

Configuring MailSite to use TLS 1.2

A guide for MailSite Administrators

MailSite technical White Paper

October 2020



Table of Contents

Introduction	3
1. Prerequisites	4
Verifying a Certificate with CertLM	4
Verifying a Certificate with DigiCert	5
Verifying the hostname settings for MailSite	5
Verifying SQL Server supports TLS 1.2	6
2. Configuring TLS and Ciphers	7
3. Verifying TLS and Ciphers	9
Verifying with Hardenize	9
Verifying with SSL Labs	11
4. Configuring MailSite to use the Ciphers	12
5. Verifying MailSite	13
References	15
About Rockliffe Systems	15
Disclaimer	15
Rockliffe Professional Services	15

Introduction

MailSite provides secure messaging using Transport Layer Security (TLS) and Secure Socket Layer (SSL) technology. These industry standard technologies allow for secure, encrypted email sending and delivery between email clients and servers using certificates and public key cryptography.

Recent security best practices recommend against using SSL, TLS 1.0 and TLS 1.1 because of certain vulnerabilities. These best practices also recommend preferred Ciphers and recommend against using certain Ciphers.

This white paper describes how to configure both Windows Server and MailSite so that the TLS security best practices are implemented.

Familiarity with Windows IIS and Windows Server administration is assumed, along with a technical understanding of the Microsoft Windows operating system.

1. Prerequisites

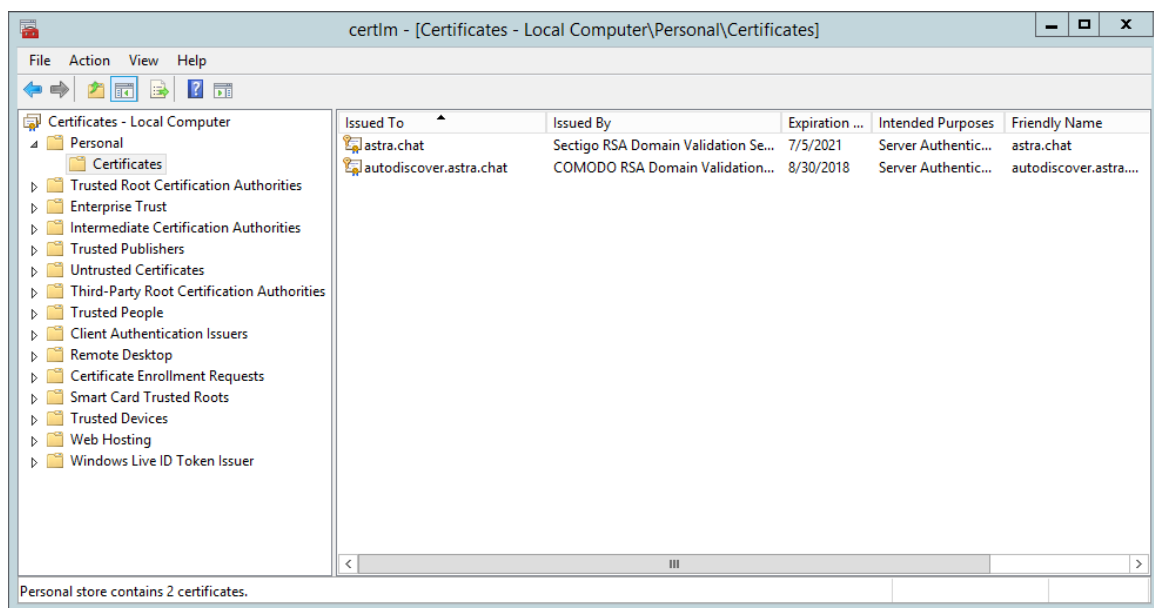
Before configuring TLS and Cipher Suites, you must have a valid certificate installed on your Windows Server. If you do not have a certificate installed, refer to the MailSite TLS Installation Guide:

https://www.mailsite.com/Resources/docs/MailSite_TLS_SSL_Installation_Guide.pdf

If you already have the certificate installed, there are two ways to verify it, the first is using the built-in CertLM console, the second is using the third-party DigiCert utility.

