BigFix ServiceNow Data Flow
Implementation Guide

Special notice

Before using this information and the product it supports, read the information in Notices.

Edition notice

This edition applies to BigFix version 10 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. ServiceNow Data Flow

This module provides an overview and features of the BigFix ServiceNow Data Flow.

BigFix ServiceNow Data Flow - Overview

With the BigFix ServiceNow Data Flow (also called Data Flow Service), organizations can now enrich ServiceNow CMDB with the rich, up-to-date data provided by the BigFix Platform. The ServiceNow CMDB can be used to discover the information that has only been available traditionally in the Configuration Management Database (CMDB), such as Department, Owner and Location, back to BigFix. With this data, BigFix Operators are enabled with much more granular grouping of endpoints for targeting of actions and reporting.

After the data sources and mappings are configured, the Data Flow Service periodically looks for changes in the source system, analyzes and transforms the results, and imports the results into the target data source.
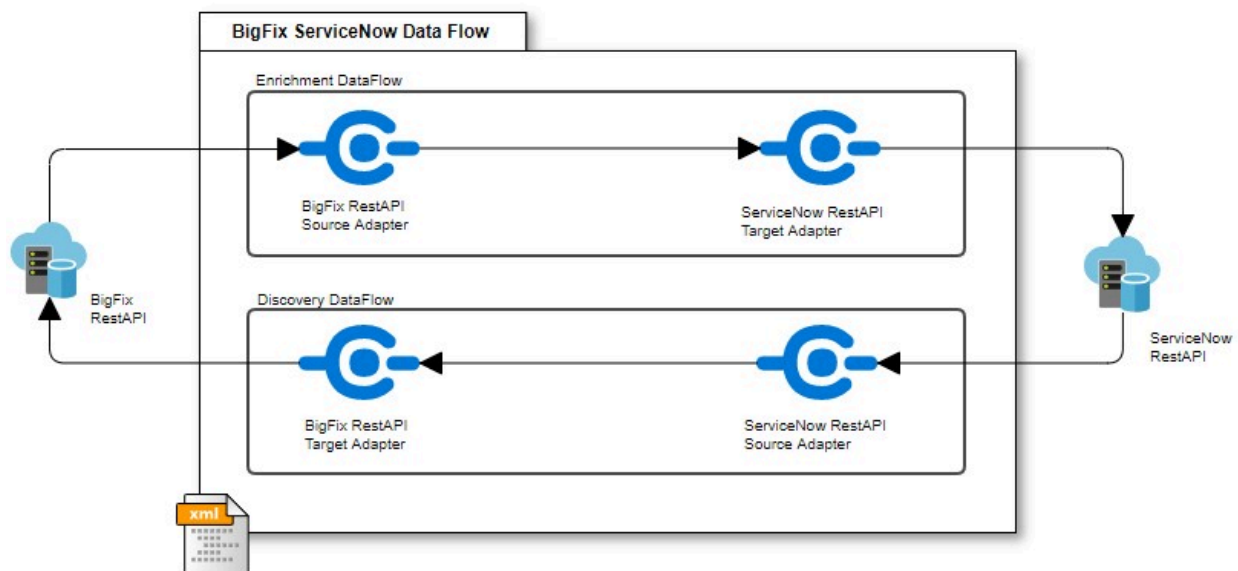
Features

- Highly scalable multi-process architecture

- Bi-directional synchronization of#hardware#asset data between BigFix and ServiceNow

- Concurrent execution of data transfers#between#the#two data sources

- Secured credential management for encrypting passwords

- Property value transformations

- Throttling of datasource updates

- Weight-based algorithm for machine correlation

Chapter 2. Detailed system requirements

This section provides comprehensive information on the system requirements for Integration Services. Prior to service deployment, it is necessary for the user to possess the access outlined below.

BigFix Service Account Requirements

- admin access (not SOAP role admin access)

To facilitate the import of ServiceNow CMDB data into BigFix, a Master Operator account is required. Otherwise, the minimum account requirements to send BigFix endpoint data to ServiceNow are the following:

- A non-master operator account with permissions against the in-scope computers.

- Read access to the BigFix ServiceNow Data Flow site.

- The **Can use REST API** setting set to *Yes*

- The **Can Create Actions** setting set to *No*.

ServiceNow Service Account Requirements

- read and write acces for CMDB_CI_COMPUTERS , SYS_CHOICE and CORE_COMPANY tables

The ServiceNow Administrator should have a service account that leverages basic authentication with read and write access to the CMDB tables.

Table 1. ServiceNow Data Flow

Prerequisites	Operating system	Hardware	Configuration	BigFix Service Account	Supported BigFix versions	Supported ServiceNow versions	Recommendations
Microsoft VC++ Redistributable package 2012. Install it from Microsoft website.	• Windows 2016 • Windows 2019	• 6-8 Cores • 32 GB RAM RAM Utilization depends on number of devices, example: • 50k devices utilize 3.5GB RAM • 300k devices utilize 22GB RAM*	• Network Access to BigFix Root Server • Network Access to ServiceNow REST APIs	• Master Operator account required • Access to InScope Devices • No Ability to Create Actions • Access to REST API • Access to Any Site Containing In-Scope Properties	BigFix Server version 10	• Orlando • Madrid • New York • Rome • Quebec • Paris • San Diego	In larger environments, make sure you deploy the integration solution on a dedicated server.

*12 hours execution for 300K devices consumes maximum 22 GB

RAM
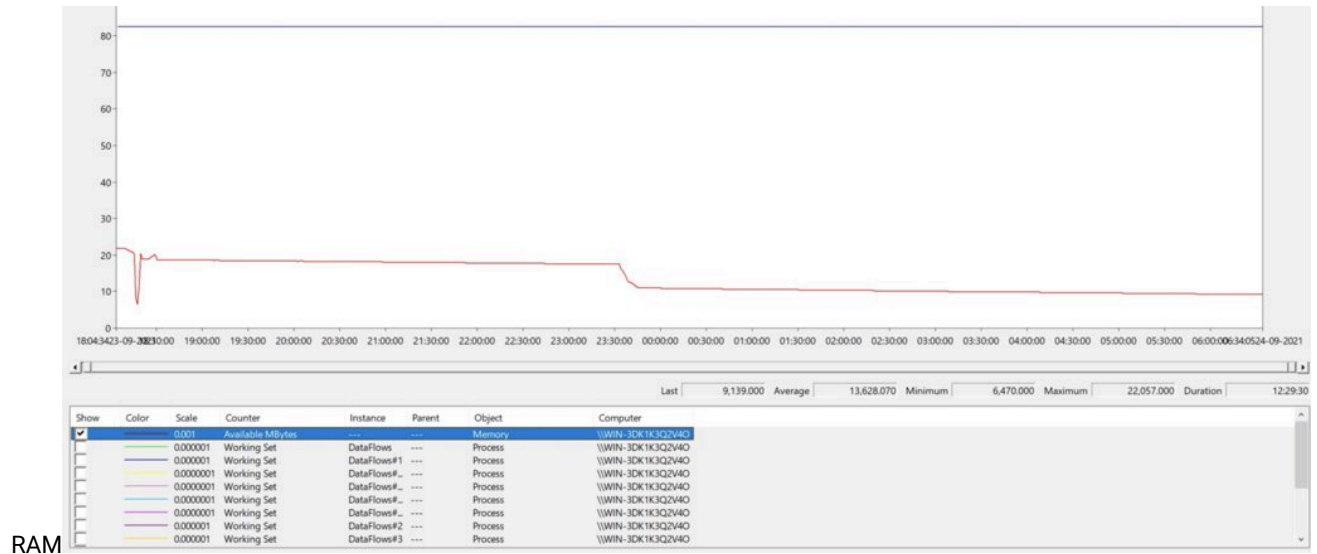
Chapter 3. Fundamental concepts

In this module you can find fundamental concepts and terminology of BigFix ServiceNow Data Flow solution.

