SigningHub Upgrade Guide 7.7.x to 8.x.x

SigningHub

ASCERTIA LTD

FEBRUARY 2022

DOCUMENT VERSION- 1.0.0.0

CONTENTS

1 Audience

This guide assists the following users in upgrading SigningHub from version 7.7.x to version 8.x.x.

- System Administrators
- Enterprise Admins (who has the intended access rights)

2 Introduction

As a successor to SigningHub 7.7.x, version 8.x.x marks a major update to the core areas of SigningHub for implementing advanced signing protocols, improving user experience, and providing more administrative control. The upgrade process is a combination of automatic and manual steps for which SigningHub provides the required tools and technology to automate much of the upgrade process.

This upgrade documentation provides detailed upgrade instructions and completes in the following parts.

Below is a list of notable and deprecated features that will be introduced in SigningHub 8.x.x.

New feature roll-outs and enhancements:

- Cloud Signature Consortium (CSC) v1.0.4.0 protocol implementation.
- Introduction of Level of Assurance (LoA) for signature fields.
- Enabling multiple signing servers to be configured and which can be selected while signing a document.
- A new screen that allows the selection of “Signing Service Providers” at the point of signing.
- The ability to set a custom name for the “Levels of Assurance”.
- “Levels of Assurance” is now controllable through the Service Plan and Enterprise Roles.
- A new feature “Enable PDF/A Compliancy” has been added under the Service Plan to retain document compliance to PDF/A standards for PDF/A complaint documents that have been uploaded, shared or processed through SigningHub.
- “Electronic Signature” has been added as a “Level of Assurance”, for which only an OTP as an authentication permission is required at the point of signing.
- An “Electronic Signature” is produced as an annotation.
- Improvements have been made to the XML signing implementation.
- The Signing implementation has been improved to accept PKCS#1 from all RSSPs including ADSS server.
- SigningHub now produces Long Term Validation (LTV) signatures by default; this no longer requires any LTV configuration in the ADSS Server Signing Profiles.
- SigningHub Certification Profiles (for eSeals) need to have certificates configured against the defined certificate alias.
- Workflow Evidence Reports can now be digitally signed using eSeals. An eSeal signing capacity must be configured within SigningHub to sign the Workflow Evidence Report.

- Support for the Cloud Signature Consortium (CSC) API enables customers to leverage Remote Signing Service Providers (RSSP) for signing documents. SigningHub 8.x.x now enables SigningHub Mobile Web and Native apps (Android and iOS) to leverage the CSC API for document signing.
- On the document viewer, the separate signature fields of “Electronic Signature” and “Digital Signature” have been merged into a single “Signature” field. You can simply drop the “Signature” field in the document and select a Level of Assurance for it.
- The term “Witness Signing” has been updated to Electronic Seal (eSeal).
- “Hand Signature” is now replaced with “Electronic Signature”.

Discontinued/deprecated features:

- The default Service Plan that used to be assigned to an unregistered user by the application has been removed completely from Global Settings. An unregistered user will follow the document owner's Service Plan and assigned Enterprise Role (when the document owner is an individual user the service plan configurations will be used)
- The "next-signer" parameter in the GetPackages API response has been deprecated and has a static value of an empty string. In the next release, the "next-signer" parameter will no longer be available.

3 Upgrade to SigningHub 8.x.x

Before starting with the upgrade of SigningHub 7.7.x to SigningHub 8.0.0, it is crucial to take a backup of the system.

3.1 Taking a full backup of the current environment

- Before initialising the system installer to upgrade SigningHub 7.7.x, it is imperative that a full backup is created of the existing system. This includes the SigningHub **database, installation directory, document storage (if not set to ‘database’)** and the **IIS virtual directory** and note **site bindings** configurations. An administrator account is required to create a backup of the system.
- This information will be used to compare the SigningHub configurations of version 7.7.x to version 8.x.x

3.2 Upgrading to SigningHub 8.x.x

In the following steps, we will run the SigningHub 8.x.x installation wizard to begin the upgrade process and then run a database script for updating data tables.

- Run the installer and choose the option to install SigningHub 8.x.x using an existing database. Following the wizard, choose the appropriate option during installation and use the credentials from your current database to connect the system to the existing instance.

The duration of installation depends upon the size of the database.

- Run the following script for your respective database. The script will add a new “LastLoggedIn” column under the “User” table for enhanced performance and retrieving user activities faster. Ensure that a successful response is received on the script execution before moving to the next steps.

The script for the SQL database.

```
MERGE INTO [user] D
using (SELECT T.userid,
              Max(lastmodifiedon) LASTMODIFIEDON
       FROM   (SELECT U.userid,
                      Max(U.lastmodifiedon) LASTMODIFIEDON
               FROM   useractivitylog U
               GROUP  BY U.userid
               UNION ALL
               SELECT D.userid,
                      Max(D.lastmodifiedon) LASTMODIFIEDON
               FROM   documentlog D
               GROUP  BY D.userid) T
       GROUP  BY T.userid) S
ON ( D.id = s.userid )
WHEN matched THEN
UPDATE SET D.lastloggedin = S.lastmodifiedon;
```

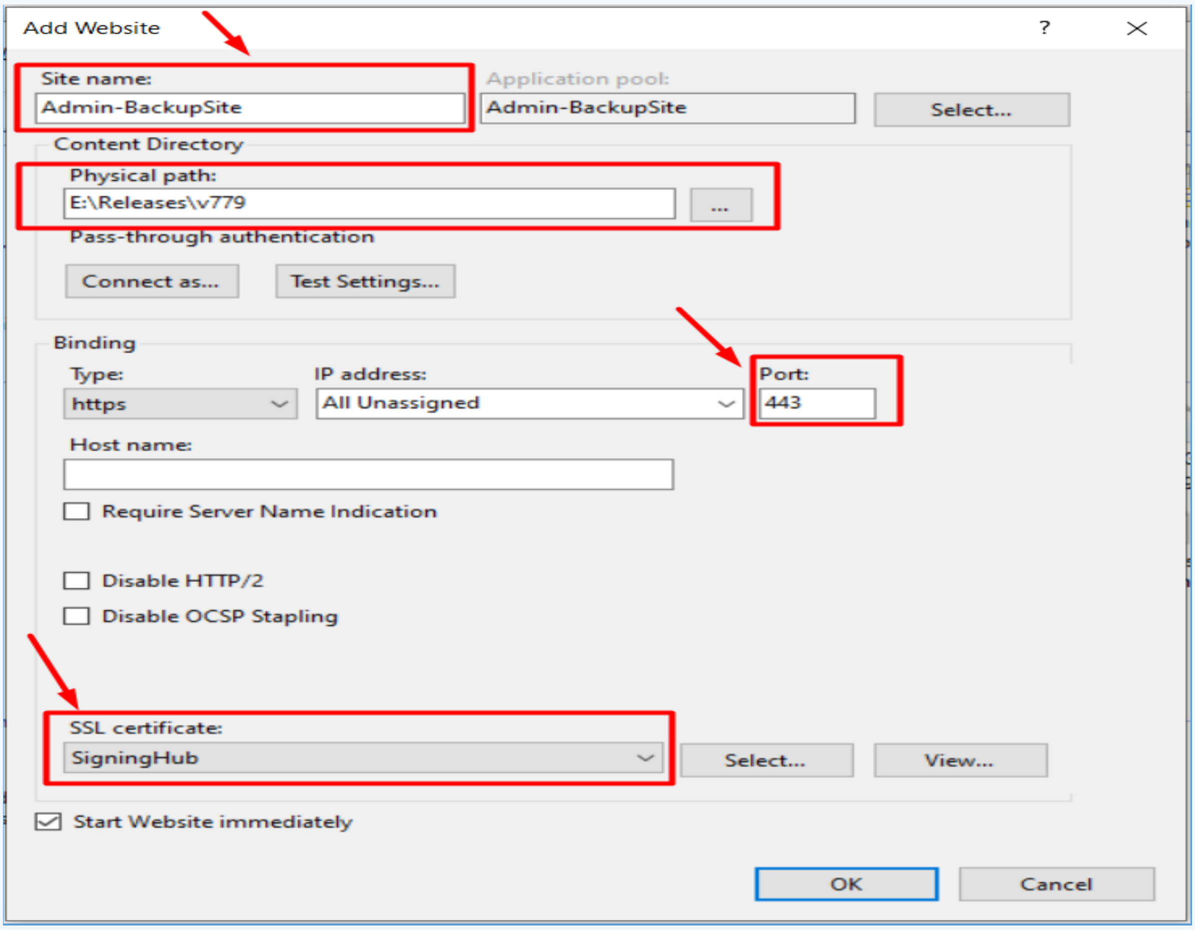
The script for the Oracle database.

```
MERGE INTO "user" D
using (SELECT T.userid,
              Max(lastmodifiedon) LASTMODIFIEDON
       FROM   (SELECT U.userid,
                      Max(U.lastmodifiedon) LASTMODIFIEDON
               FROM   useractivitylog U
               GROUP  BY U.userid
               UNION ALL
               SELECT D.userid,
                      Max(D.lastmodifiedon) LASTMODIFIEDON
               FROM   documentlog D
               GROUP  BY D.userid) T
       GROUP  BY T.userid) S
ON ( D.id = s.userid )
WHEN matched THEN
  UPDATE SET D.lastloggedin = S.lastmodifiedon;
```

3.3 Hosting the Admin Site of SigningHub 7.7.x on an appropriate localhost URL

- It is necessary to host the Admin site of SigningHub 7.7.x on an appropriate localhost URL. This step will allow the system admin to compare the profile settings between the old and the newer versions.
  - Open **Internet Information Services (IIS) Manager**. Expand Server Node and right-click on **Sites** to select the "**Add Website…**" option.
  - It will open the following dialog, to provide '**site name**" and "**Physical Path"** (pointing to SigningHub Admin backup installation directory). Change **Port** if required and select the SSL certificate.

Make sure the physical path is pointing to the old installation directory that you had selected for the backup before. This will help you to easily compare the SigningHub Admin's new configurations with the old one.


Add Website

Site name: Admin-BackupSite

Application pool: Admin-BackupSite

Content Directory

Physical path: E:\Releases\v779

Pass-through authentication

Binding

Type: https

IP address: All Unassigned

Port: 443

Host name:

□ Require Server Name Indication

□ Disable HTTP/2

□ Disable OCSP Stapling

SSL certificate: SigningHub

☑ Start Website immediately

3.4 Redis Server

- You must uninstall the old Redis server and install a new instance of the Redis Server to keep it up to date. Follow **Appendix G – Installing Redis Server** in our installation guide, which is shipped with the installer.

4 ADSS Server Configuration

4.1 Reconfigure Server Side Signing Profiles

1. Log into ADSS Server with an Administrator account, go to **Signing Service > Signing Profiles**. Open the Signing Profile to be reconfigured.

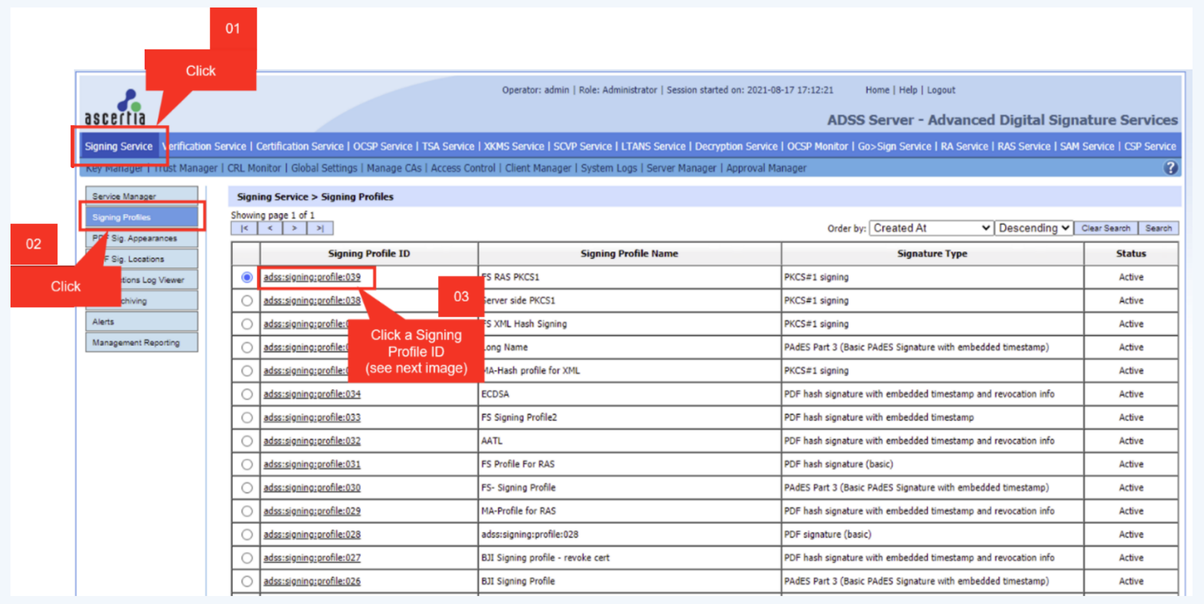
2. Change the **Signature Type** to **PKCS#1** from **PDF/PAdES Hash**, as shown in the image below.

> If you are installing a fresh instance of the SigningHub application using 'sample data", then you must need to follow the steps mentioned above to make signing work via PKCS#1.

In the following example, we will configure an existing Server Side Signing Profile in the ADSS Server based on **PDF/PAdES Hash**.

1. Go to "Signing Service > Signing Profiles".

2. Click a Signing Profile ID.


01
Click
02
Click
03
Click a Signing Profile ID (see next image)
ascertia
Operator: admin | Role: Administrator | Session started on: 2021-08-17 17:12:21
Home | Help | Logout
ADSS Server - Advanced Digital Signature Services
Signing Service | Verification Service | Certification Service | OCSP Service | TSA Service | XKMS Service | SCVP Service | LTANS Service | Decryption Service | OCSP Monitor | Go>Sign Service | RA Service | RAS Service | SAM Service | CSP Service
Key Manager | Trust Manager | CRL Monitor | Global Settings | Manage CAs | Access Control | Client Manager | System Logs | Server Manager | Approval Manager
Service Manager
Signing Profiles
PDF Sig. Appearances
PDF Sig. Locations
Transactions Log Viewer
Archiving
Alerts
Management Reporting
|< < > >|
Clear Search
Search

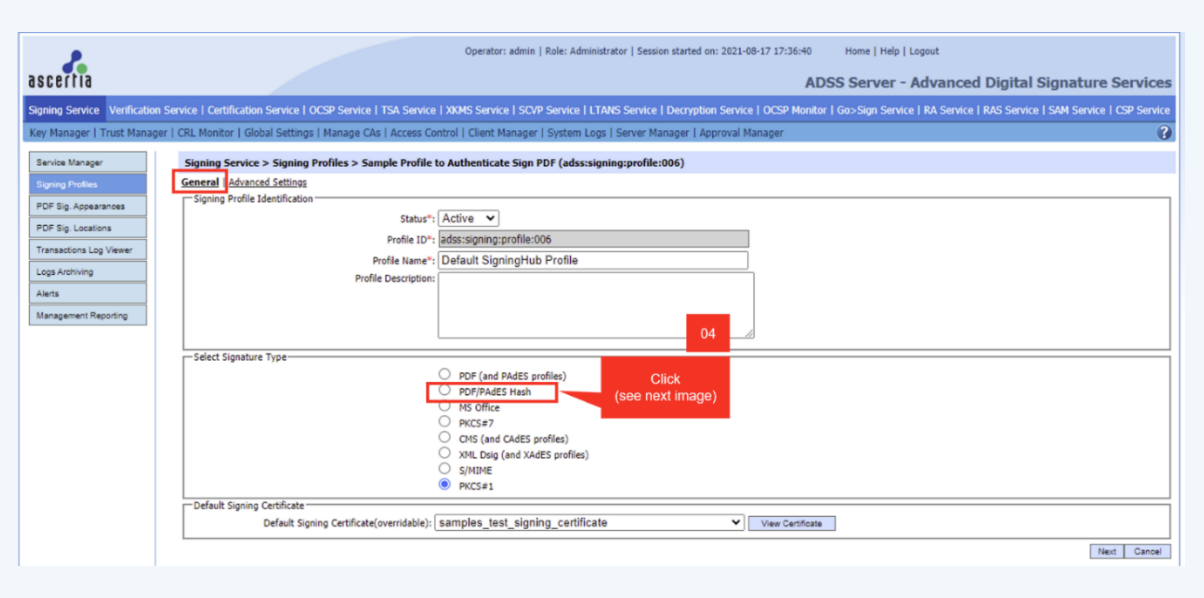
Signing Service > Signing Profiles

Showing page 1 of 1

Order by: Created At Descending

	Signing Profile ID	Signing Profile Name	Signature Type	Status
●	adss:signing:profile:039	S RAS PKCS1	PKCS#1 signing	Active
○	adss:signing:profile:038	erver side PKCS1	PKCS#1 signing	Active
○	adss:signing:profile:0	S XML Hash Signing	PKCS#1 signing	Active
○	adss:signing:profile:0	ong Name	PAdES Part 3 (Basic PAdES Signature with embedded timestamp)	Active
○	adss:signing:profile:0	A-Hash profile for XML	PKCS#1 signing	Active
○	adss:signing:profile:034	ECDSA	PDF hash signature with embedded timestamp and revocation info	Active
○	adss:signing:profile:033	FS Signing Profile2	PDF hash signature with embedded timestamp	Active
○	adss:signing:profile:032	AATL	PDF hash signature with embedded timestamp and revocation info	Active
○	adss:signing:profile:031	FS Profile For RAS	PDF hash signature (basic)	Active
○	adss:signing:profile:030	FS- Signing Profile	PAdES Part 3 (Basic PAdES Signature with embedded timestamp)	Active
○	adss:signing:profile:029	MA-Profile for RAS	PDF hash signature with embedded timestamp and revocation info	Active
○	adss:signing:profile:028	adss:signing:profile:028	PDF signature (basic)	Active
○	adss:signing:profile:027	BJI Signing profile - revoke cert	PDF hash signature with embedded timestamp and revocation info	Active
○	adss:signing:profile:026	BJI Signing Profile	PAdES Part 3 (Basic PAdES Signature with embedded timestamp)	Active