Verifying a Certificate with CertLM

On the Windows desktop, click Search, type CertLM, and open the Local Computer Certificate Management Console:



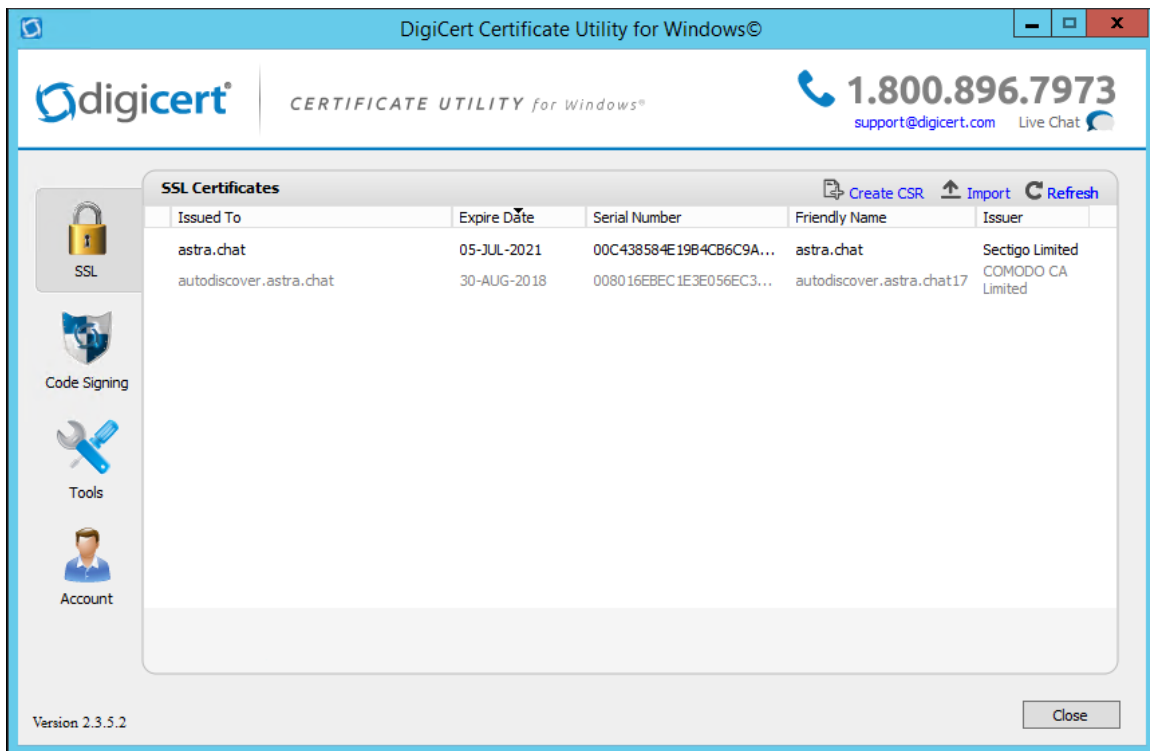
Navigate to Local Computer: Personal: Certificates and verify that there is a certificate for your host name that has not expired.

Verifying a Certificate with DigiCert

Download the DigiCert Utility from this website:

<https://www.digicert.com/util/>

Unzip the file and save DigiCertUtil.exe to your drive. Run DigiCertUtil.exe and accept the license terms:



Verify that there is a certificate for your host name that has not expired.

Verifying the hostname settings for MailSite

The *Common Name (CN)* of the certificate must match the hostname of the Reverse DNS (PTR) record for the IP addresses that the MailSite services are listening on, or the Windows HOSTS file must be updated to override the PTR record returned by your DNS servers. MailSite Fusion does a reverse DNS lookup to find out the Common Name of the certificate to use before searching the certificate store for an appropriate certificate.

Example: The network adapters in your mail server are assigned the IP addresses 192.168.1.10 and 192.168.1.11 and your DNS servers report that the reverse DNS entries for 192.168.1.10 and 192.168.1.11 are both mail.yourcorp.com. MailSite Fusion will look for a certificate with a common name of mail.yourcorp.com in the

certificate store.

If MailSite Fusion is unable to locate an appropriate certificate it will log the following error indicating the name of the Common Name of the certificate that it attempted to locate:

TLS/SSL: The service failed to find a suitable certificate in the predefined MY System store for the LocalMachine : No certificates were found matching the Subject 'smtp.yourcorp.com'.