Data Sources

Data Sources represent the connection information required to for the BigFix Service Data Flow service to interact with BigFix and ServiceNow instances. Administrators provide the connection strings and may optionally set the **VerifyCert** flag to enable or disable the SSL certificate validation.

> **Note:** If your instance leverages a self-signed certificate for the BigFix REST API, this option needs to be set to *false*.

Administrators provide credentials for each data source using the IntegrationServices CLI, with the – ProvideCredentials command and an optional *DataSource Name* argument.

BigFix Service Account Requirements

To facilitate the import of ServiceNow CMDB data into BigFix, a Master Operator account is required. Otherwise, the minimum account requirements to send BigFix endpoint data to ServiceNow are the following:

- A non-master operator account with permissions against the in-scope computers.

- Read access to the BigFix ServiceNow Data Flow site.

- The **Can use REST API** setting set to *Yes*

- The **Can Create Actions** setting set to *No*.

ServiceNow Service Account Requirements

The ServiceNow Administrator should have a service account that leverages basic authentication with read and write access to the CMDB tables.

Adapters

Adapters provide the logic to facilitate bi-directional communication with either ServiceNow or BigFix. The Data Flow service provides two adapters which can be configured to direct the flow of data from one system to another. Data flows are configured with one Source Adapter and one Target Adapter. The Source Adapter gathers data from the configured data source using the property collection provided in the configuration, performs any data transformations, identifies changes from the last execution, and hands those changes over to the configured Target Adapter. The Target Adapter then retrieves the changes from the Source Adapter, validates and maps changes against the target data set, performs any data transformations, and updates the target data source with the changes. The properties are matched between Source and Target adapters based on their property name which are case sensitive.

> **Note:** The Data Flow services can be set in a Preview Only mode, as described in a following section. In this mode, the solution writes any discovered changes to a CSV file in the installation directory for testing of the configuration of the data flows.

BigFix Adapter

Whenever initiated in the context of a Data Flow, the BigFix Adapter extracts data from BigFix by querying the REST API with a dynamically generated query based on the property configuration in the adapter configuration of the data flow. It then parses those results, performs any required transformations, identifies changes from previous executions, and persists the changes to a cache file on the disk.

> **Note:** The BigFix Adapter looks for machines that have reported within a specific duration only. You can configure the duration by using the **bigfixrest.MaxComputerAge** setting. The default value is 12 hours.

As a Target Adapter, the BigFix Adapter processes changes received from the source adapter, and updates the mailbox file for each machine.

> **Note:** The mailbox file is a flat representation of the data gathered from all data flows in relation to a given data source. The updated mailbox file is then pushed through the BigFix REST API to a specific endpoint, which enables a BigFix Analysis to make that data available in the Console, WebReports, WebUI, Inventory,and Compliance.

ServiceNow Adapter

When initiated in the context of a Data Flow, the ServiceNow Adapter extracts data from the CMDB_CI_COMPUTER table in ServiceNow, parses the results, and persists the changes to a cache file on the disk.

As a Target Adapter, the ServiceNow Data Flow Adapter processes changes received from the Source Adapter, detects changes, and updates the CMDB_CI_COMPUTER table.

Data Flows

A Data Flow facilitates the flow of information from a source system to a target system. It is configured to run on start of the service and then again at a configurable interval. By default, the solution is configured to run 4 data flows concurrently. Upon execution, the data flow causes both the Source Adapter and the Target Adapter to initialize and gather the latest data from the respective data sources. Once they are initialized, the source adapter transfers the changed records to the Target Adapter for processing. The Target Adapter attempts to map the records based upon the configured correlation logic.

> **Note:** If multiple matches are found, the change record is ignored. If a single match is found, the Target Adapter performs an update. If no match is found, the change record is inserted.

Machine correlation

In an ideal scenario, every computer contains an identifier that can uniquely identify the system in both the source and target data sources. For instance, if your organization guarantees that a device is always uniquely identified by the host name and that data was available in both systems, then simple key matching could be performed to associate the records between the systems.

However, the definition of a computer between data sources and organizations is often more complex. Host names change, IP addresses change, NIC changes, hard drives change, operating systems are reinstalled or upgraded, and so on. In most of these cases, the assets are not necessarily considered "new".

Within ServiceNow DataFlow, the initial step involves comparing the source key of the source adapter with the target key of the target adapter. If the match is found, it is a primary key match for the record. This implies that the correlation between the records in ServiceNow and Bigfix will remain intact, irrespective of any subsequent checks on the identity properties. If the match is not found the process proceeds to use the weighted confidence algorithm for machine correlation matching.

```xml
<dataflow displayname="Transfers Asset Data from Bigfix to ServiceNow" datatype="asset" schedule="0 */6 * * *">
    <dataflowdescription/>
    <sourceadapter displayname="Bigfix Adapter" adapterclass="bigfix" datasourcename="BigFixRestAPI">
        <device_properties>
            <sourcekey displayname="BigFix Computer ID" propertyname="BigFix ServiceNow Data Flow-Hardware Attributes-1" datatype="string"/>
            <targetkey displayname="ServiceNow SYS_ID" propertyname="ServiceNow CMDB Attributes-ServiceNow Custom Properties-2" datatype="string"/>
            <property displayname="Computer Name" propertyname="BigFix ServiceNow Data Flow-Hardware Attributes-2" datatype="string"/>
            <identityproperty displayname="IP Address" propertyname="BigFix ServiceNow Data Flow-Hardware Attributes-19" datatype="string" weight="20"/>
            <identityproperty displayname="MAC Address" propertyname="BigFix ServiceNow Data Flow-Hardware Attributes-20" datatype="string" weight="20"/>
        </device_properties>
    </sourceadapter>

    <targetadapter displayname="ServiceNow Adapter" adapterclass="servicenow" datasourcename="ServiceNowAPI">
        <device_properties>
            <sourcekey displayname="ServiceNow SYS_ID" propertyname="sys_id" datatype="string"/>
            <targetkey displayname="BigFix Computer ID" propertyname="correlation_id" datatype="string"/>
            <property displayname="Name" propertyname="name" datatype="string" weight="20"/>
            <identityproperty displayname="IP Address" propertyname="ip_address" datatype="string" weight="20"/>
            <identityproperty displayname="MAC Address" propertyname="mac_address" datatype="string" weight="20"/>
        </device_properties>
    </targetadapter>
</dataflow>
```

A weighted confidence algorithm that is configured within the data flow performs this initial mapping. Each data flow is configured with the **MinimumConfidenceLevel** property which is in global setting, which defines the weight of combined matches that are acceptable for assuming a match. If the combined weight of matching properties exceeds this threshold, then the record is considered a match and the key is mapped to improve performance of the subsequent updates. This provides a lot of flexibility to adapt to the natural changes in an environment.

For ex: Lets assume the dataflow is from Bigfix to ServiceNow. In the first dataflow execution all the data from Bigfix gets loaded to ServiceNow. In the subsequent executions the machine correlation plays important role. Lets assume that the minimumconfidence level is set to 60 and below machine details are present in both Bigfix and ServiceNow. In the next execution the ip address from Bigfix is compared with ServiceNow.