3. Under the “General” tab, click “PDF/PAdES Hash”.


Operator: admin | Role: Administrator | Session started on: 2021-08-17 17:36:40
Home | Help | Logout
ADSS Server - Advanced Digital Signature Services
Signing Service | Verification Service | Certification Service | OCSP Service | TSA Service | XKMS Service | SCVP Service | LTANS Service | Decryption Service | OCSP Monitor | Go>Sign Service | RA Service | RAS Service | SAM Service | CSP Service
Key Manager | Trust Manager | CRL Monitor | Global Settings | Manage CAs | Access Control | Client Manager | System Logs | Server Manager | Approval Manager
Service Manager
Signing Profiles
PDF Sig. Appearances
PDF Sig. Locations
Transactions Log Viewer
Logs Archiving
Alerts
Management Reporting
General | Advanced Settings
04
Click
(see next image)
View Certificate
Next
Cancel

Signing Service > Signing Profiles > Sample Profile to Authenticate Sign PDF (adss:signing:profile:006)

Signing Profile Identification

Status*: Active

Profile ID*: adss:signing:profile:006

Profile Name*: Default SigningHub Profile

Profile Description:

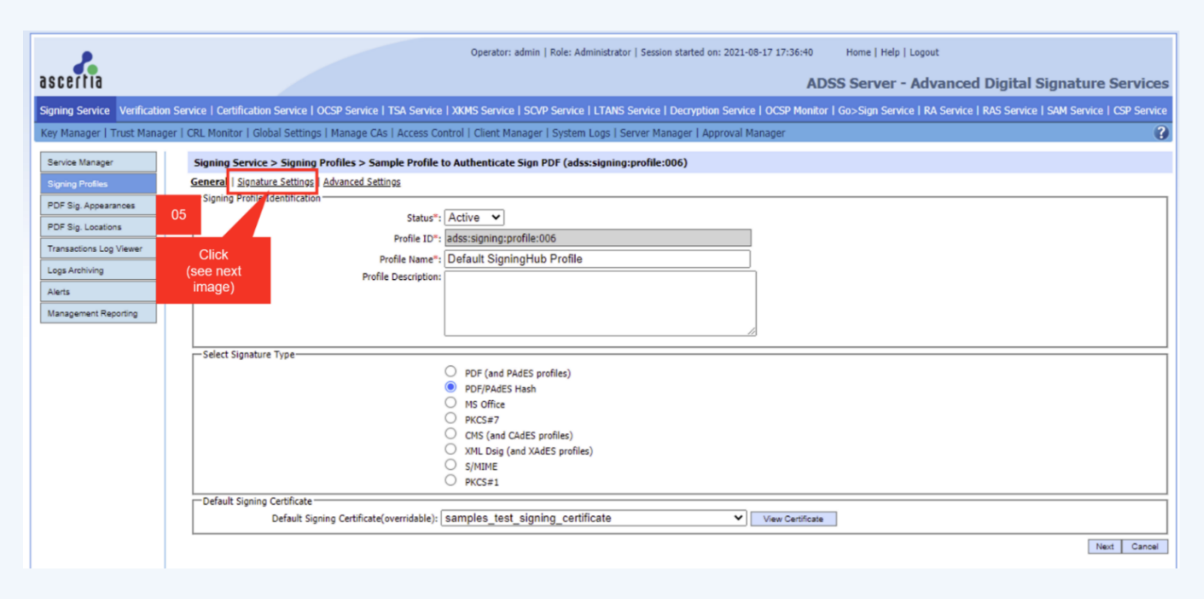
Select Signature Type

○ PDF (and PAdES profiles)
○ PDF/PAdES Hash
○ MS Office
○ PKCS#7
○ CMS (and CAdES profiles)
○ XML Dsig (and XAdES profiles)
○ S/MIME
● PKCS#1

Default Signing Certificate

Default Signing Certificate(overridable): samples_test_signing_certificate

4. Click the “Signature Settings” tab.


Operator: admin | Role: Administrator | Session started on: 2021-08-17 17:36:40
Home | Help | Logout
ADSS Server - Advanced Digital Signature Services
Signing Service | Verification Service | Certification Service | OCSP Service | TSA Service | XKMS Service | SCVP Service | LTANS Service | Decryption Service | OCSP Monitor | Go>Sign Service | RA Service | RAS Service | SAM Service | CSP Service
Key Manager | Trust Manager | CRL Monitor | Global Settings | Manage CAs | Access Control | Client Manager | System Logs | Server Manager | Approval Manager
Service Manager
Signing Profiles
PDF Sig. Appearances
PDF Sig. Locations
Transactions Log Viewer
Logs Archiving
Alerts
Management Reporting
General | Signature Settings | Advanced Settings
05
Click
(see next image)
View Certificate
Next
Cancel

Signing Service > Signing Profiles > Sample Profile to Authenticate Sign PDF (adss:signing:profile:006)

Signing Profile Identification

Status*: Active

Profile ID*: adss:signing:profile:006

Profile Name*: Default SigningHub Profile

Profile Description:

Select Signature Type

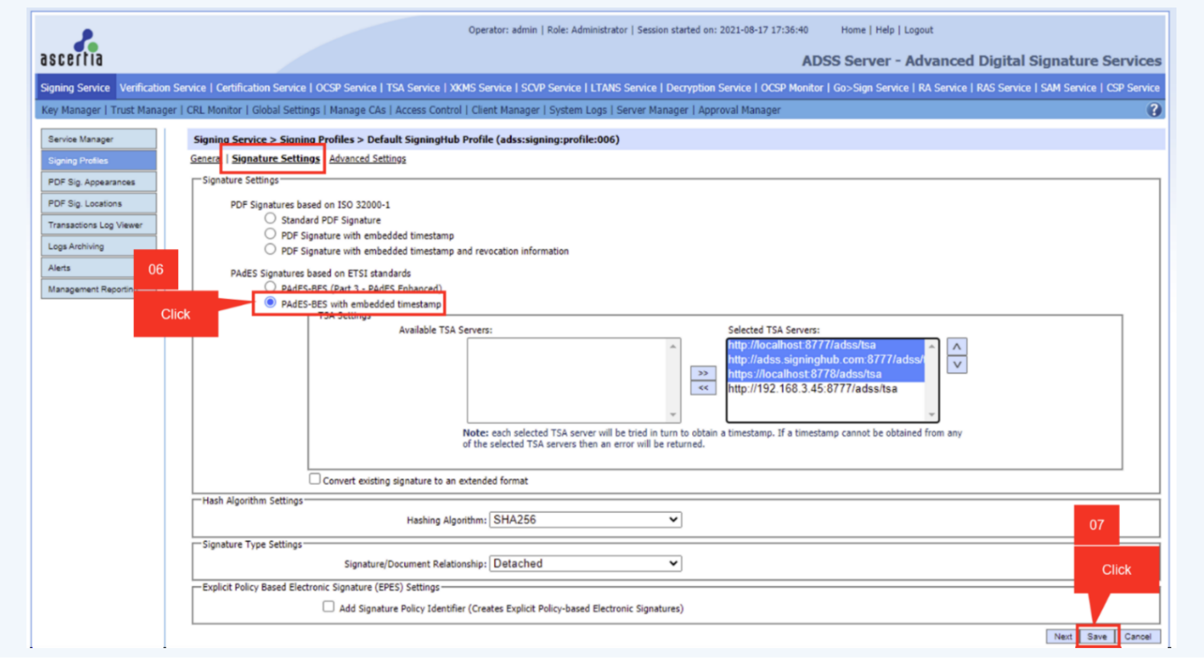
○ PDF (and PAdES profiles)
● PDF/PAdES Hash
○ MS Office
○ PKCS#7
○ CMS (and CAdES profiles)
○ XML Dsig (and XAdES profiles)
○ S/MIME
○ PKCS#1

Default Signing Certificate

Default Signing Certificate(overridable): samples_test_signing_certificate

5. Under the “PAdES Signatures based on ETSI standards” section, click “PAdES-BES with embedded timestamp”

6. Click “Save”.


ascertia
Operator: admin | Role: Administrator | Session started on: 2021-08-17 17:36:40
Home | Help | Logout
ADSS Server - Advanced Digital Signature Services
Signing Service | Verification Service | Certification Service | OCSP Service | TSA Service | XKMS Service | SCVP Service | LTANS Service | Decryption Service | OCSP Monitor | Go>Sign Service | RA Service | RAS Service | SAM Service | CSP Service
Key Manager | Trust Manager | CRL Monitor | Global Settings | Manage CAs | Access Control | Client Manager | System Logs | Server Manager | Approval Manager
Service Manager
Signing Profiles
PDF Sig. Appearances
PDF Sig. Locations
Transactions Log Viewer
Logs Archiving
Alerts
Management Reporting
06
Click
07
Click
Next
Save
Cancel

Signing Service > Signing Profiles > Default SigningHub Profile (adss:signing:profile:006)

General | Signature Settings | Advanced Settings

Signature Settings

PDF Signatures based on ISO 32000-1
○ Standard PDF Signature
○ PDF Signature with embedded timestamp
○ PDF Signature with embedded timestamp and revocation information

PAdES Signatures based on ETSI standards
○ PAdES-BES (Part 3 - PAdES Enhanced)
● PAdES-BES with embedded timestamp

TSA Settings

Available TSA Servers:

Selected TSA Servers:
http://localhost:8777/adss/tsa
http://adss.signinghub.com:8777/adss/t
https://localhost:8778/adss/tsa
http://192.168.3.45:8777/adss/tsa

Note: each selected TSA server will be tried in turn to obtain a timestamp. If a timestamp cannot be obtained from any of the selected TSA servers then an error will be returned.

□ Convert existing signature to an extended format

Hash Algorithm Settings

Hashing Algorithm: SHA256

Signature Type Settings

Signature/Document Relationship: Detached

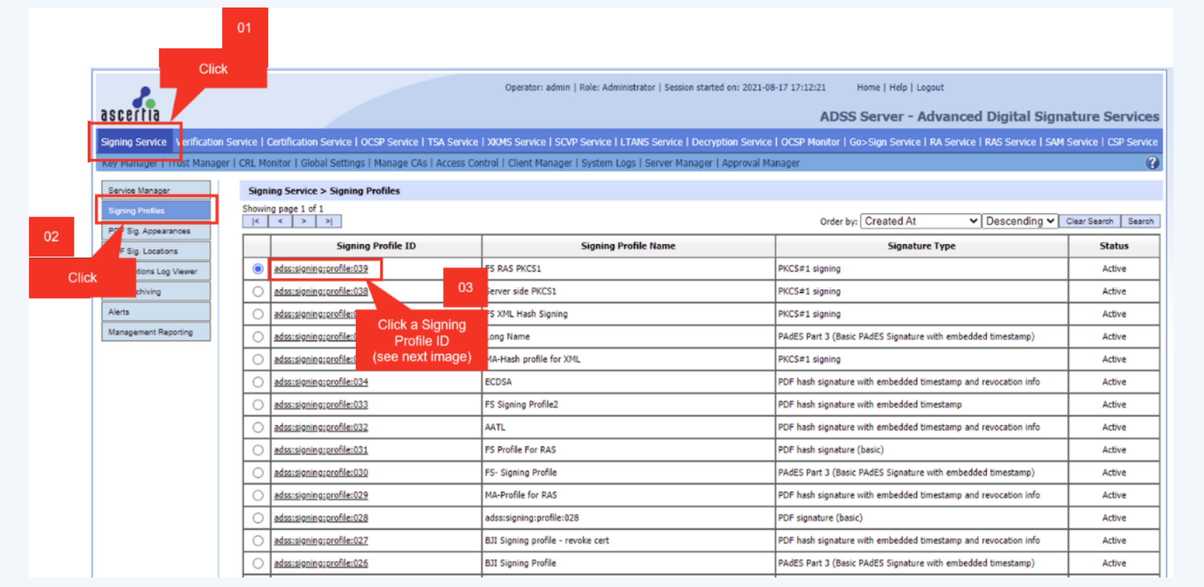
Explicit Policy Based Electronic Signature (EPES) Settings

□ Add Signature Policy Identifier (Creates Explicit Policy-based Electronic Signatures)

In the following example, we will configure an existing Server Side Signing Profile in the ADSS Server based on **PKCS#1**.

1. Go to “Signing Service > Signing Profiles”.

2. Click a Signing Profile ID.


01
Click
02
Click
03
Click a Signing
Profile ID
(see next image)
ascertia
Operator: admin | Role: Administrator | Session started on: 2021-08-17 17:12:21
Home | Help | Logout
ADSS Server - Advanced Digital Signature Services
Signing Service | Verification Service | Certification Service | OCSP Service | TSA Service | XKMS Service | SCVP Service | LTANS Service | Decryption Service | OCSP Monitor | Go>Sign Service | RA Service | RAS Service | SAM Service | CSP Service
Key Manager | Trust Manager | CRL Monitor | Global Settings | Manage CAs | Access Control | Client Manager | System Logs | Server Manager | Approval Manager
Service Manager
Signing Profiles
PDF Sig. Appearances
PDF Sig. Locations
Transactions Log Viewer
Logs Archiving
Alerts
Management Reporting
|< < > >|
Clear Search
Search

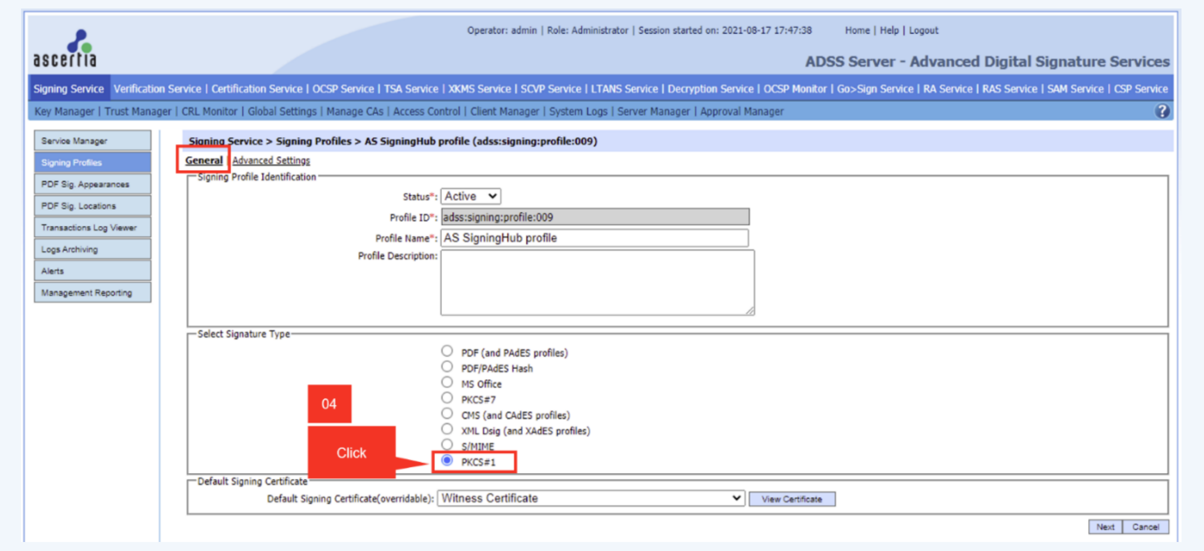
Signing Service > Signing Profiles

Showing page 1 of 1

Order by: Created At Descending

	Signing Profile ID	Signing Profile Name	Signature Type	Status
●	adss:signing:profile:039	FS RAS PKCS1	PKCS#1 signing	Active
○	adss:signing:profile:038	erver side PKCS1	PKCS#1 signing	Active
○	adss:signing:profile:	FS XML Hash Signing	PKCS#1 signing	Active
○	adss:signing:profile:	ong Name	PAdES Part 3 (Basic PAdES Signature with embedded timestamp)	Active
○	adss:signing:profile:	1A-Hash profile for XML	PKCS#1 signing	Active
○	adss:signing:profile:034	ECDSA	PDF hash signature with embedded timestamp and revocation info	Active
○	adss:signing:profile:033	FS Signing Profile2	PDF hash signature with embedded timestamp	Active
○	adss:signing:profile:032	AATL	PDF hash signature with embedded timestamp and revocation info	Active
○	adss:signing:profile:031	FS Profile For RAS	PDF hash signature (basic)	Active
○	adss:signing:profile:030	FS- Signing Profile	PAdES Part 3 (Basic PAdES Signature with embedded timestamp)	Active
○	adss:signing:profile:029	MA-Profile for RAS	PDF hash signature with embedded timestamp and revocation info	Active
○	adss:signing:profile:028	adss:signing:profile:028	PDF signature (basic)	Active
○	adss:signing:profile:027	BJI Signing profile - revoke cert	PDF hash signature with embedded timestamp and revocation info	Active
○	adss:signing:profile:026	BJI Signing Profile	PAdES Part 3 (Basic PAdES Signature with embedded timestamp)	Active