The HOSTS file is located in the %SYSTEMROOT%\SYSTEM32\DRIVERS\ETC on your server can be updated to override the reverse DNS entries and point MailSite Fusion to the appropriate certificate.

For more information, refer to this KB doc:

<https://www.mailsite.com/support/docs/html/1/05/10512.asp>

Verifying SQL Server supports TLS 1.2

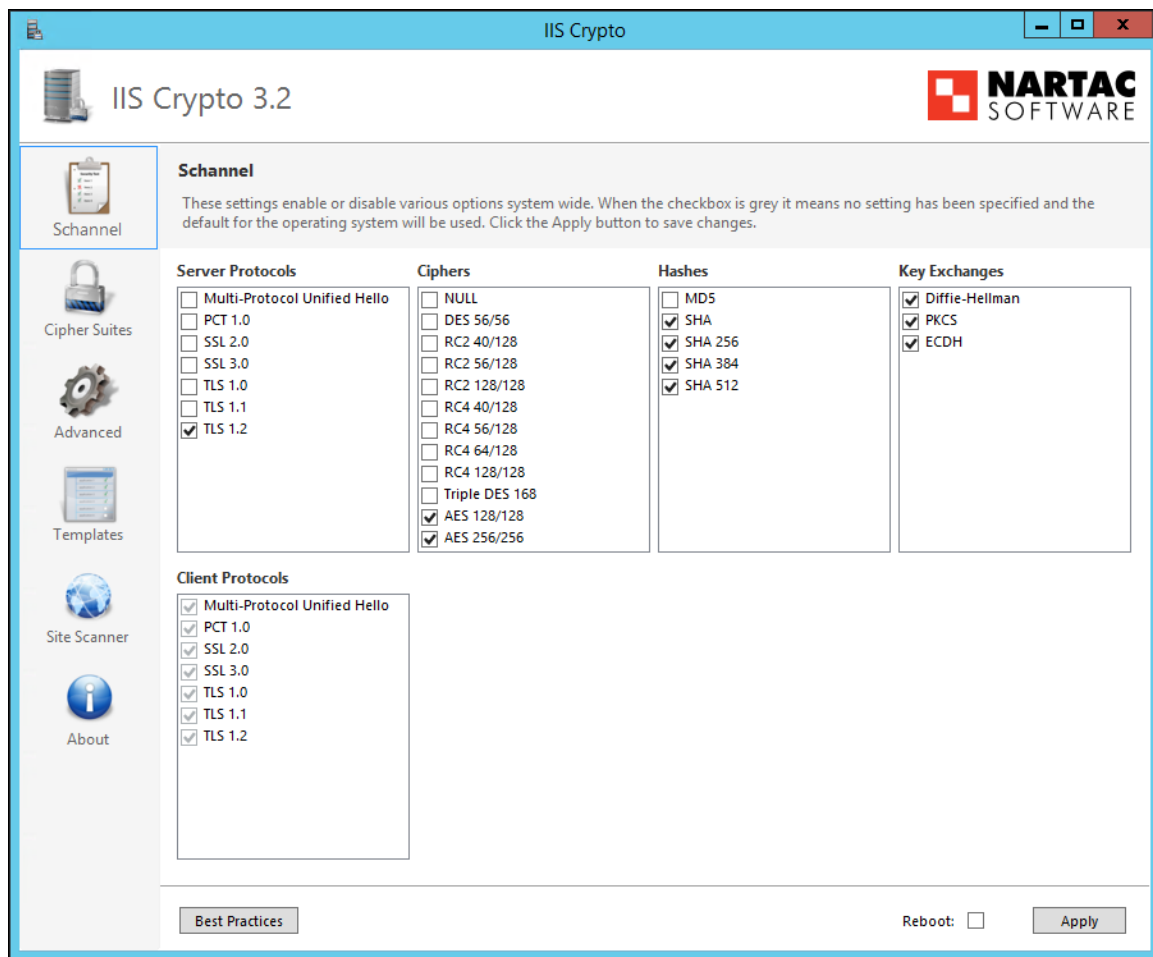
Older versions of Microsoft SQL Server use TLS 1.0 and 1.1 and do not support TLS 1.2. If you are using the MailSite SQL Connector, it is imperative that you ensure that your version of the SQL Server client and the SQL Server are compatible with TLS 1.2. To verify this, please refer to this Microsoft Support Article:

<https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server>

2. Configuring TLS and Ciphers

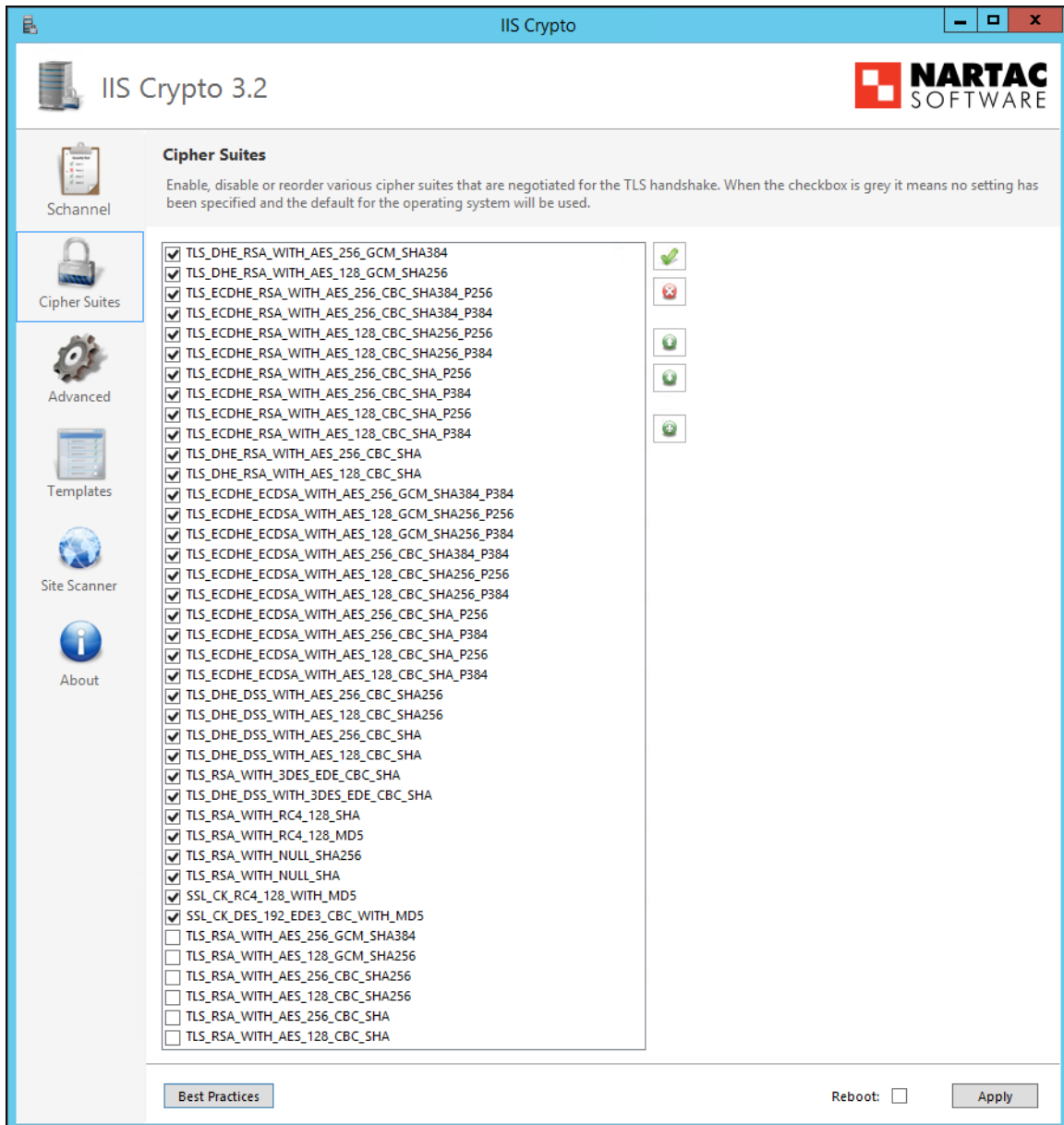
Download and run IISCrypto:

<https://www.nartac.com/Products/IISCrypto>



Enable and disable the Protocols, Ciphers, Hashes and Key Exchanges to match the above screenshot. Apply the changes but do not reboot yet.