Machine	IP Address(weight = 30)	MAC Address(weight = 30)	Hostname(weight =30)
1	19.45.67.2	2345.567.222	Machine1

As the ip address matches, the confidence level is now 30 (weight of ip address) . Next the system compares the mac address in Bigfix and ServiceNow and it matches so the confidence level is 60(weight of ip address + weight of mac address). Now as the confidence level is 60 which is equal to the miniumconfidencelevel, the record is either updated or kept in ServiceNow.

In the below example the mac address and hostname of the machine is changed but ip address remains as is. Now following the same steps as mentioned , the minimumconfidencelevel will not be reached and the system assumes it to be a new record and inserts it into ServiceNow.

Machine	IP Ad-dress(weight = 30)	MAC Ad-dress(weight = 30)	Hostname(weight =30)
1	19.45.67.2	2345.567.2234	Machine2

Advanced Configurations

Data Flows

With BigFix ServiceNow Data Flow, administrators can uniquely design data flows to optimize performance and accuracy of machine correlation. The default configuration provides data flows to separate the synchronization of data for laptops, servers, and virtual machines. An administrator can synchronize a data flow on any number of different configuration properties, such as location, subnet, device type, operating system and so on.

Property Transformations

You can manipulate the value of a property by using property transformations. This could be useful in several scenarios requiring calculated fields such as maintenance windows or enumerations. Property transformations are implemented in Python language.

```
<property displayname= "Sample Property"

sourcecolumnname= "SampleProp"

datatype= "Integer">

<transformationlogic>

<![CDATA[this_value+1]]>

</transformationlogic>

</property>
```

Filter Queries

Administrators can use Filter Queries to filter data extracted from the source system to limit the scope of the data flow.

```
<sourceadapter   displayname     = "My first source adapter"

                 adapterclass    = "bigfixrest"

                 datasourcename  = "MyDataSource">

    <filterquery>

        <![CDATA[
```

```
        relay hostname of it is "Relay1"
    ]]>
  </filterquery>
  <properties></properties>
</sourceadapter>
```

Preview Data

The BigFix ServiceNow Data Flow can be configured to export *changes* instead of updating the target system. This feature enables administrators to test Data Flow configurations without the solution updating the target system. To enable this functionality, the **PreviewOnly** setting in the configuration file should be set to *True*. While this setting is enabled, the Target Adapter writes any planned changes in to a CSV file in the installation path, where the installation path is `C:\Program Files (x86)\BigFix Enterprise\Dataflow`.

Naming convention of CSV files:

- ServiceNow Dataflow from Bigfix To ServiceNow: Preview-[0]-[servicernow]-YYYYMMDDHHMMSS.csv.

  Ex.: Preview-[0]-[servicernow]-20220511140308.csv

- ServiceNow Dataflow from ServiceNow to Bigfix: Preview-[1]-[bigfix]-YYYYMMDDHHMMSS.csv

  Ex.: Preview-[1]-[bigfix]-202205118004051.csv

Update Throttling

With Update Throttling, adminstrators can tune the performance of the service so as not to negatively impact the target data source. This can be enabled and tweaked with the following two settings for each adapter in the configuration file: **QueueRefreshInterval** and UpdateBatchSize.

The **QueueRefreshInterval** determines the frequency that a given adapter looks for changes to be sent to the target data source. It is set to 120 seconds or about 30 potential updates per hour by default. The **UpdateBatchSize** determines the number of records that can be processed in a single update and its default value is 0.

In a scenario where **QueueRefreshInterval** is set to 120 seconds and **UpdateBatchSize** is set to 50, the solution would be throttled to 1500 updates per hour or 36,000 updates per day.

Chapter 4. Deployment and configuration

This module provides the steps to deploy the BigFix ServiceNow Data Flow solution.

Before you deploy the Fixlet, please note the following pre-requisites:

- read and write acces for CMDB_CI_COMPUTERS , SYS_CHOICE and CORE_COMPANY tables in ServiceNow
- admin access for ServiceNow (not SOAP role admin access)

1. Enable a content site.

   Navigate to BigFix License Overview Dashboard. In **Compliance/Lifecycle** panel, click **Enable BigFix ServiceNow Data Flow** Fixlet to gather the required content.
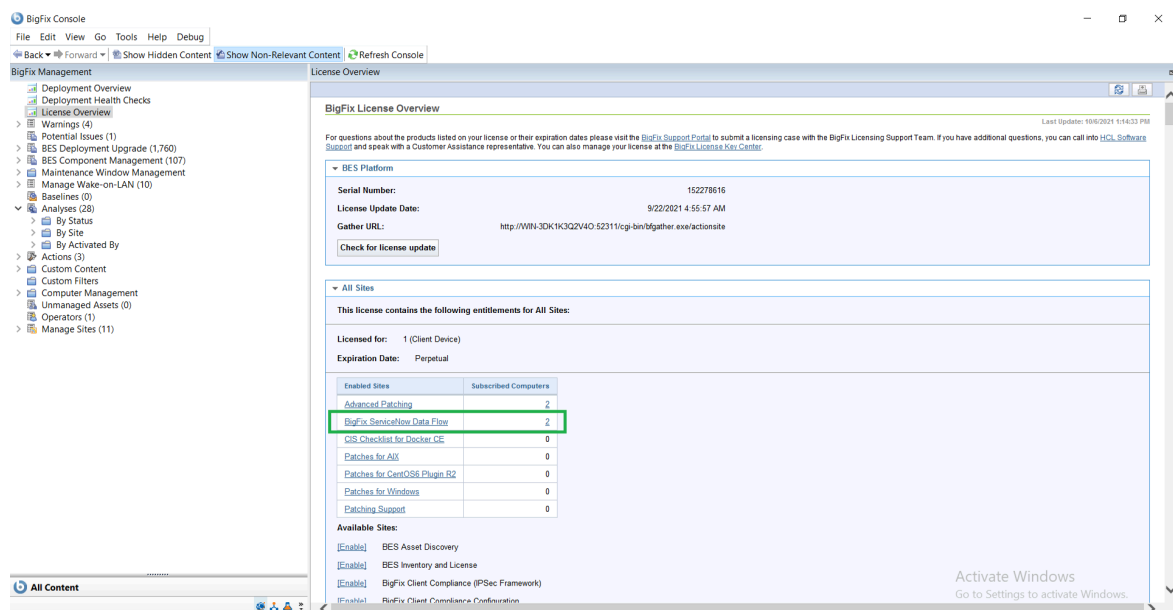
2. Create a Custom Site.

   Go to Custom Sites and create a new site. Name it as **ServiceNow CMDB Attributes** and select **All Computers** in Computer Subscriptions.

3. Deploy the solution to the target server.

   To deploy ServiceNow version **1.2** follow the steps in the Deploy BigFix ServiceNow Data Flow Service Fixlet.

   Note: Hardware analysis must be activated before the job run starts.

Chapter 5. ServiceNow Fixlets and Tasks

Learn more about available Fixlets and Tasks for ServiceNow.

