

# Organization Settings

Here you can change your organization settings. Note: In the list below you can find just some information to introduce the feature. You can click on the headline of the feature to get to the detailed explanations.

- [Organization Details](#)
  - [Default Callback URL](#)
  - [Design of the document viewer for recipients](#)
  - [Disposable Certificate](#)
  - [BankId Authentication](#)
  - [Generic Signing Plugin](#)
  - [Notification Plugin](#)
  - [Policy for the document viewer for recipients](#)
  - [Signature Appearance](#)
  - [Activity-Engine Custom Localizations](#)
  - [Retention Period](#)
  - [Backup](#)
  - [Timestamp Configuration](#)
  - [Automatic Remote Signature Profiles](#)
  - [Default Signature Settings](#)
  - [Envelope Defaults](#)
  - [Audit log Settings](#)
  - [Signature PAdES Configuration](#)
  - [Email Settings](#)
  - [User Logout Redirect Url](#)
  - [Default redirect url before sending a draft](#)
  - [Envelope Details Page](#)
  - [Extended Signing Options](#)
  - [Recipient settings](#)
  -
- [Organization Details](#)
- [Default Callback URL](#)
  - If you set a callback, every finished or changed envelope will cause a request on your defined URL. With this URL you can add your own service for e.g. performing an automatic archiving via eSAW API. If the URL is empty no callback is fired on finish or change of the envelope. More details about the callbacks are available in our [API Reference - SOAP](#) and below this enumeration as a separate chapter.
    - Placeholder for envelope complete callback: **##EnvelopeId##** and **##Action##** (only *envelopeFinished* action available)
    - Placeholder for envelope status change callback: **##EnvelopeID##** and **##Action##** (*workstepFinished*, *workstepRejected*, *workstepDelegated*, *workstepOpened*, *sendSignNotification*, *envelopeExpired*, *workstepDelegatedSenderActionRequired*)
- [Design of the document viewer for recipients](#)
  - Set a default redirect URL for finished documents
  - Upload and download designs
  - Information about the biometric encryption key
- [Disposable Certificate](#)
  - Configuration of the LRA to use the disposable certificates. Settings for LRA credentials, certificate type and disclaimer usage.
  - Configure disposable type
- [SwissCom OnDemand Certificate](#)
  - Configuration for the SwissCom OnDemand Certificate **v 3.3**
  - SwissCom OnDemand Certificate UI configuration **v 21.27**
- [BankId Authentication](#) **v 3.4**
  - Set the authentication certificate
- [Generic Signing Plugins](#) **v 20.42**
  - Configure the signing plugin
- [Notification Plugins](#)
  - Configure notification plugins
- [Policy for the document viewer for recipients](#)
  - Upload and download the default policy for the document viewer for recipients
- [Retention Period](#)
  - Enable Retention Period of Organization Drafts and Envelopes. This will automatically delete envelopes after a certain time, when they reached a final state (expired, finished, canceled). Please note that templates are not affected by the retention period.
- [Backup](#)
  - Download all finished envelopes. A backup-process will be started and you will be informed if the backup is ready for download.
- Due its complexity of the configuration, we highly recommend you to [contact us](#) about the SAML configuration.
  - Add provider for the SAML signer authentication
  - Examples of Use Cases
    - ADFS integration for eSAW backend users
    - Signer authentication with external SAML service

## v3.2

- SAML Settings for User Authentication
  - Add provider for the SAML user authentication
- Recipient Settings
  - Set the recipient settings of your organization
- Default Signature Settings
  - Default signature method (preselected)
  - Imprint settings, such as font-type, font-size, date-format
  - Biometric signature batch configuration (allow usage of biometric signature over different physical documents). Check with your legal consultant about its usage (default is disabled)
  - Settings for draw to sign signatures
- Envelope Defaults
  - default organization settings about reminders for signers
- Audit Log Settings
  - Settings of the audit log (audit trail). It is not recommended to disable the audit-log, because it is an important evidence (see [signature guide](#)).
  - Settings for separate logs per document
- Email Settings
- User Logout Redirect Url
- Envelope Details Page
- Signature PAdES (PDF Advanced Electronic Signature) Configuration

Note that the following configuration items have been moved to other pages inside the Settings, and therefore are no longer part of the Organization Settings:

- The OAuth authentication provider configuration and the SAML authentication configuration
- The Organization API Tokens have been moved to Api Token and Apps (since eSAW 20.42)

## Organization Details

In the Organization Details section, basic configuration of the Organization is made:

- Set your company logo
- Organization Name
- CustomizationID (display-only; might be required for integrations with SSP API)
- Contact URL (can be inserted into notification templates - for more information please see [Notification Template Settings](#))
- Support URL (can be inserted into notification templates - for more information please see [Notification Template Settings](#))