Next, select the Cipher Suites tab, disable the bottom suites, and move the two suites to the top of the list as indicated:



IIS Crypto

IIS Crypto 3.2 NARTAC SOFTWARE

Cipher Suites

Enable, disable or reorder various cipher suites that are negotiated for the TLS handshake. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used.

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_NULL_SHA256
- TLS_RSA_WITH_NULL_SHA
- SSL_CK_RC4_128_WITH_MD5
- SSL_CK_DES_192_EDE3_CBC_WITH_MD5
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Best Practices Reboot: Apply

Select the Reboot option and select Apply. Your windows server will reboot immediately.

3. Verifying TLS and Ciphers

To verify that you have disabled TLS 1.0, 1.1 and SSL and to verify the Ciphers, you will need an operating website under running under Windows IIS. If you have that you can use two third party sites to verify that Windows has TLS configured correctly and is using the right Ciphers.

Verifying with Hardenize

From an external web browser go to this website and enter your domain or host name:

<https://www.hardenize.com>

When the report completes, on the left-hand panel under WWW select TLS. You should see a report like this:

WWW TLS

Transport Layer Security (TLS) is the most widely used encryption protocol on the Internet. In combination with valid certificates, servers can establish trusted communication channels even with users who have never visited them before. Network attackers can't uncover what is being communicated, even when they can see all the traffic.



Test passed, but there are warnings

Some aspect of your site's configuration require your attention.

TLS Configuration: www.rockliffe.com (52.52.133.211)

Supported protocols	TLS v1.2
Server suite preference	✓
TLS v1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 256 bits (DHE 2048 bits)
Server preference	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 128 bits (DHE 2048 bits)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 256 bits (ECDHE 256 bits)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 128 bits (ECDHE 256 bits)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA 256 bits (ECDHE 256 bits)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 128 bits (ECDHE 256 bits)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA 256 bits (DHE 2048 bits)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 bits (DHE 2048 bits)

Analysis

- ⚡ **TLS 1.3 not supported**

TLS 1.3 is the latest revision of the TLS protocol and a significant improvement over earlier versions. Developed over a period of several years and extensively analyzed prior to the release, TLS 1.3 removed insecure features, and improved both security and performance. This version of TLS should be the main protocol used with modern clients.
- ✓ **TLS 1.2 supported**

Good. This server supports TLS 1.2, which can provide strong security when configured correctly. This version of the TLS protocol is necessary to provide good security with a wide range of clients that don't yet support TLS 1.3.
- ✓ **Deprecated protocols not supported**

Excellent. This server doesn't support any of the deprecated protocol (TLS 1.1 and earlier).

Verify that TLS 1.2 is working, that the top two Ciphers are preferred, and that the deprecated protocols are not supported.

Verifying with SSL Labs

From an external web browser, go to this website, select Test Your Server and enter your domain or host name:

<https://www.ssllabs.com>

When the report completes, scroll down to the section titled Configuration:

Configuration	
Protocols	
TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No
Cipher Suites	
# TLS 1.2 (suites in server-preferred order)	
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS 256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS 128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS WEAK 256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS WEAK 128

Verify that TLS 1.2 is working, TLS 1.1, TLS 1.0, SSL 3 and SSL 2 are disabled. Also verify that the top two Ciphers are preferred, and that the deprecated protocols are not supported.

