ADSS WebRA Server – Release Notes

This document provides a high-level description of the new features in each release of ADSS WebRA Server.

ADSS WebRA Server 2.3.0 — September 2021

New Features

- SAML authentication using the standard SAML 2.0
  - Customers deploying ADSS Web RA Server can now use SAML to authenticate users accessing the enrolment portal to request and manage their certificates.
- HMAC Data Integrity
  - ADSS Web RA Server now supports the ability to provide HMAC security for all log entries recorded to the ADSS Web RA Server database, this helps to prevent tampering of the logs and provides validation of information logged by the server.
- SigningHub 7.7.9 Compatibility
  - ADSS Web RA now supports SigningHub 7.7.8 to onwards.
- Digital Onboarding
  - ADSS Web RA Server now supports the ability to register, enrol and vet a user for a digital certificate via an easy-to-use mobile application. ADSS Web RA Server digital onboarding walks a user through a simple enrolment process where they use their mobile device to capture images of their identity documents, capture an image of themselves and will perform facial recognition against their identity document and will perform a liveliness check to verify their identity prior to the issuance of a digital certificate

Improvements in this release

- Performance Improvements
  - ADSS Web RA Server has had several improvements made to improve performance.
- Improve Log file of Web RA Web, Admin
  - ADSS Web RA Server logging has been improved for Info and Debug to improve operator troubleshooting.

ADSS WebRA Server 2.3.0 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6 and above
SigningHub	v7.7.8 and above
ADSS Server	v6.6.0.17 v6.7 v6.8.0.5

ADSS WebRA Server 2.2.0 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.8
SigningHub	v7.7.8
ADSS Server	v6.6 v6.7 v6.8.0.2*
Note: Web RA 2.2 now supports the CMPv2 enrolment protocol for device certificates and can also be used to communicate with Certificate Transparency Log Servers, this functionality requires ADSS Server 6.8.0.2.	

ADSS WebRA Server 2.1.3.3 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6
SigningHub	v7.7.8
ADSS Server	6.6.0.17

For further details contact us on sales@ascertia.com or visit www.ascertia.com.

ADSS WebRA Server 2.2.0 — May 2021

New Features

- CMP Protocol is implemented for device enrolment
  - CMP Protocol is now implemented for device enrolment**.**
- WebRA application will communicate to CT Logs server on behalf of ADSS Server
  - WebRA application can now communicate to CT Logs server on behalf of ADSS Server
- WebRA online documentation
  - Web RA now contains links to the online administrator and user manuals.
- Enrolment without vetting
  - Web RA now supports manual enrolment for certificates without the need to display a vetting form.
- Revoke without vetting
  - Web RA now supports revocation of certificates without the need to display a vetting form
- System information page
  - Web RA now includes a page that displays information about Web RA version, Operating System, database server etc to authorised operators.
- Dual control for configuration changes
  - Web RA now supports dual control for configuration changes, when enabled, an additional administrator is required to authorise configuration changes.
- Sample data is now available as an option when deploying Web RA.
  - Sample data includes, default connectors, default service profile, subscriber agreement, service plan and other settings.
- Device Certificate change of ownership
  - Device certificates can now be transferred from one person to another person within an enterprise. The new device owner can renew, revoke or delete device certificates.
- Renew certificate can now be controlled via policy

  Certificate renewal can now be enabled or disabled via new policy controls in Web RA

Improvements in this release

- Streamlined Certificate Renewals
  - It is now possible to renew the certificate directly without admin approval if vetting is not enabled in the ADSS Service Profile.
- WebRA admin portal session expiry is now
  - The Web RA administrator operator session timeout is now configurable from general settings.
- PFX password regeneration
  - It is now possible to regenerate new PFX password and download new PFX file.
- Organization name is now logged when validating CSR's
  - If a CSR contains an invalid organization name Web RA now records this in the debug logs to help identify the error.
- Access control on certificate renewal request for enterprise RAOs and Admin RAOs
  - Enterprise RAOs can view and approve certificates in the renewal request and approve request lists for allowed enterprises
- Logging Improvements
  - Improvements have been made to make logging information easier to interpret.
- API Updates
  - User management APIs are now available for registration, update, forgot password and invitation accept/decline
- SCEP Multitenancy Improvements
  - It is now possible to configure multiple SCEP profiles in the service plan.

