imagicle

UC Suite Security Features

Introduction

Imagicle has spent a lot of efforts and developments to achieve a high grade of security in its applications included in the UC Suite. All services, libraries and interfaces to external appliances have been secured and encrypted, thus avoiding any undesired data sniffing.

You can consult our Release Notes to understand all security improvements we added in the past years. Please subscribe to our Newsletter from same web page, to be updated about any enhancement we are introducing in Imagicle UC Suite.

In the following paragraphs, we are listing several security features and best practices to achieve a secure environment.

Microsoft Windows OS vulnerabilities

Microsoft is taking good care about its OS vulnerabilities and Microsoft issues several updates and service packs each year to solve security breaches encountered by customers or caused by viruses or malwares. This includes "IIS", which is heavily used by Imagicle as embedded web server for its web portal, mobile apps and clients' gadgets.

That's why we are recommending our customers to run Windows Updates on a regular base, as explained in our Installation Requirements.

Other Microsoft applications and components

Imagicle US Suite embeds a MS-SQL Server Express instance and we always make sure that security updates are always included in our Virtual Appliances and software packages. Consequently, we more and more recommend our partners and customers to keep their Imagicle UC Suite updated to latest software release, to make sure that proper SQL and runtime libraries updates (.NET, C++, ASP, others) are in place.

Imagicle Web Portal and APIs

These are the most risky interfaces that we open to the outside world. Through the web portal and web APIs, there are a number of security breaches which might really cause a lot of damage to customers. For example, you can enter some Javascript commands into a web portal's field, and those Java instructions might cause undesired data sniffing from SQL or even passwords retrieval.

Imagicle has identified a no-profit foundation called "Open Web Application Security Project" (OWASP) that works mainly to improve the software security. Thousands of OWASP members (including Imagicle) are sharing web-related security issues encountered in their software and, thanks to all contributors, OWASP has compiled a list of the TOP TEN web security breaches which are affecting most of the web accesses worldwide. The list is available here.

Imagicle provides a default Admin account to access UC Suite web portal. We STRONGLY suggest to immediately change the default password to a complex one, by following directions included in this KB article.

Antivirus

Installing an antivirus in Imagicle UC Suite server is indeed a good practice and it prevents malwares to hit operating systems and Imagicle applications. We have described how to configure your antivirus application to protect Imagicle server, without interfering with Imagicle apps performances, in this KB.

Data encryption at rest

As dictated by several worldwide regulations related to data security and privacy, Imagicle offers the possibility to leverage Microsoft BitLocker to encrypt the content of Imagicle UC Suite hard drive.

BitLocker is Microsoft's encryption program that provides full-disk encryption of the hard drives. By utilizing the latest encryption algorithms and leveraging the power and efficiency of modern CPUs, the entire contents of the startup disk are encrypted, preventing unauthorized access to the data stored on the disk, except for those with either the login account to decrypt the disk, or those owning the recovery key.

By enabling BitLocker's whole-disk encryption, data is secured from prying eyes. All attempts to access HD data, physically or over the network, are stopped with either a prompt to authenticate or error messages stating the data cannot be accessed, even when attempting to access data backups, as BitLocker encrypts those too. Please find extensive instructions about how to enable BitLocker in this article.

As an alternative to Microsoft BitLocker, customers can also leverage VMware own disk encryption.

TLS 1.2 Protocol

TLS 1.2 grants a high level of security and encryption to all communications involving web portal and email systems. A detailed article is available here, explaining how to enable such protocol within Imagicle UC Suite.

A specific article is also available to enable secure TLS connection to MS-SQL server. Please read here.

HTTPS Protocol and relevant Digital Certificate

Imagicle can implement HTTPS protocol to access own web portal, XML Phone Services, ECC-Curri web service and other https-based accesses hosted by IIS. You can decide to leverage the existing self-signed Digital Certificate or the certificate issued by your own Domain Controller or a certificate issued by a well-known Certificate Authority. All those cases are fully explained in this article.

Once updated Digital Certificate is in place, you can leverage it to enable encrypted https/XML transactions between Imagicle UC Suite and Cisco Call Manager:

- Imagicle External Call Control (CURRI ECC) for Phone Lock and Contact Manager's Caller ID. See here.
- Imagicle Phone Services for Phone Lock, Contact Manager, Call Recording. See here.

Email Server Secure Connections

Imagicle can provide email notifications to user and administrators, related to scheduled reports and alerts generated by Imagicle Monitoring service. Imagicle UC Suite routes email notifications to an existing customer's email server using SMTP protocol, with automatic SSL or TLS negotiation on any TCP port (465, 587, others). See relevant KB here.

Imagicle Digital Fax application supports fax handling through user's email client, allowing email-to-fax and fax-to-email transactions. To enable this feature, Digital Fax leverages above secure SMTP connection to send fax-related email notifications. To send faxes, Digital Fax connects to customer's email server using one of the following protocols, with automatic protocol negotiation:

- SSL/TLS POP3 on TCP port 995 (or any other)
- SSL/TLS IMAP4 on TCP port 993 (or any other)
- EWS using HTTPS on TCP port 443, with Proxy support

EWS basic and Oauth2 authentications are both supported. See relevant articles here and here.

Imagicle Secure Call Recording

Imagicle Call Recording application allows to record encrypted calls, leveraging Secure SIP and TLS audio streams coming from Cisco UCM. To enable Secure Call Recording, you can use the existing, self-signed Certificate included in Imagicle UC Suite server. Please consult this article, explaining how to download the Digital certificate and upload it in CUCM.

Secure SIP configuration for Call Recording is fully explained in this article.

Imagicle Secure Advanced Queuing

Imagicle Advanced Queuing application allows to enable encrypted calls between Cisco UCM and Imagicle server, leveraging Secure SIP and TLS audio streams. To enable Secure Advanced Queuing calls, you can use the existing, self-signed Certificate included in Imagicle UC Suite server. Please consult this article, explaining how to download the Digital certificate and upload it in CUCM.

Secure SIP configuration for Advanced Queuing is fully explained in this article.

Active Directory Secure Connection

As of March 2020, Microsoft has updated security requirements for LDAP connections to Active Directory. So now Secure LDAP (LDAPS) has become mandatory for all LDAP connections to Active Directory. LDAP connections to Active Directory will not work unless Secure LDAP is configured.

Imagicle follows above Microsoft statement and therefore Secure LDAP using SSL on port 636 is automatically enabled for both authentication and users' synchronization. If required, you can still configure non-secure LDAP on port 389, but obviously this is not recommended.

More info are available in this article.

Attendant Console Secure Connection

Starting from 2021.Winter.1 release, Attendant Console connects to UC Suite through a secure, TLS 1.2 encrypted TCP session on port 51235. If required, you can still leverage previous non-secure connection on TCP port 51234.

More info are available in this article.

FTP/SFTP Server

If you are running Windows Server 2019 or later but you are not using application that involves SFTP server usage (like Call Analytics or Hotel Pack) you can stop and disable the OpenSSH server or any alternative SFTP server running on the Imagicle virtual machine, that will prevent attacks on TCP port 22.

If Imagicle Call Analytics application is not used within Imagicle UC Suite, you can completely disable FTP server feature from Windows IIS control panel, to prevent attacks on TCP port 21.

Embedded MS-SQL Server Express Database Instance

Imagicle UC Suite includes its own SQL Server Express database, which provides an admin access using a local "sa" account and a complex password. You can change admin credentials or create a new account by following the directions available in this KB.