Configuring the Inbound Gateway

> **Note**
>
> Given the potential for service disruption during this process, Coro recommends scheduling these changes at a time of least impact.

Configuring the Inbound Gateway requires changes to an organization's own DNS and email infrastructure, as well as enabling the Gateway inside your Coro workspace. This section describes the steps required.

Changes are required in your DNS and email service

To set up the Coro Inbound Gateway to protect your incoming emails, you must perform some configuration steps in your email and DNS services *before* you can configure your Coro workspace. You need to:

- Obtain all **prerequisites**.
- Set up your original email provider to recognize Coro as the **gateway for inbound email**.
- Update your email domain **DNS settings**, mapping your highest priority mail exchanger (MX) record to Coro's Inbound Gateway server IP address.

Prerequisites

Before you begin, make sure you have the following information:

- IP address(es) of Coro's Inbound Gateway email proxy service. Contact **Coro Support** for details.
- MX record details for Coro's Inbound Gateway email proxy service. Contact **Coro Support** for details.
- The identity of your email service provider
- Your email domain

Setting Coro as an inbound gateway with the original email provider

Coro can be configured with the following email providers:

- **Gmail**
- **Microsoft 365**
- **Third party MTA**