- CSR Based Enrolment improvements
    - Web RA now implements a policy to request a user loads a CSR instead of relying on the settings in the ADSS Server certification profile.
- UI Improvements for selecting enrolment profiles
    - Web RA now provides separate selections for different enrolment profiles to provide a better user experience when creating different identity types during enrolment.
- In Service Plan and in ADSS Service Profiles now “Advance Settings” option is at the last step
    - In Service Plan ‘Advance Settings’ tab is moved to the last Step from middle Step
- Implement route guards on Web and Admin portal to resolve the redirection issues and also improve the performance and security of the application
    - Improvements are made in the Web and Admin portal performance, security and resolve the redirection issues by implementing route guards
- Pagination in listing API's
    - Implement pagination in listing API’s for GET all requests and GET all certificates API’s
- JWT access token expiry time is now configurable and refresh token is also implemented
    - Now DEK will be used as JWT signing key and JWT access token expiry time is now configurable and refresh token is also implemented.
- Sample data for application is now optional while deploying the application. Sample data includes default connectors, default service profile, subscriber agreement, service plan and some other settings which are not required to initiate the application
    - Now sample data e.g. default connectors, default service profile, subscriber agreement, service plan and some other settings for the application will be optional while deploying the application.
- Proper object for OTP authentications will be shown in case of New, renew, revoke requests in response of get profile by id API
    - Now proper object for OTP authentications will be shown in case of new, renew and revoke requests in response of GET profile by ID in API.

ADSS WebRA Server 2.2.0 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.8
SigningHub	v7.7.8
ADSS Server	v6.6 v6.7 v6.8.0.2*
Note: Web RA 2.2 now supports the CMPv2 enrolment protocol for device certificates and can also be used to communicate with Certificate Transparency Log Servers, this functionality requires ADSS Server 6.8.0.2.	

ADSS WebRA Server 2.1.3.3 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6
SigningHub	v7.7.8
ADSS Server	6.6.0.17

For further details contact us on sales@ascertia.com or visit www.ascertia.com.

ADSS WebRA Server 2.1.3.2 October 2020

New Features

- Implementation of API Resource (Authenticate, Certificates, Requests)

- Instant revoke in case of no vetting from ADSS Web RA User Portal

ADSS WebRA Server 2.1.3.2 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6
SigningHub	v7.7.8
ADSS Server	6.6.0.17

For further details contact us on sales@ascertia.com or visit www.ascertia.com.

ADSS WebRA Server 2.1.3.1 October 2020

New Features

- Application now support syslog servers for better logging of the application
- Implement more features of APIs for certificate requests
- Application handles the invalid configuration of KEK (Key encryption key) in ADSS and show a proper error page
- Connection strings are now encrypted for API instances
- Log files are now configured to be archived after 30 days by default, configurations can be updated for NLog in configuration files

ADSS WebRA Server 2.1.3.1 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6
SigningHub	v7.7.8
ADSS Server	6.6.0.17

For further details contact us on sales@ascertia.com or visit www.ascertia.com.

ADSS WebRA Server 2.1.3 September 2020

New Features

- Subscribers agreements can now be configured in certificate profiles and have been made independent of vetting forms. Previously subscriber agreements were linked to vetting forms, Enterprises had to configure a vetting form in order to apply a subscriber agreement to their certificate profile.
- ADSS Web RA Server can now be installed and integrated with the Ascertia SigningHub Enterprise application, this integration enables customers to perform vetting of users who are enroling, provides the ability to create certificates with all of the subject distinguished name elements supported by ADSS Server and then have the user and their certificates automatically created in SigningHub Enterprise.
- Administrators can now perform vetting on enterprises that have been registered via the user portal, this provides greater control over enterprise creation.
- ADSS Web RA Server dashboards now dynamically adjust in size to accommodate the information displayed that needs to be displayed.