Deploy BigFix ServiceNow Data Flow Service

Upgrade BigFix ServiceNow Data Flow Service to v1.2

Uninstall BigFix ServiceNow Data Flow Service

Manage BigFix ServiceNow Data Flow Service

Manage BigFix ServiceNow Data Flow Datasources

Manage BigFix ServiceNow Data Flow Data Flows

Manage BigFix ServiceNow Data Flow Service Settings

Deploy BigFix ServiceNow Data Flow Service

1. Select **Deploy BigFix ServiceNow Data Flow Service** Fixlet from the BigFix ServiceNow Dataflow external site.
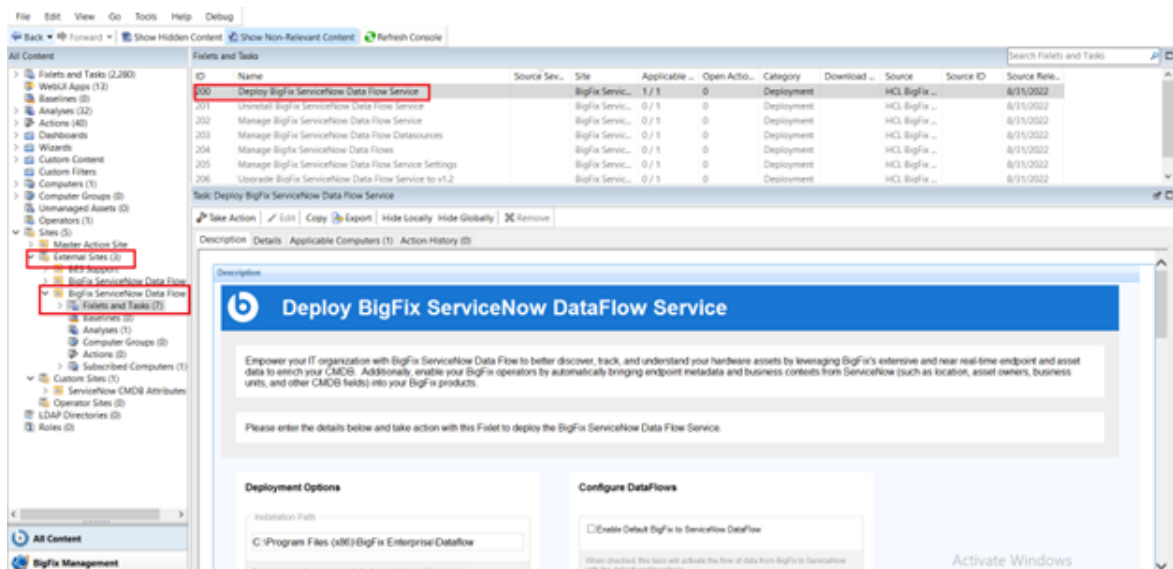
> **Note:** Please note following pre-requisites (the Fixlet will attempt to deploy these automatically):
> - Microsoft Visual Studio C++ Redistributable 2012: https://www.microsoft.com/en-in/download/details.aspx?id=30679
> - Microsoft ODBC Driver 17 for SQL Server: https://www.microsoft.com/en-us/download/details.aspx?id=56567

2. Provide all the required details.

- ◦ Deployment Options
  - ▪ Installation path - by default the path is C:\Program Files (x86)\BigFix Enterprise\Dataflow . It is possible to provide an alternate path.
  - ▪ Initialize Schema - checked by default
  - ▪ Start Services - checked by default. When enabled, the service will start automatically after the installation
- ◦ Configure DataFlows
  - ▪ Enable Default BigFix to ServiceNow Dataflow - when checked, the dataflow from Bigfix to ServiceNow will be enabled.
  - ▪ Enable Default ServiceNow to BigFix Dataflow - when checked, the dataflow from ServiceNow to Bigfix will be enabled.
  - ▪ Enable Preview Mode - checked by default. Preview setting is set to true. Enabling Preview Mode allows you to preview and validate the changes that will be made to BigFix and/or ServiceNow in a file rather than making the changes in the target system.

- ◦ Configure BigFix DataSource
  - ▪ Connection String - URI for the BigFix RestAPI. Ex : https://win-lfj8dd2ilij:52311/api
  - ▪ Account - user name used to login to Bigfix Console
  - ▪ Password - password used to login to Bigfix Console
- ◦ Configure ServiceNow Datasource
  - ▪ Connection String - ServiceNow instance URL should be provided in the below format. Ex : https://dev114254.service-now.com/api/now/table
  - ▪ Account - user name used to login to ServiceNow instance

▪ Password - password used to login to ServiceNow instance

◦ Configure BigFixServiceNow ETL

Depending on which Dataflow is enabled, respective ETL gets checked. It is required to provide the ETL in the Unix cron format. Refer to the link for more information about the scheduler.

◦ Advanced Settings

To provide proxy details click on **Advanced Settings**. This option is not mandatory.

3. Click on **Take Action** and select the target device where the Service should be installed and click **OK**. The BigFix SeviceNow Dataflow will be installed in the location provided with a folder named Dataflow.
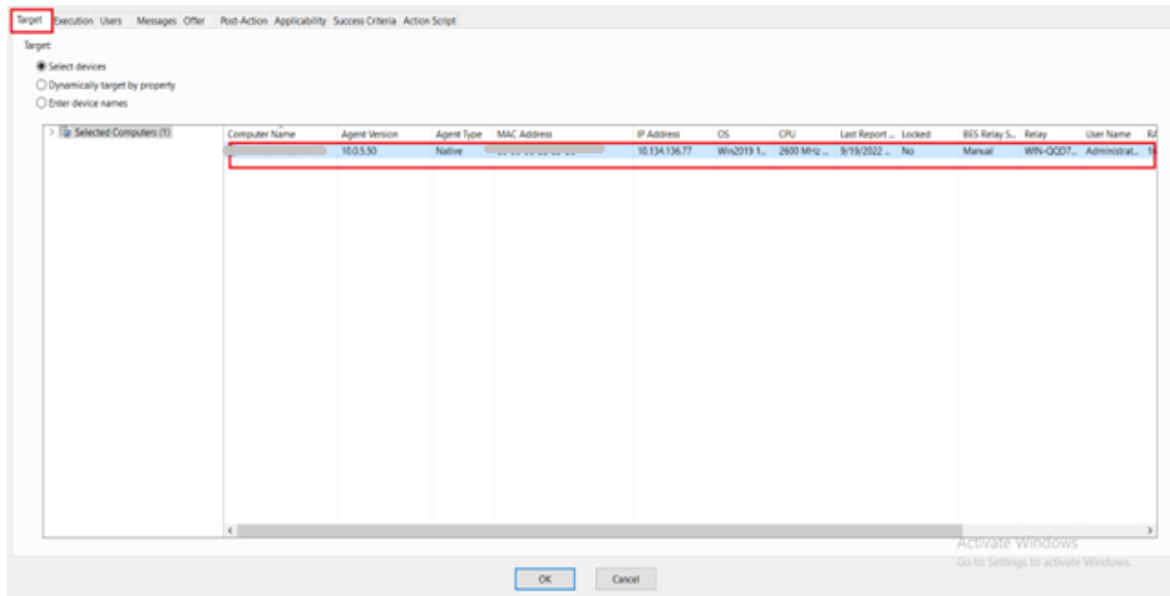
The installation completion steps are logged in install.log and the dataflow process is logged in the logs folder inside the Dataflow folder. Default file location is C:\Program Files (x86)\BigFix Enterprise\Dataflow \install.log.

Upgrade BigFix ServiceNow Data Flow Service to v1.2

Note: This Fixlet can be used only if there is previous version of BigFix ServiceNow Dataflow Service already installed.

