Release Notes

ADSS Web RA Server 2.9.3

Document Issue 1.0

July 2024

This document provides information about Ascertia ADSS Web RA Server. Browse through the following topics to find out about new features, product enhancements, improvement, known issues, and limitations for this release.

For information related to tested 3rd party components such as operating systems, database servers, and Hardware Security Modules, please review Ascertia Platform Support, this can be found here: https://manuals.ascertia.com/WebRA-v2.9.3/ADSS-WebRA-Server-Platform-Support.pdf

Product Enhancements

- **OpenID Connect PKCE Support**

  Jira ID – (WRA- 14264)

  ADSS Web RA Server's OpenID connect authentication scheme has been enhanced to support PKCE. OIDC PKCE is designed to enhance security by preventing CSRF and authorization code injection attacks. Within Web RA Server, OpenID connect is used to authenticate users, and to perform additional authentication during certificate renewal and certificate revocation. User registration also supports auto-registration of Virtual ID and SigningHub account, certificate generation and auto-provisioning Virtual ID certificate to SigningHub.

- **Enterprise Branding**

  Jira ID – (WRA- 13174)

  Web RA Server now supports enterprise level branding, operators can now offer a fully branded user experience to Web RA Enterprises. Web RA can now be fully branded and integrated with an organisation or trust service provider corporate brand.

- **Authentication Updates.**

  Jira ID – (WRA-13847)

  ADSS Web RA Server authentication logic has been updated, operators now have more control and flexibility in managing authentication. Enterprises owners can now set the default login authentication mechanism and registration preferences for their users.

Improvements

- **Display chain within Web RA certificate viewer**

  Jira ID – (WRA- 14756)

  The full certificate chain including intermediate and root certificates are now displayed within the Web RA certificate viewer.

ADSS Web RA Server 2.9.2

New Features

- **Certificate Locator**

  Jira ID – (WRA- 12051)

  Introducing ADSS Web RA Certificate Locator, this release of ADSS Web RA Server adds support for operators to scan network hosts and local CAPI and Java key stores to locate digital certificates that can then be manually or automatically sent to Web RA Server. Web RA Server now provides the ability for operators to assign newly discovered certificates to Web RA users to enable automatic email notification for certificate expiry events, or to enable certificate owners to configure Web RA to start managing the certificate using an existing mechanism such as SCEP, ACME, EST etc. Web RA users can assign, manage, renew, and revoke certificates that have been assigned to them via the Web RA user portal. Users can view external certificate statistics from the dashboard and can perform sorting, modifications, advanced search, and reporting on certificates if allowed in their user role.

- **Certificate Linting Reports.**

  Jira ID – (WRA- 12876)

  Web RA now enables users to generate a report on certificates to check for consistency with standards, policy and guidelines. Web RA Server will inform users if certificates are not compliant with the following linting sources:

  - CA/Browser Forum EV SSL Certificate Guidelines

  - ETSI ESI

  - Mozilla's PKI policy

  - Apple's CT policy

  - Various RFCs (e.g. RFC 5280, 6818, RFC 4055, RFC 8399

Improvements

- **ACME external binding.**

  Jira ID – (WRA- 14321)

ADSS Web RA Servers ACME implementation has been updated, when the external account binding is set to None, Web RA no longer requires users to create a request in Web RA. Web RA now allows operators to define a default certification profile for ACME client within a user's role, this will be used by ACME clients when a request uses just a user's email address in the request.

- **Net Core Upgrade.**

  Jira ID – (WRA- 14488)

  ADSS Web RA now supports .Net core 8.0

- **Regular Release Uninstaller.**

  Jira ID – (WRA- 14034)

  The ADSS Web RA Server installer has been improved to enable a regular release to be uninstalled from 2.9.2 onwards.

ADSS Server 2.9.1

New Features

- **Regular Release via Installer**

  Jira ID – (ADSS-13190)

  Users can now install regular release updates through the installer in ADSS Web RA Server.

  Simple User Self-Registration Portal

  Jira ID – (ADSS-13041)

  ADSS Web RA Server now allows users to register via citizen ID as the unique identifier through APIs. User registration through APIs also supports auto-registration of Virtual ID and SigningHub account, certificate generation and auto-provisioning Virtual ID certificate to SigningHub

Improvements

- **Upgrade to Angular 16**

  Jira ID – (ADSS-13330)

  ADSS Web RA Server is now upgraded from Angular 15 to Angular version 16.

Technical Support

If Technical Support is required, Ascertia has a dedicated support team. Ascertia Support can be reached/accessed in the following ways:

Website	Ascertia Community Portal
Email	support@ascertia.com
Knowledge Base	Ascertia Community Portal

In addition to the free support services detailed above, Ascertia provides formal support agreements with all product sales. Please contact sales@ascertia.com for more details.

Premier Success Services

The Ascertia Premier Success team assists business around the world to design, deploy, and maintain Ascertia solutions. We offer a wide range of services to assist you with our e-business solution this includes, planning and systems architecture, installation, system integration, deployment support, and custom software development.

Whether you choose to operate your Ascertia solution on-premise, via an Ascertia Trust Service Provider, or via Ascertia Hosted Services, the Ascertia Premier Success Team can design and implement the right solution for you. For more information about Ascertia Premier Success please visit our Web site at: https://www.ascertia.com/