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 Verifying a Certificate with DigiCert Verifying the hostname settings for MailSite	4 5 5
verifying SQL Server supports TLS 1.2	6
2. Configuring TLS and Ciphers	7
3. Verifying TLS and Ciphers	9
Verifying with Hardenize Verifying with SSLLabs	9 11
4. Configuring MailSite to use the Ciphers	.12
5. Verifying MailSite	.13
References	.15
About Rockliffe Systems	.15
Disclaimer	15
	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:

	certlm - [Certificates - Lo	tlm - [Certificates - Local Computer\Personal\Certificates]						×
File Action View Help								
🗢 🄿 🖄 🖬 🔒								
Certificates - Local Computer Certificates - Local Computer Certificates Certificates Certificates Certificates Certificates Certificates Certificate Certification Authorities Cintrusted Publishers Cintrusted Publishers Cintrusted People Cient Authentication Issuers Cient Authentication Issuers Certificate Enrollment Requests Certificate Enrollment Requests Cimat Card Trusted Roots Cimat Optices Veb Hosting Windows Live ID Token Issuer	Issued To	Issued By Sectigo RSA Domain Validation Se COMODO RSA Domain Validation	Expiration 7/5/2021 8/30/2018	Intended Purposes Server Authentic Server Authentic	Friend astra.c autodi	ly Nar	ne r.astra	
	<	Ш						>
Personal store contains 2 certificates.	[

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:

Ø		DigiCert Certificate	Utility for Windows©		_ 🗆 🗙
🖸 dig	icert [®] CERTIFICA	TE UTILITY for 1	Vindows®	1.800.8 support@digicert.c	96.7973 com Live Chat
	SSL Certificates			Create CSR 🛕 I	mport C Refresh
\Box	Issued To	Expire Date	Serial Number	Friendly Name	Issuer
	astra.chat	05-JUL-2021	00C438584E19B4CB6C9A	astra.chat	Sectigo Limited
SSL	autodiscover.astra.chat	30-AUG-2018	008016EBEC1E3E056EC3	autodiscover.astra.chat17	COMODO CA Limited
Code Signing Code Signing Tools Account					
Version 2.3.5.2					Close

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

E.		IIS Crypto		_ D X
IIS C	Crypto 3.2			NARTAC SOFTWARE
Schannel	Schannel These settings enable or disable v default for the operating system v	rarious options system wide. When t will be used. Click the Apply button	he checkbox is grey it means no se to save changes.	tting has been specified and the
Cipher Suites Cipher Suites Advanced	Server Protocols Multi-Protocol Unified Hello PCT 1.0 SSL 2.0 SSL 3.0 TLS 1.0 TLS 1.1 V TLS 1.2	Ciphers NULL DES 56/56 RC2 40/128 RC2 56/128 RC2 128/128 RC4 40/128 RC4 56/128 RC4 40/128 RC4 56/128 RC4 56/128 W RC4 128/128 Triple DES 168 ✓ AES 128/128 ✓ AES 256/256	Hashes MD5 SHA SHA 256 SHA 384 SHA 512	Key Exchanges ✓ Diffie-Hellman ✓ PKCS ✓ ECDH
Site Scanner	Client Protocols Image: Multi-Protocol Unified Hello Image: PCT 1.0 Image: SSL 2.0 Image: SSL 3.0 Image: TLS 1.0 Image: TLS 1.1 Image: TLS 1.2			
	Best Practices			Reboot: Apply

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:

E.	IIS Crypto	_ D X
IIS (Crypto 3.2	NARTAC SOFTWARE
Schannel	Cipher Suites Enable, disable or reorder various cipher suites that are negotiated for the TLS been specified and the default for the operating system will be used.	handshake. When the checkbox is grey it means no setting has
Cipher Suites Advanced Templates Site Scanner Other	 ▼ 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_128_CBC_SHA256_P256 ♥ 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_128_CBC_SHA_P256 ♥ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256 ♥ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256 ♥ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256 ♥ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ♥ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ♥ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384 ♥ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384 ♥ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256 ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256 ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384 ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384 ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384 ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384 ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384 ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ♥ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ♥ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ♥ TLS_ECDHE_ECDS_WITH_MDS ♥ TL	
	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 Some aspect	, but there ar of your site's	e warnings configuration require your attention.			
Suppor	ted protocols	TI Sv1 2	(02.02.100.211)			
Server sui	te preference	✓				
S	ILS VI.2 Berver preference	TLS_DHE_RS/ TLS_ECDHE_I TLS_ECDHE_I TLS_ECDHE_I TLS_ECDHE_I TLS_ECDHE_RS/ TLS_DHE_RS/	A_WITH_AES_256_GCM_SHA384 256 bits (DHE 2048 bits) A_WITH_AES_128_GCM_SHA256 128 bits (DHE 2048 bits) RSA_WITH_AES_256_CBC_SHA384 256 bits (ECDHE 256 bits) RSA_WITH_AES_128_CBC_SHA256 128 bits (ECDHE 256 bits) RSA_WITH_AES_256_CBC_SHA 256 bits (ECDHE 256 bits) RSA_WITH_AES_128_CBC_SHA 128 bits (ECDHE 256 bits) A_WITH_AES_256_CBC_SHA 256 bits (DHE 2048 bits) A_WITH_AES_128_CBC_SHA 128 bits (DHE 2048 bits) A_WITH_AES_128_CBC_SHA 128 bits (DHE 2048 bits)			
Analysi	is					
*	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 supported	protocols not	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 SSLLabs

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:

nfi	guration	
R	Protocols	
Ľ	TLS 1.3	No
	TLS 1.2	Yes
	TLS 1.1	No
	TLS 1.0	No
	SSL 3	No
	SSL 2	No
F	Cipher Suites	
	Cipher Suites # TLS 1.2 (suites in server-preferred order)	E
	Cipher Suites # TLS 1.2 (suites in server-preferred order) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS	256
7	Cipher Suites # TLS 1.2 (suites in server-preferred order) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS	256 128
5	Cipher Suites # TLS 1.2 (suites in server-preferred order) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH seep256r1 (eq. 3072 bits RSA) FS	256 256 226
	Cipher Suites # TLS 1.2 (suites in server-preferred order) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH seep256r1 (eq. 3072 bits RSA) FS WEAK TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH seep256r1 (eq. 3072 bits RSA) FS	256 128 256 128
ב	Cipher Suites # TLS 1.2 (suites in server-preferred order) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH seep256r1 (eq. 3072 bits RSA) FS_WEAK TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH seep256r1 (eq. 3072 bits RSA) FS_WEAK TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256 (0xc014) ECDH seep256r1 (eq. 3072 bits RSA) FS_WEAK	256 128 256 128 256
Ţ	Cipher Suites # TLS 1.2 (suites in server-preferred order) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256 128 256 128 256 128
Ē	Cipher Suites # TLS 1.2 (suites in server-preferred order) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH seep256r1 (eq. 3072 bits RSA) FS WEAK TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH seep256r1 (eq. 3072 bits RSA) FS WEAK TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH seep256r1 (eq. 3072 bits RSA) FS WEAK TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc013) ECDH seep256r1 (eq. 3072 bits RSA) FS WEAK TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc013) ECDH seep256r1 (eq. 3072 bits RSA) FS WEAK TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH seep256r1 (eq. 3072 bits RSA) FS WEAK TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH seep256r1 (eq. 3072 bits RSA) FS WEAK TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH seep256r1 (eq. 3072 bits RSA) FS WEAK	256 128 256 128 256 128 256 128 256

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:

1 Miles and a second se		Registry Editor		
File Edit View Favorites Help				
▶ - 📕 MozillaPlugins	^	Name	Туре	Data ^
DDBC		ab BuildName	REG_SZ	Excalibur
Dracle		🕫 ClusterVariant	REG_DWORD	0x00000004 (4)
Policies	=	100 ConfigVersion	REG_DWORD	0x00002df7 (11767)
	_	ab CurrentState	REG SZ	DE6AF5800B9621AC37C24DD833DB4143DE
⊿ 🄑 Rockliffe		ab DefaultDomainName	REG SZ	astra.chat
⊿ → MailSite		100 DialupNow	REG DWORD	0x00000000 (0)
AirSync		100 DialupStatus	REG DWORD	0x00000001 (1)
		200 DialupTime	REG DWORD	0x5f7771e4 (1601663460)
			REG DWORD	0x00000000 (0)
		ab InstallDir	REG SZ	C:\Program Files (x86)\MailSite
DatabaseMailboxConfig			REG DWORD	0x000003f3 (1011)
UHAP		ablicense	REG SZ	54H4-PE36-RTM5-V996-I MVI-8HHW-TB
Directory		Will icensel ast Checked	REG DWORD	0vd7f12cc4 (3622907076)
Domains		MailboxPluginsLoaded	REG_DWORD	0x00000007 (7)
		ab MailleBoxDir	REG_DWORD	C:\MailSite\BOX\
D - M ExpressPro		Maill istBlugingl gaded	REG_DWORD	0-0000001f (21)
Liter		ab Maill og Dir	REG_DWORD	Ci/MailSita/LOG/
		ab MailSpeelDir	REG_32	
			REG_32	C:(Maliste(SPOOL)
MailFilter1			REG_DWORD	0,0000001(1)
MailFilter2			REG_DWORD	0x00092700 (600000)
MailEiter3		QuotaLastChecked	REG_DWORD	0x598960ad (1502195885)
MailFilter3Config		QuotaMsgSize	REG_DWORD	0x0000000 (0)
MailUsers		QuotaNoMsgs	REG_DWORD	0x00000000 (0)
Afwan Fuadi		QuotaSiteLastChecked	REG_DWORD	0x5989b0ad (1502195885)
Agung Alam		QuotaSiteMsgSize	REG_DWORD	0x00000000 (0)
Arfina.Niata		20 QuotaSiteNoMsgs	REG_DWORD	0x00000000 (0)
Budi.Hutasuhut		CuotaSiteTotSize	REG_DWORD	0x000000c (12)
Devi.Pertiwi		and QuotaTotSize	REG_DWORD	0x000000c (12)
▶ 🚡 fikko.adhipranta		negistryFormatVersion	REG_DWORD	0x00000005 (5)
Jefri.Susilo		and SChannelAlgorithms	REG_SZ	159,158,3112,3111,3092,3091,57,51
▶ MailboxTemplate		100 ServerMajorVersion	REG_DWORD	0x0000000a (10)
Muhamad.Zulkhaizar		🕮 SmtpMailFiltersLoaded	REG_DWORD	0x0000000f (15)
Postmaster		(ab) Version	REG_SZ	10.3.0 🗸
	~	<	ш	>
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Rockliffe	\Mail	lite		

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:

Security Properties
General SMTP DHAP TLS
General SMTP DHAP TLS SMTP Protocol When receiving SMTP connections: Allow TLS When sending mail using SMTP: Use TLS if available POP3 Protocol When receiving POP3 connections: Allow TLS Disable Plain Text Logins Enable alternate SSL port 995 IMAP4 Protocol When receiving IMAP4 connections: Allow TLS Disable Plain Text Logins Enable alternate SSL port 993
OK Cancel Apply Help

