CertAgent/Dhuma 8.0.0.2 Release Notes

/***\

Information in this document is subject to change without notice and does not represent a commitment on the part of Information Security Corporation. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the agreement. The purchaser may make one copy of the software for backup purposes. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose other than the purchaser's personal use without the prior written permission of Information Security Corporation.

CertAgent/Dhuma is commercial computer software and, together with any related documentation, is subject to the restrictions on U.S. Government use as set forth below.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software Clause at DFARS 52.227-7013. "Contractor/manufacturer" is Information Security Corporation, 1100 Lake Street, Suite 248, Oak Park, IL 60301, U.S.A.

CertAgent is a registered trademark of Information Security Corporation and is protected by U.S. Patent No. 5,699,431

This document was last modified on: March 22, 2024

***/

Table of Contents

1 Version 8.0.0.2

1.1 Changes

1.1.1 Added a 250 MB minimum free disk space requirement to start and operate CertAgent/Dhuma.

1.2 Bug Fixes

1.2.1 Corrected database fatal error handling.

1.2.2 OCSP requests are now rejected when CertAgent/Dhuma shutdown is pending.

2 Version History

2.1 Version 8.0.0.1

2.1.1 Bug Fixes

2.1.1.1 Intermediate certificates without the cRLSign key usage bit are now properly rejected when validating certificate paths.

2.2 Version 8.0.0.0

2.2.1 Changes

2.2.1.1 Updated Apache Tomcat to 9.0.84.

2.2.1.2 Java 17.0.8 or above is now required.

2.2.1.3 Supports TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ciphersuites only.

2.2.1.4 Removed support for RSA PKCS#1v1.5 encryption/decryption. Supports RSA OAEP encryption/decryption only if an RSA system credential is used.

2.2.1.5 Updated NIAP Conformance options:

- Removed the ‘Disable EST RA via Basic Authentication’ and ‘Disable RAMI Management of EST Users’ options.
- Changed the ‘Accepting Certificate Requests using SHA1, SHA-256, SHA-384, and SHA-512 only’ option to ‘Accepting Certificate Requests using SHA-256, SHA-384, and SHA-512 only’.
- Added a ‘Disabled Dhuma API’ option.

2.2.1.6 Removed the SHA-1 signature support:

- The previously configured SHA-1 option will change to SHA-384 automatically.
- Certificate requests, certificates and CRLs with the SHA-1 signature are now rejected.

2.2.1.7 Added a local CA policy for EST users:

- the EST username matches either the CN in the request’s subject DN or the EST username matches a name in the request’s requested subjectAltName and the username/password combination hasn’t already been used to obtain a certificate,
- the EST username has no limitations on issuance,
- the EST username is limited to issuing an unlimited number of certificates for some period of days, or
- the EST username is limited to issuing some number of certificates.

2.2.1.8 EST users can now be managed via RAMI.

2.2.1.9 Updated CACLI:

- Added a ‘-gentlskey’ option to generate a TLS key pair and a certificate request.
- Added an ‘-importtlscerts’ option to import the issued TLS certificate, its chain and apply the new TLS credential to the system.
- Added an ‘-applytlskey’ option to apply an existing TLS credential to the system.
- Added a ‘-gensyskey’ option to generate a new system credential.
- Added an ‘-initialize’ option to generate a new root CA and a set of role credentials.

2.2.1.10 Dhuma now supports an admin audit log query via DBAccess.

2.2.1.11 Dhuma now supports OCSP requests with the hash of issuer’s public key using SHA-384 or SHA-512 in addition to SHA-1 and SHA-256.