1. Select **Upgrade BigFix ServiceNow Data Flow Service to v1.2** Fixlet from the BigFix ServiceNow Dataflow external site to upgrade the existing BigFix ServiceNow dataflow to the latest version.
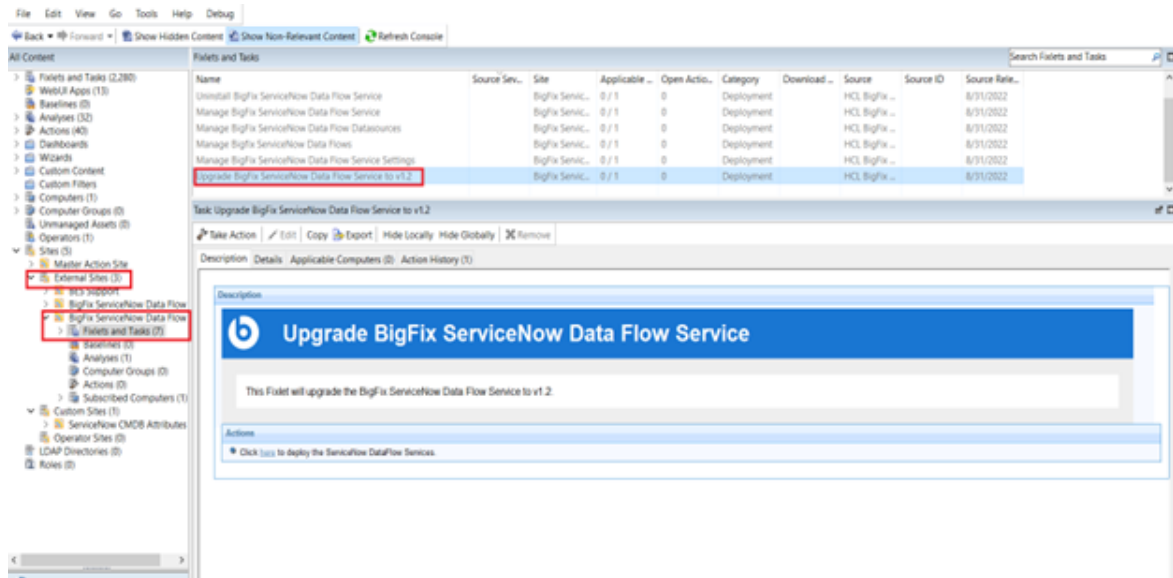
2. Select **Take Action** and select the target device to upgrade the Service. Click **OK**.
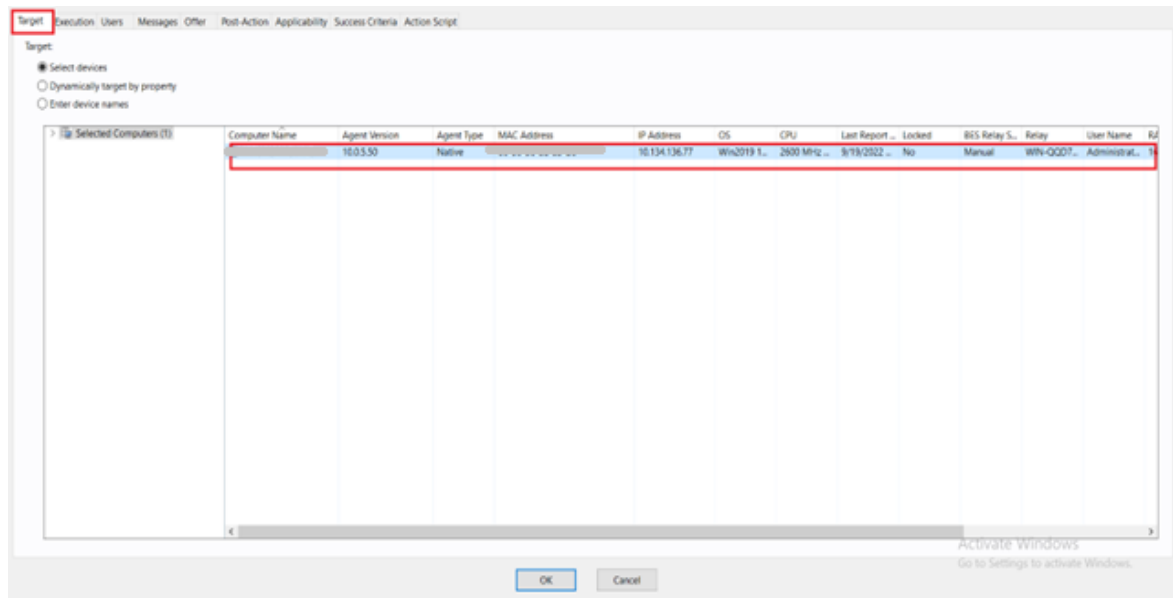
The upgradation completion steps are logged in bfsnow_upgrade.log. The default file location is C:\Program Files (x86)\BigFix Enterprise.

Uninstall BigFix ServiceNow Data Flow Service

1. To uninstall existing BigFix ServiceNow Dataflow select **Uninstall BigFix ServiceNow Data Flow Service** Fixlet from the BigFix ServiceNow Dataflow external site.
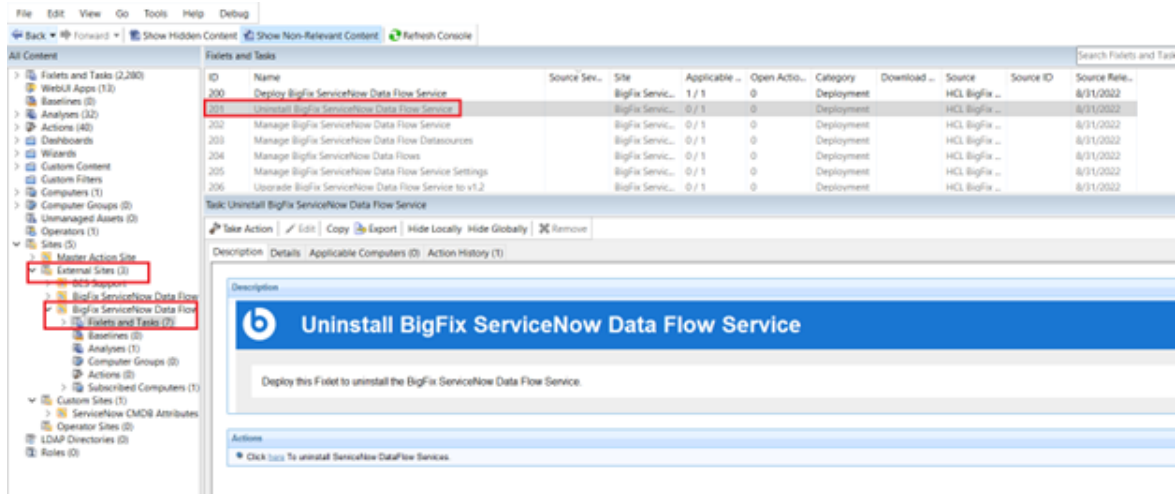
2. Select target devices under Target tab and click **OK**.
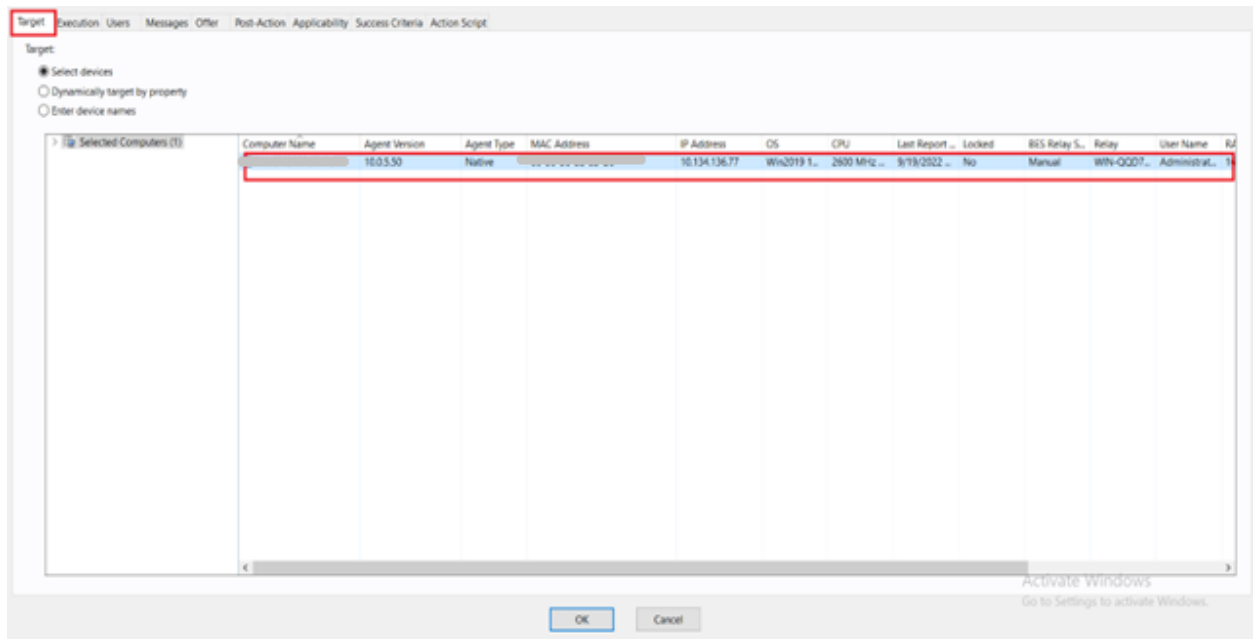
The uninstall completion steps can be checked in the bfsnow_uninstall.log file. The default file location is C:\Program Files (x86)\BigFix Enterprise.