3. Under the “General” tab, click “PKCS#1”


Operator: admin | Role: Administrator | Session started on: 2021-08-17 17:47:38
Home | Help | Logout
ADSS Server - Advanced Digital Signature Services
Signing Service | Verification Service | Certification Service | OCSP Service | TSA Service | XKMS Service | SCVP Service | LTANS Service | Decryption Service | OCSP Monitor | Go>Sign Service | RA Service | RAS Service | SAM Service | CSP Service
Key Manager | Trust Manager | CRL Monitor | Global Settings | Manage CAs | Access Control | Client Manager | System Logs | Server Manager | Approval Manager
Service Manager
Signing Profiles
PDF Sig. Appearances
PDF Sig. Locations
Transactions Log Viewer
Logs Archiving
Alerts
Management Reporting
Next
Cancel
View Certificate

Signing Service > Signing Profiles > AS SigningHub profile (adss:signing:profile:009)

General | Advanced Settings

Signing Profile Identification

Status*: Active

Profile ID*: adss:signing:profile:009

Profile Name*: AS SigningHub profile

Profile Description:

Select Signature Type

○ PDF (and PAdES profiles)
○ PDF/PAdES Hash
○ MS Office
○ PKCS#7
○ CMS (and CAdES profiles)
○ XML Dsig (and XAdES profiles)
○ S/MIME
● PKCS#1

04

Click

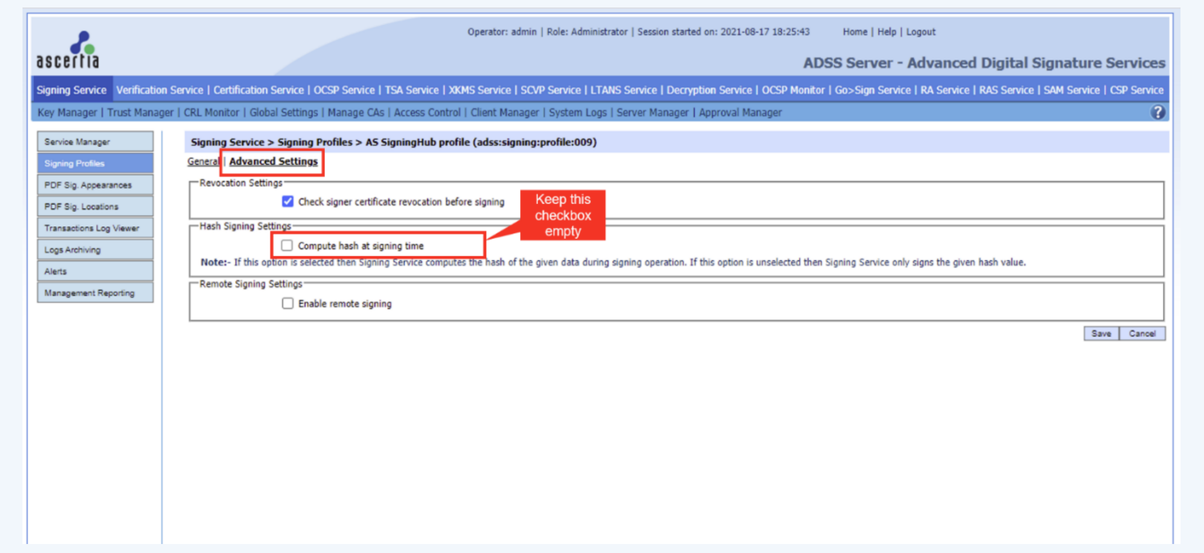
Default Signing Certificate

Default Signing Certificate(overridable): Witness Certificate

Once the **PKCS#1** signature type is selected, the signature settings will no longer be visible. SigningHub now produces Long Term Validation (LTV) signatures by default.

For XML signing, with the addition of support for PKCS#1 in the signing implementation, XML signing configuration has been removed and will make use of the same Signing Profiles that are used for document signing. Moreover, SigningHub produces XAdES-X-L signature format as a default for XML signing.

The "**Compute hash at signing time**" option must be turned OFF under **Advanced Settings.** SigningHub computes hash by itself and sends this hash to ADSS Server for signing.


Operator: admin | Role: Administrator | Session started on: 2021-08-17 18:25:43
Home | Help | Logout
ADSS Server - Advanced Digital Signature Services
Signing Service | Verification Service | Certification Service | OCSP Service | TSA Service | XKMS Service | SCVP Service | LTANS Service | Decryption Service | OCSP Monitor | Go>Sign Service | RA Service | RAS Service | SAM Service | CSP Service
Key Manager | Trust Manager | CRL Monitor | Global Settings | Manage CAs | Access Control | Client Manager | System Logs | Server Manager | Approval Manager
Service Manager
Signing Profiles
PDF Sig. Appearances
PDF Sig. Locations
Transactions Log Viewer
Logs Archiving
Alerts
Management Reporting
Save
Cancel

Signing Service > Signing Profiles > AS SigningHub profile (adss:signing:profile:009)

General | Advanced Settings

Revocation Settings

☑ Check signer certificate revocation before signing

Hash Signing Settings

□ Compute hash at signing time

Keep this checkbox empty

Note:- If this option is selected then Signing Service computes the hash of the given data during signing operation. If this option is unselected then Signing Service only signs the given hash value.

Remote Signing Settings

□ Enable remote signing

5 SigningHub Admin Configuration

The following sections illustrate the changes that the installer configures automatically and highlight the manual steps that still need to be executed by the system administrators.

5.1 Certification Profiles

Two new configurations are added to the Certification Profiles.

1) Level of Assurance
2) Key Protection

A Level of Assurance indicates the level of trust that the certificates will introduce when it is used to sign the document. The available selections are: Electronic Seal (eSeal), Advanced Electronic Seal (AdESeal), Qualified Electronic Seal (QESeal), Advanced Electronic Signatures (AES), High Trust Advanced Electronic Signatures (AATL) and Qualified Electronic Signatures (QES). These values are pulled from "Configurations -> Document Settings -> Signature Types -> Level of Assurance".

Certification Profiles are used to create certificates dynamically. Administrators need to manually set the Level of Assurance in the profile to indicate the level of trust attached to that particular Certificate Profile.

The installer automatically sets the value for the Level of Assurance for all the existing Certification Profiles to "**Advanced Electronic Signatures**".

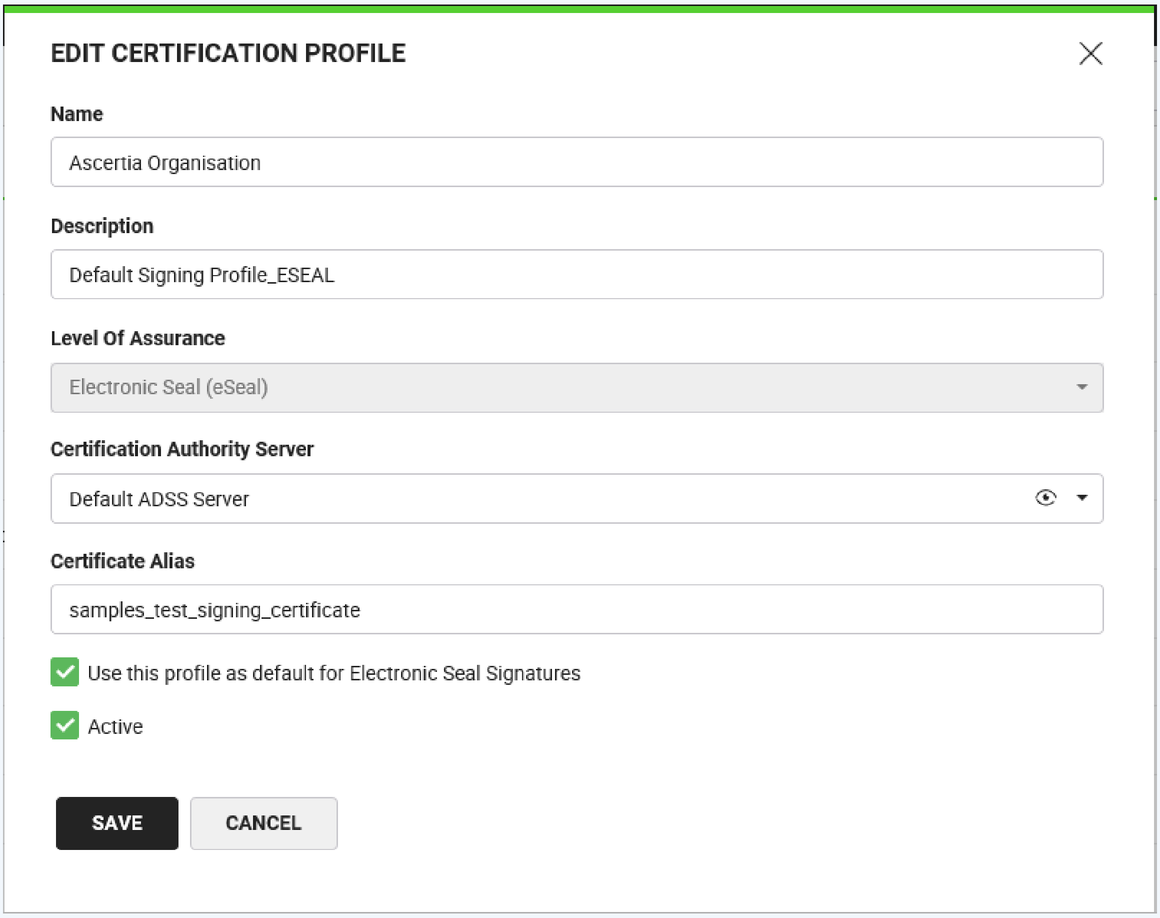
Every certificate that is created using the Certification Profile has key pairs created on the remote server. The **Key Protection** indicates the protection method of the private key on the remote server. This means that the private key can be protected with a user password, a system-generated password or by remote authorisation controlled by the end user through a mobile device.

The existing certificates that were generated using a **system password** will be automatically updated with the key protection value set to "**User Password**".

In the previous versions of SigningHub, Witness Signing was configured using Signing Profiles. In SigningHub 8.x.x, all Certificate Profiles that are configured with an Electronic Seal (eSeal) Level of Assurance can be used to sign e-Signature fields. In SigningHub 8.x.x, the terms Witness Signing and e-Signatures have been replaced by Electronic Seal (eSeal) Level of Assurance and the recipients will be able to use only those certificates that are set to the corresponding Level of Assurance to sign the document.

A Certification Profile that has Electronic Seal (eSeal) as a Level of Assurance can be set as the default after upgrading to SigningHub 8.x.x. This default Electronic Seal (eSeal) Certification Profile will be used for signing across the system if there is no Electronic Seal (eSeal) signing capacity configured for a user.

See the details on configuring a Certification Profile (or Electronic Seal (eSeal) particularly in the image below.



EDIT CERTIFICATION PROFILE

Name

Ascertia Organisation

Description

Default Signing Profile_ESEAL

Level Of Assurance

Electronic Seal (eSeal)

Certification Authority Server

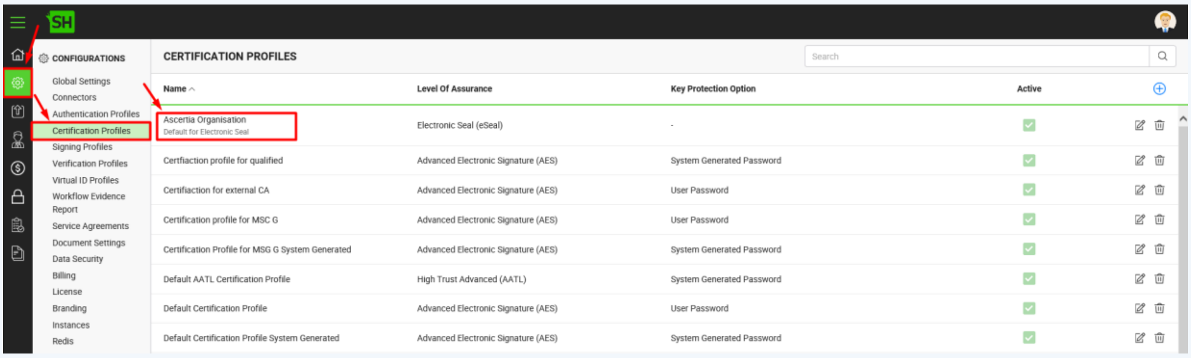
Default ADSS Server

Certificate Alias

samples_test_signing_certificate

☑ Use this profile as default for Electronic Seal Signatures

☑ Active



CERTIFICATION PROFILES

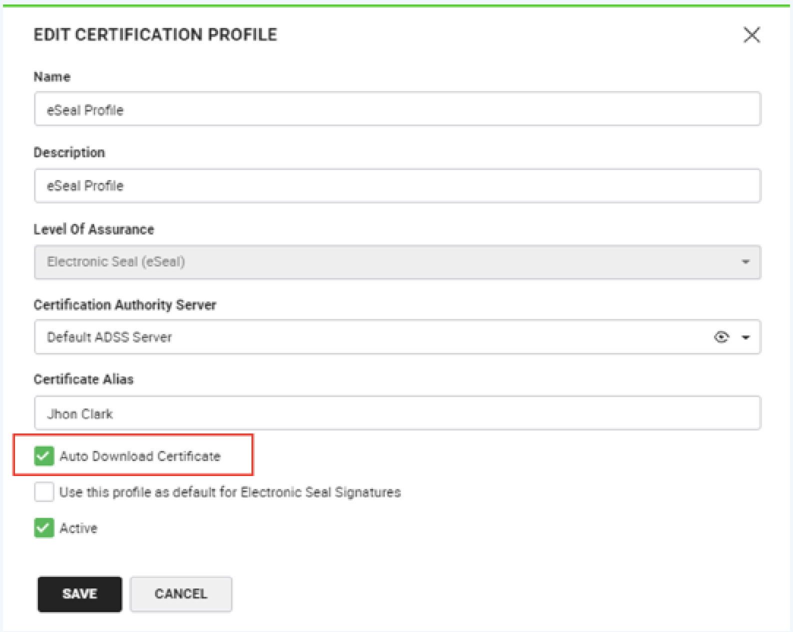
Name	Level Of Assurance	Key Protection Option	Active
Ascertia Organisation Default for Electronic Seal	Electronic Seal (eSeal)	-	✓
Certfiaction profile for qualified	Advanced Electronic Signature (AES)	System Generated Password	✓
Certifiaction for external CA	Advanced Electronic Signature (AES)	User Password	✓
Certification profile for MSC G	Advanced Electronic Signature (AES)	User Password	✓
Certification Profile for MSG G System Generated	Advanced Electronic Signature (AES)	System Generated Password	✓
Default AATL Certification Profile	High Trust Advanced (AATL)	System Generated Password	✓
Default Certification Profile	Advanced Electronic Signature (AES)	User Password	✓
Default Certification Profile System Generated	Advanced Electronic Signature (AES)	System Generated Password	✓

5.1.1 Reconfigure Certification Profiles for eSeal

Automatically Import the eSeal Certificate from ADSS Server

If you are upgrading to SigningHub 8.x.x with Ascertia ADSS Server 6.9, then you can configure an eSeal based Certification Profile to automatically import the required certificate for eSeal signatures from ADSS Server.

1. Go to SigningHub Admin > Certification Profiles.
2. Edit an existing eSeal based Certification Profile or create a new one.
3. From the dialog, select the "Auto Download Certificate" field.



EDIT CERTIFICATION PROFILE

Name: eSeal Profile

Description: eSeal Profile

Level Of Assurance: Electronic Seal (eSeal)

Certification Authority Server: Default ADSS Server

Certificate Alias: Jhon Clark

☑ Auto Download Certificate

□ Use this profile as default for Electronic Seal Signatures

☑ Active

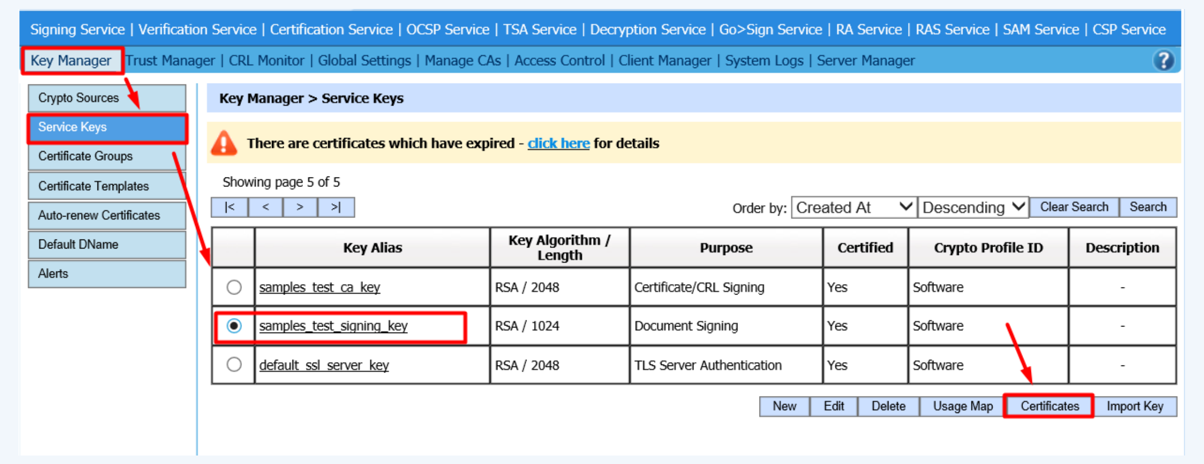
'Auto Download Certificate' is an optional configuration and only works when connecting to ADSS Server version 6.9 or above. For the ADSS Server versions (i.e. 6.8 or below), this must be configured as a manual step as explained in next section.