**ORGANIZATION**

**Organization Details**

Logo

Organization Name

Customization Id

Contact URL

Support URL

**Default callback URLs**

Callback for completed envelope

Callback for envelope status change

**Design of the document viewer for recipients**

Default redirect URL for finished documents

Viewer Design

**Automatic Remote Signature Profiles**

TestAutomatic

**Recipient Settings**

☒ Default for: Send finished document(s) to all recipients

☒ Allow to set envelope meta data

☒ Default for: Allow recipient to access envelope again after it has been completed and closed

☒ Show warning dialog, if there are fewer signature fields than signers

**Delegation**

☐ Delegation disabled

☒ Delegation enabled - Do not use by default

☐ Delegation enabled - Do use by default

**Authentication methods**

☒ Allow Pin Authentication

☐ Allow SMS Authentication

☒ Allow WindowsLive Authentication

**Authentication Parameters**

Currently considered for OAuth authentication only. Configure value 0 to allow infinite attempts.

Maximum Login Attempts

0

**Force sender to define Authentication**

(none)

☐ Force input of phone number when using SMS code authentication

☐ Allow skipping forced authentication upon using Biometric Signatures

Overview of the organization settings

## Default Callback URL

In section "Default Callback URLs" you can define which URLs should be invoked as callback for envelopes sent via WebUI. When sending envelopes via API, the callback URL can be specified on envelope level via API.

Following callback URLs can be defined for envelopes sent via WebUI:

Callback type	Status Change
Callback for completed envelope	Gets fired whenever an envelope gets finished (completed or rejected)
Callback for envelope status change	Gets fired whenever an envelope's status value changes (workstepFinished, workstepRejected, workstepDelegated, workstepOpened, sendSignNotification, envelopeExpired, workstepDelegatedSenderActionRequired)

In both URLs, you can use following placeholders:

Placeholder	Value
<b>##Envelopeld##</b>	the envelope id; typically in GUID format
<b>##Action##</b>	the action which triggered the callback; usually one of workstepFinished, workstepRejected, workstepDelegated, workstepOpened, sendSignNotification, envelopeExpired, workstepDelegatedSenderActionRequired. But consider in a callback handler implementation, that future versions may fire additional callbacks.

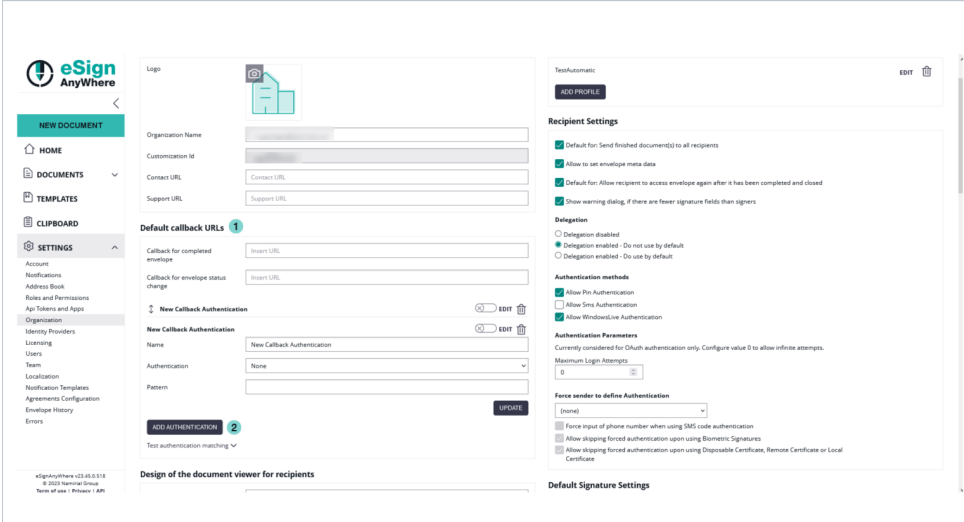
For envelopes sent via WebUI, it is currently not supported to specify a workstep event callback handler URL.

Read the Integration Guide, section [Api Reference - Introduction REST#CallbackTypes](#), for further information about integrating with callback handlers.

You can define an authentication for the callback.

v3.6

The next screenshot shows an overview where you can find the settings:

Figure	Description
	<ol style="list-style-type: none"> <li>1. Default callback URLs settings</li> <li>2. Add authentication</li> </ol>

If you click on the button “add authentication” the following window appears:

Figure	Description
--------	-------------

NEW DOCUMENT

HOME

DOCUMENTS

TEMPLATES

CLIPBOARD

SETTINGS

Account

Notifications

Address Book

Roles and Permissions

Api Tokens and Apps

Organization

Identity Providers

Licensing

Users

Team

Localization

Notification Templates

Agreements Configuration

Envelope History

Errors

Organization

Identity Providers

Licensing

Users

Team

Localization

Notification Templates

Agreements Configuration

Envelope History

Errors

algosign/where v2.0.0.0.0.0.0

© 2023 Terminal Group

Terms of use / Privacy / API

Logo

Organization Name

Customization Id

Contact URL

Support URL

Default callback URLs

Callback for completed envelope

Callback for envelope status change

New Callback Authentication

New Callback Authentication

Authentication

Pattern

ADD AUTHENTICATION

Test authentication matching

Design of the document viewer for recipients

TestAutomatic

ADD PROFILE

Recipient Settings

Default for: Send finished document(s) to all recipients

Allow to set envelope meta data

Default for: Allow recipient to access envelope again after it has been completed and closed

