Email Setup

Last Modified on 23/02/2024 11:33 am ACDT

> This article is part of the systems administration guide. You will require administration access to view the pages mentioned in this article.

The following is done once and typically will not need to be changed.

Enter SMTP settings

Sending emails requires the user to supply a suitable email server and configure CareRight to connect that server.

In this hosting scenario, it is the responsibility of the user to ensure that CareRight has the correct permissions to send emails using the global email from address.

CareRight supports sending emails using SMTP servers only. The following configuration parameters are available:

Administration.> Global Settings.

Fill in the following fields, clicking **Change** to save each value:

1. **SMTP Authentication Method** - If the server requires authentication, specifying the correct authentication type of your email provider is **compulsory**. Supported options are plain, login or cram_md5.
2. **SMTP Domain** - If you need to specify a HELO domain, you can do it here.
3. **SMTP Host** - hostname or IP Address of the mail server.
4. **SMTP Openssl Verify Mode -** allows you to turn off verification of certifications on SSL. **This is not recommended, contact Clintel to have your local certificates added to the store.**
5. **SMTP Password** - If your mail server requires authentication, set the password in this setting.
6. **SMTP Port** - TCP/IP port that your mail server used (default: 25 or 587)
7. **SMTP Start TLS** - Enable Start TLS Automatically - This allows an unencrypted connection (such as on port 25) to upgrade itself to an encrypted connection if the SMTP server supports this
8. **SMTP Username** - If your mail server requires authentication, set the username in this setting.

If the SMTP server requires authentication, it must be one of the support methods (Plain, Login or CRAM-MD5) and cannot have multi-factor authentication (MFA) enabled.

Services that require MFA or other authentication methods (such as Office 365) are not supported, but can work if a connector using a supported method is placed in front of it. Your email provider must be able to configure this for you.

Notes

- Customers hosting with Clintel who need to connect to an SMTP server on port 25 will require a change request submitted; to unblock access to main services. This is because Amazon Web Services (AWS) hosting blocks outgoing connections on port 25 by default. Contact Clintel to facilitate this.
- Port 25 is unencrypted and should not be used across the internet, unless you can enable the **Start TLS** option.
- Email is unencrypted by default and should not include confidential or sensitive information. Some third parties offer an encrypted email service where the email sent will contain a link to a secure location.
- Office365: It is extremely important to check that the Location's email from address should be reflective of Global

setting's email address if authentication is enabled on your organisation's email provider. If the location's email address is different from the Global settings, an error message will display whenever a mail attempts to send.

Microsoft Outlook / Office 365 via SMTP

There are times that default security options of outlook supersedes the default expectation of SMTP. This will vary depending on the email provider. Office365 / Outlook specifically have a distinct point of view in security therefore there are settings that were not expected by SMTP.

In this scenario, Clintel has investigated some potential mitigations for these encounters. Published here are some steps that could support.

No Authentication

If Multifactor Authentication is disabled on email instance, **SMPT Authentication Method** should be set to **None** and **SMPT OpenSSL Verify** should be set to **Disable Certificate Verification**.

Careright:

Please check your details below if using authentication on Outlook.

SMTP Authentication Method	Login
SMTP Domain	smtp.office365.com
SMTP Host	smtp.office365.com
SMTP OpenSSL Verify Mode	Peer verification
SMTP Password	
SMTP Port	587
SMTP Starttls	True
SMTP Username	

Office365 Portal:

- Login to Office 365. Visit **Admin account > Admin Center > Users > Active Users.**
- Select the managed user > Mail > Manage email apps
- At this point, **Authenticated SMTP** should be enabled.

Azure Portal: (Security Defaults)

- Login to Azure Portal Admin Account > Active Directory >
- In Managed: Go to Properties> Manage security defaults

- **Security defaults should be disabled, in favour of appropriate Conditional Access Policies.**

Azure Portal: (Permissions)

- Login to Azure Portal Admin Account > Active Directory
- In Managed: Go to Security> Conditional Access
- Depending on the development of your tenancy, there could be permissions that contradict your organisation's SMTP configuration.

Add App Password:

App passwords provide a method of authentication when integrating to any third-party software whenever 2-Factor Authentication is enabled on Office365 accounts. An official guide made by Microsoft on how to configure their product link below.