Why do we need a certificate for eSeals?

SigningHub's new design for applying eSeals requires the eSeal signing certificate to be imported into the SigningHub Certification Profile. In previous releases, this function was performed by ADSS Server.

How to get the certificate from ADSS Server when connecting to ADSS Server 6.8 or below?

To export the certificate for Electronic Seal (eSeal) from ADSS Server, log into the ADSS Server Console with an Administrator account.


Signing Service | Verification Service | Certification Service | OCSP Service | TSA Service | Decryption Service | Go>Sign Service | RA Service | RAS Service | SAM Service | CSP Service
Key Manager | Trust Manager | CRL Monitor | Global Settings | Manage CAs | Access Control | Client Manager | System Logs | Server Manager
Crypto Sources
Service Keys
Certificate Groups
Certificate Templates
Auto-renew Certificates
Default DName
Alerts
|< < > >|
Clear Search
Search
New
Edit
Delete
Usage Map
Certificates
Import Key

Key Manager > Service Keys

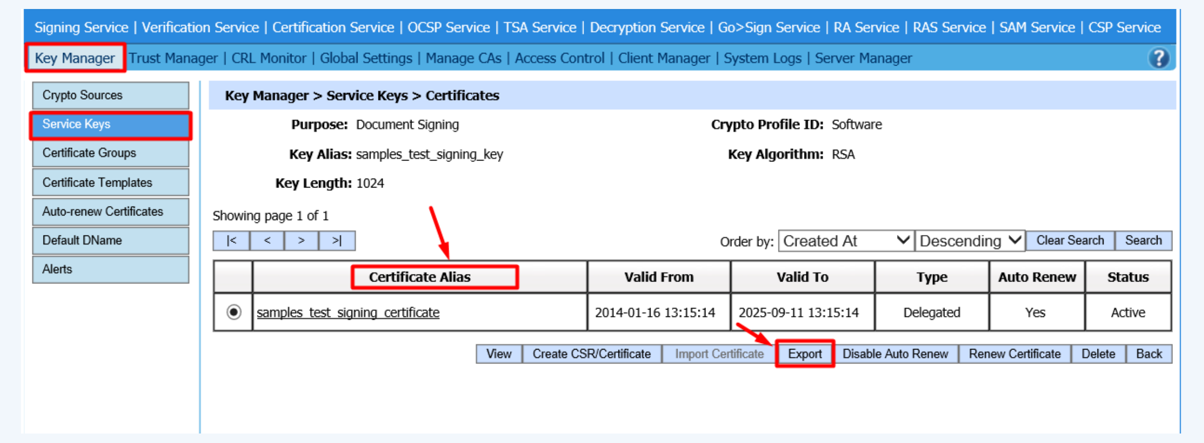
There are certificates which have expired - click here for details

Showing page 5 of 5

Order by: Created At Descending

	Key Alias	Key Algorithm / Length	Purpose	Certified	Crypto Profile ID	Description
○	samples_test_ca_key	RSA / 2048	Certificate/CRL Signing	Yes	Software	-
●	samples_test_signing_key	RSA / 1024	Document Signing	Yes	Software	-
○	default_ssl_server_key	RSA / 2048	TLS Server Authentication	Yes	Software	-

1. Go to **Key Manager > Service Keys**, select the intended **Key Alias** and click on **Certificates**.
   The list of certificates will appear as shown below.


Signing Service | Verification Service | Certification Service | OCSP Service | TSA Service | Decryption Service | Go>Sign Service | RA Service | RAS Service | SAM Service | CSP Service
Key Manager | Trust Manager | CRL Monitor | Global Settings | Manage CAs | Access Control | Client Manager | System Logs | Server Manager
Crypto Sources
Service Keys
Certificate Groups
Certificate Templates
Auto-renew Certificates
Default DName
Alerts
|< < > >|
Clear Search
Search
View
Create CSR/Certificate
Import Certificate
Export
Disable Auto Renew
Renew Certificate
Delete
Back

Key Manager > Service Keys > Certificates

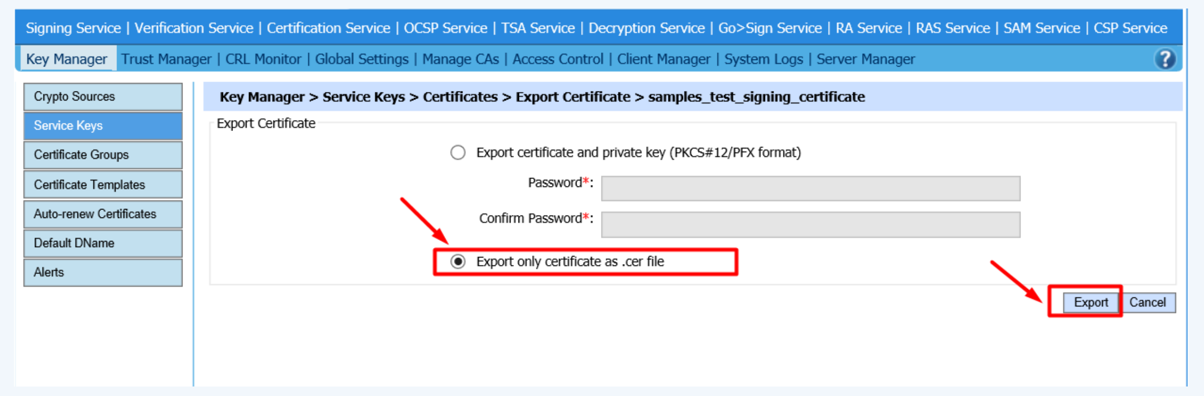
Purpose: Document Signing
Crypto Profile ID: Software
Key Alias: samples_test_signing_key
Key Algorithm: RSA
Key Length: 1024

Showing page 1 of 1

Order by: Created At Descending

	Certificate Alias	Valid From	Valid To	Type	Auto Renew	Status
●	samples_test_signing_certificate	2014-01-16 13:15:14	2025-09-11 13:15:14	Delegated	Yes	Active

2. Select the required **Certificate Alias** and click on the **Export** button.


Signing Service | Verification Service | Certification Service | OCSP Service | TSA Service | Decryption Service | Go>Sign Service | RA Service | RAS Service | SAM Service | CSP Service
Key Manager | Trust Manager | CRL Monitor | Global Settings | Manage CAs | Access Control | Client Manager | System Logs | Server Manager
Crypto Sources
Service Keys
Certificate Groups
Certificate Templates
Auto-renew Certificates
Default DName
Alerts
Export
Cancel

Key Manager > Service Keys > Certificates > Export Certificate > samples_test_signing_certificate

Export Certificate

○ Export certificate and private key (PKCS#12/PFX format)

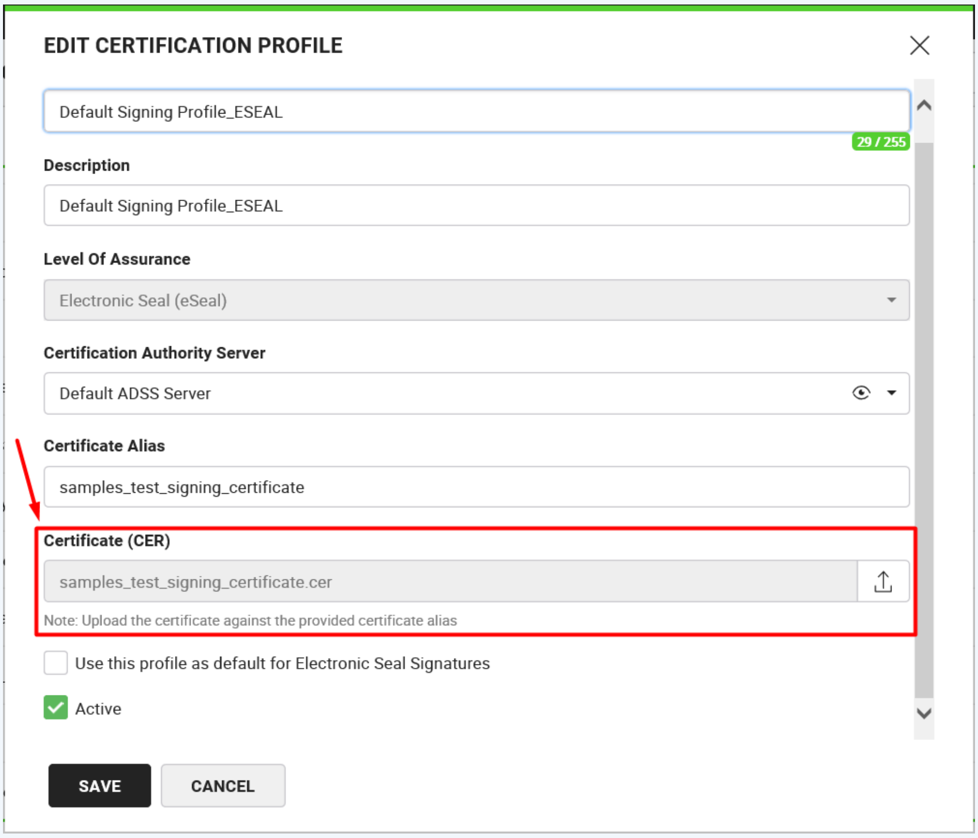
Password*:

Confirm Password*:

● Export only certificate as .cer file

3. Select the **Export only certificate as a .cer file**, and click on the **Export** button to save the certificate file. This will download the certificate.

The SigningHub's Certification Profile (for eSeal) needs to be reconfigured to have the eSeal certificate imported to the defined certificate alias. This is mandatory, once upgraded to SigningHub 8.x.x, to perform eSeal signatures when connecting to an ADSS Server 6.8 or below. Within the SigningHub's Certification Profile, browse to the certificate that was exported from ADSS Server in the above steps, click **SAVE** to apply the eSeal certificate to the Certification Profile.


EDIT CERTIFICATION PROFILE

Default Signing Profile_ESEAL

29 / 255

Description: Default Signing Profile_ESEAL

Level Of Assurance: Electronic Seal (eSeal)

Certification Authority Server: Default ADSS Server

Certificate Alias: samples_test_signing_certificate

Certificate (CER): samples_test_signing_certificate.cer

Note: Upload the certificate against the provided certificate alias

□ Use this profile as default for Electronic Seal Signatures

☑ Active

5.1.2 Signing Profiles

In the previous versions of SigningHub, the same Signing Profile could be configured for client-held keys and server-held keys. In SigningHub 8.x.x, separate Signing Profiles should be configured for server and client-held keys.

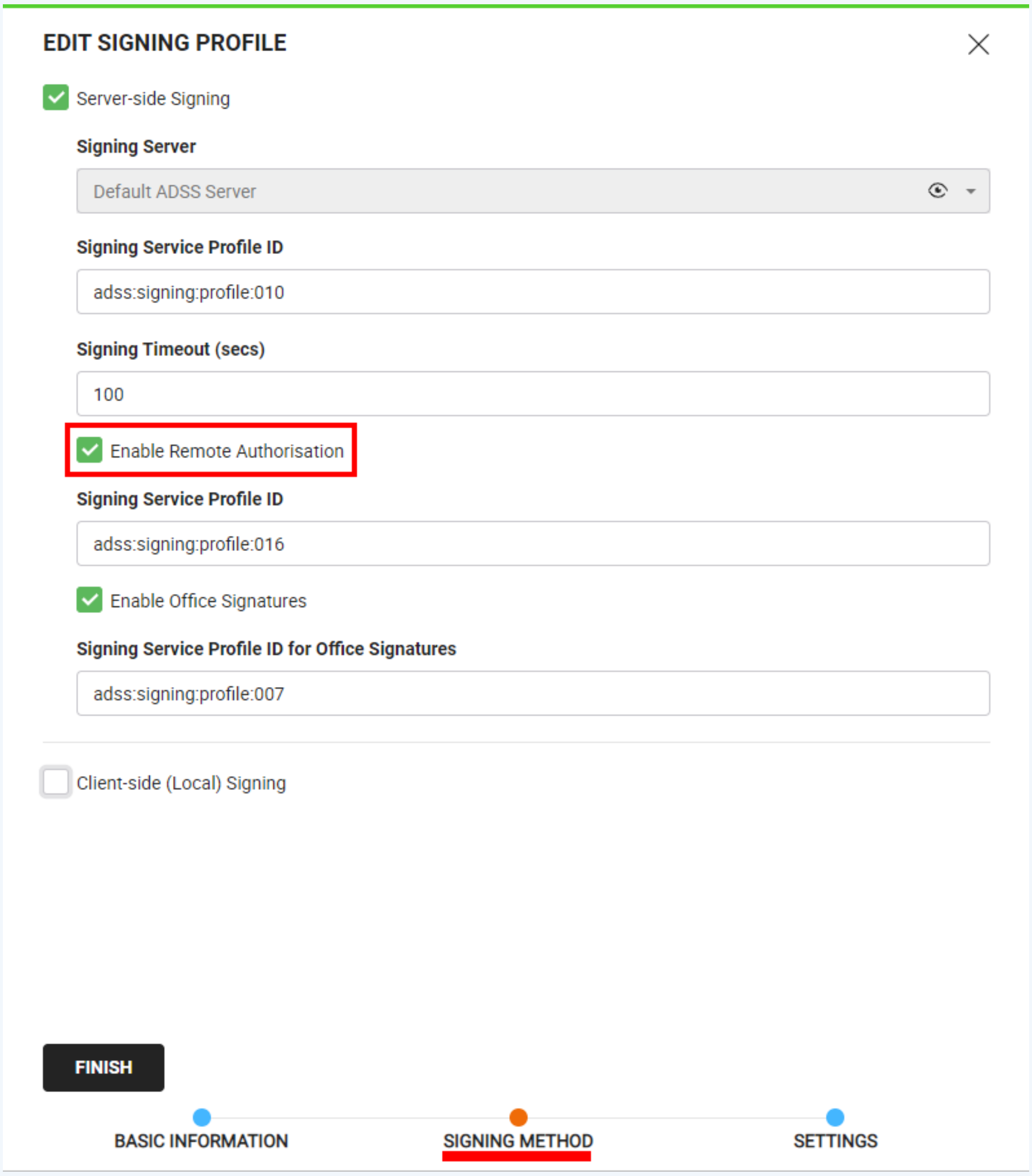
The installer leaves the existing Signing Profiles that are configured for both server and client-held keys as it is for backward compatibility.

Signature appearance design and text-based signature font are removed from the user's Signing Profile. Signature Appearance designs can now be configured in the Service Plan and under Enterprise Roles. For the text-based Signature font, the enterprise administrators can now only configure it in the Enterprise Roles.

Custom signature appearance designs (if any), have to manually move to the following installation directory.
{{deployment_directory}}\default\appearances

Remote authorisation can now be configured in a Signing Profile. For this, an option to "Enable Remote Authorisation" must be configured manually by providing 'Signing Service Profile ID" in the already existing Signing Profile for RAS. In previous versions, it was configured separately in a Service Plan. By moving the configuration to Signing Profiles, users can configure multiple remote authorisation servers. This can be configured in Signing Profiles in the same way an office Signing Profiles would be configured.

The following images illustrate the configuration of a Signing Profile.



