

DJIGZO EMAIL ENCRYPTION

Djigzo Gateway PDF Encryption Setup Guide



October 20, 2011, Rev: 5454

Contents

1 Introduction	4
2 Portal	4
3 PDF encryption setup	5
3.1 Option 1: Static password	6
3.1.1 Enable PDF encryption	6
3.1.2 Set a static PDF password	6
3.1.3 Edit PDF encryption template	7
3.2 Option 2: Send back to sender	7
3.2.1 Enable PDF encryption	7
3.2.2 Enable Send to originator	9
3.2.3 Set password validity	9
3.2.4 Set password length	9
3.2.5 Edit PDF encryption template	10
3.3 Option 3: Send password by SMS	10
3.3.1 Enable PDF encryption	10
3.3.2 Allow SMS	12
3.3.3 Set recipients mobile number	12
3.3.4 Set password validity	12
3.3.5 Set password length	12
3.3.6 Edit PDF encryption template	12
3.4 Option 4: One Time Password (OTP)	13
3.4.1 Enable PDF encryption	13
3.4.2 Enable OTP	13
3.4.3 Enable Auto create client secret	14
3.4.4 Enable Auto invite	14
3.4.5 Set password length	14
3.4.6 Edit PDF encryption template	14
3.5 Example OTP encryption	14
3.5.1 Message received in Gmail	15
3.5.2 Portal signup	15
3.5.3 Portal login	15
3.5.4 Generate OTP	15
3.5.5 Open PDF	15
4 Enable PDF reply	15
4.1 Reply allowed	18
4.2 Reply URL	18
4.3 Reply sender	19
5 Final	19
A Setup SMS gateway	20
A.1 Clickatell transport	20

B Allow access to portal	22
B.1 Open the firewall	22
B.2 Protect login page	22

1 Introduction

Although S/MIME encryption is one of the most secure ways to encrypt email, the problem with S/MIME is that it requires the recipient to use an S/MIME capable email client¹ and the recipient must have a certificate and a private key. Although installing a certificate and a private key is not hard, even less so when using the gateways built-in CA functionality, it may still be too cumbersome for some recipients. Especially when only a few secure email messages need to be exchanged over a longer period.

As an alternative to S/MIME encryption, PDF encryption can be used. The PDF standard allows a PDF to be encrypted with a password². Files can be added to the PDF and are encrypted as well. Because most recipients already have a PDF reader installed, they do not need to install or configure any software.

When the gateway PDF encrypts a message, it converts the complete email message, including all attachments, to a PDF. The PDF is then password encrypted and attached to a new message (which is based on a template). This message does not contain any information other than a general note that the message contains an encrypted PDF. This guide will explain in detail how to setup PDF encryption for the Djigzo gateway.

Note: This guide assumes that the Djigzo gateway has already been installed and configured for sending and receiving email. For a more detailed guide on setting up and managing a Djigzo gateway see the *Djigzo Administration Guide*.

2 Portal

The Djigzo gateway contains a built-in portal which can be used by external recipients to reply to a PDF and to retrieve one time passwords (OTP). To support PDF reply and OTP, some portal settings should be specified. The global portal settings can be opened by selecting *Settings* → portal (see figure 1).

The portal settings will be briefly explained:

Password The password is used by the external user to login to the portal. If no password is set for the user, the user cannot login to the portal.

Note: It's strongly advised not to set the portal password for the global settings. Every external user should have a personalized password.

Enabled If set, the user can login to the portal using the email address of the user as the login name and the portal password for the user. If not set, the user cannot login.

¹Most email clients however support S/MIME out of the box

²The PDF is encrypted with AES128 with a key based on the password.

Portal settings for global preferences

Portal settings

Password	<input type="text"/>	<input checked="" type="checkbox"/> inherit
Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Auto invite	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Base URL	<input type="text"/>	<input checked="" type="checkbox"/> inherit

Figure 1: Portal settings

Note: the enabled setting is only used to specify whether the user can login. If not set, users can still reply to a PDF since replying to a PDF does not require the user to login.

Auto invite If the *Auto invite* setting is set and a one time password encrypted PDF is sent to the user, the user is “invited” to select a new password.

