

DataSync Agent FAQs

ServiceNow App

Does DataSync work with ServiceNow Database Encryption?

ServiceNow provides an option for [Database Encryption](#) where data is encrypted at rest in the database. Since Database Encryption happens at the database layer and the Perspectium application runs at the application layer, by the time we call to get data from ServiceNow, the data will be accessible to our application to be shared out. ServiceNow's documentation mentions with Database Encryption that you can add another level of encryption by also encrypting at the application layer which is what our application [supports](#) as well.

DataSync Agent

How do I check the Agent version in Windows?

To check what version of the Agent you are running you can use the following command in the command window from the agent directory:

```
bin\version.bat
```

You could also double-click the **version.bat** file in the Agent's bin directory.

What Java processes does the DataSync Agent run?

The Perspectium DataSync Agent leverages two Java virtual machine instances, or processes, to run.

These Java processes can be [started as a service](#) or interactively through the executables in the Agent's **bin** folder.

Should I configure my DataSync Agent to connect to the Perspectium Mesh via HTTPS or AMQPS?

When you received your Perspectium Mesh credentials, you may have been given two different addresses. Such as:

- <https://user.perspectium.net>
- <amqps://user.perspectium.net>

The choice between these different protocols will vary per customer (largely firewall rules). ServiceNow does not handle AMQP connections, so do not include AMQP within the ServiceNow instance URL for any of your **<instance_connection>** directives.

How does the Agent handle ServiceNow schema changes?

The DataSync Agent handles schema changes in your ServiceNow instance as follows:

- Columns that are added to a ServiceNow table will be automatically added to the table in the database.
- When a column's max size is increased, the Agent will automatically increase the column's size to the maximum size for that database. In the case of MySQL, the column will automatically transition to a CLOB data type.
- If a column is changed from a different data type to another data type, the data in this column will be skipped (the record itself will insert /update all other columns).

How does the SQL agent commit to the database?

The DataSync SQL Agent leverages the default connection commit strategy of the JDBC driver for which Oracle is auto commit. The agent does not explicitly decide when to perform a commit. The JDBC driver makes this decision.

The Agent retrieves a message from the message store in the order they were published, performs the required processing such as decryption, validation etc., possibly determines the type of SQL operation required (such as update or insert), and then issues the request to the database. The Agent then determines the response and does any further processing required. Once completed, the Agent will fetch the next message from the message store in the queue.

NOTE: You can configure either multiple tasks to run against a single queue or you can configure multiple instances of a single task to run against a single queue. This is done primarily when throughput of the Agent is an issue. Both of these configurations introduce more than a single consumer of the queue and so the order in which the database transaction occurs could be different than the order of the messages within the message store due to scheduling of the task or thread.

What are the required external libraries HDFSFileSubscriber handler?

The HDFSFileSubscriber handler requires the use of the Hadoop external library. You will need the jar files from each of these Hadoop libraries:

1. Hadoop Annotations
2. Hadoop Auth
3. Hadoop Client
4. Hadoop Common
5. Hadoop HDFS
6. Hadoop Mapreduce
7. Hadoop Yarn

The Maven repository for these files can be found [here](#). Once you have these files they need to be placed in the [extlib](#) folder in the File Replicator agent's directory.

How can I improve my DataSync Agent's overall performance?

- If you find that your DataSync Agent is running slowly due to a large number of SQL statements being processed, you may want to configure the Agent to perform SQL statements in batches.

NOTE: This feature should only be used when you send messages of the same table into one queue. If your queue has messages from different tables (including `sys_audit`, `sys_journal_field`, `sys_attachment` and `sys_attachment_doc` records), do not enable this feature as it will cause errors in saving records. To properly use this feature, separate your dynamic and bulk shares to save each type of table record to a different queue.