EDIT SIGNING PROFILE

☑ Server-side Signing

Signing Server: Default ADSS Server

Signing Service Profile ID: adss:signing:profile:010

Signing Timeout (secs): 100

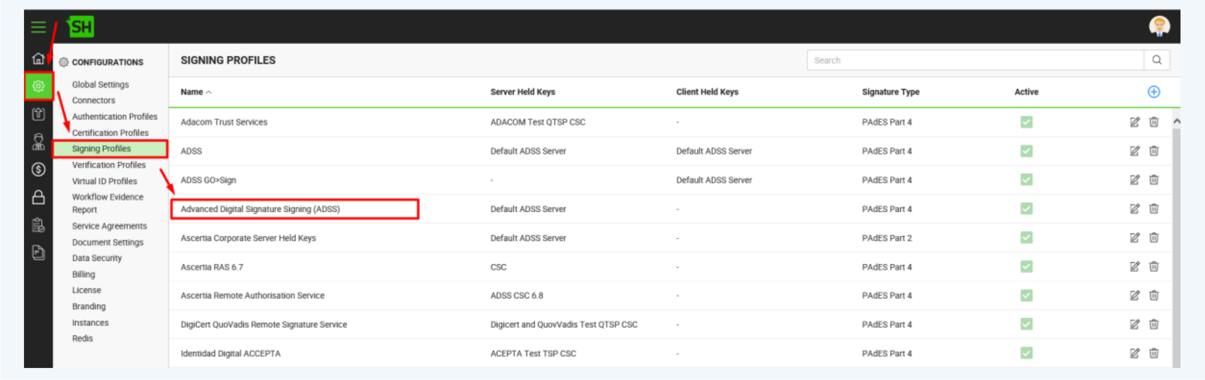
☑ Enable Remote Authorisation

Signing Service Profile ID: adss:signing:profile:016

☑ Enable Office Signatures

Signing Service Profile ID for Office Signatures: adss:signing:profile:007

□ Client-side (Local) Signing

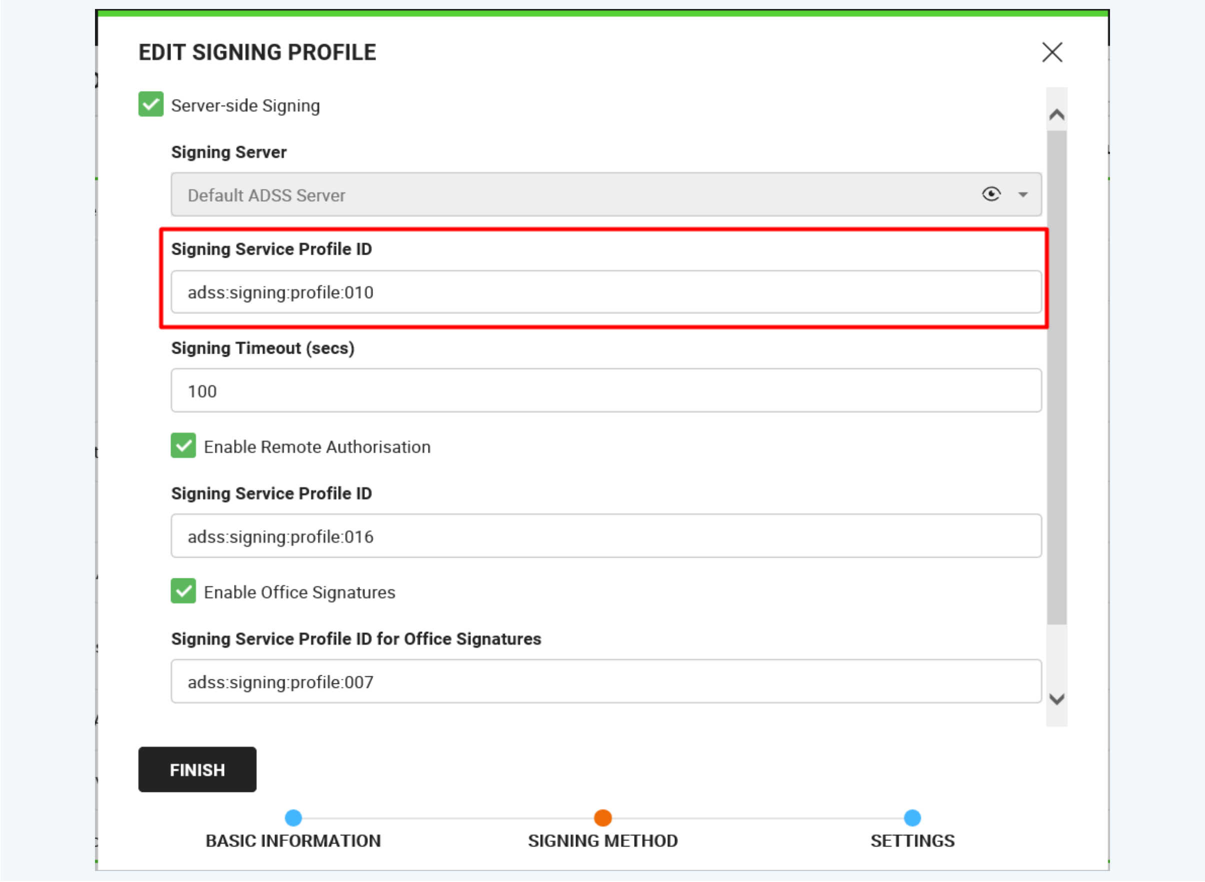


SIGNING PROFILES

Name	Server Held Keys	Client Held Keys	Signature Type	Active
Adacom Trust Services	ADACOM Test QTSP CSC	-	PAdES Part 4	✓
ADSS	Default ADSS Server	Default ADSS Server	PAdES Part 4	✓
ADSS GO>Sign	-	Default ADSS Server	PAdES Part 4	✓
Advanced Digital Signature Signing (ADSS)	Default ADSS Server	-	PAdES Part 4	✓
Ascertia Corporate Server Held Keys	Default ADSS Server	-	PAdES Part 2	✓
Ascertia RAS 6.7	CSC	-	PAdES Part 4	✓
Ascertia Remote Authorisation Service	ADSS CSC 6.8	-	PAdES Part 4	✓
DigiCert QuoVadis Remote Signature Service	Digicert and QuovVadis Test QTSP CSC	-	PAdES Part 4	✓
Identidad Digital ACCEPTA	ACEPTA Test TSP CSC	-	PAdES Part 4	✓

5.1.3 Reconfigure Signing Profiles for PKCS#1 Changes

- From SigningHub 8.x.x onwards, all users can upload XMLs using the SigningHub API. SigningHub will no longer need a separately configured XML Signing Profile to perform XML Signing. Instead, the Signing Profile configured for Server-side signing will be used. The **Enable XML Signing** option has been removed from the Signing Profile.



EDIT SIGNING PROFILE

☑ Server-side Signing

Signing Server: Default ADSS Server

Signing Service Profile ID: adss:signing:profile:010

Signing Timeout (secs): 100

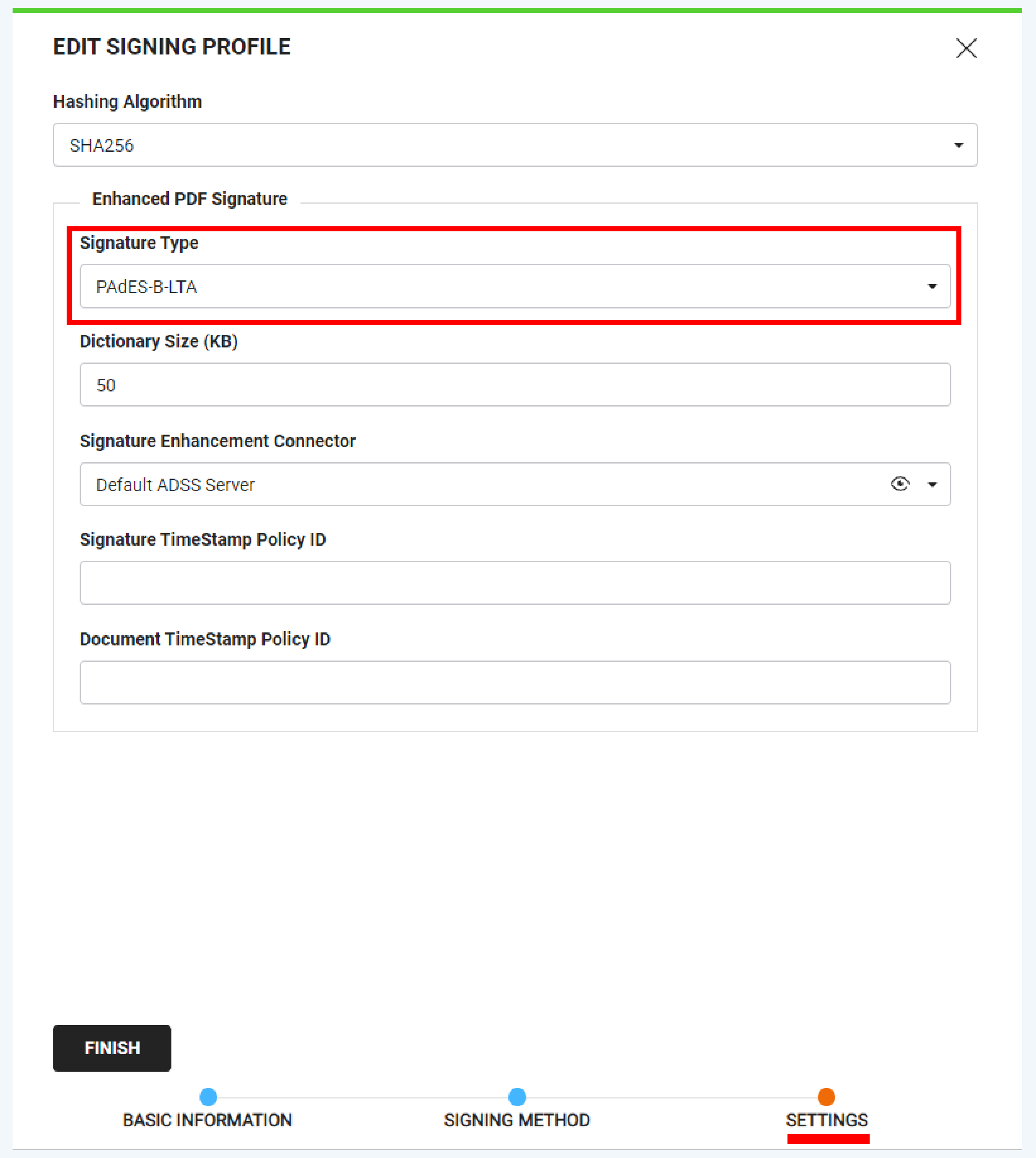
☑ Enable Remote Authorisation

Signing Service Profile ID: adss:signing:profile:016

☑ Enable Office Signatures

Signing Service Profile ID for Office Signatures: adss:signing:profile:007

- SigningHub now produces **Long Term Validation (LTV)** signatures by default; this no longer requires any additional LTV configuration in ADSS Server Signing Profiles. However, to enhance signatures, the signature type (i.e. **PAdES-B-LT** or **PAdES-B-LTA**) configured under SigningHub Admin will be used as shown below.



EDIT SIGNING PROFILE

Hashing Algorithm: SHA256

Enhanced PDF Signature

Signature Type: PAdES-B-LTA

Dictionary Size (KB): 50

Signature Enhancement Connector: Default ADSS Server

Signature TimeStamp Policy ID:

Document TimeStamp Policy ID:

5.2 Witness Signatures

5.2.1 New features in SigningHub 8.x.x

Another major change introduced in SigningHub 8.x.x is related to the Witness Signing Capacity and its management within the SigningHub web application.

In the previous versions of SigningHub, witness signatures were managed in Signing Profiles and a default alias was set within the ADSS Server, which was used for witness signatures. This same configuration has been aligned with the rest of the certificates in SigningHub 8.x.x. This configuration is now available in Certification Profiles instead of Signing Profiles.

In SigningHub 8.x.x, the installer will now automatically create new Certification Profiles against all existing witness signature profiles. The installer will also add the "_ESEAL" suffix at the end of the profile name for identification purposes. This will help the administrator to search and shortlist the Certification Profiles.

5.2.2 Manual Configuration

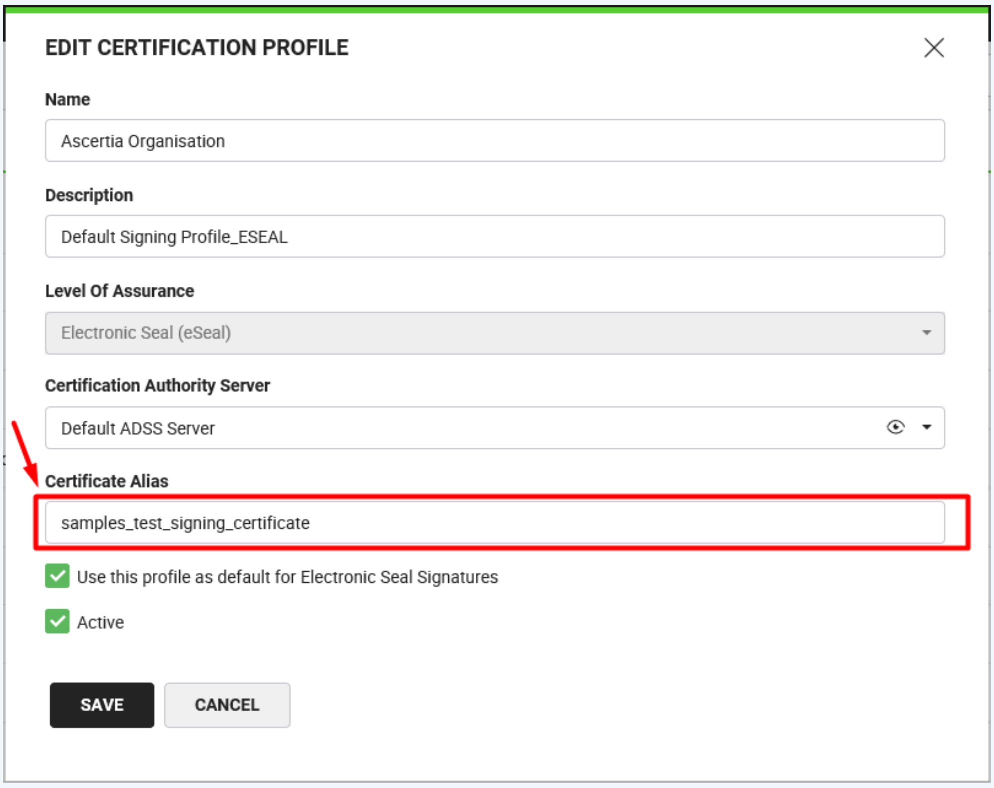
The following manual configuration steps are easy to follow if you have the previous version of SigningHub accessible on the localhost URLs:

- Take the Certification Profile name from the SigningHub 8.x.x instance and search the same name in the previous version of SigningHub's Signing Profiles. Remember to leave out the "**_ESEAL**" term while searching on the older version as this term is added by the system installer to easily identify the profiles, which require manual configuration.
- Once you find the profile name in the previous version of SigningHub, copy this ADSS Signing Profile name/ID and search for this same ADSS profile name/ID in ADSS Server.
- Go to **Ascertia ADSS Server -> Signing Service** and select the corresponding ADSS Signing Profile and copy the Default Signing Certificate configured in this Signing Profile. (This default certificate is created under ADSS Server Key Manager. In Key Manager, go to **Key Manager** > Service Keys > Search to view the key alias that is configured for selected "Default Certificate Alias" and copied from the ADSS Signing Profile).
- Now paste the certificate alias in the SigningHub 8.x.x Certification Profile that you initially selected in the first step.
- Select the ADSS server from the drop-down list, where the certificate alias resides.

SigningHub administrators must select one Certification Profile associated with Electronic Seal (eSeals) as the default profile. This profile will be used by all the recipients who are expected to complete an Electronic Seal (eSeal) but do not have the Electronic Seal (eSeal) Level of Assurance configured in their subscribed Service Plans. This is applicable for Advanced Electronic Seal (AdESeal) and Qualified Electronic Seal (QESeal).

See the details on configuring certificate alias for all of three eSeal Levels of Assurance (as above) under Certification Profile as shown in the image below. The Certificate

Alias parameter is the **Default Signing Certificate**, copied from **ADSS Signing Profile**.



