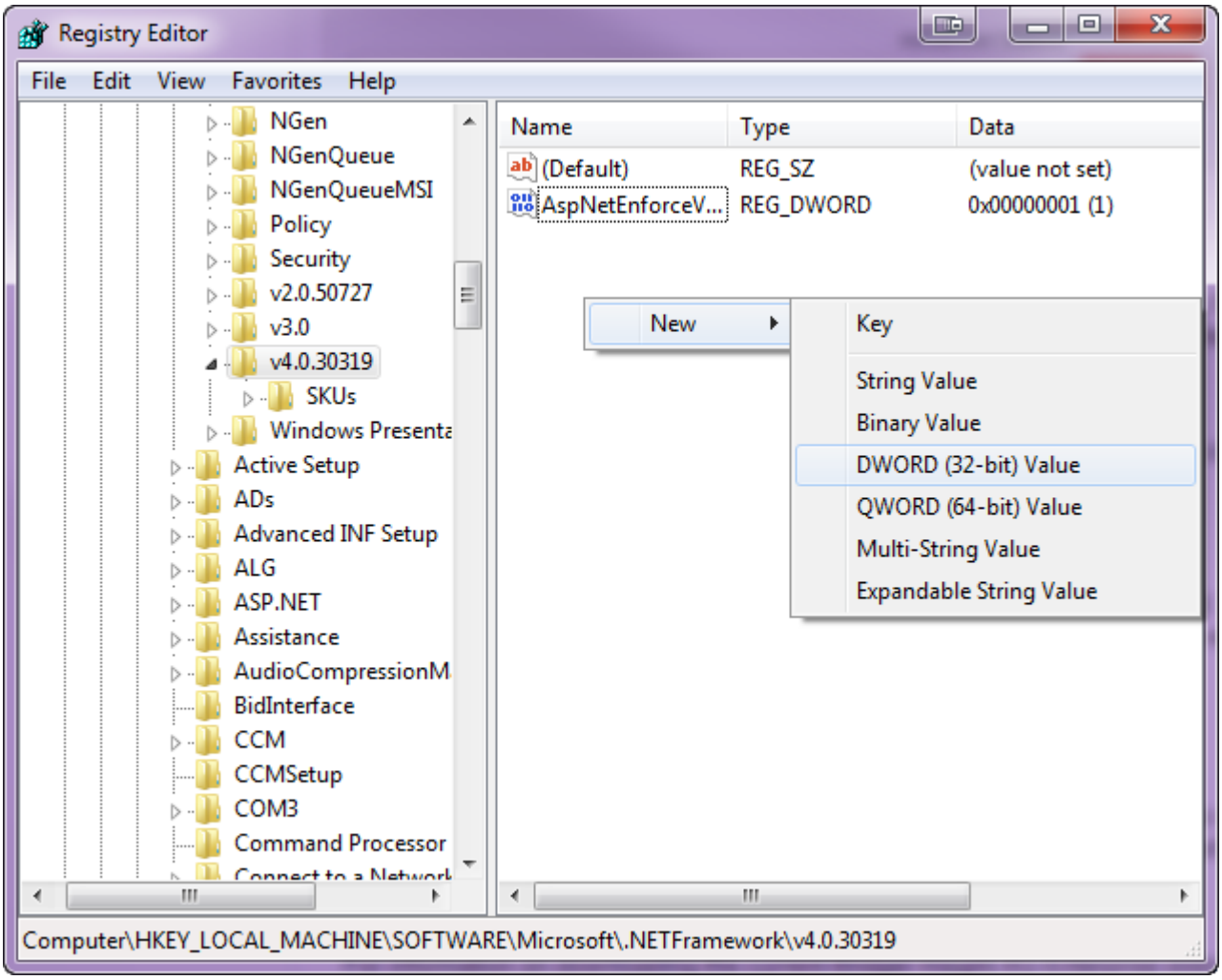
It will be necessary to add a DWORD value in the Windows Registry Editor so .NET will use the most secure protocol (TLS 1.2).

