Network Setup

Interaction with the company infrastructure

The following protocols and connections can be used to interact with the customer IT infrastructure. Such protocols and ports must be Allowed in the customer firewall or NAT system.

Protocol	Direction (From Imagicle UC Suite Perspective)	TCP-IP Ports (Remote peer)	TCP-IP Ports (Imagicle Server)	Usage	Imagicle Applications
LDAP	OUT	TCP 389	Any (TCP)	The LDAP connection is optionally used to collect information from the customer LDAP or Active Directory server in order to populate the users list.	All
SMTP (SSL/TLS)	OUT	TCP 25 TCP 465 (SSL)	Any (TCP)	Used to send email notifications to advise about alarms, fax notifications, voicemail notifications, scheduled reports. Can be used with or without SSL/TLS support.	All
IMAP4	OUT	TCP 143 TCP 993 (SSL/TLS)	Any (TCP)	Used by Stonefax to retrieve email messages from the company mail server to allow the mail2fax feature. This is alternative to the POP3 protocol	Digital Fax
POP3	OUT	TCP 110 TCP 995 (SSL/TLS)	Any (TCP)	Used by Stonefax to retrieve email messages from the company mail server to allow the mail2fax feature. This is alternative to the IMAP4 protocol.	Digital Fax
EWS	OUT	TCP 443	Any (TCP)	Used by Stonefax to retrieve email messages from the company MS-Exchange email server to allow the mail2fax feature. This protocol can be also implemented to connect to MS-Office365 cloud-based email service	Digital Fax
Microsoft Sharing Protocol	IN/OUT	UDP 137 UDP 138 TCP 139 TCP 445 UDP 445	Any (TCP)	Optionally used to access customer's network shared folders for backup purposes (IAS backup, fax backup).	All
PMS Link	IN/OUT	TCP nnn	TCP nnn	Specific ports may be used by Hotel Link to connect to customer's PMS, depending on the PMS model/version. Please contact Imagicle for further details.	Hotel Link

Interactions between Imagicle Attendant Console Clients and the UC Suite

Following protocols and connections are used between Attendant Console clients and UC Suite server(s). These connections are used by following clients:

- Attendant Console Professional
- Attendant Console Enterprise
- Desktop CTI

Protocol	Direction (From Imagicle Server Perspective)	TCP-IP Ports (Remote peer)	TCP-IP Ports (Imagicle Server)	Usage	Imagicle Applications
Legacy	IN	Any (TCP)	TCP 51234	Client-Server plain communications between Attendant Console clients and Imagicle CTI Server.	AC Enterprise, Professional, Desktop CTI
Legacy	IN	Any (TCP)	TCP 51235	Client-Server TLS 1.2 encrypted communications between Attendant Console clients and Imagicle CTI Server.	AC Enterprise, Professional, Desktop CTI

Legacy (Microsoft only)	IN	Any (TCP)	TCP 21050	Client-Server plain communications between One Desktop for Microsoft UC and Imagicle CTI Server (Mondago GoConnect).	AC Enterprise, Professional
HTTP	IN	Any (TCP)	TCP 80	Optionally used for Centralized Live Update system	AC Enterprise, Professional, Desktop CTI

Interactions with the PBX

The following protocols are used to interact with any PBX. Such protocols and ports must be allowed in the customer firewall or NAT system.

Protocol	Direction (From Imagicle UC Suite Perspective)	TCP-IP Ports (Remote peer)	TCP-IP Ports (Imagicle Server)	Usage	Imagicle Applications
AXL(Cisco specific)	OUT	TCP 8443,8080	Any (TCP)	Secure protocol to retrieve configuration information from Cisco CallManager (phone status, users list, CallManager Version).	All
TAPI	IN/OUT	TCP 2748	Any (TCP)	TAPI (CTI) Protocol	All
SIP	IN/OUT	UDP 5060	UDP 5060	SIP communications to establish outgoing and incoming calls from/to Imagicle Stonefax (fax server)	Digital Fax
SIP	IN/OUT	UDP 5062 TCP 5062	UDP 5062 TCP 5062	SIP communications to establish outgoing and incoming calls from/to Imagicle ACD and IVR services.	Advanced Queuing
SIP	IN/OUT	TLS 5063	TLS 5063	Secure SIP communications to establish encrypted outgoing and incoming calls from/to Imagicle queuing and auto attendant services	Advanced Queuing
SIP	IN/OUT	UDP 5064	UDP 5064	SIP communications for presence notifications	Advanced Queuing Attendant Console Ent./Pro.
SIP	IN/OUT	UDP 5066	UDP 5066	SIP communications for Hotel Link voice services calls (incoming and outgoing voice calls)	Hotel Link
SIP	IN/OUT	UDP 5070 TCP 5070	UDP 5070 TCP 5070	SIP communications for Call Recording (incoming voice calls)	Call Recording
SIP	IN/OUT	TLS 5071	TLS 5071	Secure SIP communications for Imagicle Call Recording (incoming voice calls)	Call Recording
SIP	IN/OUT	UDP 5060	UDP 5060	SIP Communication to Imagicle Manager Assistant instance	Manager Assistant
SIP	IN/OUT	TLS 5061	TLS 5061	Secure SIP Communication to Imagicle Manager Assistance instance	Manager Assistant
H.323	IN/OUT	TCP 1720	TCP 1720	H.323 communications to establish outgoing and incoming calls from/to Imagicle voice/fax applications, depending on the version of Imagicle UC Suite.	Digital Fax VoiceMail
H.323	IN/OUT	TCP 1721	TCP 1720 TCP 1721	H.323 communications to establish outgoing and incoming calls from/to Imagicle UC Suite.	Digital Fax
RTP/T.38	IN/OUT	UDP > 1024*	UDP >= 5000	Real-time voice streams. Real-time data streams for T.38 fax relay.	Digital Fax, Advanced Queuing, VoiceMail, Call Recording, Hotel Link