EDIT CERTIFICATION PROFILE

Name: Ascertia Organisation

Description: Default Signing Profile_ESEAL

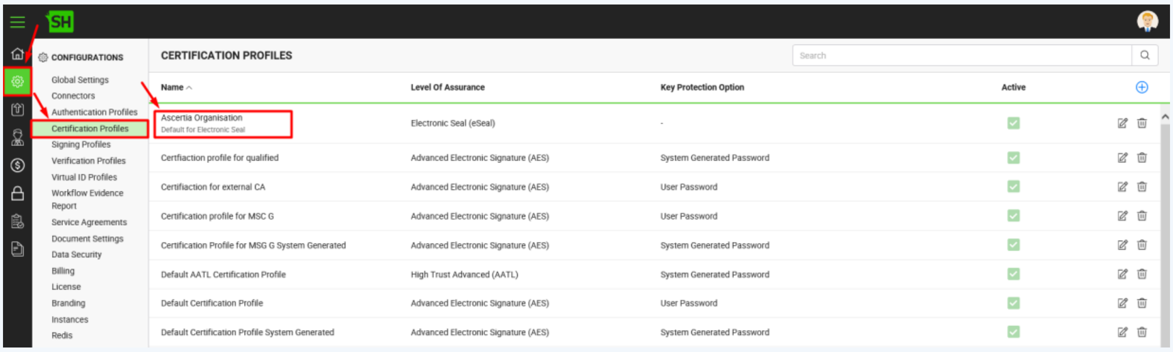
Level Of Assurance: Electronic Seal (eSeal)

Certification Authority Server: Default ADSS Server

Certificate Alias: samples_test_signing_certificate

☑ Use this profile as default for Electronic Seal Signatures

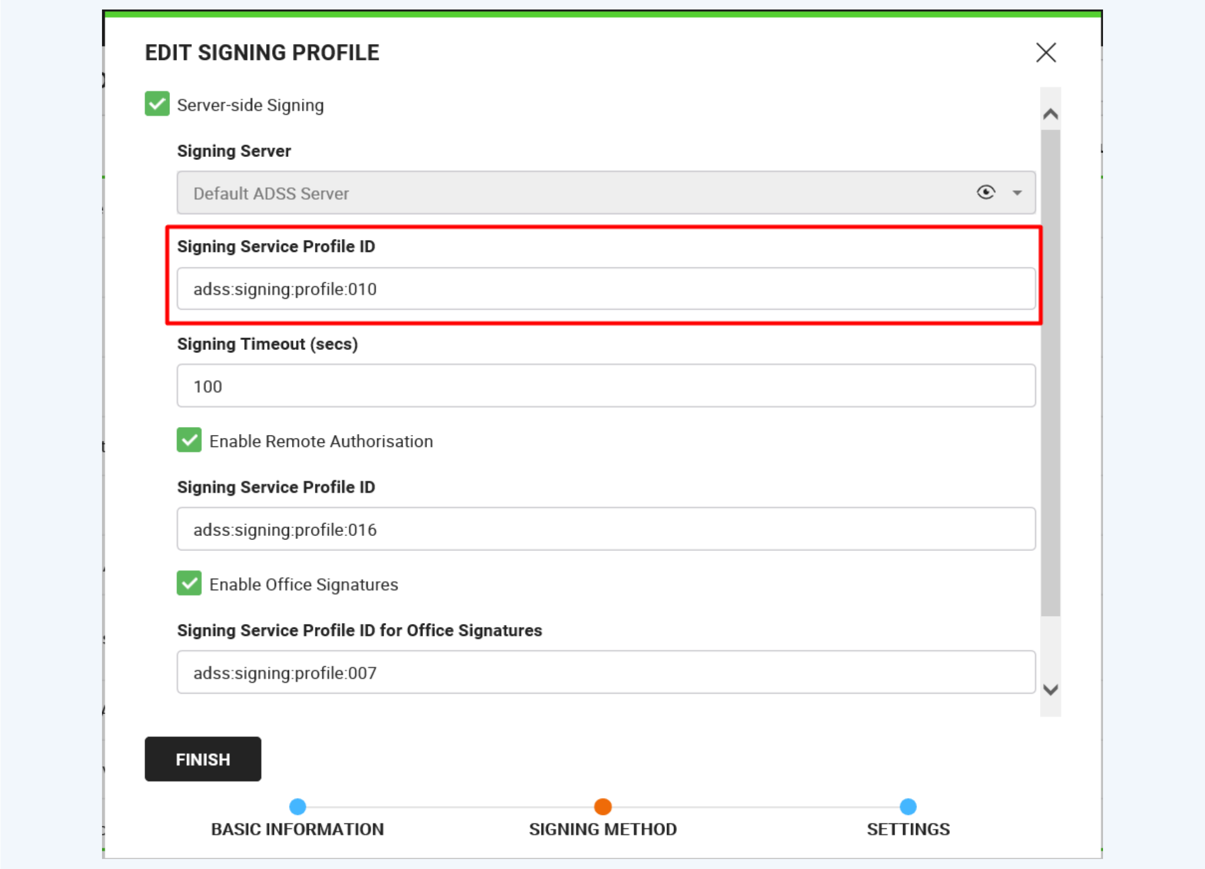
☑ Active



CERTIFICATION PROFILES

Name	Level Of Assurance	Key Protection Option	Active
Ascertia Organisation Default for Electronic Seal	Electronic Seal (eSeal)	-	✓
Certfiaction profile for qualified	Advanced Electronic Signature (AES)	System Generated Password	✓
Certifiaction for external CA	Advanced Electronic Signature (AES)	User Password	✓
Certification profile for MSC G	Advanced Electronic Signature (AES)	User Password	✓
Certification Profile for MSG G System Generated	Advanced Electronic Signature (AES)	System Generated Password	✓
Default AATL Certification Profile	High Trust Advanced (AATL)	System Generated Password	✓
Default Certification Profile	Advanced Electronic Signature (AES)	User Password	✓
Default Certification Profile System Generated	Advanced Electronic Signature (AES)	System Generated Password	✓

- From SigningHub 8.x.x onwards, all users can upload XMLs using the SigningHub API. SigningHub will no longer need a separately configured XML Signing Profile to perform XML Signing. Instead, the Signing Profile configured for server-side signing will be used. The **Enable XML Signing** option has been removed from the Signing Profile.



EDIT SIGNING PROFILE

☑ Server-side Signing

Signing Server

Default ADSS Server

Signing Service Profile ID

adss:signing:profile:010

Signing Timeout (secs)

100

☑ Enable Remote Authorisation

Signing Service Profile ID

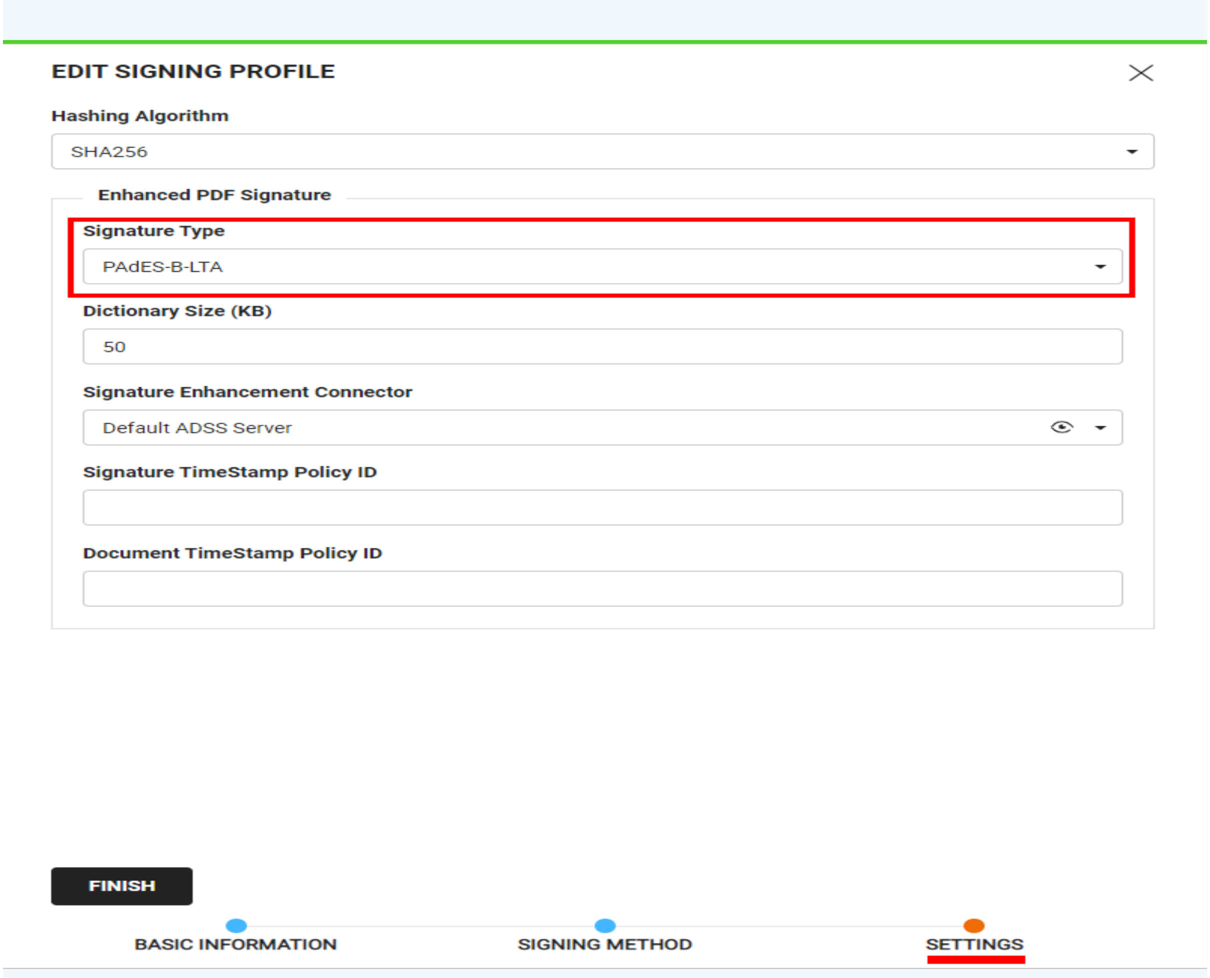
adss:signing:profile:016

☑ Enable Office Signatures

Signing Service Profile ID for Office Signatures

adss:signing:profile:007

- SigningHub now produces **Long Term Validation (LTV)** signatures by default; this no longer requires any additional LTV configurations in ADSS Server Signing Profiles. However, to enhance signatures the signature type (i.e. **PAdES-B-LT**or **PAdES-B-LTA**) configured under SigningHub Admin will be used as shown below.



EDIT SIGNING PROFILE

Hashing Algorithm

SHA256

Enhanced PDF Signature

Signature Type

PAdES-B-LTA

Dictionary Size (KB)

50

Signature Enhancement Connector

Default ADSS Server

Signature TimeStamp Policy ID

Document TimeStamp Policy ID

5.3 Service Plans

SigningHub 8.x.x has significant changes to Service Plan configurations. It is recommended to review the Service Plans for the below changes.

The following options are either completely removed from the Service Plan or their location has been changed on the UI/UX:

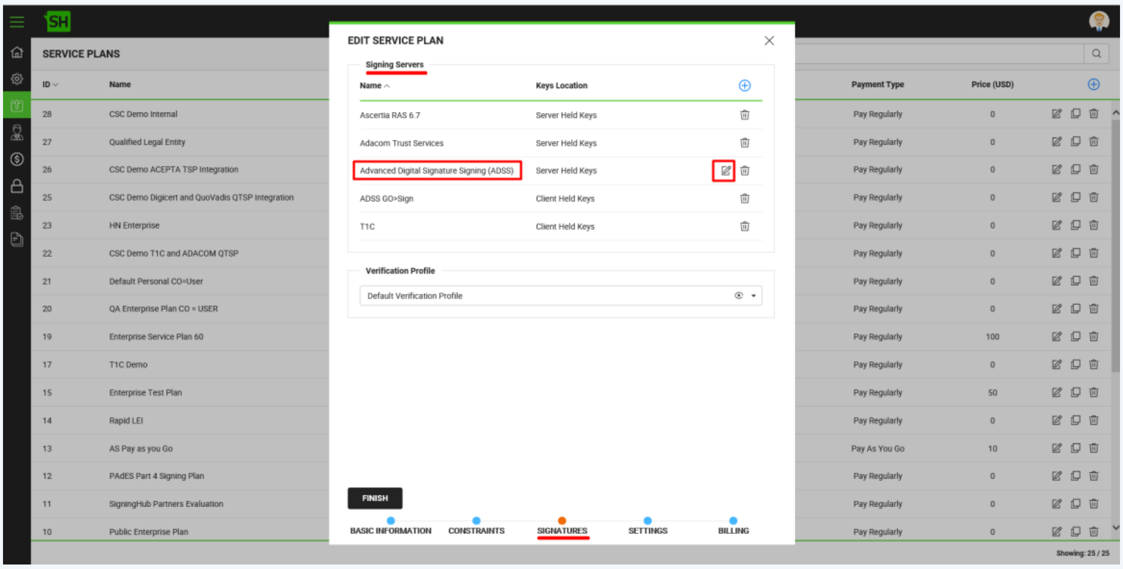
- **Protect server-side signing keys with user password**: This option has been removed from the Service Plan. It is now handled in the **Certification Profile > Key Protection Option** configuration.
- **Push newly created certificates to ADSS CSP**: This option has been moved to Service Plans > Singing Servers.
- **Add witness signature to e-signatures**: This option has been completely removed from the Service Plan configurations and Electronic Seal (eSeal) is now being used in its place for witness signatures.
- **Remote Authorised Signing via ADSS Server SAM**: This option has been moved to the Signing Profile.
- **Signing Capacities**: This option has been moved to **Service Plan > signing servers**.
- **Default Signing Capacity**: This option has been removed from the Service Plan configurations and is now only available under Enterprise Roles.

The following new options have been introduced:

- Password should be provided at the time of user registration: If this option is enabled, then the user must set up a password while registering. This is necessary to be turned on if the Certification Profiles selected are configured with the key protection level of “user password”.
- More than one signing server can be configured that can be used to sign the document
  - Signing Profiles are mapped to represent a signing server; administrators can add multiple Signing Profiles in a Service Plan ensuring that the recipients using the Service Plan will be able to use these servers to sign the document.
  - Each Signing Profile is defined against a server; it can be a CSC protocol-based signing server or an ADSS server.
  - For ADSS based signing servers, administrators can configure multiple capacities (Certification Profiles) based on the Level of Assurance that is needed by the end-users.
- All Levels of Assurance are now available under a new tab named “Documents” under Service Plan.
- Signature Appearances Design is now available under Service Plan only. These are no more available under signing profiles.

Custom signature appearance designs (if any), have to be moved manually to the following installation directory.
{{deployment_directory}}\default\appearances

See the details on configuring a Service Plan after the upgrade. This configuration is in a sequence as highlighted in the images below.



SERVICE PLANS

ID	Name	Payment Type	Price (USD)
28	CSC Demo Internal	Pay Regularly	0
27	Qualified Legal Entity	Pay Regularly	0
26	CSC Demo ACEPTA TSP Integration	Pay Regularly	0
25	CSC Demo Digicert and QuoVadis QTSP Integration	Pay Regularly	0
23	HN Enterprise	Pay Regularly	0
22	CSC Demo T1C and ADACOM QTSP	Pay Regularly	0
21	Default Personal CO=User	Pay Regularly	0
20	QA Enterprise Plan CO = USER	Pay Regularly	0
19	Enterprise Service Plan 60	Pay Regularly	100
17	T1C Demo	Pay Regularly	0
15	Enterprise Test Plan	Pay Regularly	50
14	Rapid LEI	Pay Regularly	0
13	AS Pay as you Go	Pay As You Go	10
12	PAdES Part 4 Signing Plan	Pay Regularly	0
11	SigningHub Partners Evaluation	Pay Regularly	0
10	Public Enterprise Plan	Pay Regularly	0

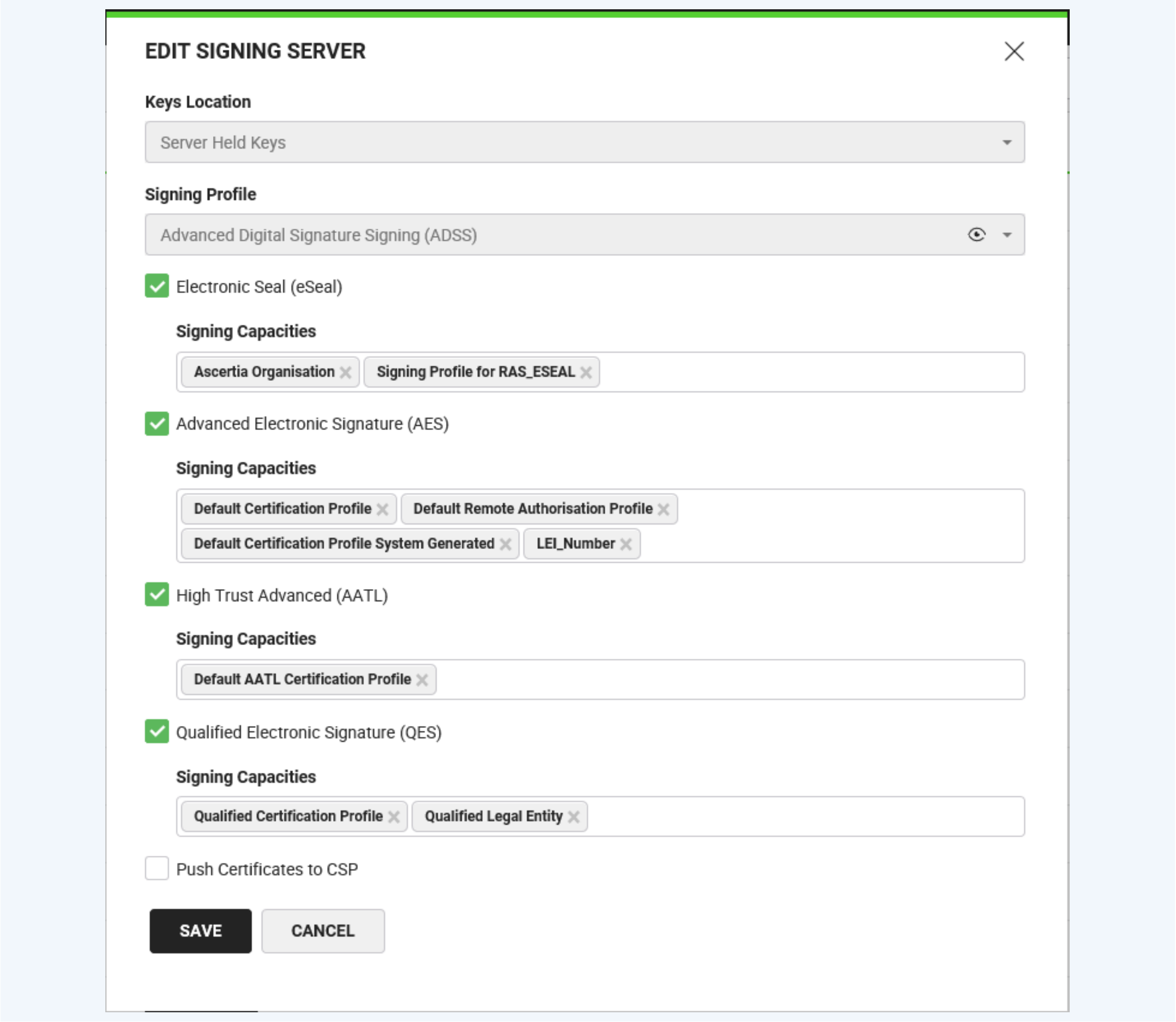
Showing: 25 / 25

EDIT SERVICE PLAN

Signing Servers

Name	Keys Location
Ascertia RAS 6.7	Server Held Keys
Adacom Trust Services	Server Held Keys
Advanced Digital Signature Signing (ADSS)	Server Held Keys
ADSS GO>Sign	Client Held Keys
T1C	Client Held Keys