Base URL To access the portal functionality, external users need to connect to the portal. The URLs to which external users need to connect to are written to the emails and encrypted PDFs (for example the reply link in the PDF). To make sure the URLs are externally accessible URLs, the gateway has to know what the correct external URL of the portal is³. The *Base URL* is not directly used, but is used as the base for the following URLs: PDF reply URL and OTP URL. The *Base URL* can only be set for the global settings.

Example: In most setups, the base URL should look similar to*:

`https://www.example.com/web/portal`

* replace `www.example.com` with the domain name or IP address of the real server.

3 PDF encryption setup

This section explains how to configure PDF encryption. There are different options to password encrypt the PDF.

1. The PDF can be encrypted using a pre-defined static password.

³In most typical setups, the gateways internal IP address is different from the external IP address (NAT).

2. The PDF can be encrypted using randomly generated password. The password will be sent by SMS Text to the recipient.
3. The PDF can be encrypted using randomly generated password. The password will be sent back by email to the sender of the message.
4. The PDF can be encrypted using a One Time Password (OTP) algorithm.

The different password options will be separately explained.

3.1 Option 1: Static password

This section will explain how to configure PDF encryption with static passwords.

To enable static password mode, the following steps are required:

1. Enable PDF encryption.
2. Set a static PDF password.
3. Edit PDF encryption template.

3.1.1 Enable PDF encryption

To make sure that PDF encryption is allowed, the following settings should be specified:

- *Encrypt Mode*: should be set to *Allow*.
- *PDF Encryption allowed*: should be selected.

These settings can be set for the global settings, for a domain or for a specific user.

Note: The default settings of *Encrypt Mode* and *PDF Encryption allowed* are set to allow encryption.

3.1.2 Set a static PDF password

A new user object for the external recipient should be added. A new user can be added by clicking *Add user* on the left hand side menu. Once the external user has been added, the static PDF password can be specified on the settings page (see figure 2).

Note: the external recipient must be an external user, i.e., the *Locality* setting should be set to *External*. If not, the message won't be encrypted⁴.

⁴Every user by default is an external user unless the *Locality* has been set to *Internal* for the user, for the domain or for the global settings.

Password			
Password	<input type="text" value="test"/>	<input type="checkbox"/>	inherit
Password ID	<input type="text"/>	<input checked="" type="checkbox"/>	inherit
Validity interval	<input type="text" value="0"/> (min)	<input checked="" type="checkbox"/>	inherit
Send to originator	<input type="checkbox"/>	<input checked="" type="checkbox"/>	inherit

Figure 2: Password preferences

3.1.3 Edit PDF encryption template

The encrypted PDF will be attached to a standard message which is based on a template. The standard template can be modified to contain specific information about the company sending the message. The PDF template can be modified by selecting the global settings and then select *templates*. On the template page, multiple templates can be selected. The template for the static password mode is *Encrypted PDF* (see figure 3).

3.2 Option 2: Send back to sender

With this mode, a PDF password will be automatically generated and sent back to the sender of the message by email.

To enable send back to sender mode, the following steps are required:

1. Enable PDF encryption.
2. Enable Send to originator.
3. Set password validity.
4. Set password length.
5. Edit PDF encryption template.

3.2.1 Enable PDF encryption

To make sure that PDF encryption is allowed, the following settings should be specified:

- *Encrypt Mode*: should be set to *Allow*.
- *PDF Encryption allowed*: should be selected.

These settings can be set for the global settings, for a domain or for a specific user.

Note: The default settings of *Encrypt Mode* and *PDF Encryption allowed* are set to allow encryption.