How to add App Password on Microsoft Email / Outlook / Office365

SMTP for Google Mail (Gmail, Google Apps for Business) Accounts

Careright:

SMTP Authentication Method	login
SMTP Domain	smtp.gmail.com
SMTP Host	smtp.gmail.com
SMTP OpenSSL Verify Mode	Peer Verification
SMTP Password	
SMTP Port	587
SMTP Start TLS	true
SMTP Username	

Please Note:

We have received reports regarding the increased security on google accounts. Therefore, we have researched additional support for Careright clients when setting up SMTP.

Google:

Gmail has implemented increased security on their accounts. This means it is highly necessary to enable 2-step verification on your organisation's account to match the security standards of Careright and Google.

Enable 2-step verification

1. Open your Google Account.
2. In the navigation panel, select Security.
3. Under “Signing in to Google,” select 2-Step Verification > Get started.
4. Follow the on-screen steps.

Next, **Create App Password** (Application password for Careright)

1. Go to your Google Account.
2. Select Security.
3. Under "Signing in to Google", select App Passwords.

   You may need to sign in. If you don't have this option, it might be because:

   - 2-Step Verification is not set up for your account.
   - 2-Step Verification is only set up for security keys.
   - Your account is through work, school, or other organisation.
   - You turned on Advanced Protection.
4. At the bottom, choose Select app and choose the app you are using > Select device and choose the device you're using > Generate.
5. Follow the instructions to enter the App Password. The App Password is the 16-character code in the yellow bar on your device.
6. Tap Done.

Secure your organisation's app password and use it as the SMTP password for Careright's Global Settings

Set "Email from" address in Locations

The “from” address used for all email communication is set per location. You need to specify the Email From address for each Location.

1. Click **Administration**.
2. Click **Locations**.
3. For the location you wish to send Emails from, click the name.
4. Click **Edit**.
5. Scroll down to **Correspondence** and fill in the **Email** From details.
6. Email From: no-reply@your-organisation.com.au e.g. no-reply@clintel.com.au
7. Click **Update Location**.

Set permissions

You need to ensure anyone editing Email Templates has the correct permissions. Users that are required to read, edit and send letters also need to have the right permissions. See Groups for more details on setting permissions (allowed actions).

Grouping	Allowed action	Description
Correspondence	Can view Email Messages	-
Correspondence	Can create and send Email message from template	Can send template Email messages i.e. content is preset and read only
Correspondence	Can configure Email templates	Can create/edit Email templates (Message Types) in the Administration area

Set Appointment Status conditions

An appointment status indicates what state the appointment booking currently is in. For example, when first created, an appointment usually is set to "Booked." Most of the automated Email sending functionality is centred around notifications related to appointment statuses.

BackEach status, needs to be associated with one of the following conditions:.

- Completed
- Cancelled
- Confirmed
- Unconfirmed

An example list of configured appointment statuses might be:

Appointment Status	Appointment Condition	Active / inactive
Booked	Unconfirmed	Active

Confirmed - SMS	Confirmed	Active
Confirmed - Phone	Confirmed	Active
Confirmed - Other	Confirmed	Active
Arrived	Confirmed	Active
Cancelled - SMS	Cancelled	Inactive
Cancelled - By Patient	Cancelled	Inactive
Cancelled - By Clinic	Cancelled	Inactive
Completed - Unbilled	Confirmed	Inactive
Completed - Billed	Completed	Inactive
Completed - No Billing Required	Completed	Inactive

Additionally each appointment can be considered either *active* or *inactive*. Appointments in the conditions Cancelled or Completed are considered inactive. All other conditions are active.

The Email system is driven by the *appointment condition* and not by the specific appointment status.

For example, you can set an email reminder to be sent 3 days before an appointment if the appointment is in an *unconfirmed* state. If the patient calls to confirm or responds to a SMS message and the appointment is changed to a confirmed state, then no further reminder emails would be sent.

Setting the Appointment Status Conditions

1. Click **Administration**.
2. Click **Appointments**
3. Click **Appointment Status**.
4. For each **Appointment Status**, click **Edit**.
5. Select the **Condition** from the list.
6. Click U**pdate Appointment Status**.

Enter SMTP settings - Managed service

Where CareRight is deployed with AWS SES in a managed service capacity, the following environment variables take precedence over UI settings.

SMTP_HOST
SMTP_PORT
SMTP_START_TLS
SMTP_OPENSSL_VERIFY_MODE
SMTP_AUTH
SMTP_USERNAME
SMTP_PASSWORD
SMTP_DOMAIN