4. Configuring MailSite to use the Ciphers

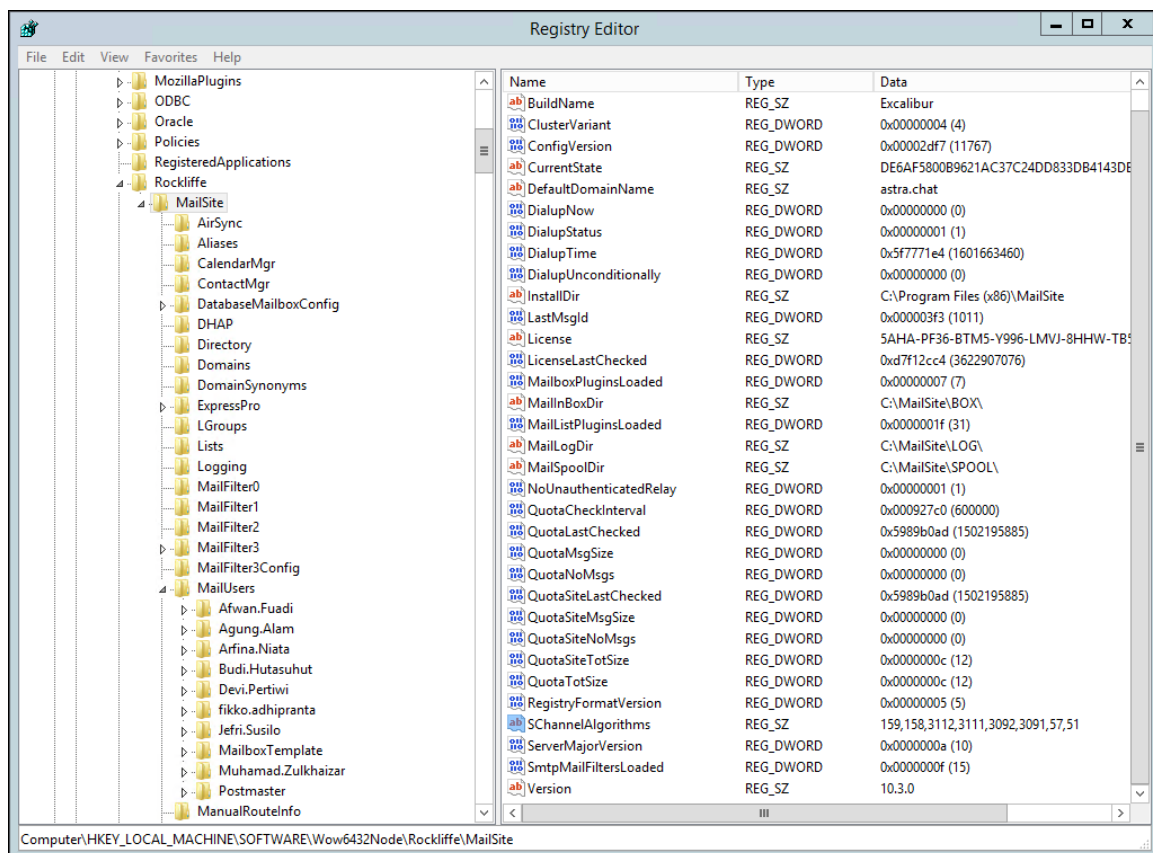
Now that you have Windows configured with the right TLS and Cipher settings, you can configure MailSite to use the corresponding Ciphers.

MailSite reads a registry configuration option to determine which Ciphers to use. This is described in this KB doc:

<https://www.mailsite.com/support/docs/html/1/05/10551.asp>

To match the Ciphers that we just configured with IISCrypto, do not use the entry from KB 10551, but use this value:

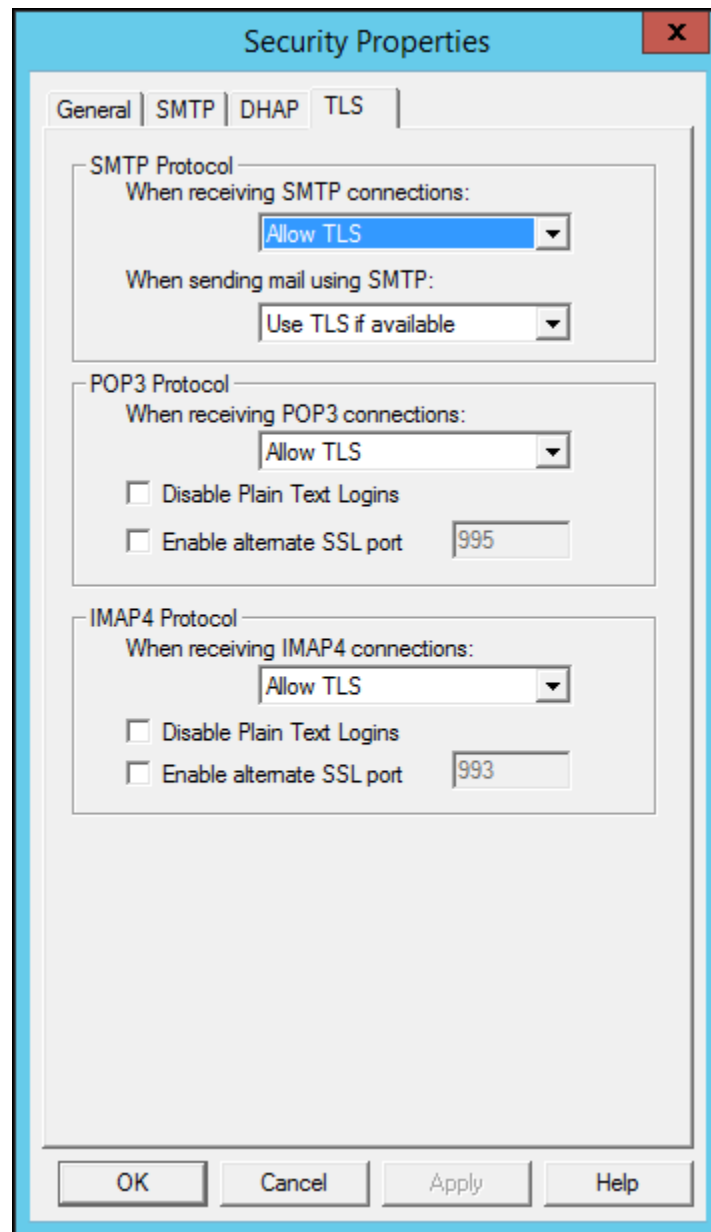
159,158,3112,3111,3092,3091,57,51



Note that the Cipher IDs are in decimal correlate to the hexadecimal Cipher SuiteID from the Hardenize or SSLlabs reports.

5. Verifying MailSite

Once you have the Windows and MailSite settings configured, verify that you have the right TLS settings for the MailSite services:



You can choose to Require TLS or Allow/Use TLS for each of the MailSite services. After making your choice, stop and start the services, and send a message to and from MailSite. Open the SMTPRA and SMTPDA log files and look for entries like this:

```

SMTPRA - Notepad
File Edit Format View Help
OperationProtocol) 0102cb00 <<< 220 astra.chat MailSite ESMTP Receiver Version 10.3.0.2 Ready
OperationProtocol) 0102cb00 >>> EHLO mail-ej1-f51.google.com
OperationProtocol) 0102cb00 <<< 250-astra.chat
OperationProtocol) 0102cb00 ... 250-SIZE 20000000
OperationProtocol) 0102cb00 ... 250-ETRN
OperationProtocol) 0102cb00 ... 250-ENHANCEDSTATUSCODES
OperationProtocol) 0102cb00 ... 250-X-IMS 3 64100
OperationProtocol) 0102cb00 ... 250-DSN
OperationProtocol) 0102cb00 ... 250-VRIFY
OperationProtocol) 0102cb00 ... 250-AUTH LOGIN SCRAM-MD5 CRAM-MD5
OperationProtocol) 0102cb00 ... 250-AUTH=LOGIN
OperationProtocol) 0102cb00 ... 250-STARTTLS
OperationProtocol) 0102cb00 ... 250 8BITMIME
OperationProtocol) 0102cb00 >>> STARTTLS
OperationProtocol) 0102cb00 <<< 220 2.5.0 Ready to start TLS
MSSocketOperation) Connection secured using Unknown with Cipher AES_256(256), Exch Unknown(256), Hash SHA(160)
OperationProtocol) 0102cb00 >>> EHLO mail-ej1-f51.google.com
OperationProtocol) 0102cb00 <<< 250-astra.chat
OperationProtocol) 0102cb00 ... 250-SIZE 20000000
OperationProtocol) 0102cb00 ... 250-ETRN
OperationProtocol) 0102cb00 ... 250-ENHANCEDSTATUSCODES
OperationProtocol) 0102cb00 ... 250-X-IMS 3 64100
OperationProtocol) 0102cb00 ... 250-DSN
OperationProtocol) 0102cb00 ... 250-VRIFY
OperationProtocol) 0102cb00 ... 250-AUTH LOGIN SCRAM-MD5 CRAM-MD5
OperationProtocol) 0102cb00 ... 250-AUTH=LOGIN
OperationProtocol) 0102cb00 ... 250 8BITMIME
OperationProtocol) 0102cb00 >>> MAIL FROM:<john.g.davies@gmail.com> SIZE=2987
OperationProtocol) 0102cb00 <<< 250 2.0.0 <john.g.davies@gmail.com> OK
OperationProtocol) 0102cb00 >>> RCPT TO:<john@astra.chat>
OperationProtocol) 0102cb00 <<< 250 2.0.0 <john@astra.chat> OK
OperationProtocol) 0102cb00 >>> DATA
OperationProtocol) 0102cb00 <<< 354 Ready for data
OperationAntiSpam) Message B0000001009@astra.chat received spam score of: 1
OperationProtocol) 0102cb00 <<< 250 2.0.0 Message received OK
OperationProtocol) 0102cb00 >>> QUIT
OperationProtocol) 0102cb00 <<< 221 2.0.0 astra.chat closing
  