- Administrative UI Improvements. The display of certificate profiles within service plans have been updated to enable administrators to easily distinguish between each profile.
- Improved new API calls and associated documentation for the following API's:
  - /account
  - /virtualid
  - /request/revoke
  - /desktopsigning/certificate/provision/{request_id}
  - /request/submit
- Default SMTP connector support. ADSS Web RA Server will now use the default SMTP connector if no SMTP connector is defined within a service plan.

ADSS WebRA Server 2.1.3 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6
SigningHub	v7.7.8
ADSS Server	6.6.0.17

For further details contact us on sales@ascertia.com or visit www.ascertia.com.

ADSS WebRA Server 2.1.2.4 November 2020

New Features

- Session timeout setting is implemented for Admin portal
- On refreshing ADSS service profile authentication profile will not be reset

ADSS WebRA Server 2.1.2.4 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6
ADSS Server	6.6.0.17

For further details contact us on sales@ascertia.com or visit www.ascertia.com.

ADSS WebRA Server 2.1.2.3 September 2020

New Features

- Proper error page is displayed and response is logged in debug logs while accessing Web RA admin and web portal if ADSS DEK encryption is invalid.

ADSS WebRA Server 2.1.2.3 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6
ADSS Server	6.6.0.17

For further details contact us on sales@ascertia.com or visit www.ascertia.com.

ADSS WebRA Server 2.1.2.2 August 2020

New Features

- Support for unlimited license now implemented under Web RA
- Enhanced security and remove vulnerability issues across the application
- Improved performance across application

ADSS WebRA Server 2.1.2.2 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6
ADSS Server	6.6.0.17

For further details contact us on sales@ascertia.com or visit www.ascertia.com.

ADSS WebRA Server 2.1.2.1 August 2020

New Features

- Enhanced security and remove vulnerability issues across the application
- Improved performance across application

ADSS WebRA Server 2.1.2.1 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6
ADSS Server	6.6.0.17

For further details contact us on sales@ascertia.com or visit www.ascertia.com.

ADSS WebRA Server 2.1.2 July 2020

New Features

- On uploading a CSR, application verifies if a certificate is already issued against this public key or not, making sure that accepting CSR is to generate the certificate is safe and secure
- If a public key is reused, the application shows an error and provide a link to the certificate where the public key is already used, to make the decision making easier for the RAOs
- Subject Distinguished Names are not mandatory to fill
- Admin RAO can configure the application to enforce signed requests between the application and corresponding ADSS Server as a CA
- RAO has a better user experience by having predefined options to decline a certificate request, RAO can still add custom messages and reasons to audit and communicate the details
- Similarly, RAO has a better user experience by having proper confirmation messages before approving a certificate request
- Admin RAO and enterprise RAO can change the status of the enterprise user to Block, Suspended, and Active to improve user management within the application and provide more control to the admin RAO and enterprise RAO

- Certificate issued by the face to face method are attached to the enterprise that is selected during the process, enterprise RAO can now have a control over those certificates' lifecycle

ADSS WebRA Server 2.1.2 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6
ADSS Server	6.6.0.17

For further details contact us on sales@ascertia.com or visit www.ascertia.com.

ADSS WebRA Server 2.1.1 June 2020

New Features

- While having a CSR uploaded, application verifies if the public key is already used to generate a certificate and throws an error
- Certificates can also be searched based on the search criteria of enterprise name
- Second factor authentication of OTP is provided on login, create certificate request, certificate renewal request and on certificate revocation request
- Licensing is introduced in the application to limit the certificate generation
- Admin RAOs can now use branding to change the colour scheme of user portal and admin portal
- Admin RAO can now change the mobile number of enterprise owner
- Admin RAO can now only approve the certificates which are flagged in the certificate profile for Admin RAO, enterprise member certificates are to be vetted only by the enterprise RAO
- Admin RAO can change the status of the enterprise to Block, Suspended, and Active, improving the better management of the enterprises within the application
- New certificate request statuses are introduced for renew and revoke from pending to renewal pending and revocation pending
- Newly uploaded CSR files are now verified by the application for signature verification, key algorithm, Weak Debian key verification, Key length verification
- Renewal of certificate is removed from the application

ADSS WebRA Server 2.1.1 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6
ADSS Server	6.6.0.17

For further details contact us on sales@ascertia.com or visit www.ascertia.com.