Manage BigFix ServiceNow Data Flow Service

1. To stop, start or restart the DataFlow Service and to validate configuration file use **Manage BigFix ServiceNow Data Flow Service** Fixlet from the BigFix ServiceNow Dataflow external site. The current service state of the dataflow is displayed on the UI.
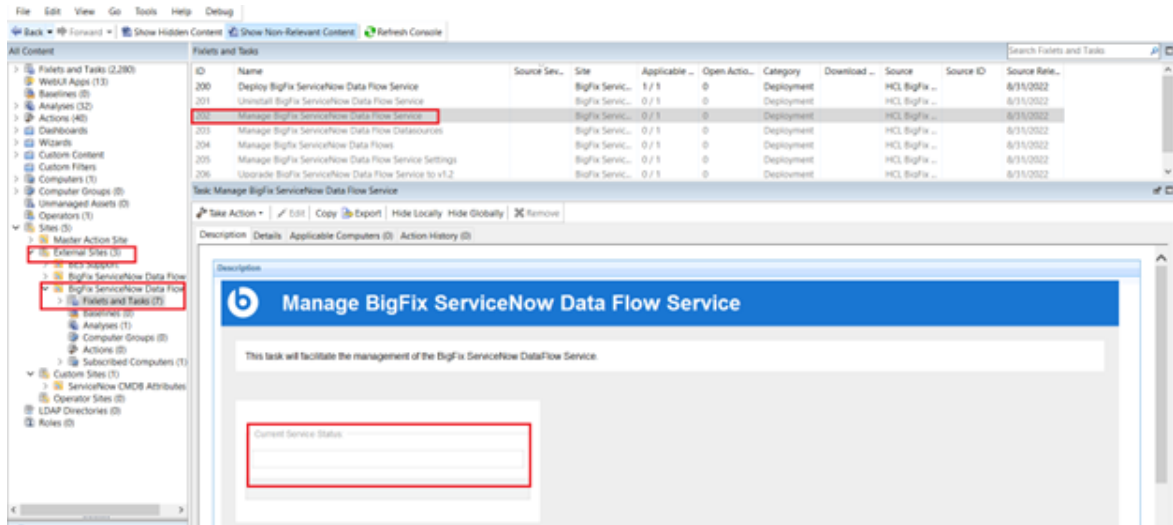
2. Choose the desired action from the **Take Action** list.
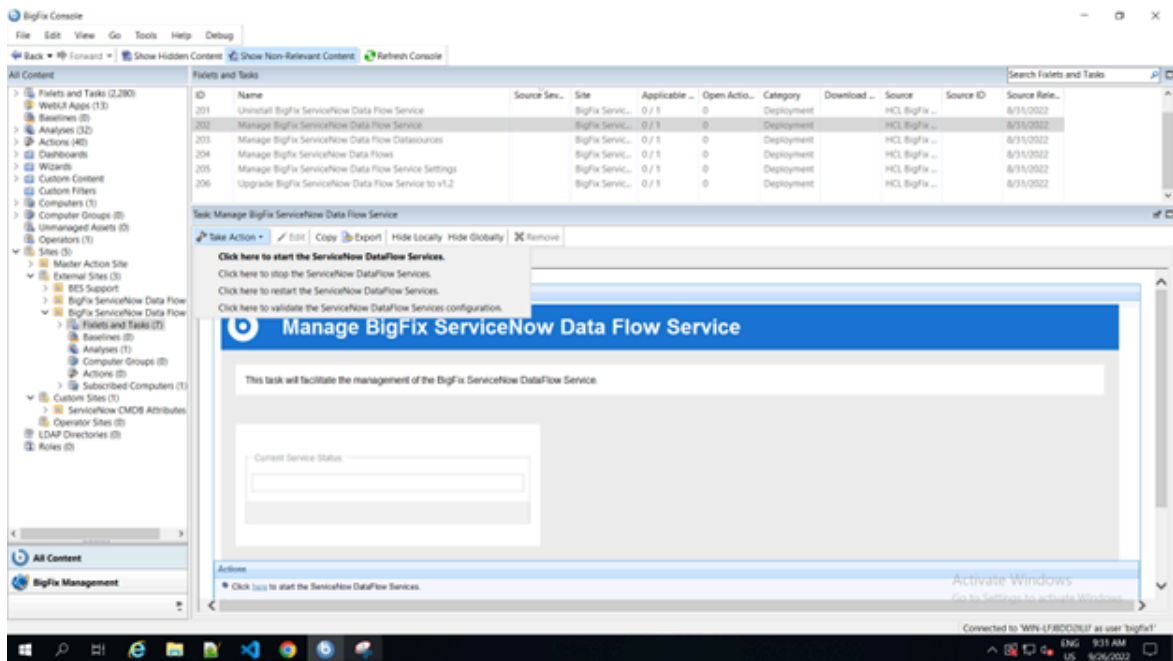
3. Select target devices under Target tab and click **OK**.
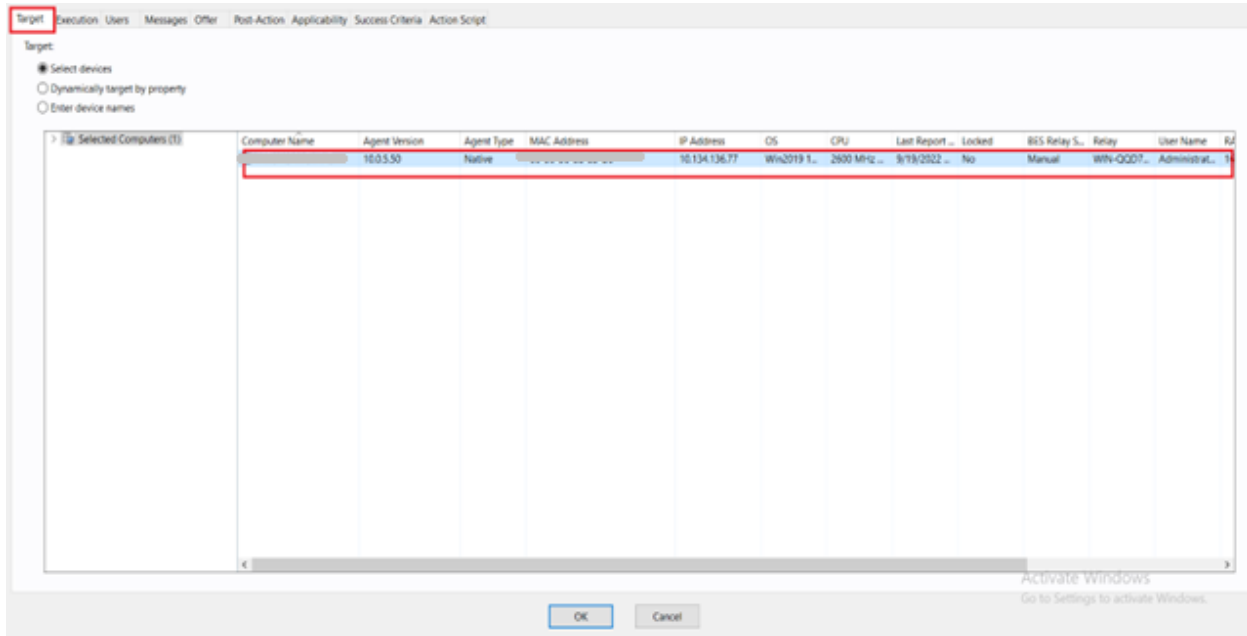
Check manage_services.log in the Dataflow folder for any issues.

