

DJIGZO EMAIL ENCRYPTION

Djigzo Gateway SMTP Authentication Guide



October 19, 2011, Rev: 5454

1 Introduction

This guide will briefly explain how to setup Postfix to allow authenticated users to relay email to external recipients. This guide explains how to configure plain password authentication and therefore assumes that TLS has already been setup to protect against password sniffing (see [djigzo-tls-guide](#) for more information on setting up TLS). This guide assumes that Djigzo is installed on Ubuntu 10.04.

Note: commands that should be executed by the user are shown on lines starting with a \$ sign (the \$ sign is not part of the command to execute). The commands can be copied and pasted to the command line.

2 Install and configure Dovecot

Dovecot common should be installed which will provide the SASL back-end for Postfix.

2.1 Install

```
$ sudo apt-get install dovecot-common
```

2.2 Configure

Dovecot SASL should be configured for Postfix. The Dovecot configuration is stored in the file `/etc/dovecot/dovecot.conf`.

The following *socket listen* configuration fragment should be added just below the existing commented out *socket listen* fragment:

```
socket listen {
  client {
    path = /var/spool/postfix/private/auth-client
    mode = 0660
    user = postfix
    group = postfix
  }
}
```

Note: instead of adding a new *socket listen* fragment, the existing *socket listen* can be commented out and modified.

2.3 Authentication mechanisms

By default Dovecot only enables plain text passwords. Other, more secure, SASL mechanisms (for example login and digest-md5) can be enabled by adding the SASL mechanisms to the mechanisms of *auth default*. Note that some SASL mechanisms require additional configuration.

The following example shows that *plain* and *login* authentication mechanisms are enabled:

```
auth default {
  # Space separated list of wanted authentication mechanisms:
  #   plain login digest-md5 cram-md5 ntlm rpa apop anonymous gssapi otp skey
  #   gss-spnego
  # NOTE: See also disable_plaintext_auth setting.
  mechanisms = plain login
```

Note: Outlook express and Windows Mail require *login* authentication. It is therefore advised to add *login* to the list of supported authentication mechanisms.

Restart Dovecot

Dovecot should be restarted after the configuration file has been modified.

```
$ sudo /etc/init.d/dovecot restart
```

3 Configure Postfix

Postfix should be configured to support SMTP authentication for the SMTP daemon.

The following lines should be added to Postfix main configuration file (use MTA raw config or directly edit the configuration file */etc/postfix/main.cf*):

```
smtpd_sasl_auth_enable = yes
broken_sasl_auth_clients = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth-client
```

Add *permit_sasl_authenticated* to *smtpd_recipient_restrictions* to allow relaying after the sender has successfully authenticated.

The final *smtpd_recipient_restrictions* line should look similar to:

```
smtpd_recipient_restrictions = permit_sasl_authenticated, permit_mynetworks,
  reject_unauth_destination ${djigzo_reject_unverified_recipient?},
  reject_unverified_recipient}
```

Make sure to apply the new MTA settings (or manually restart Postfix).

4 Add a user account for relaying

A user should be added which will be used for authenticating the SMTP connection. A user named *sender* will be added:

```
$ sudo adduser --no-create-home --shell /bin/false sender
```

Select a strong password and leave all other settings default (i.e. empty).

Note: by default Dovecot allows all users with a login account to authenticate. Dovecot however support different ways to authenticate users (for example users stored in a SQL database or LDAP). See the Dovecot documentation for more information.

5 Finish

It should now be possible to setup an authenticated SMTP session with a mail client. Make sure to protect the session with TLS.