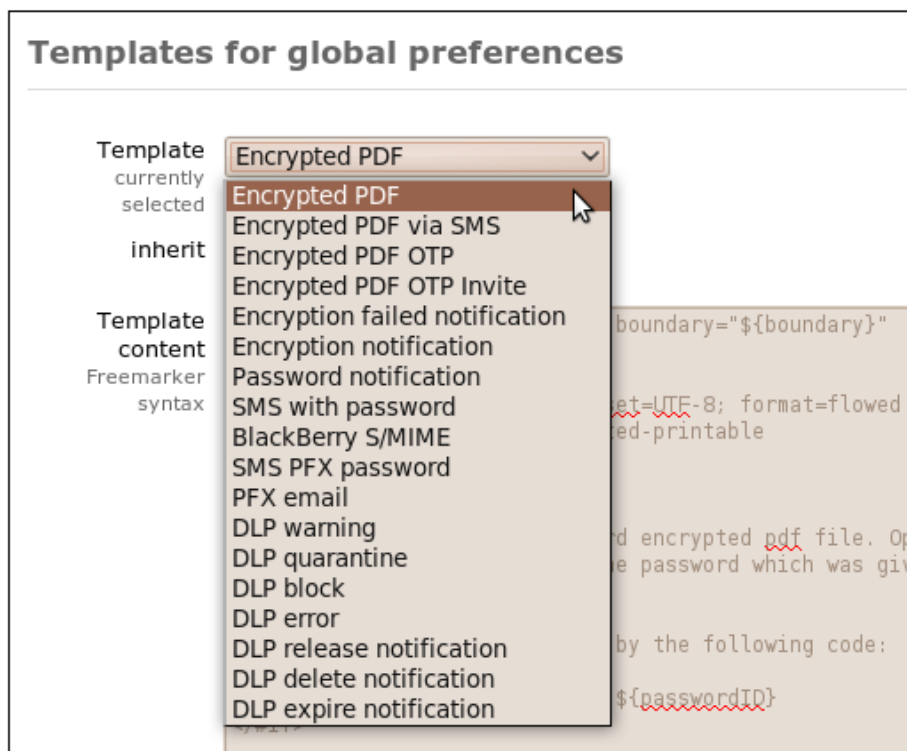


Figure 3: Templates

```
x-original-to martijn@djigzo.com
received from secure.djigzo.com (unknown [192.168.0.6]) by djigzo.com

The message with Subject:

test

has been sent encrypted to the following recipients:

"m..brinkers"@gmail.com

The passwords are:

recipient: m..brinkers@gmail.com password: ejvximbie7ifs id: 9683946

---
Djigzo open source email encryption
```

Figure 4: PDF passwords

3.2.2 Enable Send to originator

To enable automatic password generation and to make the gateway send the generated passwords back to the sender by email, the option *Send to originator* should be selected (see figure 2). The generated passwords will be sent back to the sender by email (see figure 4 for an example message). If an email is sent to multiple recipients, a new password will be generated for each recipient.

To make it possible for a recipient to determine which password belongs to which message, a unique password id will be generated for every new encrypted email. The message with the encrypted PDF, will also contain the unique password id.

Note: The message containing the newly generated passwords, which is sent back to the sender, is based on the *Password notification* template (see figure 3).

3.2.3 Set password validity

By default, a new password will be generated for every new message. The time (in minutes) a generated password will be valid can be set by changing the value of *Validity interval* (see figure 2). If a password is still valid, a new password will not be generated and the existing password and password id will be used.

3.2.4 Set password length

The length of the randomly generated password is by default 16 bytes (128 bits). The length of the generated password can be set using the advanced setting *Password length*.

Note: make sure the generated password is long enough to make it harder to “guess” the password.

3.2.5 Edit PDF encryption template

The encrypted PDF will be attached to a standard message which is based on a template. The standard template can be modified to contain specific information about the company sending the message. The PDF template can be modified by selecting the global settings and then select *templates*. On the template page, multiple templates can be selected. The template for the send back to sender mode is *Encrypted PDF* (see figure 3).

3.3 Option 3: Send password by SMS

In this mode, a PDF password will be automatically generated and the password will be sent by SMS Text to the recipient’s mobile number. This mode requires that the SMS gateway is correctly setup (see Appendix A on how to setup the SMS gateway).

To enable SMS mode, the following steps are required:

1. Enable PDF encryption.
2. Allow SMS.
3. Set recipients mobile number.
4. Set password validity.
5. Set password length.
6. Edit PDF encryption template.

3.3.1 Enable PDF encryption

To make sure that PDF encryption is allowed, the following settings should be specified:

- *Encrypt Mode*: should be set to *Allow*.
- *PDF Encryption allowed*: should be selected.

These settings can be set for the global settings, for a domain or for a specific user.

Note: The default settings of *Encrypt Mode* and *PDF Encryption allowed* are set to allow encryption.