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	x
File	Edi	t Format	View	Help		
Ope	ratio	Protocol)	0102cb6	90 <<<	220 astra.chat MailSite ESMTP Receiver Version 10.3.0.2 Ready	~
Ope	ratio	Protocol)	0102cb6	30 >>>	EHLO mail-ej1-f51.google.com	
Ope	ratio	Protocol)	0102cb6	30 <<<	250-astra.chat	
Ope	ratio	Protocol)	0102cb6	00	250-SIZE 20000000	
Ope	ratio	Protocol)	0102cb6	00	250-ETRN	
Ope	ratio	Protocol)	0102cb6	90	250-ENHANCEDSTATUSCODES	
Ope	ratio	Protocol)	0102cb6	30	250-X-IMS 3 64100	
Ope	ratio	Protocol)	0102cb6	90	250-DSN	
Ope	ratio	Protocol)	0102cb	90	250-VRFY	
Ope	ratio	Protocol)	0102cb6	90	250-AUTH LOGIN SCRAM-MD5 CRAM-MD5	
ope	ratio	Protocol)	0102CD0		250-AUTHELOGIN	
ope	ratio	Protocol)	0102CD0	90	250-STARTILS	
ope	ratio	Protocol)	0102CD0	90	250 8BITMIME	
Ope	ratio	Protocol)	0102CD0	90 >>>		
ope	ratio	Protocol)	0102CD6	30 <<<	220 2.5.0 Ready to Start ILS	
000	ocket	Deration)	0101cb/	LION S	ECUPE USINg UNKNOWN WICH CLDNEY AES_256(256), EXCH UNKNOWN(256), HdSh SHA(160)	
Ope	ratio	Protocol)	0102CD0	10 <i>} } }</i>	Ento mail-cji-tsi.googie.com	
Ope	ratio	Protocol)	0102CD0	20		
One	ratio	Protocol)	0102Cb0	a	256-5122 20000000	
One	ratio	Protocol)	0102cb0	a	256-ENMANCEDSTATUSCODES	
One	ratio	Protocol)	0102cb0	30	256-2, TMS 3 64100	
One	ratio	Protocol)	0102cb	30	250-DSN	
One	ratio	Protocol)	0102cb	30	250-URFY	
One	ratio	Protocol	0102cb	aa	259-AUTH LOGIN SCRAM-MD5 CRAM-MD5	
Ope	ratio	Protocol)	0102cb		250-AUTH=LOGIN	
Ope	ratio	Protocol	0102cb6	00	250 8BITMIME	
Ope	ratio	Protocol)	0102cb0	30 >>>	MAIL FROM: <john.g.davies@gmail.com> SIZE=2987</john.g.davies@gmail.com>	
Ope	ratio	Protocol)	0102cb0	30 <<<	250 2.0.0 <john.g.davies@gmail.com> OK</john.g.davies@gmail.com>	
Ope	ratio	Protocol)	0102cb6	30 >>>	RCPT TO: <john@astra.chat></john@astra.chat>	
Ope	ratio	Protocol)	0102cb6	30 <<<	250 2.0.0 <john@astra.chat> OK</john@astra.chat>	
Ope	ratio	Protocol)	0102cb6	30 >>>	DATA	
Ope	ratio	Protocol)	0102cb6	30 <<<	354 Ready for data	
Ope	ratio	nAntiSpam)	Message	B000	0001009@astra.chat received spam score of: 1	
Ope	ratio	Protocol)	0102cb6	30 <<<	250 2.0.0 Message received OK	
Ope	ratio	Protocol)	0102cb6	30 >>>	QUIT	
Ope	ratio	Protocol)	0102cb6	30 <<<	221 2.0.0 astra.chat closing	
						$\overline{\mathbf{v}}$
2						>
L • 1						 11

				SMTPDA - Notepad	- 15		x
File	Edit	Format	View H				
rite (((((((((((((((((((operation	roimai rationDN rationDN rationDN rationCN rationCN MSSoc OnTransm merica-c ionNretwo	View m STransact STransact STransact STransact STransact STransact STransact itredouma ittedouma ittedoum om.mail.p. rkConnect	<pre>tep tion) 0554F8a0 Looking up host name financeofamerica.com for DNS records of Type 15 and Class 1 tion) 0554F8a0 AN Record: Name financeofamerica.com, Type 15, Class 1, TTL 28. tion) 0554F8a0 AN Record: Name financeofamerica.com.mail.protection.outlook.com, Type 1, Class 1, TTL 8. tion) 0554F8a0 A Record: PNemper 104.47.45.36. tion 0554F8a0 A Record: IP Number 104.47.45.36. tion 0554F8a0 A Record: IP Number 104.47.45.36 at 11:45:04. tion) 0554F8a0 A Record: IP Number 104.47.45.36 at 11:45:04. tion) 0554F618 Outgoing SMTP call established to 104.47.45.36 at 11:45:04. tion) 0554F618 Outgoing SMTP call established to 104.47.45.36 at 11:45:04. tion) 0554F618 B00037102120mx.rockliffe.com: Begin sending Message B00037102120mx.rockliffe.com from 10.42.8.5 (mx.roc) mary) 0554F618 B00037102120mx.rockliffe.com: Begin sending Message B00037102120mx.rockliffe.com from 10.42.8.5 (mx.roc) protection.out tion) 0554F618 Outgoing SMTP call to 104.47.45.36 completed at 11:45:06.</pre>	outlo:	com)	



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 <u>sales@mailsite.com</u>.

www.mailsite.com