Show warning dialog, if there are fewer signature fields than signers

Delegation

Delegation disabled

Delegation enabled - Do not use by default

Delegation enabled - Do use by default

Authentication methods

Allow Pin Authentication

Allow SMS Authentication

Allow Windows/Live Authentication

Authentication Parameters

Currently considered for OAuth authentication only. Configure value 0 to allow infinite attempts.

Maximum Login Attempts

Force sender to define Authentication

Force input of phone number when using SMS code authentication

Allow skipping forced authentication upon using Biometric Signatures

Allow skipping forced authentication upon using Disposable Certificate, Remote Certificate or Local Certificate

Default Signature Settings

Default for Default Signature Method

General signature settings

## 1. New callback authentication

In this section you can define:

- The name of the callback (default value: "New Callback Authentication")
- The authentication (None or basic, default: none)
- The pattern (the URL should contain the given pattern)
  - The pattern "\*" matches anything

If you choose "basic" as authentication the following window appears:

Figure	Description
	<ol style="list-style-type: none"> <li>Select basic authentication</li> <li>Basic authentication settings</li> </ol>

Within this section you can define:

- The domain
- The username
- The password

After filling in the dates for the authentication you can test if the URL matches any pattern of the authentications. If no pattern matches you get an information. The following screenshots show you a warning and a successful matching of the patterns.

Warning	Matching pattern
---------	------------------

The left screenshot shows the 'Default callback URLs' section with fields for 'Callback for completed envelope' and 'Callback for envelope status change'. Below this is the 'New Callback Authentication' section with fields for 'Name', 'Authentication', 'Pattern', 'Domain', 'Username', and 'Password'. There is an 'UPDATE' button. The 'Authentication methods' section has checkboxes for 'Allow Pin Authentication', 'Allow SMS Authentication', and 'Allow Windows/Live Authentication'. The 'Authentication Parameters' section has a 'Maximum Login Attempts' field. The 'Force sender to define Authentication' section has a dropdown menu. The 'Default Signature Settings' section has a 'Default for Default Signature Method' dropdown, a 'Font Family' dropdown, a 'Font Size' dropdown, and a 'Date time format' dropdown. The 'Test authentication matching' section has a 'URL' field and a 'TEST' button.

The right screenshot shows the 'Test authentication matching' section with a 'URL' field and a 'TEST' button. Below this is the 'Design of the document viewer for recipients' section.

If you have more than one authentication and you check the URL for the pattern and more than one authentication matches, always the first one of the list will be highlighted green.

After those settings you can send an envelope as usual. If you have authentication activated but the given dates are wrong you get an information.

In the next Screenshot you can see both scenarios (with a valid authentication and with a invalid authentication). If you click on the exclamation mark following text appears: "Response status code does not indicate success:401 (unauthorized)".

The screenshot shows the '34 DOCUMENTS' page with a table of documents. The table has three columns: 'Envelope', 'Status', and 'Actions'. The 'Envelope' column contains document details like 'To: Jane Doe'. The 'Status' column shows the document status, with a warning icon indicating a failed notification delivery. The 'Actions' column contains links for document actions. The table is filtered by 'Recent Activity' and has a 'SELECT ALL' button. The page also includes a 'NEW DOCUMENT' button and a 'BULK SIGNING ASSISTANT' button.



Using the following two websites by your own risk. These two websites are not part of Namirial!

If you want to try the callback URL without authentication you can try it with: <https://webhook.site>

If you want to try the callback URL with authentication you can try it with: postman echo

## Design of the document viewer for recipients

In this section you can define the redirect URL for finished documents. Moreover you can upload the current design, reset the design to default, download the current design and download the design template. For more information about designing the viewer please also have a look at the [Viewer Guide](#).

## Disposable Certificate



The Disposable Certificate section is visible only when all of the following preconditions are fulfilled:

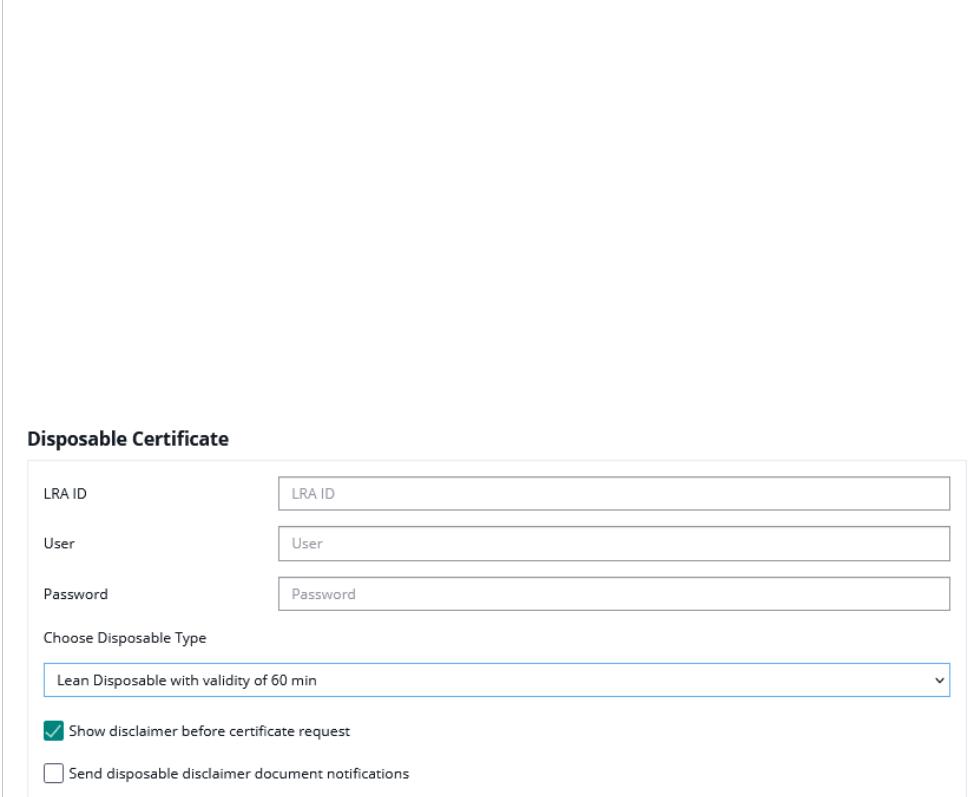
- Connection to the Trust Service Provider (Namirial TSP) is configured properly on the SIGNificant Server Platform configuration (WSC\_global.xml)
- The feature flag "Disposable Certificate" is enabled for the organization
- The feature flag "UseCustomizationId" is enabled for the organization (and CustomizationService is running properly)

In addition, the Client Authentication TLS certificates need to be installed properly, and the service user must have permission to use their private key, to use Disposable Certificates and other trust services.

In this section of your organization you can define a disposable certificate. For this setting you need following dates:

- LRA ID
- User
- Password
- Choose a disposable type
  - Regular disposable
  - Lean disposable with validity of 60 min (**choose this type unless instructed different or stated different in contracts for the service**)
  - Lean disposable with validity of 30 days

Moreover, you can decide if you want to get a disclaimer before certificate request and if you want to send disposable disclaimer document emails. The following screenshot shows you where to find those settings.

Figure	Description
	1. Disposable certificate settings

For more details and information of how to use the disposable certificate please also see the [Envelope Structure](#).

BankId Authentication

v3.4



This feature is not available with basic subscription, so please [contact](#) your Namirial sales.

It is possible to set an AuthenticationCertificateThumbprint in the organization settings:

## Swedish BankId

Authentication Certificate

Authentication Certificate

You can use different bankId AuthenticationCertificateThumbprints in different organizations.

You can find a sample configuration (REST and SOAP) on the following page: [Envelope Structure](#)

## Generic Signing Plugin

v 20.42



This feature is not available with basic subscription, so please [contact](#) your Namirial sales.

In your organization settings you can find the configuration for the generic signing plugin. Configure the plugin in this settings to use the signature in creating an envelope. Please see the next figure (sample of a plugin).

The screenshot displays the eSign AnyWhere settings interface. On the left is a sidebar with navigation options: HOME, DOCUMENTS, TEMPLATES, CLIPBOARD, and SETTINGS (highlighted). Under SETTINGS, there are links for Account, Notifications, Address Book, Roles and Permissions, Api Tokens and Apps, Organization (selected), Identity Providers, Licensing, Users, Team, Localization, Notification Templates, Agreements Configuration, Envelope History, and Errors. The main content area is titled 'Swedish BankId' and contains an 'Authentication Certificate' field. Below this is the 'Generic Signing Plugins' section, which includes a 'Test Plugin' dropdown set to 'Authentication Certificate'. Below the dropdown are input fields for User Id, Email address, Password, Number, and Phone number, followed by an 'OTP Type' dropdown set to 'SMS'. There is an 'UPDATE' button. Below the 'Test Plugin' section is the 'Automatic Profiles' section with a 'Profile' dropdown and an 'ADD PROFILE' button. At the bottom left of the main area is the 'Notification Plugins' section, showing 'MailjetPlugin (Default)'. On the right side of the interface, there are several configuration sections: 'Default sealing certificate' (Active), 'Add certificate' button, 'Envelope Defaults' (with checkboxes for preventing editing and sending reminders, and input fields for reminder timing), 'Audit Trail Settings' (with checkboxes for enabling audit trail and generating separate audit trail), 'Signature PAdES Configuration' (with dropdowns for HTML5, Biometric, and Digital Remote signatures, and checkboxes for Audit Trail), and 'Timestamp Configuration' (with a 'Server URL' input field).