Verification Profile: Default Verification Profile



EDIT SIGNING SERVER

Keys Location

Server Held Keys

Signing Profile

Advanced Digital Signature Signing (ADSS)

☑ Electronic Seal (eSeal)

Signing Capacities

Ascertia Organisation ×, Signing Profile for RAS_ESEAL ×

☑ Advanced Electronic Signature (AES)

Signing Capacities

Default Certification Profile ×, Default Remote Authorisation Profile ×, Default Certification Profile System Generated ×, LEI_Number ×

☑ High Trust Advanced (AATL)

Signing Capacities

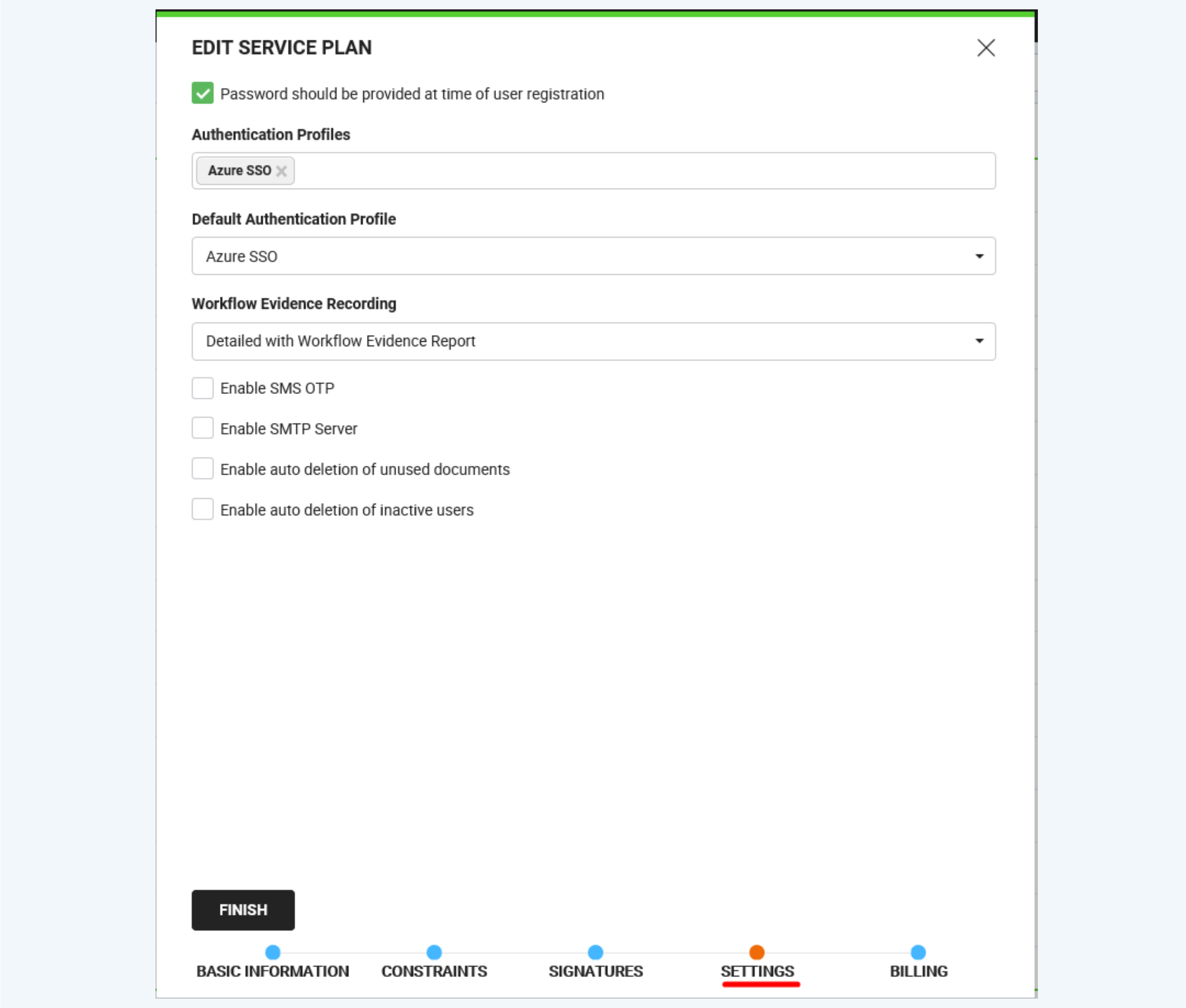
Default AATL Certification Profile ×

☑ Qualified Electronic Signature (QES)

Signing Capacities

Qualified Certification Profile ×, Qualified Legal Entity ×

□ Push Certificates to CSP



EDIT SERVICE PLAN

☑ Password should be provided at time of user registration

Authentication Profiles

Azure SSO

Default Authentication Profile

Azure SSO

Workflow Evidence Recording

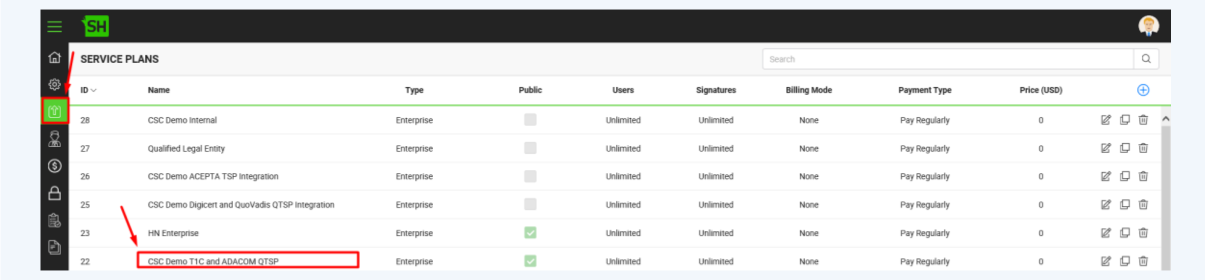
Detailed with Workflow Evidence Report

□ Enable SMS OTP

□ Enable SMTP Server

□ Enable auto deletion of unused documents

□ Enable auto deletion of inactive users



SERVICE PLANS

ID	Name	Type	Public	Users	Signatures	Billing Mode	Payment Type	Price (USD)
28	CSC Demo Internal	Enterprise	□	Unlimited	Unlimited	None	Pay Regularly	0
27	Qualified Legal Entity	Enterprise	□	Unlimited	Unlimited	None	Pay Regularly	0
26	CSC Demo ACEPTA TSP Integration	Enterprise	□	Unlimited	Unlimited	None	Pay Regularly	0
25	CSC Demo Digicert and QuoVadis QTSP Integration	Enterprise	□	Unlimited	Unlimited	None	Pay Regularly	0
23	HN Enterprise	Enterprise	☑	Unlimited	Unlimited	None	Pay Regularly	0
22	CSC Demo T1C and ADACOM QTSP	Enterprise	☑	Unlimited	Unlimited	None	Pay Regularly	0

5.4 Remote Authorisation

The Enable Remote Authorisation option previously associated with a Service Plan is now part of the Signing Profile to have all the signature types including **RAS**, **XML**, or **Office Signatures** available in one location.

The Signing Profile should be **RAS enabled** in the **ADSS server**.

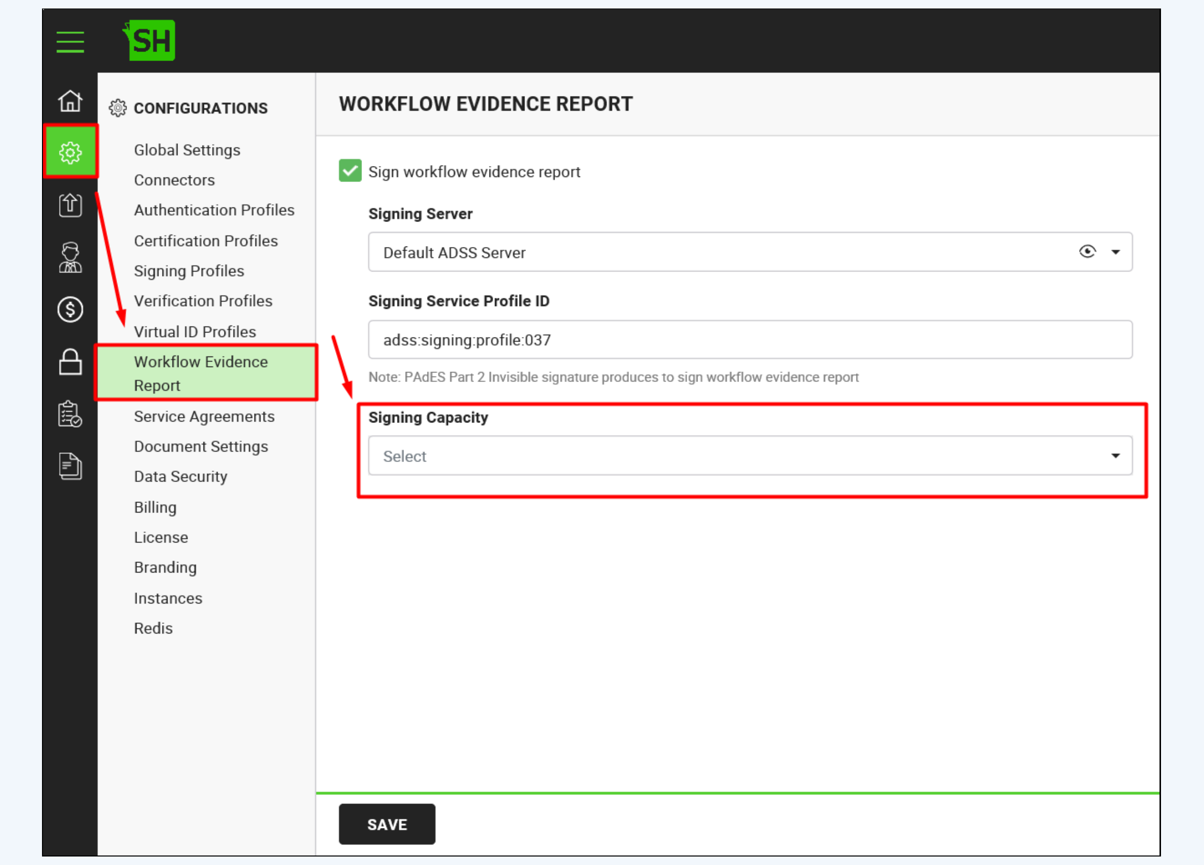
- Previously configured Remote Authorisation Signing (RAS) configuration will not work until a system administrator has reconfigured the signing profiles. Now a new Certification Profile has to be configured using “Remote Authorisation” as a “Key Protection Option” and any level of assurance other than ‘Electronic Seal, Advanced Electronic Seal or Qualified Electronic Seal’. A new Signing Profile has to be configured for RAS. Set this newly created Certification and Signing Profiles under the intended Service Plan.
- With the deprecation of Virtual Profiles, previously generated user certificates for Remote Authorisation Signing (RAS) will be converted to Custom Signing Certificates, so the users can use their already generated certificates for Remote Authorisation Signing. Previously configured Virtual ID profile name will be set as the Certificate Friendly Name.
- The “**Compute hash at signing time**” option must be turned OFF under **Advanced Settings** of Signing Profile and **User Signature Key Pair Settings** of linked SAM profile **.** SigningHub computes hash by itself and sends this hash to ADSS Server for signing.

5.5 Workflow Evidence Report Configuration

After upgrading to SigningHub 8.x.x, the Signing Server is no longer required to be selected separately for adding an invisible signature in the evidence report. The Signing Server and Signing Service Profile ID for ADSS Server have been replaced with a Signing Profile under the Workflow Evidence Report and Document Settings (Lock PDF Fields) in SigningHub Admin configurations.

Workflow Evidence Reports can now be digitally signed using eSeals. A correctly configured eSeal signing capacity must be selected, to make the Workflow Evidence Report configurations workable.

Within SigningHub Admin, select “Configurations > Workflow Evidence Report”, set the Signing Capacity drop down to the eSeal certificate you would like the Workflow Evidence Report signed with, click save once the certificate has been selected.



WORKFLOW EVIDENCE REPORT

☑ Sign workflow evidence report

Signing Server: Default ADSS Server

Signing Service Profile ID: adss:signing:profile:037

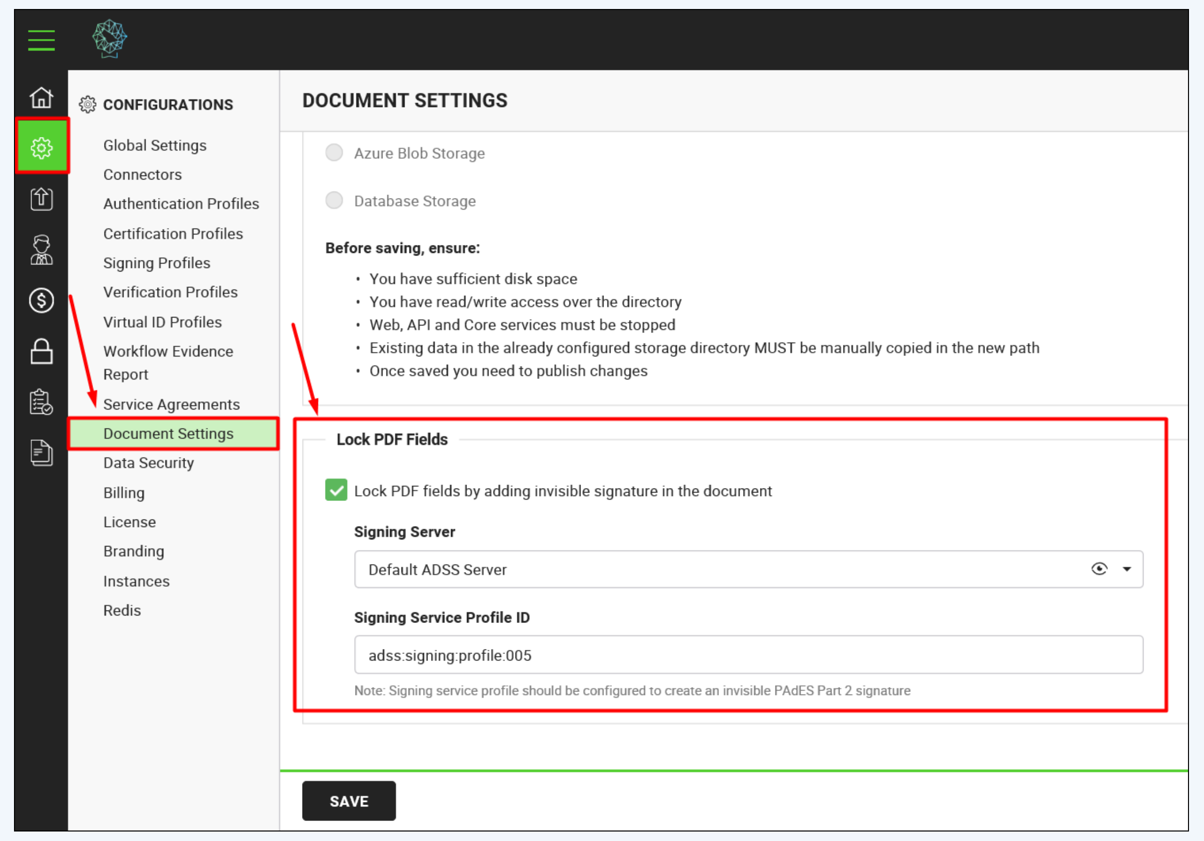
Note: PAdES Part 2 Invisible signature produces to sign workflow evidence report

Signing Capacity: Select

5.6 Configure Document Settings (Lock PDF Fields)

- To add an invisible signature in a document to lock the PDF fields, the Signing server is no longer required to be selected separately, the signing server and signing service profile ID have now been replaced with a Signing Profile, where the selected Signing Profile will be used to obtain the signing server related information.

Below is an example of an existing configuration for the Document Settings (Lock PDF Fields), where the Signing Server and Signing Service Profile ID has to be provided.



DOCUMENT SETTINGS

○ Azure Blob Storage

○ Database Storage

Before saving, ensure:

- You have sufficient disk space
- You have read/write access over the directory
- Web, API and Core services must be stopped
- Existing data in the already configured storage directory MUST be manually copied in the new path
- Once saved you need to publish changes

Lock PDF Fields

☑ Lock PDF fields by adding invisible signature in the document

Signing Server

Default ADSS Server

Signing Service Profile ID

adss:signing:profile:005

Note: Signing service profile should be configured to create an invisible PAdES Part 2 signature

Below is an example of the required changes, the signing server is no longer required to be selected separately.