HTTP (Cisco specific)	IN	Any (TCP)	TCP 80	CURRI invocation for External Call Control (Cisco UCM specific)	Contact Manager, Phone Lock
FTP	IN	Any (TCP)	TCP 21 TCP 22	(S)FTP CDR upload	Call Analytics

***** Cisco devices normally work in the 16384-32766 UDP port range.

Interactions with IP Phones and other voice devices

Following protocols are used to interact with the IP phones, ATA devices, Voice Gateways and Session Border Controllers. Such protocols and ports must be allowed in the customer firewall or NAT system.

Protocol	Direction (From Imagicle Server Perspective)	TCP-IP Ports (Remote peer)	TCP-IP Ports (Imagicle Server)	Usage	Imagicle Applications
HTTP (Cisco specific)	IN	Any (TCP)	TCP 80	XML services, accessed by IP Phones	Contact Manager Phone Lock IVR Manager
HTTP (Cisco specific)	OUT	TCP 80	Any (TCP)	XML notifications to Cisco IP Phones	Contact Manager Phone Lock
RTP/T.38	IN/OUT	UDP > 1024*	UDP >= 5000	Real-time voice streams. Real-time data streams for T.38 fax relay.	Digital Fax Advanced Queuing VoiceMail Call Recording Hotel Link

***** Cisco devices normally work in the 16384-32766 UDP port range.

Interactions among Imagicle UC Suite nodes in a cluster

Following protocols are used for inter-node communications between two joined nodes in the same Imagicle High Availability cluster. If HA environment involves a Disaster Recovery scenario, below protocols and ports must be allowed among different Data Centers, over a WAN.

Protocol	TCP/UDP Ports (from/to Imagicle Nodes)	Usage
Microsoft Share Protocol	UDP 137 UDP 138 UDP 445 TCP 139 TCP 445	Various file sharing
HTTP	TCP 80 TCP 443	Various IIS activities
SQL	TCP 1433***** UDP 1434	Database updates
RDP	TCP 3389	Remote Desktop transactions
IPC	TCP 52000-52999 (range)	Inter process communications

	TCP 4369 TCP 5672 TCP 15672 TCP 25672	

*****SQL Server listens to inbound communications using a random TCP port. To force a specific port (TCP 1433), please follow the procedure available here: https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-server-to-listen-on-a-specific-tcp-port

Note: Maximum allowed latency (RTT) for inter-nodal communications is 100msec.

Other network communication

Following protocols and connections can be used to interact with the customer IT infrastructure. Such protocols and ports must be Allowed in the customer firewall or NAT system.

Protocol	From	To	Usage
HTTP	Management workstation Users workstations (Any TCP port)	UC Suite and Manager Assistant TCP port 80	Application administration. WEB access to Imagicle applications for end-users.
HTTPS	Management workstation Users workstations (Any TCP port)	UC Suite and Manager Assistant TCP port 443	As above, using secure HTTP connections.
ANY	UC Suite (Any TCP/UDP port)	UC Suite (Any TCP/UDP port)	In the case of **High Availability** configurations that involve multiple UC Suite nodes, **full connectivity** must be available between UC Suite servers (no firewall or NAT) to allow content synchronizations between multiple nodes.

Communications with Internet services

There are a number of external Internet-based services that should reachable from IAS Server. These include Imagicle Online Cloud Licensing Server and Internet email services, like Office365 and Google Mail.

Protocol	From	To	Usage
HTTPS	UC Suite TCP Port 443, 8080, others	https://*.imagicle.com, Google Mail, MS-Office365, etc.	Imagicle Online Cloud Licensing Server and Internet email services

Starting from Imagicle UC Suite rel. 2019.Summer.1, Imagicle UC Suite allows to configure a proxy server to reach above Internet services. More info are available in this KB.

Single Sign On (SSO)

To leverage the Single Sign On authentication, the user PC should be able to reach some cloud services. Please refer at this page for the details.

Traffic requirements

In addition to the network connections described above and related firewall rules, following considerations and requirements must be considered in a deployment scenario.

- SIP / H.323 / T.38:
  Voice and fax streams with real time requirements:
    - Low Latency (maximum 80 ms RTT)
    - Wide Bandwidth (up to 80 Kbps for each simultaneous call, depending on the adopted voice codec)
- TAPI / JTAPI
  Call Control with real time requirements:
    - Low Latency (maximum 80 ms RTT)
    - Lightweight protocol (no need for wide bandwith)
- (S)FTP
    - Basically file transfer with no real-time requirements
    - Used bandwidth depends on the actual traffic figure
- AXL
    - Medium Latency (up to 150 ms RTT)
    - Low Bandwidth
- ECC CURRI (HTTP)
    - Low Latency (maximum 80 ms RTT)

Additional Server requirements

The Internet Options of the Imagicle Application Suite server should have the **proxy settings disabled**. Configuring a proxy may impact on service-to-service communications with the PBX or with other UC Suite nodes.