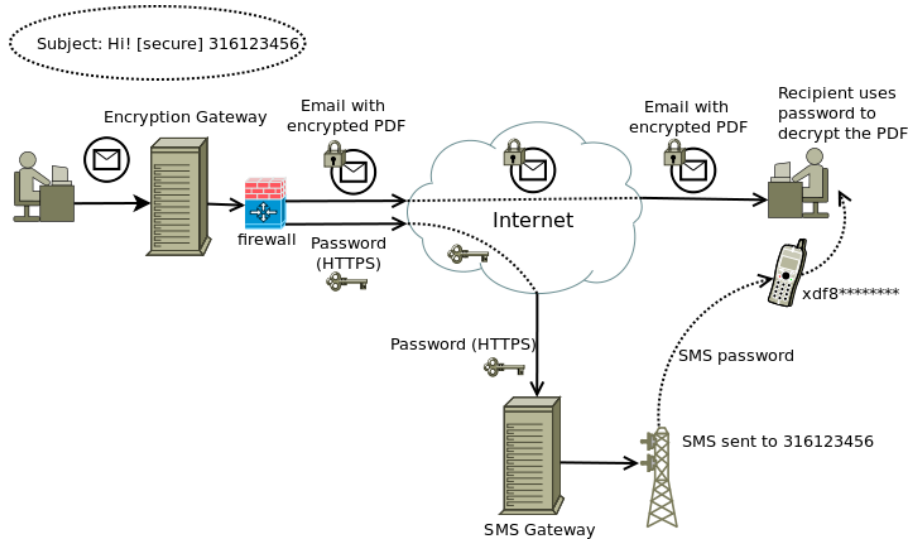


Figure 5: PDF encryption with SMS

SMS

Phone number	<input type="text"/>	<input checked="" type="checkbox"/> inherit
Send SMS	<input type="checkbox"/>	<input checked="" type="checkbox"/> inherit
Receive SMS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> inherit

Figure 6: SMS settings

3.3.2 Allow SMS

By default, senders are not allowed to send SMS Text messages. To allow the sender to send SMS Text messages, the *Send SMS* property should be selected (see figure 6). The *Send SMS* setting can be set for the global settings, for a domain or for a specific user.

3.3.3 Set recipients mobile number

The generated password will be sent by SMS Text to the recipient. The gateway therefore has to know which phone number to use. A user object for the recipient should be added and the *Phone number* settings should be set (see figure 6). The telephone number should be in international format (i.e., it should start with a country code).

Note: instead of explicitly setting the mobile number of the recipient, the sender can also add the phone number to the subject line of the email. See the *Digzo Administration Guide* for more information on how to setup the gateway to allow the mobile number to be specified on the subject line of the email.

3.3.4 Set password validity

By default, a new password will be generated for every new message. The time (in minutes) a generated password will be valid can be set by changing the value of *Validity interval* (see figure 2). If a password is still valid, a new password will not be generated and the existing password and password id will be used.

3.3.5 Set password length

The length of the randomly generated password is by default 16 bytes (128 bits). The length of the generated password can be set using the advanced setting *Password length*.

Note: make sure the generated password is long enough to make it harder to “guess” the password.

3.3.6 Edit PDF encryption template

The encrypted PDF will be attached to a standard message which is based on a template. The standard template can be modified to contain specific information about the company sending the message. The PDF template can be modified by selecting the global settings and then select *templates*. On the template page, multiple templates can be selected. The template for the password by SMS mode is *Encrypted PDF via SMS* (see figure 3).

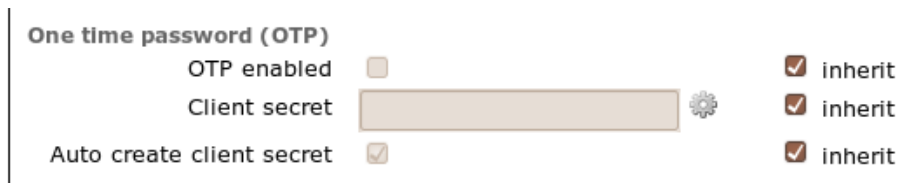


Figure 7: OTP settings

3.4 Option 4: One Time Password (OTP)

In the one time password mode, a password will be generated using a "One Time Password" (OTP) algorithm. The generated passwords will be based on the *Client Secret* of the recipient and the *Password ID* of the email. Because the *Password ID* of the email will always be different for every PDF, the generated password will be different for every PDF.