6 What’s new in SigningHub 8.x.x

6.1 Enterprise Roles

Enterprise administrators will encounter significantly different UI/UX, especially when creating and managing roles. The features of the Service Plan, as highlighted earlier in this document, can be controlled for the end-users by the enterprise administrators using roles. Login with an enterprise administrator account and go to Enterprise Settings to perform the configurations explained in the following sections.

6.1.1 New Feature in SigningHub 8.x.x

- Go to **Enterprise Settings > Roles > Document Settings > Allowed Signature Fields**. The Advanced Electronic Signature (AES) is set as the **default** Level of Assurance. If a document owner specifies a Level of Assurance other than Advanced Electronic Signature and it is not configured in the role, the end-user will not be able to sign that signature field. The selected level offers the assurance provided by the Certification Authority (CA) issuing the certificate against a particular Certification Profile.

For individual users, PhontPhreaks will be used as a default font for signing.

6.1.2 Features Removed/Replaced

- Go to **Enterprise Settings > Roles > Signature Appearance**. Previously configured signature appearances will be set and PhontPhreaks will be set as the default. The Signature Appearance and Allowed Signature Fonts can be selected.
- Go to **Enterprise Settings > Roles > Signature Settings**:
  - The Witness Signing Capacities and Default Witness Signing Capacity options have been removed from Enterprise Roles. Witness signing is now covered under the Electronic Seal (eSeal) Level of Assurance.
  - The Default Signing Method has been removed; it is now dependent upon the signing capacity that is configured by the document owner requesting a signature from the recipient.
  - All the Signing Capacities are now moved under Singing Servers, which are now categorised as per the Level of Assurance. The Default Signing Capacity is also available on the Signing Server.
  - The authentication method is now applied based on the selected Signing Capacity. This can be configured under Certification Profiles in Admin configurations. There will be four major categories of Signing Capacities including:

- Electronic Signature (eSignature)
- Electronic Seal (eSeal)
- Advanced Electronic Seal (AdESeal)

- Qualified Electronic Seal (QESeal)
- Advanced Electronic Signature (AES)
- High Trust Advanced Signature (AATL)
- Qualified Electronic Signature (QES)

  The authentication method will depend on the signing capacity. For instance, Signing Capacities selected for Remote Authorisation will have the authentication method set to **"Authorisation via Mobile App"** and cannot be updated.

- The OTP via SMS option will only appear under the authentication method if the OTP has been enabled in the Service Plan previously, otherwise, it needs to be configured under the Service Plan. OTP via SMS is no longer available under Primary authentication and it can now only be used as a secondary authentication method. It is not possible to set "No Authentication" as a primary Authentication Method and "OTP vis SMS" as a Secondary Authentication to only use OTP authentication.
- Options for web browsers and mobile apps are no longer available. The signing server settings will reflect these components.

6.2 Personal Settings

Users will also see new options available in their personal settings.

6.2.1 New features in v8.x.x

Default Level of Assurance is the new option that can have two different cases:

- For Enterprise users:
  - If “Electronic and Digital Signatures” were allowed before the upgrade (i.e. 778x), then the “eSeal” and “AES” will be allowed under personal settings where eSeal will be set as the default Level of Assurance.
  - If only “Electronic Signature” was allowed before the upgrade (i.e. 778x), then the “eSeal” will be allowed under personal settings and set as the default Level of Assurance.
  - If only “If Only “Digital Signature” was allowed before the upgrade (i.e. 778x), then the “AES” will be allowed under personal settings and also set as the default Level of Assurance.
  - If “Electronic and Digital Signatures” both were not allowed before the upgrade (i.e. 778x), then the “eSeal” will be allowed under personal settings and set as default Level of Assurance.

- For Individual users:
  - All the Levels of Assurance will be allowed (configured under SigningHub Admin), and “*Electronic Signature”* will be set as a default under personal settings.

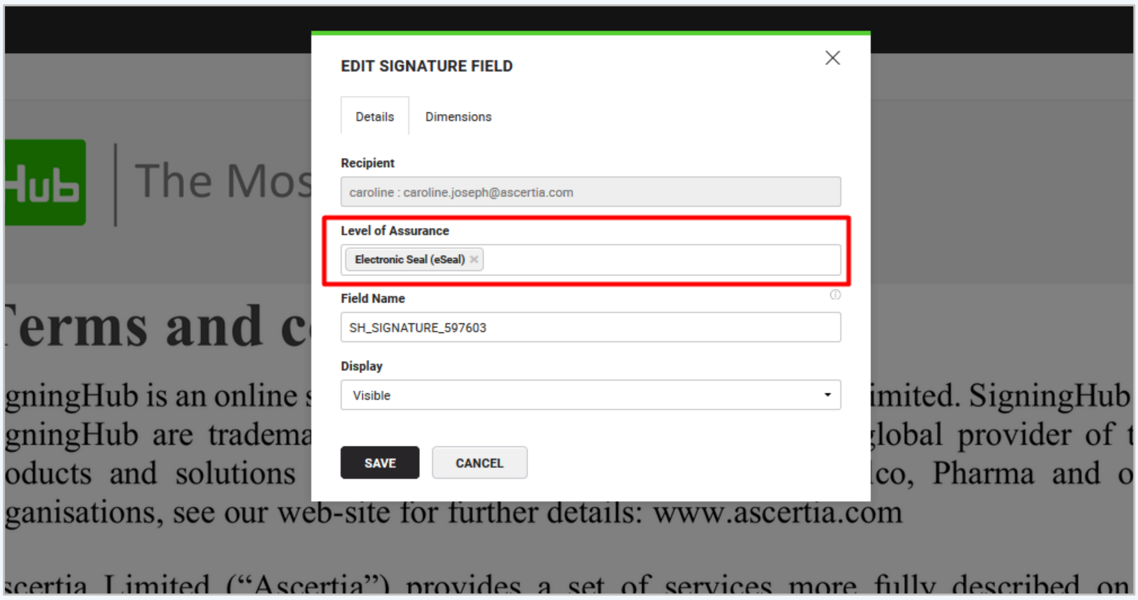
- It is possible to set a required Level of Assurance on the signature field in draft mode when preparing a document Workflow.
- Templates that are already created, while editing those templates or upon sharing the Digital Signature fields, now have the “Advanced Electronic Signature (ASE)” as a Level of Assurance and for Electronic Signature fields “Electronic Seal (eSeal)” will be set as a Level of Assurance.

6.2.2 Features Removed/Replaced

Go to **Personal Settings > Signature Details**. Signing Methods for web browsers and Mobile Apps are no longer available and are now applicable as per the signing server configurations.

6.3 Document Owner View: Document in Draft Mode

As a document owner, when a user drops a signature field on the document the field will have the same Level of Assurance as it’s set in the user’s personal settings. You can change or add further assurance levels that will be allowed to a recipient to sign with. Click ⚙ **Manage Recipients** in the signature field and select these from the available list.



EDIT SIGNATURE FIELD

Recipient: caroline : caroline.joseph@ascertia.com

Level of Assurance: Electronic Seal (eSeal)

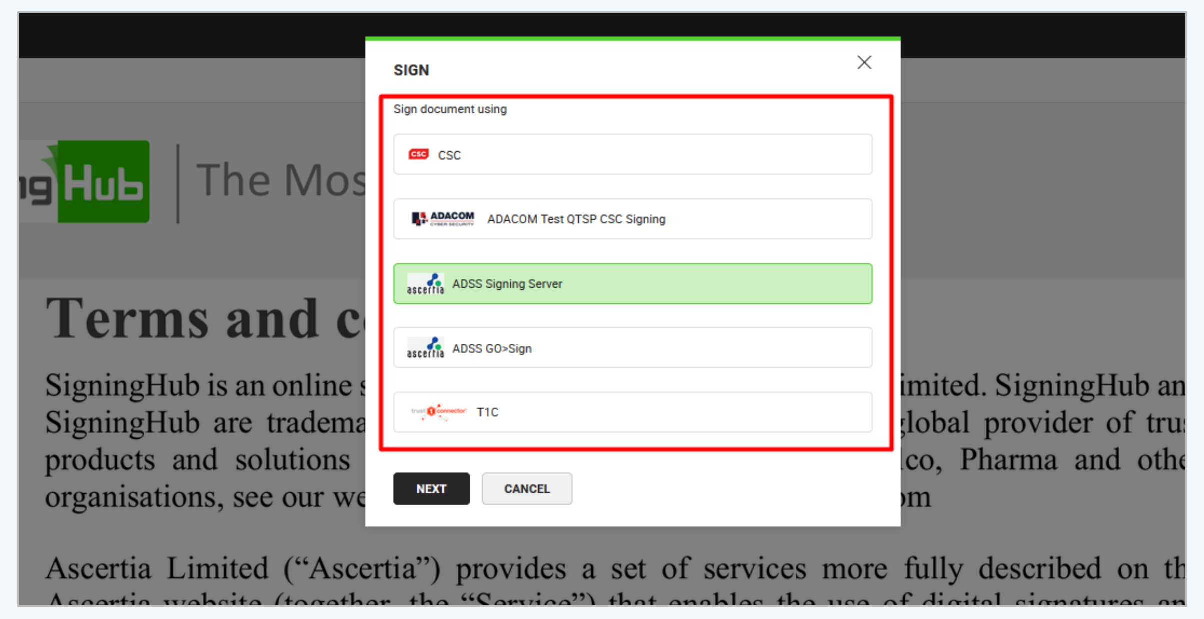
Field Name: SH_SIGNATURE_597603

Display: Visible

6.4 Document Recipient View: Document in Pending Mode

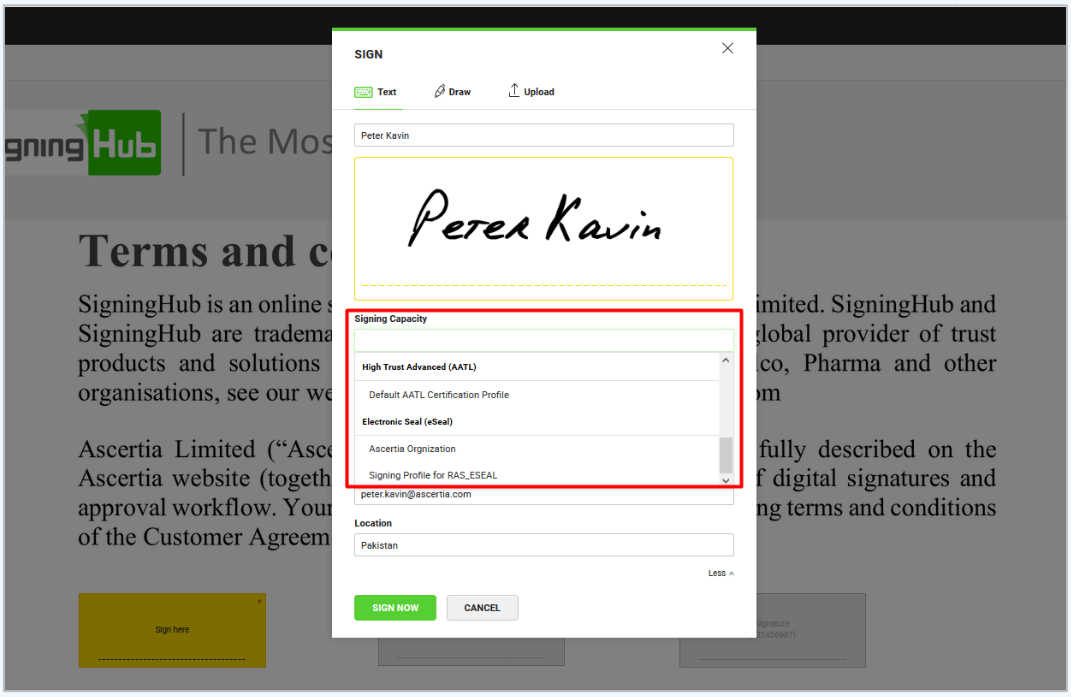
Once a document is shared with the recipient, the recipient will be able to sign the document with only those certificates whose Level of Assurance matches with the configured Level of Assurance in the signature field. The Signing Server options will appear as configured in the recipient's Service Plan and Enterprise Roles settings.

Signing Capacities will appear for the user as per the Level of Assurance set by the document owner. Selecting the Singing Server will display all the singing servers including Servers and Client Held Keys.



After selecting a signing server, the next window will display the Singing Capacity. These are categorised based on the Level of Assurance.

1. Select the required Signing Capacity from the list.



Peter Kavin

Signing Capacity

High Trust Advanced (AATL)

Default AATL Certification Profile

Electronic Seal (eSeal)

Ascertia Orgnization

Signing Profile for RAS_ESEAL

peter.kavin@ascertia.com

Location

Pakistan

2. Click on the **SIGN NOW** button to sign a document and complete the Workflow. An authentication window may appear if it was set against your selected signing capacity.

7 Summary

Once SigningHub is upgraded to version 8.x.x and all required configurations have been performed, a signing Workflow can be executed.

A document owner will create a new Workflow, upload the document to be signed, and then add a signature by assigning the Level of Assurance according to the Enterprise Role configured under Document Settings.

The document recipient can sign the document by selecting a Signing Server from the multiple servers available. The recipient will also choose a Signing Capacity based on the assigned Level of Assurance and is subject to the Service Plan/Enterprise Role of the recipient. The Workflow concludes once a document is signed.

The document owner can use the Workflow History to view the Signing Capacity and Level of Assurance that were selected while signing a document.

8 Frequently Asked Questions

8.1 How to reconfigure RAS after upgrade from 778x to 8.x.x?

The Enable Remote Authorisation option previously associated with a Service Plan is now part of the Signing Profile to have all the signature types including RAS, XML, or Office Signatures available in one location.

Signing Profile should be **RAS** The **enabled** in **ADSS server**.

1) Previously configured Remote Authorisation Signing (RAS) configurations will not work until a System administrator has reconfigured the profiles. Now a new Certification Profile has to be configured using “Remote Authorisation” as a “Key Protection Option” and “QES” as a “Level of Assurance”. There must be a new Signing Profile that has to be configured for RAS. Set this newly created certification and Signing Profiles under the intended Service Plan.
2) With the deprecation of Virtual Profiles, previously generated user certificates for Remote Authorisation Signing (RAS) will be converted to Custom Signing Certificates, so the users can use their already generated certificates for Remote Authorisation Signing. Previously configured Virtual ID profile name will be set as the Certificate Friendly Name in the database.

8.2 How will the “Witness Signatures” feature work once it’s upgraded to SigningHub 8.x.x?

- In the previous versions of SigningHub, witness signatures were managed in Signing Profiles and a default alias was set within the **ADSS Server**, which was used for witness signatures. This same configuration has been aligned with the rest of the certificates in SigningHub v8.x.x. These configurations are now available in Certification Profiles instead of Signing Profiles.
- In SigningHub 8.x.x the installer will now automatically create new Certification Profiles against all existing witness signature profiles. The installer will also add the “**_ESEAL**” postfix at the end of the profile name for identification purposes. This will help the administrator to search and shortlist the Certification Profiles.

Here are the steps to manually reconfigure eSeal that replaced Witness Signatures, which are easy to if you have the previous version of SigningHub accessible on the localhost URLs:

1. Take the Certification Profile name from the SigningHub 8.x.x instance and search the same name in the previous version of SigningHub’s Signing Profiles. Remember to leave out the “_ESEAL” term while searching on the old version

as this term is added by the system installer to easily identify the profiles, which require manual configuration.

2. Once you find the profile name in the previous version of SigningHub, copy this ADSS Signing Profile name/ID and search for this same ADSS profile name/ID in ADSS Server.

3. Go to **Ascertia ADSS Server -> Signing Service** and select the corresponding ADSS Signing Profile and copy the default certificate configured in this Signing Profile.

4. This default certificate is created under ADSS Server Key Manager. In **Key Manager**, go to **Service Keys > Search** to view the key alias that was copied from the ADSS Signing Profile. Click on the key alias and copy the value of the certificate alias.

5. Now paste the certificate alias in the SigningHub 8.x.x Certification Profile that you initially selected in the first step.

> Select the ADSS server from the drop-down list, where the certificate alias resides. SigningHub administrators must select one Certification Profile that is associated with Electronic Seal (eSeals) as the default profile. This profile will be used by all the recipients who are expected to complete an Electronic Seal (eSeal) but do not have the Electronic Seal (eSeal) Level of Assurance configured in their subscribed Service Plans. This is applicable for Advanced Electronic Seal (AdESeal) and Qualified Electronic Seal (QESeal).

8.3 Which Levels of Assurance will be available for an individual user?

For Individual Users, all the Levels of Assurance will be allowed under personal settings (that are configured under SigningHub Admin), and “Electronic Signature (eSignature)” will be set as a default under personal settings.

To make the witness signatures workable for the individual users, the system admin has to remove Electronic Signature (eSignature) and allow Electronic Seal (eSeal) under the user’s Service Plan.

8.4 How to set up Signature Appearance Designs for an individual user?

For an individual user, all the signature appearances will be available. The System Admin needs to remove those signature appearances from the Service Plan, which are not required for the individual users.

> Custom signature appearance designs (if any), have to be moved manually to the following installation directory: ***{{deployment_directory}}\default\appearances***