```

```

SMTPDA - Notepad
File Edit Format View Help
( OperationDNSTransaction) 0554f8a0 Looking up host name financeofamerica.com for DNS records of Type 15 and Class 1
( OperationDNSTransaction) 0554f8a0 Response received of DSN status 0
( OperationDNSTransaction) 0554f8a0 AN Record: Name financeofamerica.com, Type 15, Class 1, TTL 298.
( OperationDNSTransaction) 0554f8a0 NX Record: Preference 0, Name financeofamerica-com.mail.protection.outlook.com.
( OperationDNSTransaction) 0554f8a0 AR Record: Name financeofamerica-com.mail.protection.outlook.com, Type 1, Class 1, TTL 8.
( OperationDNSTransaction) 0554f8a0 A Record: IP Number 104.47.45.36.
( OperationDNSTransaction) 0554f8a0 AR Record: Name financeofamerica-com.mail.protection.outlook.com, Type 1, Class 1, TTL 8.
( OperationDNSTransaction) 0554f8a0 A Record: IP Number 104.47.73.10.
( OperationNetworkConnection) 0554f618 Outgoing SMTP call established to 104.47.45.36 at 11:45:04.
( MSSocketOperation) The server financeofamerica-com.mail.protection.outlook.com presented a certificate with the name mail.protection.outlook.com possibly indicating a man-in-the-middle attack.
MSSocketOperation) Connection secured using Unknown with Cipher AES_256(256), Exch RSA_KEYX(2048), Hash SHA_384(0)
( OperationTransmittedSummary) 0554f618 B0003710212@mx.rockliffe.com: Begin sending Message B0003710212@mx.rockliffe.com from 10.42.8.5 (mx.rockliffe.com)
( financeofamerica-com.mail.protection.out) 0554f618 B0003710212@mx.rockliffe.com: Message B0003710212@mx.rockliffe.com sent at 11:45:06 to 104.47.45.36
( OperationNetworkConnection) 0554f618 Outgoing SMTP call to 104.47.45.36 completed at 11:45:06.
  
```

References

The material in this document is compiled from numerous sources; in particular the Microsoft Windows® support documents. Additional information can be found on Microsoft's website.

About Rockliffe Systems

Rockliffe is a privately owned company that is dedicated to building rock solid mobile communication software for service providers, enterprises and consumers. Based in California's Silicon Valley and with European headquarters in the UK and Asian headquarters in Jakarta, Rockliffe has numerous OEM relationships as well as a strong base of industry-leading strategic partners and technology partners. Rockliffe is a world class expert in mobile email and chat software having delivered four mobile communication products to market.

Disclaimer

Although Rockliffe has made reasonable efforts to ensure the accuracy at the time of publication, the accuracy of the information contained in this guide is not guaranteed. It is provided free of charge by Rockliffe. and has been prepared and validated on MailSite test and production platforms. Rockliffe disclaims all warranties, either express or implied, regarding this document and Rockliffe is not liable for any damages arising directly or indirectly from the information in this document.

Rockliffe Professional Services

Rockliffe Professional Services cover remote and onsite assistance with performance tuning, migrations, integrations, upgrades, email security audits, training, and custom software development. To discuss your requirements and arrange for a quote please contact sales@mailsite.com.

www.mailsite.com