To enable OTP mode, the following steps are required:

1. Enable PDF encryption.
2. Enable OTP.
3. Enable Auto create client secret.
4. Enable Auto invite.
5. Set password length.
6. Edit PDF encryption template.

3.4.1 Enable PDF encryption

To make sure that PDF encryption is allowed, the following settings should be specified:

- *Encrypt Mode*: should be set to *Allow*.
- *PDF Encryption allowed*: should be selected.

These settings can be set for the global settings, for a domain or for a specific user.

Note: The default settings of *Encrypt Mode* and *PDF Encryption allowed* are set to allow encryption.

3.4.2 Enable OTP

OTP should be enabled by selecting the *OTP enabled* setting (see figure 7).

3.4.3 Enable Auto create client secret

The *Client secret* of a recipient is used for generating a One Time Password. Every recipient therefore requires a *Client secret*. The gateway will automatically generate a random client secret for a recipient if the setting *Auto create client secret* is checked and the recipient does not yet have a client secret (see figure 7).

3.4.4 Enable Auto invite

A recipient needs to login to the portal to generate the one time password of the PDF ⁵. The recipient therefore requires a portal password. If the *Auto invite* option is enabled and there is not yet a portal password for the recipient, an invite link will be added to the email. After clicking the invite link, the recipient can choose a portal password for the portal account. Alternatively, the portal password can be set by the gateway administrator.

3.4.5 Set password length

The length of the randomly generated password is by default 16 bytes (128 bits). The length of the generated password can be set using the advanced setting *Password length*.

Note: make sure the generated password is long enough to make it harder to “guess” the password. In the OTP mode, the password will be generated by the portal. The password can be copied and pasted into the PDF password dialog. The password can therefore be longer than with the other modes since the recipient does not have to enter the password manually.

3.4.6 Edit PDF encryption template

The encrypted PDF will be attached to a standard message which is based on a template. The standard template can be modified to contain specific information about the company sending the message. The PDF template can be modified by selecting the global settings and then select *templates*. On the template page, multiple templates can be selected. The template for the OTP mode is *Encrypted PDF OTP* and *Encrypted PDF OTP invite* if the recipient is invited (see figure 3).

3.5 Example OTP encryption

The following section will give a brief overview of the steps an end-user will need to take to read a PDF encrypted message which was encrypted with an OTP.

The following steps will be shown:

⁵Alternatively, using the client secret, the one time password can be locally (i.e., client side) generated using Javascript or some other client application.

1. Message received in Gmail
2. Portal signup
3. Portal login
4. Generate OTP
5. Open PDF.

3.5.1 Message received in Gmail

A PDF encrypted message in Gmail looks like a normal email message with an attached PDF document (see figure 8). The email contains some text explaining what the required steps are to open the encrypted email.

3.5.2 Portal signup

Clicking the link in the email opens the portal signup page on which the recipient needs to choose a password (see figure ??). The portal signup only has to be done the first time. Once the recipient has selected a password, the recipient can login with the selected password.

3.5.3 Portal login

After the password has been selected, the recipient has to login with the new password (see figure 10).

3.5.4 Generate OTP

After logging in, the page on which the One Time Password (OTP) can be generated will be opened. The password ID, from the email, has already been filled in (see figure 11)⁶. Clicking the *Generate password* button will generate the One Time Password for the PDF (see figure 12).

3.5.5 Open PDF

The generated password can be copied and pasted into the PDF reader password dialog. The PDF will be opened. Message attachments are added to the PDF and can be opened from the attachment pane at the bottom of the PDF (see figure 13).

4 Enable PDF reply

A recipient of an encrypted PDF can reply to the encrypted PDF message by clicking the *Reply* link embedded in the PDF. The browser will connect via a secure https connection to the on-line reply portal running on the gateway (see

⁶The password ID is taken from the link. If the password ID is not filled in, it can be copied and pasted from the email.

