IDOL
HubSpot Connector

Software Version 12.9.0

Release Notes

Micro Focus®

Legal notices

Copyright notice

© Copyright 2021 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for updated documentation, visit https://www.microfocus.com/support-and-services/documentation/.

Support

Visit the MySupport portal to access contact information and details about the products, services, and support that Micro Focus offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- Search for knowledge documents of interest
- Access product documentation
- View software vulnerability alerts
- Enter into discussions with other software customers
- Download software patches
- Manage software licenses, downloads, and support contracts
- Submit and track service requests
- Contact customer support
- View information about all services that Support offers

Many areas of the portal require you to sign in. If you need an account, you can create one when prompted to sign in. To learn about the different access levels the portal uses, see the Access Levels descriptions.

Contents

New in this Release

The following new features were released in HubSpot Connector version 12.9.0.

- The connector can obtain details about your HTTP proxy from the system. Instead of setting `ProxyHost`, `ProxyPort`, `ProxyUsername`, and `ProxyPassword`, you can set the new configuration parameter `UseSystemProxy` to `TRUE`.

- The connector can communicate with other IDOL components that have been configured to require GSSAPI authentication. To enable this, set the `GSSServiceName` parameter in the `[Ingestion]`, `[DistributedConnector]`, and `[ViewServer]` sections of the configuration file, for requests to CFS, Distributed Connector, and IDOL View Server respectively.

- ACI servers can now communicate with a License Server that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

- Tasks scheduled to start at the same time run in the order that they are enumerated by the `N` parameter (in the `[FetchTasks]` section of the configuration file).

- Scheduled actions that have the same start time now run in the order that the schedules were created (with `action=schedule`).

- The `Admin` action was modified to ensure that the IDOL Admin interface can not run in an iframe, to improve clickjacking protection.

- The connector can insert documents into Digital Safe, through the Digital Safe REST API, in EML format. To do this, configure `IngesterType=DigitalSafeREST` and `StoreBinaryAndMeta=FALSE`.

- In schedules defined with the `schedule` action, you can now add holiday periods during which no actions are started.

- Communications can be secured with TLS version 1.3.

- The `collect`, `insert`, `stub`, and `update` fetch actions accept metadata as structured XML, as an alternative to a flat list of name and value pairs. For information about whether a connector supports these actions, refer to the Administration Guide.

- Elliptic Curve certificates and keys are supported, to enable the use of ECDSA and ECDH ciphers in TLS communications with other IDOL components.

- The connector can send documents to NiFi Ingest when NiFi requires a username and password for authentication. To configure the connector, set the new configuration parameters `IngestNiFiUsername` and `IngestNiFiPassword`.

- The connector can send files to a Micro Focus Digital Safe, through the Digital Safe REST API or the Digital Safe SOAP API.

- Performance monitoring accepts a minimum limit, maximum limit, or minimum and maximum limits for each performance counter. Earlier versions of the connector required both minimum and maximum limits. For example, you no longer need to specify a minimum level of CPU usage.

- The `[AuthorizationRoles]` section `StandardRoles` configuration parameter now accepts an asterisk (*) to represent all standard roles, so that you can easily set permissions for all roles.

- When importing parameters into your configuration file from another configuration file, you can use wildcards to select the parameters to include.

Resolved Issues

The following issues were resolved in HubSpot Connector version 12.9.0.

- The server could terminate unexpectedly when an authorization role was configured and the list of `Clients` included a hostname with a wildcard, such as `*.domain.example.com`. The `Clients` parameter accepts wildcards only in IP addresses.

- An issue with scheduling meant that tasks did not start at the correct time. The start of a task could be delayed, compared to the expected start time specified by the `ScheduleStartTime` parameter.

- Various `GetRequestLog` (`GRL`) HTML issues have been fixed:

  - Actions were not properly escaped in some places, which could allow malicious users to inject some alternative HTML in the `GetRequestLog` response.

  - The Open link in new window option did not work.

  - The auto refresh option would modify the selected open link option.

  - Links to the obsolete confighelp action have been removed.

  - The HTML page now uses a Content-Security-Policy to protect against malicious data injection by crafted actions sent to the server.

- Schedules created with `action=Schedule` were lost if the server was restarted.

- On Linux, when running some older versions of the Linux kernel, IDOL components could fail to connect to network ports.

- JavaScript could be injected into the `GetRequestLog` response by sending actions to the server.

Supported Operating System Platforms

HubSpot Connector 12.9.0 is supported on the following platforms.

Windows (x86-64)

- Windows Server 2019

- Windows Server 2016

- Windows Server 2012

Linux (x86-64)

The minimum supported versions of particular distributions are:

- Red Hat Enterprise Linux (RHEL) 6

- CentOS 6

- SuSE Linux Enterprise Server (SLES) 12

- Ubuntu 14.04

- Debian 8

Solaris (x86-64 and SPARC 64)

- Solaris 11

- Solaris 10

Notes

- The autpassword command-line tool has been updated to provide hardened AES encryption for passwords. Micro Focus strongly recommends that you reencrypt all passwords in configuration files by using the updated tool.

  The older AES encryption format and basic encryption methods are now deprecated. Passwords that you have encrypted with older versions continue to work, but the server logs a warning. Support for these older encryption methods will be removed in future.

- `IngesterType=DigitalSafeSOAP` has been deprecated. Micro Focus recommends that you use `IngesterType=DigitalSafeREST` instead. `IngesterType=DigitalSafeSOAP` is still available for existing implementations, but it might be incompatible with new functionality. The functionality might be deleted in future.

- ACI Encryption has been deprecated. Instead of using ACI encryption, Micro Focus recommends configuring Secure Socket Layer (SSL) connections between ACI servers and applications. You can use GSS authorization without using ACI encryption by configuring the `GSSServiceName` and `RequireGSSAuth` parameters. ACI encryption is still available for existing implementations, but it might be incompatible with new functionality. The functionality might be deleted in future.

Documentation

The following documentation was updated for HubSpot Connector version 12.9.0.

- *HubSpot Connector Help*