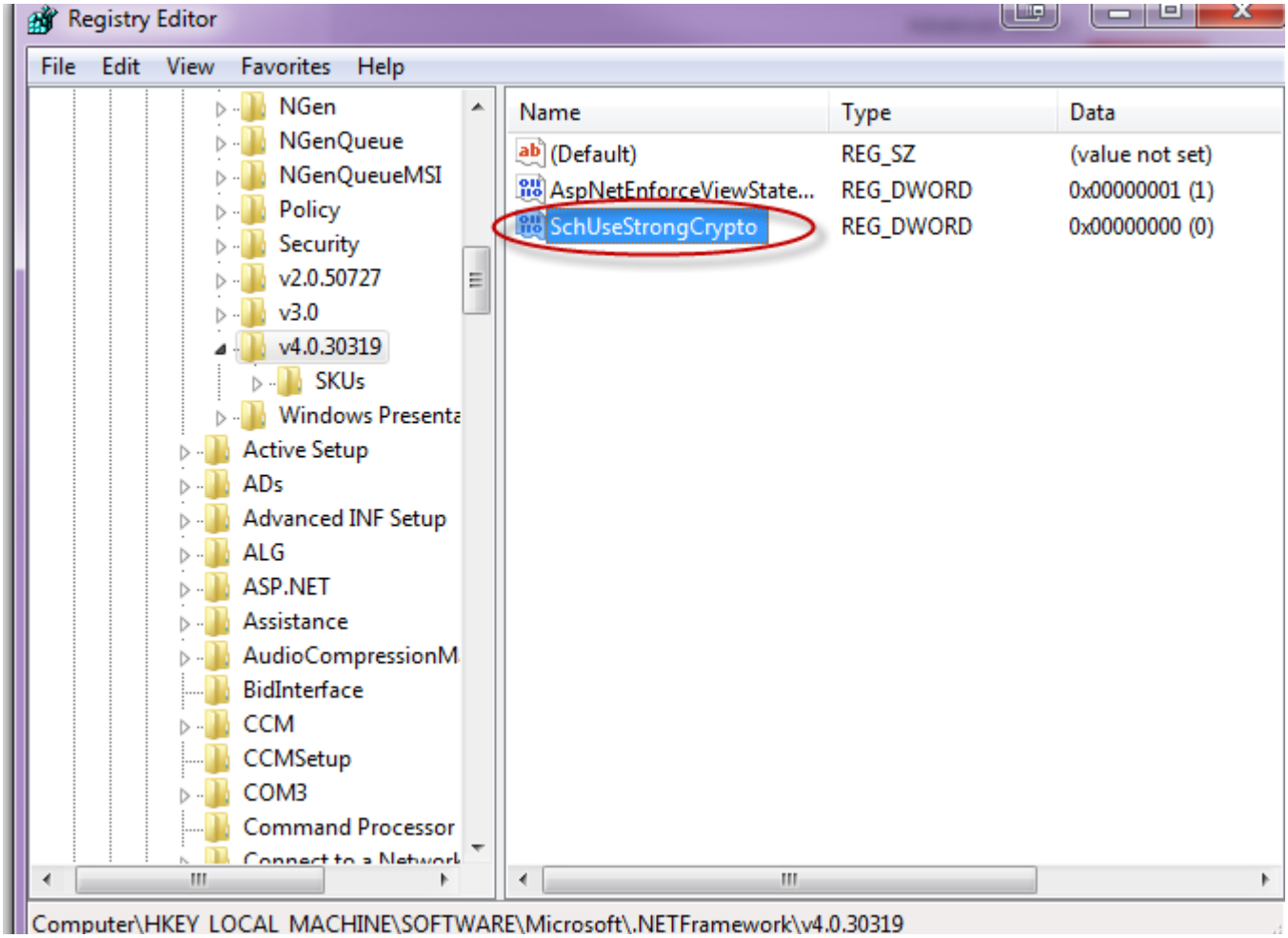
Use the steps below on Windows Server 2008R2 and older PC Windows versions (Win7, earlier Win8).