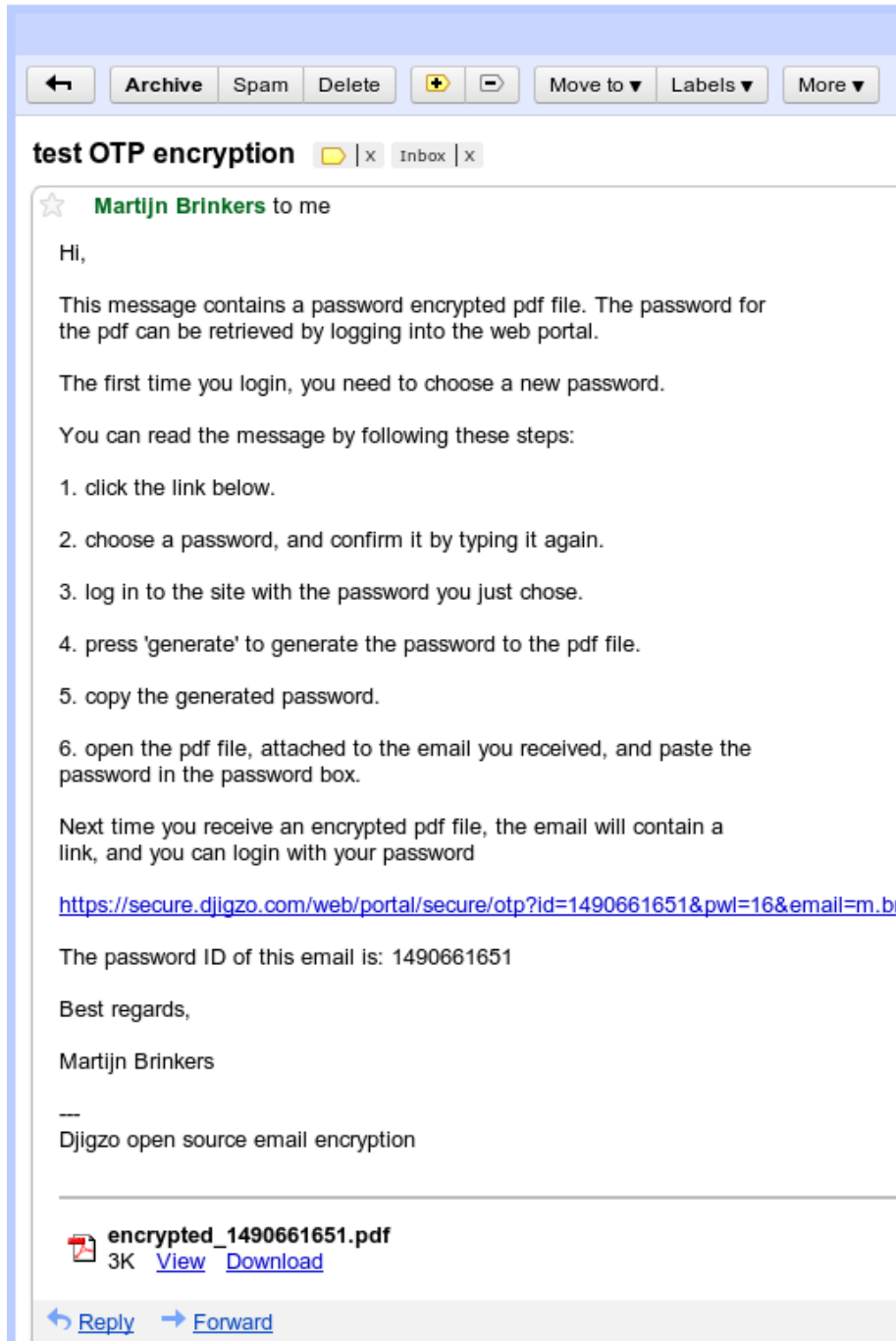



Figure 8: OTP email in Gmail

Portal sign up 
m.brinkers@gmail.com


Choose a secure password for your account. The password is required for logging into the portal. After setting the new password, you are requested to login into the portal.

New password

Repeat password

Apply

Figure 9: Portal signup

Portal login 
Please enter your email address and password

Email
Your email address

Password
Your portal password

Login

Figure 10: Portal login

[generate otp](#) [change password](#) [about](#) [logout](#) [m.brinkers@gmail.com](#) en ▾

Generate one time password for the encrypted PDF

By pressing the Generate password button, the password for the encrypted PDF will be generated using the provided password id*. You can copy-and-paste the generated password to the PDF reader password dialog.