For more information about how to create an envelope with a generic signing plugin in the UI please also have a look at the [Envelope Structure](#).

For information about how to send an envelope with a generic signing plugin in REST please see a sample configuration at the [Envelope Structure](#).

## Notification Plugin

## Notification Plugins

### Email Plugins

MailjetPlugin ⓘ



## Define notification plugin usage

Assign notification plugin to notification message

**Email** SMS

All notification messages Use default plugin (MailjetPlugin) ▼

**Add notification message**

Selection of the notification type per organization:

- default notification type is always available
- enabled plugins (with a valid configuration) are shown

It is possible to assign plugins to notification messages individually by adding a notification message type. Please note that it is possible to switch between email and SMS notification plugin usage.

## Define notification plugin usage

Assign notification plugin to notification message

**Email** SMS

All notification messages Use default plugin (MailjetPlugin) ▼

**Add notification message**

Automated delegation info

Backup notification

Confirm delegation

Delegation info

Deleted Recipient

Delivery failure of envelope to CC recipient

Disclaimer

Disclaimer (Download Link)

Envelope cancelled

Envelope completed

Envelope deleted

Policy for recipients

LOAD POLICY RESET TO DEFAULT

DOWNLOAD CURRENT POLICY

DOWNLOAD POLICY TEMPLATE

Configuration for recipients

LOAD CONFIGURATION RESET TO DEFAULT

DOWNLOAD CURRENT CONFIGURATION

DOWNLOAD DEFAULT TEMPLATE

ons

## Policy for the document viewer for recipients

In this section you can:

- upload a policy
- reset the policies to default
- download the current policy
- and download the policy template

Please see the following sample of the policy template.



## Policy Template

```
<GeneralPolicies>
  <AllowSaveDocument>1</AllowSaveDocument>
  <AllowSaveAuditTrail>1</AllowSaveAuditTrail>
  <AllowUndoLastAction>1</AllowUndoLastAction>
  <AllowAdhocPdfAttachments>0</AllowAdhocPdfAttachments>
</GeneralPolicies>
```

You can find an overview of all policies on this page: [Document-Policy](#)

## Signature Appearance v 21.16

The signature appearance section allows to configure the representation of the signature (or seal) on the PDF document. With custom signature rendering layout configuration ("stamp imprint configuration"), an organization administrator can define how the stamp imprint on the signature image looks like (e.g. fonts, elements, layout etc). It can be used e.g. to set organization wide background images (e.g. company logos) or define specific fonts for text added to the stamp imprint. While it has no impact on the legal levels of signatures (in EU, defined by eIDAS), a customer specific stamp imprint representation can create higher subjective trust and contract awareness of your customers.

A detailed guide about changing the Signature Rendering Configuration is available in chapter "[Stamp Imprint Configuration](#)".

### Signature Appearance

Custom Signature Rendering Configuration

UPLOAD CONFIGURATION RESET TO DEFAULT

↓ DOWNLOAD CURRENT CONFIGURATION

↓ DOWNLOAD DEFAULT TEMPLATE



The Signature Appearance section is visible only when all of the following preconditions are fulfilled:

- The feature flag "UseCustomStampImprintConfiguration" is enabled for the organization

## Activity-Engine Custom Localizations

This setting allows you to override localizations, enabling customization for various elements such as signature image rendering labels and text for transaction code configuration (e.g. SMS text). In this section you can

- upload a translation bundle,
- reset to default settings,
- download the current translation bundle,
- and also access the default template for localizations.

Use the template to customize any supported localizations of the SIGNificant Wokrstep Controller. Note the following procedure:

- Make a copy of the file
- Rename it to include the language code of the target language (e.g. Localizations.de.custom.json)
- Open the copied file
- Find the items that needs to be changed and adapt the values accordingly
- Remove all other items (which still have the default value) to receive updates automatically after a software update

Please see also [Language Support](#) for the available languages.

## Retention Period



Please note the following: The process starts with the next interval (interval time can be configured in the \_global.xml). Depending on the configured interval it could take some time until the process starts. After the interval was reached the senders get a notification that the envelopes will be deleted soon. Immediately afterwards the envelopes will be deleted.

Please also note that there is no limit (maximum number) for envelopes that will be deleted.

In this section you can define a retention period for the organization drafts and envelopes. Please note the following rules for the different types of documents (add the days you selected in this section to the following rules:

- Drafts will be removed X days after creation date
- completed/rejected and canceled envelopes will be removed X days after completed/rejected/canceled date
- expired envelopes will be removed X days after expiration date
- templates are not removed

Please also see the next figure:

## Retention Period



Enable Retention Period of Organization Drafts and Envelopes

Number of days to keep the documents :

12

Clipboard files will be removed after 24h.

