

Install the Certidox Mail Proxy Server

Administrator deployment guide: install the proxy, connect its IP address and authentication key, configure mail routing, enroll users and test outgoing certification.

How deployment works

The Certidox Mail Proxy Server is installed **within your organization's environment** and certifies outgoing emails automatically. Employees continue using their existing email clients. The proxy handles certification before the email leaves the configured route, and recipients can independently verify a certified message.

The installation sequence is **Install → Connect → Configure → Invite users → Test**. The setup supports Microsoft 365, Google Workspace and other SMTP-based environments, subject to the mail-routing configuration chosen by the administrator.

Scope: the steps below describe the administrator workflow. Docker images, installation commands, SMTP ports, network rules and mail-provider credentials are environment-specific and must be taken from the approved Certidox installation package. Do not invent substitute endpoint values.

STEP 01

Install the proxy

1. Log in to the Certidox administration interface and open the automatic email certification setup.
2. Choose the installation method supported in your environment: **Docker** or **manual installation**.
3. Install the Certidox Mail Proxy Server on a host your organization controls. Follow the version-specific instructions provided with your approved installation package.
4. Record the **IP address** of the installed proxy and securely copy the **authentication key** supplied during installation.
5. Confirm that the proxy process is running and that the required connectivity can be established under your organization's network and firewall policies.

Do not email the authentication key in clear text or publish it in technical documentation accessible to unauthorized users.

STEP 02

Connect to Certidox

1. Return to the Certidox setup interface and proceed to **Connect**.
2. Enter the **IP address of the Certidox SMTP proxy** created in Step 1.
3. Paste the authentication key copied during installation.
4. Use the interface's connection test and confirm that the proxy is associated with the intended Certidox account.

Connection information: the required field is the proxy's IP address, not a generic address of the mail service. Check the IP and key if the connectivity test fails.

STEP 03

Configure your email platform

1. Select your environment: **Microsoft 365, Google Workspace or another email platform**.
2. Complete the platform-specific configuration using your mail administrator's approved settings and the instructions shown by the Certidox setup interface.
3. Ensure the intended outgoing mail flow passes through the Certidox proxy; avoid routes that bypass certification.
4. Save the configuration and confirm that the platform and Certidox proxy both indicate a valid connection before activating mailboxes.

Keep existing SPF, DKIM and DMARC policies in place, checking any changes required by your organization's selected routing. Certidox certification complements conventional email authentication; it does not replace it.

STEP 04

Invite and activate users

1. Identify the mailboxes or users that should be enrolled in automatic certification.

2. Use the Certidox account administration flow to **invite users** and activate their outbound certification where applicable.
3. Verify the authorized sender addresses and domains correspond to your deployment scope.
4. Apply the changes and check that each selected mailbox is listed as enabled under the administration interface.

This configuration is designed to allow employees to keep composing and sending emails in their usual software, including desktop, laptop and mobile clients.

STEP 05

Verify the installation

1. From an enrolled mailbox, send a controlled test email to an external account you own.
2. Confirm that the message arrives with its **Certidox certification QR code**.
3. Scan the QR code using the Certidox app (not a general-purpose QR scanner) and check the recorded origin, certification time, exact certified reference and **current status**.
4. Where appropriate, use **View document** to compare the certified email-content reference with the message received.
5. Repeat the test for each email platform or route in use, including representative device types when applicable.

If the message arrives without a Certidox QR code, do not assume automatic certification is operational. Review the proxy state, mail-routing rules, enabled sender list and configuration logs before onboarding additional users.

Operational checklist

Check	Expected outcome
Proxy installation	Host running; IP address and key securely recorded.
Account connection	Certidox interface reports a successful connection to the intended proxy.
Mail platform	Outbound flow for the chosen mailboxes traverses the proxy.
Sender enrollment	Appropriate users have been invited and activated.
Delivery and certification	Controlled outbound test arrives with the Certidox QR code.
Recipient verification	Origin, certification time, certified content reference and current status can be inspected.

Confidential by design: email content is encrypted by the self-hosted proxy. No readable message content or decryption keys are stored on Certidox servers. Recipients should verify certified messages **before relying on them.**