Password id:

PDF password:

Generate password

* if the password id field is empty, copy and paste the password id from the email.

Figure 11: Generate OTP



Figure 12: OTP generated

figure 14). On the reply portal page, the user can create the reply message and add attachments. The reply will be sent via the Djigzo gateway back to the sender of the PDF encrypted message. By default the PDF reply functionality is not enabled.

To enable the PDF reply functionality, the following steps should be taken:

1. Select *Reply allowed*.
2. Set the *Reply URL*.
3. Set the *Reply sender*.

4.1 Reply allowed

The reply link will only be added when the *Reply allowed* setting is selected (under the advanced settings). The *Reply allowed* setting can be set for the global settings, for a domain or for a specific user.

4.2 Reply URL

The *Reply URL* specifies which URL should be used for the reply link. The *Reply URL* should be set to the external IP address (or domain name) on which the gateway can be accessed.

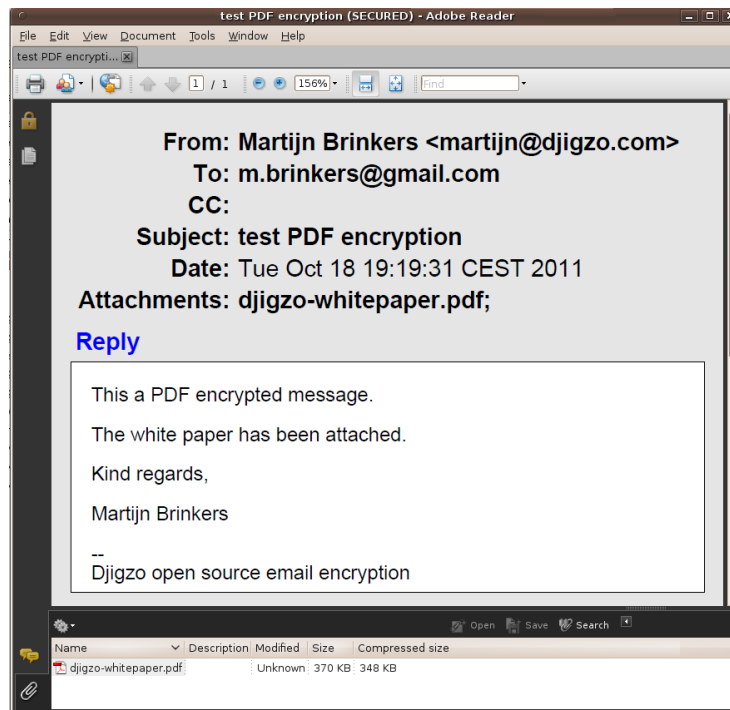


Figure 13: Decrypted PDF

Note: If the base URL has been setup correctly (see section 2), the *Reply URL* is automatically configured. You only need to set the *Reply URL* explicitly if the PDF reply page should be accessed on a different URL than the base URL.

4.3 Reply sender

The *Reply sender* should be set to an email address that will be used as the sender of the PDF reply (for example user reply@example.com). For more information why the real email address of the replier is not used, see the *Djigzo Administration Guide*. The *Reply sender* should be set to a real email address which is capable of receiving email. In most cases it's best to set the reply sender for the global preferences.

5 Final

For a discussion about the pros and cons of the different PDF password modes and a discussion of other security related issues regarding PDF encryption, see the PDF section of the Frequently Asked Questions (FAQ).

Compose a reply message

From: m..brinkers@gmail.com 
 To: martijn@djigzo.com
 Subject: Re: test PDF encryption

Attachment
max. size 5 MB

README.txt ✘

Reply:

See my answers in the attached document.

Kind regards,

Martijn Brinkers

Figure 14: PDF reply

A Setup SMS gateway

Djigzo contains an SMS gateway which is used for sending generated passwords via SMS Text messages. The SMS gateway can use different SMS transports for the delivery of SMS Text messages⁷. The default SMS transport is set to Clickatell (see <http://www.clickatell.com> for more information). SMS Text messages are sent via a secure HTTPS connection to Clickatell. When an SMS Text message is sent, it is queued for delivery until the message has been delivered with the active SMS transport (see figure 15). To test the SMS gateway an SMS Text message can be manually added with *Add SMS*.