ADSS WebRA Server 2.1 April 2020

New Features

- Improved installer is provided to improve the installation experience for on premise deployments. Installer will help to create sites on local IIS, running database scripts, configuring default TLS certificates
- Application now contains improved controls over the privacy and data collection maintaining the compliance with the GDPR
- For certificate requests approval, dual control mechanism is implemented. No certificate requests can be approved by a single RAO having dual controls enabled in the application
- Users can export PFX files for encryption certificates to comply with key recovery policies in certain regions
- Device enrolment with SCEP protocol is enhanced to support bulk registration of devices from the user interface, later these devices can enrol themselves using SCEP protocol

- Device enrolment also supports configurations for challenge password. Administrators will be able to configure the service for no password, a fixed password or random passwords for every device enrolment
- Renewal and revocation of certificates is not supported for certificates that are enrolled for virtual IDs, desktop remote signing or device certificates from the user interface
- User interface is optimized for mobile browsers to interact with the application on the go
- New and fresh look of user interface for user portal as well as the admin portal
- Administrators can now disable the registration from the user's portal by a simple configuration to control the registration of the users only from the administration portal

ADSS WebRA Server 2.1 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6
ADSS Server	6.6.0.17

For further details contact us on sales@ascertia.com or visit www.ascertia.com.

Web RA v2.0 January 2019

- An authorized operator who can be an administrator or an Enterprise RAO (Registration Authority Operators) has a separate interface to manage the certificate management service, protected by SSL and password authentication
- Administrators can configure connectors, profiles and service plans to operate the service including SMTP servers and SMS OTP gateways
- Administrators can add subscriber agreements for each type of certificate request
- Administrators can create dynamic vetting forms with various types of questions and different type of input fields for end users to fill in the required information
- Google CAPTCHA is implemented to secure sensitive user forms from automated attacks
- Administrator RAOs or Enterprise RAOs are able to review and approve pending certificate requests if the vetting is turned on
- An OEM version of ADSS Server is used to handle all certificate requests, harnessing the power of ADSS server and certificate generation features, working with one or more external CAs
- ADSS CSP is a service that allows to sign the documents using a desktop Application VCSP. The Web RA enables end users to enrol them to use CSP services with the desktop application.
- Remote authorization enrolment can be configured from Web RA
- Web RA now supports the SCEP protocol for device and application certificate enrolment
- Web RA administrator interface can also be used for face to face registration and enrolment
- Administrators can enrol Enterprise RAOs from administrative portal. End users can also enrol themselves in the Web RA via the user's portal and activate their account using the link sent to their email address
- Suitably authorised Enterprise RAOs can add or invite enterprise members individually or in bulk
- One Enterprise RAO can manage requests from more than one enterprise and their members, adding multi-tenancy support to the application
- Application contains a detailed account and access control management from administrator's portal. Application can have many administrators all with different roles and rights and can vet requests from only allowed list of enterprises.
- Web RA can be deployed in a load balanced environment to support high volume requests and throughput
- Terminated Service Provider (TSP) can be maintained as a list, where Web RA administrators can receive requests to manage the certificates on behalf of a terminated service provider. Mainly these operations involve revoking a certificate
- User portal now supports both password and OTP based login authentications
- One user can become part of multiple enterprises and request certificates using the enterprise allowed profiles

- Detailed audit logs are maintained on both administrator's and user's portal
- Domain verification for DV, OV and EV SSL certificates supported in Web RA using TXT records or by uploading a file with verifiable content
- Support of rest-based APIs for certificate management is available via secure API keys created for enterprises

ADSS WebRA Server 2.1 Product Compatibility

Product	Version(s)
Go>Sign Desktop	v6.6
ADSS Server	6.6.0.17

For further details contact us on sales@ascertia.com or visit www.ascertia.com.