When enabling retention period, please ensure to set up an appropriate process to keep copies of signed documents, audit trail evidence and other legally binding documents related to the envelope elsewhere. Data retention configuration will permanently delete the envelopes, including signed envelopes, from the eSignAnyWhere Platform according to the rules described above. We recommend to store the documents and related evidence in a DMS. When API access is granted for your account, you can implement automatic storage in a DMS after an envelope was completed. Alternatively you could e.g. keep copies in any other storage or probably keep a copy in your mail inbox.

## Backup

In this section you can download all finished envelopes you have signed or sent.

### Backup

Download all finished envelope files you have sent and signed.

FINISHED ENVELOPES

If you click on the "Finished Envelopes" button you can see that the backup is prepared.

While collecting all envelopes on the server for the backup (which may take up to several hours), following Text will be displayed:

*Your backup is queued and will be started soon. You will receive an email once your backup is ready for download.*

### Backup



Your backup is queued and will be started soon. You will receive a notification once your backup is ready for download.

If you e.g. have been logged in in several browsers while requesting the backup, or request the backup at the same time as another user does, the text might not yet be visible while the backup process is already in progress. If you press the button to start a backup process, an error message informing that you "tried to schedule a backup operation while another one is already in progress" will be shown.

Once the backup was completed, you will receive an email to download the backup:

### Backup is ready for download

Please visit your organization settings to download your backup. The download option will be available for the next 48 hours.

[ORGANIZATION SETTINGS](#)



Do not share or forward this Email. Please have a look at the [Signer Guide](#) if you need help signing the document.  
Powered by [Namirial eSignAnyWhere](#).



The backup will then be available for 48 hours to be downloaded. The download option is presented only in the organization settings, which require user login of a user with some permissions to access the organization settings, to avoid unauthorized access to the backup.

## Backup

[DOWNLOAD](#)

AVAILABLE FOR THE NEXT 47H AND 59MIN

## Timestamp Configuration

The timestamp configuration allows to set timestamp service on a per-organization basis.

Following configurations are available:

- Server URL
- User credentials
  - User
  - Password
- Hash Algorithm
  - Sha1, Sha256, Sha512

## Timestamp Configuration ⓘ







Server URL	<input type="text" value="Server URL"/>
User	<input type="text" value="User"/>
Password	<input type="text" value="Password"/>
Hash Algorithm	<input type="text" value="SHA-256"/>


## Automatic Remote Signature Profiles

v 3.2

In this section the user manager of an organization can add automatic remote signature profiles, which can be used for any workflow as a recipient (recipient type "Automatic"). This recipient signs automatically the signatures and the workflow continues automatically. For more information please also have a look at the [electronic signature guide](#).

## Automatic Remote Signature Profiles

automatic	EDIT	
Profile	EDIT	
TEST2	EDIT	
Gierlinger	EDIT	
TEST	EDIT	
demo	EDIT	
<div>ADD PROFILE</div>		

 The Automatic Remote Signature Profiles section is visible only when all of the following preconditions are fulfilled:

- The remote signature endpoints are configured in the SSP configuration (SaaS: request the change at Namirial; On-Premise: see [Namirial RemoteSignaturePlugin](#) documentation; documentation accessible after login only)
- The feature flag "AutomaticRemoteSignature" is enabled for the organization

### Default Signature Settings

In this section you can set the default signature type for the envelopes. After you have set the configuration in this section the defined signature type will be preselected if you create a new envelope.

## Default Signature Settings

Default for: Default Signature Method	Click2Sign ▼	
<b>General signature settings</b>		
Font Family	Times New Roman ▼	
Font Size	11 ▼	
Date time format	dd-MM-yyyy HH:mm:ss	<input type="checkbox"/> Use local timezone
	🔄 17-11-2023 08:53:35	
	<b>Examples:</b>	
	dd-MM-yyyy HH:mm:ss zzz	19-03-2018 17:07:47 +01:00/UTC
	dd-MM-yyyy HH:mm:ss ('GMT'z)	19-03-2018 17:07:47 (GMT+1/UTC)
	MM/dd/yyyy hh:mm:ss tt (zzz)	03/19/2018 05:07:47 PM (+01:00/UTC)
<input type="checkbox"/> Allow Biometric Signature batches over multiple documents		
<b>Extended settings for 'Draw to sign'</b>		
<input checked="" type="checkbox"/> Extra Information DrawToSign		
<input checked="" type="checkbox"/> Display Email Address		
<input checked="" type="checkbox"/> Display Ip Address		
<input checked="" type="checkbox"/> Display Name		
<input checked="" type="checkbox"/> Display Signed on Date		
<b>Local Certificate Settings</b>		
<input type="checkbox"/> Validate recipient and certificate holder name		
<LastName> <FirstName> ▼		
<input type="checkbox"/> Signing Certificate Filter on Intended Use		
nothing selected ▼		
<input type="checkbox"/> Certificate root CA verification with EUTL		



Note that settings which we name "default" or "default for ...", or combine in a grouping element with one of this terms, just define the "defaults" (i.e. the preselected configuration value) for drafts and envelopes. A user may change the value on a per-envelope level. Just in some cases, permission objects may disallow changing some values on a per-envelope level.