A.1 Clickatell transport

The default SMS transport is the *Clickatell transport*. This transport forwards all the SMS Text messages to an external SMS gateway (using a secure HTTPS connection). A Clickatell account should be available and configured before any SMS Text messages can be sent. See see <http://www.clickatell.com> for more information about the sign-up process.

During the Clickatell sign up process, an HTTP connection should be added⁸ (leave the *Callback* parameters empty). The connection has an associated *API ID* which is required by the Clickatell transport. Open the Clickatell transport

⁷Currently only Clickatell and Gnokii (direct connection to Nokia phones) are supported.

⁸See the Clickatell *HTTP API Specification v.2.x.x* document for more information

Certificates	Roots	CRLS	SMS	Settings	Queues	Logs	Admin
SMS							
delete selected invert selection							
<input type="checkbox"/>	ID	Phone Number	Created				
<input checked="" type="checkbox"/>	666	123456	01/13/2009 06:51				

Figure 15: SMS gateway

Certificates	Roots	CRLS	SMS	Settings	Queues
Clickatell SMS transport settings					
API id	<input type="text" value="123456"/>				
<small>Id of the HTTP API</small>					
User	<input type="text" value="clickatell"/>				
<small>User name</small>					
Password	<input type="password" value="●●●●"/>				
<small>Password for user</small>					
From	<input type="text"/>				
<small>Sender phone number</small>					
Balance	830.4	Update balance			
<small>SMS balance (credits)</small>					
<input type="button" value="Apply"/> <input type="button" value="Close"/>					

Figure 16: Clickatell settings

configuration page by opening the *SMS* page and clicking the *Clickatell settings* left-hand side sub-menu (see figure 16). The first three settings: *API id*, *User* and *Password* are mandatory. The *From* parameter can be set to the sender of the SMS Text message (i.e., set to the telephone number of the sender) but only after the telephone number has been approved by Clickatell.

Clickatell uses pre-paid message credits. To check how many credits are left (and for testing the login credentials), click *update balance*.

Note: The new transport settings are only used after the changes have been applied. Before clicking *Update balance*, make sure all changes are applied.

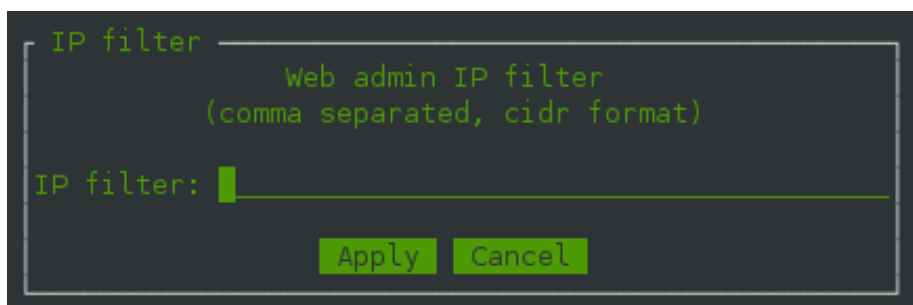


Figure 17: IP filter

B Allow access to portal

B.1 Open the firewall

If the gateway is protected by a firewall, the firewall should be opened to accept incoming connections to the gateway on the https port⁹.

B.2 Protect login page

In the default setup, the Web admin login page and the PDF reply page can be accessed on the same (https) port. To prevent unauthorized users from opening the gateway Web admin login page, it is advised to only allow access to the Web admin page from certain approved IP addresses.

The gateway contains a IP filter which can be used to block access to the Web admin pages from unauthorized IP addresses. To authorize IP addresses, open the Djigzo Virtual Appliance console and select config → IP Filter. . . . On the IP filter dialog, a comma separated list of IP ranges can be specified which will be authorized to access the Web admin login page (see figure 17).

Example: to allow access to the Web admin login page from the range 192.168.178.* and from the IP 123.45.67.89 use the following IP filter: 192.168.178.0/24, 123.45.67.89.

Note: for users not using the Djigzo Virtual Appliance, or for other ways to protect the Web admin login page against unauthorized access, see the *Djigzo Installation Guide*.

⁹If the gateway uses a different port than the default https, for example 8443, the firewall should be opened for the alternative port.