modicagroup®
INTELLIGENT MESSAGING

OMNI Platform Connectivity Options & Standards

17 November 2021

mark.goldfinch@modicagroup.com

+64 21 835 986

www.modicagroup.com

Your insurance claim #5984024366 has been received and is being reviewed.

You've earned a new cashback voucher! Scan this barcode in store to claim.

Your shift roster has been modified. 1 additional job has been added to your schedule.

Hi Lucy, visit our website to receive 20% off all products. https://bit.ly/2S3IKg1

ENTER

Congratulations - you are now in the draw to win a VIP package including flights & accom. Good luck.

Hi Lucy, you're booked in at MF Hair Tue, 12-Dec. Please respond YES to confirm. To reschedule please call.

YES

Your package will be delivered today.

Reminder: Your flight AB 987 to Hong Kong leaves tomorrow at 15:35. Check in here: https://bit.ly/2S3IKg1

Thanks for visiting our store today. Please rate your experience: https://bit.ly/2S3IKg1

Your verfication code is: 2204. Enter this online to activate your account.

Your verfication code is: 2204. Enter this online to activate your account.

Please enter PIN 4038 to change your password. Thanks for using MyGov online services.

Contents

1. Connectivity options for customers

Customers can connect to Modica's Omni platform over the internet using Transport Layer Security (TLS) to safeguard data in transit. Customer API connections are strongly recommended to be configured with authorised IP addresses.

1.1. TLS versions supported by Omni

Customers are recommended to use a modern and supported version of TLS, such as 1.2 or 1.3. The following table outlines the versions of TLS supported by Omni.

Endpoint	**Description**	**TLS version**	
		1.2	**1.3**
api.modicagroup.com[1]	Primary API endpoint	🟩	▨
omni.modicagroup.com	Primary Web Portal endpoint	🟩	🟩
api2.modicagroup.com	Secondary API endpoint	🟩	▨
omni2.modicagroup.com	Secondary Web Portal endpoint	🟩	▨
gateway.sonicmobile.com	Legacy API endpoint	🟥	

Key:

Currently supported	🟩
Planned but not available yet	▨

1.2. SMPP client applications with no TLS support

Most modern SMPP client applications (such as Kannel) offer native TLS support. Customers using SMPP applications which do not support TLS are required to use a proxy or tunnel technology (such as "stunnel") to encrypt data in transit. Omni does not offer support for "plain text" (unencrypted) SMPP because it is insecure and would result in the exposure of customers' messages to the public.

[1] Currently api.modicagroup.com supports lower versions of TLS but these are due to be removed as of 1 December 2021

1.3. Dedicated Client IPsec VPN

Wholesale aggregator customers who are unable to use TLS have the option to connect to Omni's APIs using a Dedicated Client IPsec VPN. Customers exercising this option are required to meet our standard terms and conditions and to establish a minimum of two customer IPsec VPN connections (for redundancy and high availability) using the supported options outlined within IPsec Minimum Standards.

1.4. Extended support for legacy IPsec VPNs

Extended support for legacy IPsec VPNs may be contracted by mutual agreement between the CTOs/CISOs of both organisations. This option requires an additional contract schedule to be signed, confirming acceptance of the risk and committing to transition to a supported option before the end of support date.

Phase	**Dates**	**Description**
Phase out period	**Starts:** 1 Oct 2021 **Ends:** 30 Sep 2022	Some legacy IPsec attributes are still supported for a period of 12 months to allow for time to migrate to safer and supported options.
Paid extended support period	**Starts:** 1 Oct 2022 **Ends:** 30 Sep 2023	Costs $5,000 per month or 10% of messaging costs, whichever is greater.
End of support	**At:** 1 Oct 2023	Legacy IPsec attributes are no longer available in Omni.

2. Connectivity options for suppliers

Modica partners with Mobile Network Operators (MNO) worldwide to deliver messages to every device on the planet. Three options are available to connect Omni to MNOs (exclusively for the purpose of delivering messages through their mobile networks). These options are listed below in order of preference.

2.1. Transport layer security (TLS)

A modern version of TLS (such as 1.2 and 1.3) is the safest and most reliable way to establish connectivity with our partners. It requires little to no configuration, has low maintenance costs, and offers very high availability out of the box.

2.2. Supplier IPsec VPNs

IPsec VPNs are complex to deploy, operate, and monitor, due to its many configuration items and potential failure modes. Carriers who cannot use TLS for connectivity must establish a minimum of two supplier IPsec VPN connections (for redundancy and high availability) using the supported options outlined within IPsec Minimum Standards.

Appendix

3. TLS Version History

TLS has evolved since its original creation, new TLS versions have been designed to strengthen the protocol. All versions prior to 1.2 have well known vulnerabilities. Supporting TLS 1.2 or later is now considered an important compliance requirement:

Protocol	Published	Status	Safety
SSL 2.0	1995	Deprecated in 2011	Unsafe
SSL 3.0	1996	Deprecated in 2015	Unsafe
TLS 1.0	1999	Deprecated in 2020	Unsafe
TLS 1.1	2006	Deprecated in 2020	Unsafe
TLS 1.2	2008		Safe & supported
TLS 1.3	2018		Safer & recommended

3.1. Browser TLS Support

Most major web browsers have removed support for TLS 1.0 and 1.1 within 2020, with only Microsoft Internet Explorer still supporting TLS versions earlier than 1.2:

Browser	TLS 1.0 and 1.1 Removal Dates
Apple Safari	Sept 2019: Disabled by default, end-user warning cannot be disabled.
Mozilla Firefox	June 2020: Disabled by default, end-user warning can be disabled.
MS Edge	July 2020: Disabled by default May 2021: End-user warning cannot be disabled
Google Chrome	July 2020: Disabled by default, end-user warning can be disabled. May 2021: End-user warning cannot be disabled
MS Internet Explorer	Early 2022: Removal planned (Internet Explorer is being discontinued by Microsoft and replaced by Edge)

3.2. Internet Service TLS Support

As of August 2021, 99.5% of the top 150,000 internet websites support TLS version 1.2 or higher. Less than 50% of Internet sites continue to support TLS 1.0 or 1.1.

4. IPSEC Minimum Standards

Phase	Attribute	Supported options
1	**IKE version**	Version 2
	Encryption	AES-256 using either GCM or CBC block modes
	Hashing	SHA-2 family of either: ● SHA-256 ● SHA-384 ● SHA-512
	Diffie Hellman Group (DH Group)	DH group numbers: ● 20 (ecp384) ● 21 (ecp521)
	Peer authentication	Pre-Shared Key (PSK) generated using the following recipe in 1Password or similar password generation tool: ● Memorable Password ● 10 Words ● Capitalise enabled ● Full words enabled
2	**Perfect Forward Secrecy (PFS)**	Enabled
	PFS Group	Use the same DH Group as selected in phase 1
	Source AND Destination networks	Globally Routable Address space in CIDR format. The Source and Destination Networks must be outside of private address ranges.