- To do this, open the `agent.xml` file that was created upon installation of your Agent in a text editing application. Within the `<task>` directive of the `agent.xml` file, nest the following directives:

Directive	Description
<code><batch_update/></code>	Self closing tag that configures your Agent to batch SQL UPDATE statements
<code><batch_insert/></code>	Self closing tag that configures your Agent to batch SQL INSERT statements
<code><max_batch_size></code>	Number of SQL statements that will trigger a batch SQL statement execution. A larger suggested value is 200. NOTE: By default, this directive's value will be set to 10.

- In your `agent.xml`, change the `<polling_interval>` to a lower number
- In your `agent.xml`, increase the number of `<tasks>`
 - **NOTE:** Increasing the number of task will require more memory and connections to the database. We do not recommend setting tasks to more than 10.
- In your `agent.xml`, change `<message_connection>` attributes so `use_basic_consume=false`
- In ServiceNow, change your [bulk share configuration](#) to `Insert Only=true`

Handling of long Table and Column names when replicating to the Oracle database

Since Oracle only permits a string of 30 characters by default, a table or a column name that has over 30 characters will be truncated upon replication. The first 15 characters of the name will be displayed, followed by a “_” and then the last 14 of the table name. The “_” denotes the truncated values between the first 15 and the last 14 characters.

For example, when replicating the table “Workflow Estimated Runtime Configuration” (41 characters total) to Oracle database, the replicated name will be “u_workflow_esti__configuration”.

NOTE: When replicating a table or column that have similar names, meaning if the first 15 and the last 14 of the name are the same, only one of the two records will be replicated since after truncation, both of the names will be the same.

Security

Is data at rest in the Perspectium Cloud database encrypted?

Yes, the data at rest inside the Perspectium Cloud database can be secured by encryption for an additional cost. Perspectium uses Amazon Web Services which allows the encryption of data using the industry standard AES-256 encryption algorithm. Please refer to the following link for further details on [Encrypting Amazon RDS Resources](#).

Is my connection to the database in the Perspectium Cloud secure?

The connection to our database is highly secure. We can also set it up as a secure SSL connection for an additional cost. Please refer to the following link for further details on [Using SSL to Encrypt a Connection to a DB Instance](#).

Which encryption algorithm does Perspectium used for data encrypted at ServiceNow?

The cipher Perspectium uses is Triple DES by default and Advanced Encryption Standard 128 (AES-128) as an option.

Does Perspectium support 128 bit AES encryption?

Yes, we support 128 bit AES encryption.

When we change our encryption key in ServiceNow, how does that get updated in the conf XML file?

This is done manually using a text editor.

Is the authentication data (username/password) encrypted between the agent and the cloud? Or is it sent in clear text?

This data can be sent encrypted by utilizing AMQPS on port 5671 or HTTPS.

How does data get encrypted at rest and in transit?

The data is encrypted within the ServiceNow Instance before being transmitted to Perspectium cloud using HTTPS. The payload remains encrypted while at rest within the Perspectium Message Bus until it's consumed by either a ServiceNow Instance or a DataSync Agent. The former will decrypt the data just prior to being inserted into a ServiceNow table and in the later case the DataSync Agent decrypts the data just before it's sent to the database server.

Does the Perspectium QA team assess security aspects of the offering during code reviews?

Perspectium performs a weekly infrastructure review which includes security. We also perform a daily code review as part of our sprints which includes security as needed.

What are the security features that Perspectium offers?

All Perspectium data is transmitted using HTTPS and AMQP/AMQPS as secure protocols. An option of having the data encrypted while in Perspectium's Cloud based Database is available. The on-premise DataSync Agent supports a proxy using HTTP/HTTPS to talk to external servers such as those within the Perspectium Cloud environment. VPN's can be set up at an additional cost.

Can the Perspectium Agent connect to ServiceNow through a proxy server?

Yes, you can use a proxy server to connect the Perspectium Agent to ServiceNow v3.2.2. For further details, see [Configuring the DataSync Agent to Leverage a Proxy](#).

Can't find what you're looking for?

See [additional DataSync Agent troubleshooting topics](#) or browse the [Perspectium Community Forum](#).