## Envelope Defaults

The envelope defaults section allows to set "default" parameters for drafts and envelopes which are created. Settings take immediately effect for all drafts or envelopes created after changing the value. Already created drafts, envelopes or templates will not be updated.

### Envelope Defaults

<input type="checkbox"/> Default for: Prevent editing of form fields after envelope is finished	
<b>Notification Settings</b>	
<input checked="" type="checkbox"/> Default send automatic reminders	
Send a reminder to signers after receipt (in days)	5 ▼
Continue to send reminders every day(s)	3 ▼
Warn signers before request expires (in days)	3 ▼



Note that settings which we name "default" or "default for ...", or combine in a grouping element with one of this terms, just define the "defaults" (i.e. the preselected configuration value) for drafts and envelopes. A user may change the value on a per-envelope level. Just in some cases, permission objects may disallow changing some values on a per-envelope level.

The section allows defining the following default values:

- Default value for preventing editing of form fields after envelope is finished
- Default values for the automatic reminders sent to a signer for an envelope until it is getting signed
  - Should reminders be set, in general?
  - In which interval should reminders be set? (See [User Guide](#) for more details about reminders)

If you prevent editing form fields after the envelope is finished the form fields in the PDF are all read only.

v 20.28

Therefore, after locking the form fields (after the final workstep), the form fields are not editable any more with other PDF tools.


Please also see the next figures:

Standard (Not Locked)	Locked Form Field
<div>This is an unlocked field due to the organization settings</div> <p>The form field value remains editable in the PDF file even after completing the envelope processing, according to allowed modifications as of PAdES standard. The form field content contained at signing time or at envelope completion can be checked in the stored versions which are included in the PDF file.</p>	<div>This is a locked field due to the organization setting</div> <p>The form field's final value at the end of envelope the PDF in a non-editable format. This prevents, t might try to argue with changes he did in his local</p>

Information on whether the form fields are locked or not can also be found in the audit trail. Please see the next figure:

## Sent Notifications

Name	Action	Date
	Request signing	2020-06-22   09:44:59
	All form fields have been locked	2020-06-22   09:45:08
	Envelope has been finished	2020-06-22   09:45:08
	Copy of finished document sent	2020-06-22   09:45:08

 Note: It is not recommended to disable the audit-log, because it is an important evidence (see [signature guide](#)).

In this section you can define the following settings:

- Settings of the audit log (audit trail).
- Settings for separate logs per document

## Signature PAdES Configuration

v 3.7

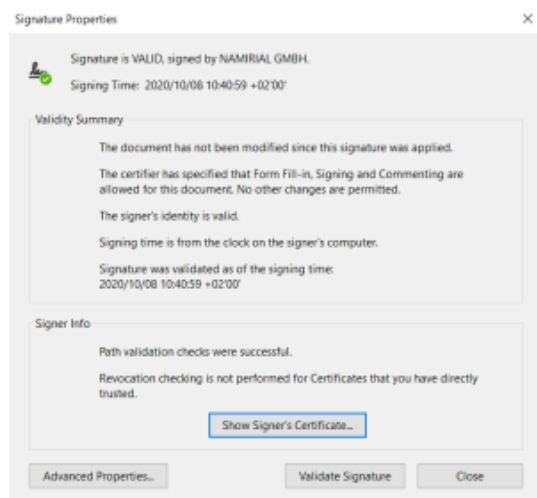
Allows to set the signature configuration based on the different PAdES levels, for following types of signatures.

- HTML5 Signatures (Click2Sign, Type2Sign, Draw2Sign)
- Biometric Signatures, SMS-OTP Signatures
- Digital Remote Signatures, Disposable Certificate, Automatic Remote Signatures, P7M-Signature, SwissCom, A-Trust, LongLiveDisposable, PushTan, LocalCertificate
- Timestamps in case they are independently added and not part of a signature

In case of having one signature field with multiple signature types allowed, the signature type is selected per signature field and not per signature method. Therefore, as soon as a signature field contains one of the signature methods listed above, its PAdES configuration is considered for all signature types. If different PAdES configurations would match, then the "highest value" PAdES configuration is considered, while the sort order from lowest to highest value is "HTML5 Signatures", "Biometric Signatures, SMS-OTP Signatures", "Digital Remote Signatures, Disposable Certificate, Automatic Remote Signatures, P7M-Signature, SwissCom, A-Trust, LongLiveDisposable, PushTan, LocalCertificate, GenericSigningPlugin"

Description of the different PAdES baseline levels supported by eSignAnyWhere:

- PAdES level BASELINE-B without using an external timestamp server
  - B-Level: Short-term electronic signature with signing certificate
    - contains just the time information from local machine; without an external server time stamp



- PAdES level which require using an external timestamp server: BASELINE-T, BASELINE-LT and BASELINE-LTA
  - T-Level: Includes B-Level and a time stamp
    - Use the configured time stamp server on the signature itself
    - Ensures that the document existed at a specific date and time, where time is granted by the external timestamp server
  - LT-Level: Includes T-Level and a full set of certification and full set of revocation data
    - Use the configured time stamp server on the signature itself
    - Allows validation of the signature without access to the signing environment.
  - LTA-Level: Includes LT-Level and a timestamp of a TSA (Time Stamping Authority)
    - produces in addition to the signature field defined a time stamp signature on the document

Figure

Description

### Signature PAdES Configuration

HTML5 Signatures

LTA

Biometric Signatures, SMS-OTP Signatures

LTA

Digital Remote Signatures, Disposable Certificate, Automatic Remote Signatures, LocalCertificate

LT

Audit Trail

LTA

HIDE INFO

**PAdES Baseline Profile Specification:**

**B-Level:** Short-term electronic signatures with signing certificate

**T-Level:** B-Level + timestamp of a TSA (Time Stamping Authority) to prove that the document existed at specific date and time

**LT-Level:** T-Level + full set of certificates and revocation data to allow validation of the document without the signing environment

**LTA-Level:** LT-Level + document timestamp of a TSA (Time Stamping Authority)

**Notes:**

- The higher the level, the better the documents validation capabilities, but the larger the file size. Please see our [Electronic Signature Guide](#)
- B/T/LT/LTA Levels are related to ETSI TS 103 172 PAdES Baseline Profile Specification
- Timestamping may cause additional costs

1. PAdES settings

## Email Settings

- Set the email sender appearance configuration

## Notification Settings

Sender appearance

Manuel Gierlinger via .com

The dropdown list allows to select one of the 3 different appearances:

- Sender's "<given-name> <surname> via <product-name>"
- <organization name> via <product-name>
- <product-name>

The product-name is an instance wide configuration (Further reading in case authorized: [GlobalXML#E-Mailconfiguration](#); value "emailSenderProductName")

If an e-mail is sent in a context that does not match the configured value (e.g. an org-specific reminder about license, but sender name is configured), those mails are automatically sent using the "next matching entry" from the list (in the example, it would use the organization-name configuration).

## User Logout Redirect Url

- Set a redirect Url for eSignAnyWhere users, when they logout (e.g. to an intranet page)

## Default redirect url before sending a draft

**Feature Flag**

This setting is available only when the feature flag "BeforeDraftSendRedirect" was granted to the organization.

Configures a Redirect URL to which the envelope creator is redirecting instead of sending an envelope. Following placeholders are available:

- ##EnvelopeId##
- ##SenderId##



- ##OrganizationId##

Instead of the page sequence

"Recipients Page" - "Designer Page" - "Summary Page"

, with a configured redirect url before sending, the sequence is following:

"Recipients Page" - "Designer Page" - "Summary Page" - (custom redirect page)

In this scenario, the custom redirect page may adopt the draft with the draft update API methods, and has to send the draft via API methods. See [Document Tagging Scenario - Example showing how to collect metadata for DMS archiving](#) for an example on how to integrate a DMS tagging using that functionality.

## Envelope Details Page

---

- Allows the sender to copy the viewer link from the envelope details page (if sender role grants required envelope permission)
- For more information please also see [this page](#)

## Extended Signing Options

---

Since version 23.52



Be careful when changing these settings, as they might have unwanted side effects. If "Allow signing of locked documents" is disabled, the user  
Per default, locked PDFs can not be signed!

- Allow signing of locked documents

## Recipient settings

---

You can set the following settings for the recipient:

- default CC for all signers
- usage of envelope metadata
- allow recipients to access envelope again after it has been completed and closed
- Show warning dialog, if there are fewer signature fields than signers
  - warning will be shown if:
    - only some of the signers have no signature field
    - when all of the signers have no signature field
- delegation settings
- allowed authentication methods for signers
- force authentication

v 20.28

If you force an authentication and the user does not select any or a specific authentication method then the user will get the following notification:



Your organization does not allow you to continue without the necessary authentication settings. Please change your envelope according to the (non-changeable) configurations listed below.

If necessary, you can go directly to the organization settings and make changes.

Mode:

(any) 

- Force input of phone number when using SMS code authentication
- Allow skipping forced authentication upon using Biometric Signatures
- Allow skipping forced authentication upon using Disposable Certificate, Remote Certificate or Local Certificate

CLOSE

[GO TO ORGANIZATION SETTINGS](#)

GO TO CREATE ENVELOPE

[← BACK](#)
[DELETE](#)
[SAVE AS ^](#)
[SIGN](#)
[NEXT](#)