

Release Notes

dataFEED Secure Integration Server

Version	Date	Release Notes
V1.30.0	21.09.2023	<p>New Features:</p> <ul style="list-style-type: none"> • MQTT functionality, with the following key features supported: <ul style="list-style-type: none"> ○ Up to 25 connections (tcp/ssl/ws/wss protocols) ○ Multiple MQTT authentication settings (anonymous/username/certificate) ○ Up to 100 publishers/subscribers per connection ○ Various publish modes ○ Advanced JSON payload editor for publisher/subscribers ○ Advanced trigger mode for publisher (configurable via integrated Lua script editor) ○ Support for MQTT store and forward ○ MQTT V5 features • Default user password change mandatory at the first login. • Support for multiple users with the same username <p>Improvements:</p> <ul style="list-style-type: none"> • Internal certificates storage • Change Default Value for Endpoint Security • Default Values at Certification Generation • Update to Softing OPC UA SDK 6.20.1 <p>Fixed Security Issues</p> <ul style="list-style-type: none"> • Arbitrary file read using /runtime/core/audit/files/ • Arbitrary file write using /runtime/uacore/nodesetxml • Remote Code Execution through Zip Slip attack • Loading Remote Javascript Scripts • Session Theft due to XSS • OPC UA Server/Client NULL pointer dereference (Denial Of Service) • CVE-2022-2336: Default credentials authentication bypass vulnerability • CVE-2022-2334; CVE-2022-1373; CVE-2022-2338; Remote code execution vulnerability in configuration restore functionality of Secure Integration Server • CVE-2022-1069; CVE-2022-2337; CVE-2022-2335; CVE-2022-2547: Multiple denial of service vulnerabilities in FastCGI interface of Secure Integration Server • CVE-2023-27334: Unlimited Method Call Resource Exhaustion • CVE-2023-29377: Access of file directory • CVE-2023-29378: File Directory rename directory traversal

		<ul style="list-style-type: none"> • CVE-2022-1748 - NULL pointer access in method invocation at server • CVE 2022-37453 - malformed write requests can cause an excess memory allocation or an out-of-bounds memory access • CVE-2022-39823 - crash if too many continuation points are used in a single browse service • CVE-2021-42262 - endless loop in case of malformed type dictionary • CVE-2021-42577, CVE-2021-45117 - a possible crash in UA client communication • CVE-2021-40873 - a possible crash in UA server communication • CVE-2021-40871 - a possible crash in UA client communication <p>Open source components:</p> <ul style="list-style-type: none"> • Nginx v1.14.0 • cURL v7.69.0.0 • zlib v1.2.11.0 • OpenSSL v1.1.1t • Jsoncpp v1.20 • fcgi v2.4.1 • paho v1.3.10
V1.22.0	14.05.2020	<p>New Features:</p> <ul style="list-style-type: none"> • Notification E-Mail Alert feature, providing the possibility to configure the alerts (details of the email, messages, selection of triggers) and to automatically send alerts according to the configured rules • Filter Endpoint Descriptions based on the port the request is performed • OPC UA Timestamp normalisation <p>Improvements:</p> <ul style="list-style-type: none"> • Configurable Lifetime for Application Certificates • Edit a user direct from the endpoint user menu • Remove Admin User from OPC UA User Group <p>Open source components:</p> <ul style="list-style-type: none"> • Nginx v1.14.0 • cURL v7.69.0.0 • xlib v1.2.11.0 • OpenSSL Toolkit v1.1.1.4 • Jsoncpp v1.20 • libfcgi v2.4.1
V1.20.0	21.02.2020	<p>New Features:</p> <ul style="list-style-type: none"> • Creation of Mapped/Companion Address Spaces (up to 55 address spaces, depending on the license context) based on the import of external Nodeset Xml2 files • Full integration of the Mapped/Companion Address Spaces with the exposing of the address space to the defined endpoints/users and filtering features • Support of OPC UA services for browsing, reading, writing and method calls targeting the Static Address Spaces nodes

		<ul style="list-style-type: none"> • Complex (structured) data types access • Added time-limited (72 hours) demo mode (no license required) • Added the possibility to activate Maintenance License <p>Improvements:</p> <ul style="list-style-type: none"> • Better handling of the endpoints access protection feature • Certificates details present in various places in GUI are more detailed • OPC UA namespaces URI are now generated compliant to the standards • Relaxed address space export policy regarding the missing attributes on the remote servers • Changed the initialization of OPC UA packets sequence number to overcome interoperability issues with certain servers <p>Open source components:</p> <ul style="list-style-type: none"> • Nginx v1.14.0 • cURL v7.50.3.0 • xlib v1.2.11.0 • OpenSSL Toolkit v1.1.1.4 • Jsoncpp v1.20 • libfcgi v2.4.1
V1.12.0	05.06.2010	<p>New features:</p> <ul style="list-style-type: none"> • Subscribe access right changes have immediate effect on existing Monitored Items (not only on future ones). • Monitored Items can be created on variables for an underlying server that is not currently available, and they will get connected when the server becomes available. • Possibility to configure performance parameters for the connections to the underlying servers, to allow interoperability with underlying servers that are very limited in performance. <p>Improvements:</p> <ul style="list-style-type: none"> • Better notifications for Monitored Items when their connection to the underlying server changes state. • Possibility to control if monitored items created by distinct clients for the same variable are merged or not. • Integrated Toolkit 5.58, using UA node set of UA specs 1.04 and certified UA compliant.
V1.10.0	31.01.2019	<p>New features:</p> <ul style="list-style-type: none"> • Address space filtering allows now to specify allowed UA services for each node. • Automatic configuration backup. <p>Improvements:</p> <ul style="list-style-type: none"> • Better compatibility with some UA servers: allows to specify an alternate discovery URL, allows empty nonce if configured so. • GUI improvements.
V1.02.0	11.09.2018	<p>New features:</p> <ul style="list-style-type: none"> • Certificate authentication token, both for incoming and outgoing UA connections. • Support for <i>Aes128Sha256RsaOaep</i>, and <i>Aes256Sha256RsaPss</i> secu-

		<p>rity policies.</p> <ul style="list-style-type: none"> • Users for outgoing UA connections (to underlying servers) are now in the unified user list. • Possibility to quickly create a test UA connection to a remote server and display diagnostic information about it. • Integrated on-line and off-line licensing against Softing licensing server.
V1.01.0	25.05.2018	<p>New features:</p> <ul style="list-style-type: none"> • Added on-line help.
V1.00.0	13.04.2018	<p>First release of dataFEED Secure Integration Server (dataFEED SIS) for Windows.</p> <p>Features:</p> <ul style="list-style-type: none"> • Aggregates up to 100 UA Servers. • Creates one or more address spaces containing the nodes from these servers. • Exposes the address spaces through up to 50 UA endpoints. • Allows to configure which nodes of which address space is available to each UA user on each endpoint, and which UA services are allowed. • Maintains a unified list of users, for administration and for UA authentication, both for incoming and outgoing UA connections. • Supports <i>opc.tcp</i> and <i>https</i> endpoints, non-secured, sign, and sign-and-encrypt security modes, <i>Basic128Rsa15</i>, <i>Basic256Sha</i>, <i>Basic256Sha256</i> security policies. • <i>Anonymous</i> and user + password authentication tokens • Browse, read, write, method call, and subscribe to data. Subscription support has some limitations derived from the way subscriptions from multiple UA clients for the same variable on an underlying server are merged.