Security

Based on these considerations, they must also be taken into account for the antivirus scanning policies that may be installed on the computers, avoiding scanning or denial of access for security reasons.

- Considerations
- ISO 27001
- PCI Compliance

Considerations

The network where agents are working, must consider the following

1. Port 3478 UDP/TCP must be opened at least for the host stun.ucontactcloud.com
2. Port 8089 UDP/TCP must be opened at least for the host (ucontactinstance).ucontactcloud.com
3. Port 443 UDP/TCP must be opened at least for the host (ucontactinstance).ucontactcloud.com
4. Ports 10000-2000 UDP must be opened at least for the host (ucontactinstance).ucontactcloud.com
5. Access to the site http://cacerts.geotrust.com/GeoTrustRSACA2018.crt and redirector.gvt1.com/ must be enabled in order to allow browsers to validate uContact SSL certificate.
6. Enable access to the activator license site: us-central1-licenciator.cloudfunctions.net/api/servers/getLicence
7. Enable access to monitoring tool: monitor.ucontactcloud.com
8. Access to the following IP´s (104.197.204.63 , 74.125.134.127) used by google chrome.
9. Verify that SIP - ALG is not active on the local or border network devices.
10. Verify that IPS - detection is not active because it can cause VoIP packet discard and voice problemas (unespected call drops).
11. Domain *.github.com must be enable for system updates

Based on this considerations, the policy of the antivirus used on the workstations they must be actuated in order to avoid port scan, blocking or denying the access by security reasons.

ISO 27001

> The international standard ISO 27001 allows the assurance, confidentiality, and integrity of data and information and the systems that process it. This allows organizations to analyze risk and apply the necessary controls to eliminate it.

If we go to the system configuration, we find the following options that will help us establish a more secure system for our users.

Within the company message option, you can set a warning message from the company, which will appear every time the agent logs in. The system will also display the date and time of the user's last logged-in session.

IMAGEN

Among the security measures it establishes are:

Password expires after a certain number of days. (Modifiable)

- Request mandatory password change after it is updated by the supervisor or for the first time the user logs in.

Account lockout after certain unsuccessful password entry attempts. (Modifiable)

At the time of changing the password, do not allow to use of the last X amount of passwords used. (Modifiable)

The system has three different states for users:

- Asset.
- Inactive.
- Blocked (due to failed login attempts).

The user is disabled if they do not log in to uContact after a certain number of days. (Modifiable)

Password Format sets the complexity that agent passwords should have. Here you can configure if you should have:

- lower case

- Capital letters
- Numbers
- Special characters
- and the minimum length of characters

If we go to the creation of agents, we can find the following fields available:

LOGIN SCHEDULE

The possibility of creating a login schedule establishes certain days of the week and hours in which the agent can connect to the system.

TEMPORARY ACCOUNT

There is also the opportunity to create temporary users, that is, an account is created that has a forced expiration on the date established in the fields.

PCI Compliance

PCI is the Payment Card Industry Data Security Standard, also known as PCI DSS and is an exclusive information security standard administered by the Security Standards Council and makes reference to a standard that contains a series of security requirements that all merchants, large or small, must comply with, this standard applies to any company that processes, stores or transmits credit card data, therefore the merchant must have a "PCI Certificate" that guarantees that all its processes and tools that it uses comply with the necessary security regulations to guarantee the integrity of the information, for which reason the uContact Omnichannel Contact Center software is "PCI Compliance" because it complies with the most common requirements that the client's process requires for its certification.

Some basic compliance requirements that some processes are required and are included in uContact are:

- Use a 128bit SSL certificate. In short: Protect data. Encrypt any public transmission of data.
- ISO 27001 Security of handling and protection of information
- ISO 27002 business continuity management process
- Install and maintain a firewall configuration to protect data.
- Do not use vendor defaults for system passwords and other security settings.
- Encrypt the transmission of cardholder data over open, public networks.
- Restrict access to data on a business need-to-know basis.
- Assign a unique ID to each person with access to the system.
- Perform regular access and security checks to network resources and data.
- Maintain a security policy and make sure all staff is aware of it.

In addition, Google Cloud undergoes an annual third-party audit to certify that all of its products are PCI DSS compliant. This means that the services provided an infrastructure on which customers can build their own services or applications for storing, processing, or transmitting cardholder data.

It is important to note that customers remain responsible for ensuring that their applications are PCI DSS compliant.