Manage BigFix ServiceNow Data Flow Datasources

1. To add or modify connection string, account ,password or the proxy settings of BigFix and ServiceNow use **Manage BigFix ServiceNow Data Flow Datasources** Fixlet from the BigFix ServiceNow Dataflow external site.
2. Choose the datasourcename from the drop down.
3. Add/Modify the datasource connection string , account and password for the selected datasource.
4. Add/Modify the proxy host, proxy username, proxy password for the selected datasource.
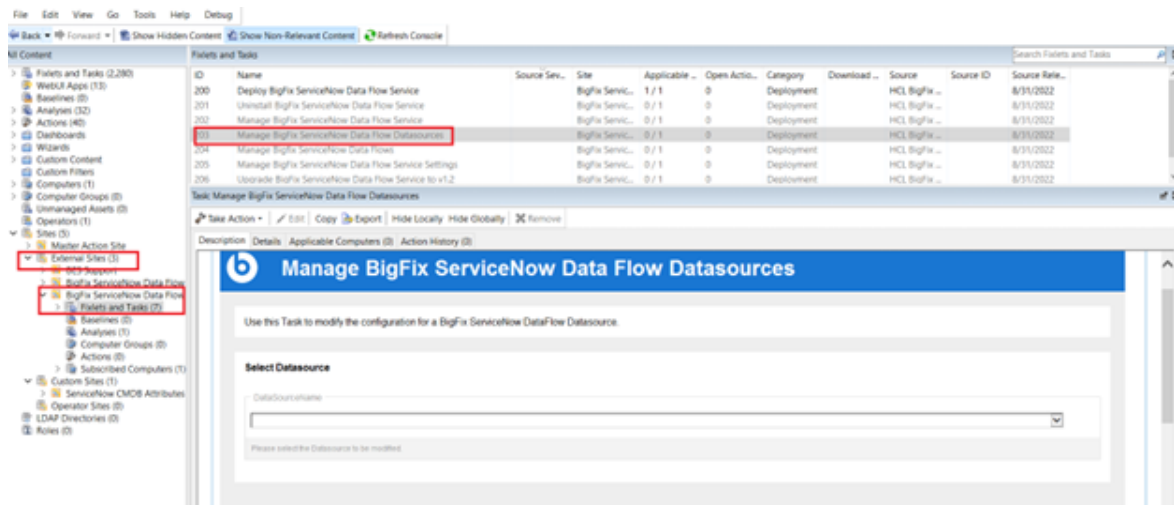
5. Select target devices under Target tab and click **OK**.
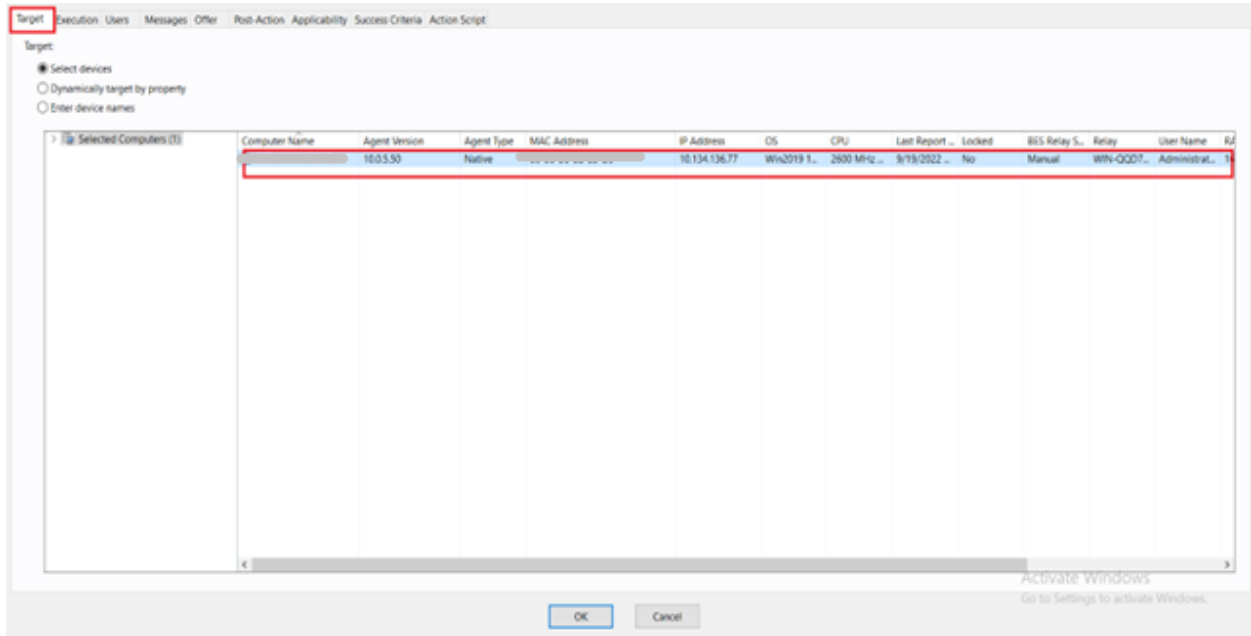
The completion steps are logged in manage_datasource.log in the Dataflow folder.

