

How to Set Up Email Encryption and Archival

<https://campus.barracuda.com/doc/39815270/>

This article applies to the Barracuda Message Archiver firmware version 5.0 and higher, and the Barracuda Email Security Gateway.

You can encrypt and archive journaled email by partnering the Barracuda Email Security Gateway and the Barracuda Message Archiver.

Requirements

Before getting started, verify that you have the following deployed and running in your environment:

- Email Server configured to utilize journaling
- [Barracuda Message Archiver](#) firmware version 5.0 or higher
- [Barracuda Email Security Gateway](#) firmware version 8.0 or higher

Important

Upon activating archived mail encryption, the Barracuda Email Security Gateway periodically contacts the Barracuda Message Center for new mail sent or received for your domain. To ensure a secure outbound connection and delivery of email to the Barracuda Message Archiver, port 4234 (Outbound TCP) must be open on the firewall or for the Barracuda Email Security Gateway. The hostname for port 4234 is `encrypt-api.cudasvc.com`.

Define Encryption Policies

Encryption is configured at the domain level while an encryption policy is configured at the global level, for example, by sender domain or email address. Global encryption policies apply to all domains from which encrypted email messages are sent. From the **Block/Accept** page in the Barracuda Email Security Gateway, specify the outbound encryption rules for global system-managed filtering including:

- **Content Filtering** – Specify message delivery filtering based on expressions
- **Custom Content Filters** – Filter based on subject line, message headers, message body and attachment file type
- **Attachment Filters** – Block, quarantine, encrypt, or redirect outbound messages based on patterns or file extensions
- **Predefined DLP and HIPAA Compliance Filters** – Filter based on predefined data leakage

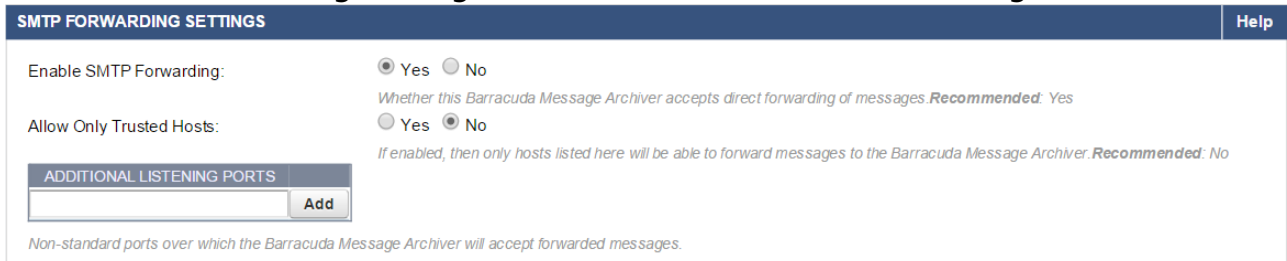
patterns as specified on the **Block/Accept > Content Filters** page

See [Encryption of Outbound Mail](#) and [Content Analysis for Outbound Mail](#) for additional information.

Activate Encrypted Mail Archiving

Use the following steps to specify encrypted email archival on the Barracuda Message Archiver:

1. Log into the *Barracuda Email Security Gateway* as the administrator, and go to the **Basic > Administration** page.
2. In the **Email Encryption Service** section, enter an email address in the **Valid Test Email Address** field to test encryption, and enter the *Barracuda Message Archiver* IP address in the associated field.
3. Specify any additional **Email Encryption Service** settings, and then click **Save**.
4. Log into the *Barracuda Message Archiver* as the administrator, and go to **Mail Sources > SMTP** page.
5. In the **SMTP Forwarding Settings** section, set **Enable SMTP Forwarding** to **Yes**:



6. In the **Trusted SMTP Servers** section, add the *Barracuda Email Security Gateway* IP address. Click **Add**, and then click **Save**.

Verify Inbound and Outbound Email Archival

1. Log into the *Barracuda Email Security Gateway* as the administrator, and go to the **Basic > Administration** page.
2. In the **Email Encryption Service** section, click **Test Encryption Connection**. The recipient will receive a notification once the test email is available in the Barracuda Message Center.

Figures

1. smtp_settings2.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.