1. Install .NET Framework 4.5.2. (or greater) https://www.microsoft.com/en-us/download/details.aspx?id=42643
2. Open the Registry Editor by typing 'regedit' from Start > Run
3. Open the following location in the Registry Editior*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319*

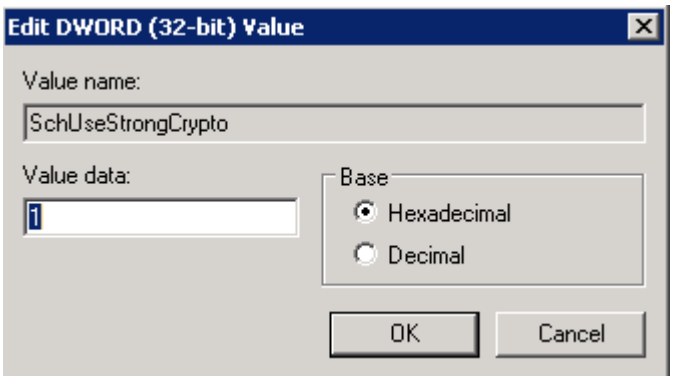

Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
SAM
SECURITY
SOFTWARE
7-Zip
Acro Software Inc
Alps
Atempo
ATI Technologies
BROADCOM
CBSTEST
Classes
Clients
Creative Tech
Dell
Dell Computer Corporation
ej-technologies
FileZilla 3
Google
Hewlett-Packard
InstalledOptions
Intel
JavaSoft
JreMetrics
Khronos
Logishrd
Logitech
Macromedia
ManageableUpdatePackage
Microsoft
.NETFramework
AssemblyFolders
NGen
NGenQueue
NGenQueueMSI
Policy
Security
v2.0.50727
v3.0
v4.0.30319

4. With the v4.0.30319 folder selected, on the right half of the screen, right click and select New > DWORD (32-bit) Value. Name the New Entry 'SchUseStrongCrypto'





5. Double click on the new DWORD 'SchUseStrongCrypto and edit the Value Data to = 1



6. REBOOT the server if prompted.

Bridger XG4 SoapUI required configuration change for TLS 1.2

1. If you are using the Bridger Insight XG4 SoapUI, you will need to make a required configuration change.

2. You will need to add the following: -Dsoapui.https.protocols=TLSv1.2

3. To this line: C:\Program Files\SmartBear\SoapUI-#.#.#\bin\soapUI-#.#.#.vmoptions

CUSTOMER SUPPORT CONTACTS

BGS Products Supported	Support Phone	Support Email/s (generates a ticket)
BAIR Analytics	800.380.1138	bair.support@lexisnexis.com
AlumniFinder (reseller) - we do not support	800.732.1565	www.alumnifinder.com
Accurint dFacts / Distrix FastData	866.277.8407	accurint.support@lexisnexis.com
AML Collections Solutions Investigative Portal Real Estate Solutions Risk Management RiskResearch	866.277.8407	risksolutions.support@lexisnexis.com https://risk.custhelp.com/app/ask
Batch & FTP Support	866.277.8764	batchtechsupport@lexisnexis.com
Banko	866.277.9986	batchtechsupport@lexisnexis.com
Bridger Insight XG	US: 800.915.8930 UK: 08.08.234.9605	bridgercustomersupport@lexisnexis.com
Device Assessment	888-270-2836 opt 1	idms.support@lexisnexis.com
National Accuracy Clearinghouse (NAC) - Batch & XML	888.297.6931 opt 2 & 3	nacbatchsupport@lexisnexis.com
TrueID	888.270.2836 Opt 2	accurintwebservices@lexisnexis.com
Instant ID Q&A or Risk Defense Platform (IDMS / KBA / Verid / Netview)	888.270.2836 Opt 1	iidqa.support@lexisnexis.com
Instant Authenticate / Instant Verify	888.270.2836 Opt 2	instantauthenticate.support@lexisnexis.com
XML WebServices: WSAccurint, WsIdentity InstantID International FlexID PhoneFinder Riskview.Riskwise XML Fraudpoint FastData XML	866-277-8763	accurintwebservices@lexisnexis.com

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government assess, predict and manage risk. Combining cutting-edge technology, unique data and advanced analytics, LexisNexis Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group plc, a world-leading provider of information solutions for professional customers across industries.