Manage BigFix ServiceNow Data Flow Service Settings

1. To change the value of a specific setting in the configuration file use **Manage ServiceNow Data Flow Service Settings** Fixlet from BigFix ServiceNow Dataflow external site.
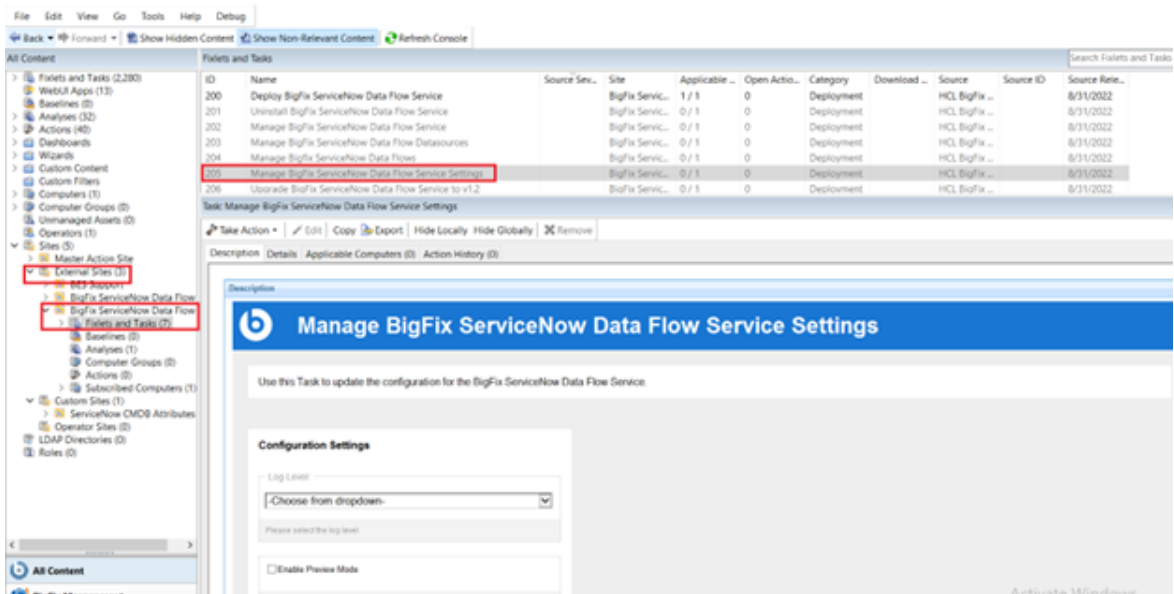
2. Provide all the required details:

- Loglevel : choose the required log level from dropdown
- Enable Preview Mode : unchecked by default. It sets the Preview to false in the configuration file . Enable to turn preview mode to true. Enabling Preview Mode allows you to preview and validate the changes that will be made to BigFix and/or ServiceNow in a file rather than making the changes in the target system.
- Max Computer age : provide suitable computer age. Max computer age retrieves the computers that have been reported to BigFix Server within the max computer age value. Ex : If maxcomputerage= 3, it pulls computer from BigFix server that were reported within last 3 hours.

3. Select target devices under Target tab and click **OK**.
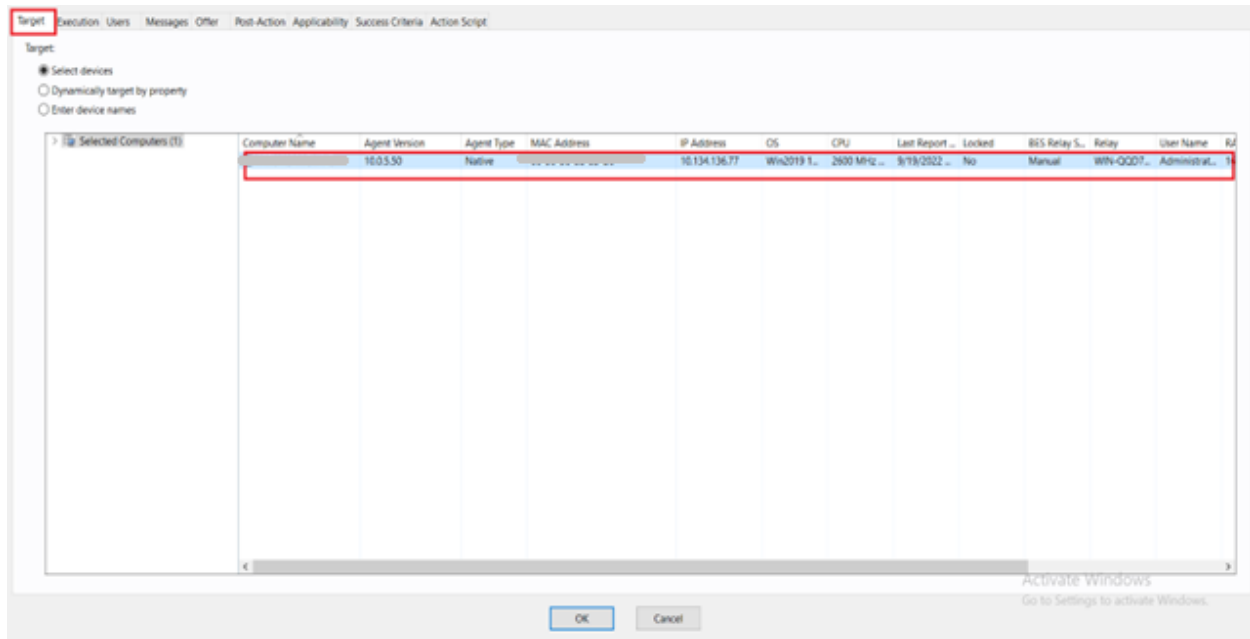
Changes in the settings are logged in the manage_settings.log in the Dataflow folder.

Manage BigFix ServiceNow Data Flows

1. To change the scheduler or to remove any dataflow from configuration file use **Manage BigFix ServiceNow Data Flows** Fixlet from the Bigfix ServiceNow Dataflow external site.
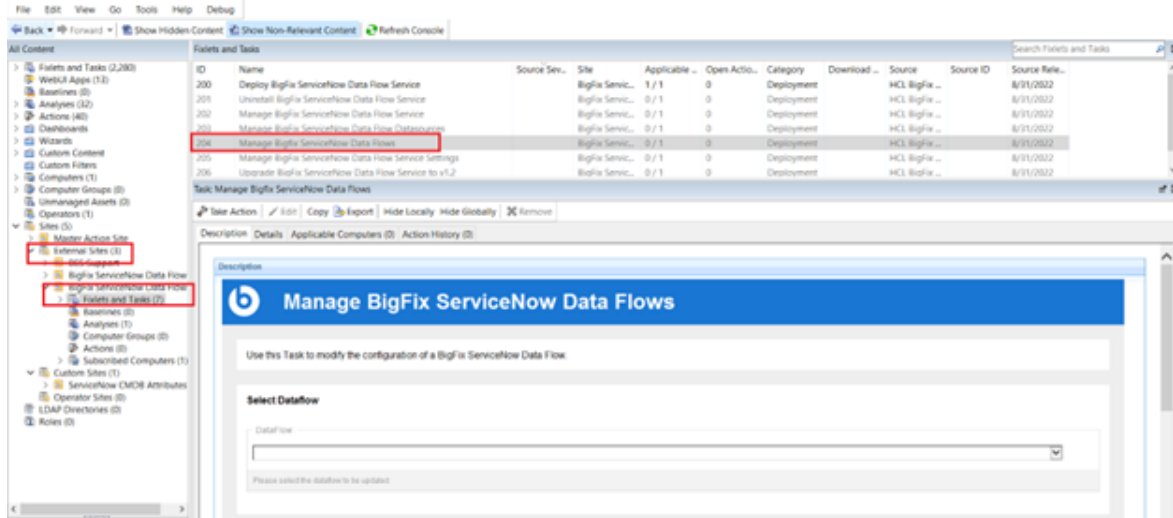
2. Provide all the required details:

    ◦ DataFlow: choose the Dataflow from dropdown
    ◦ Configure DataFlow ETL: the existing schedule from the configuration file will appear in the Configure Dataflow ETL block. Provide a different scheduler in the unix cron time format. Follow the link to learn more about the scheduler.
    ◦ Check the checkbox to remove the selected dataflow from the configuration file if needed.
3. Select target devices under Target tab and click **OK**.
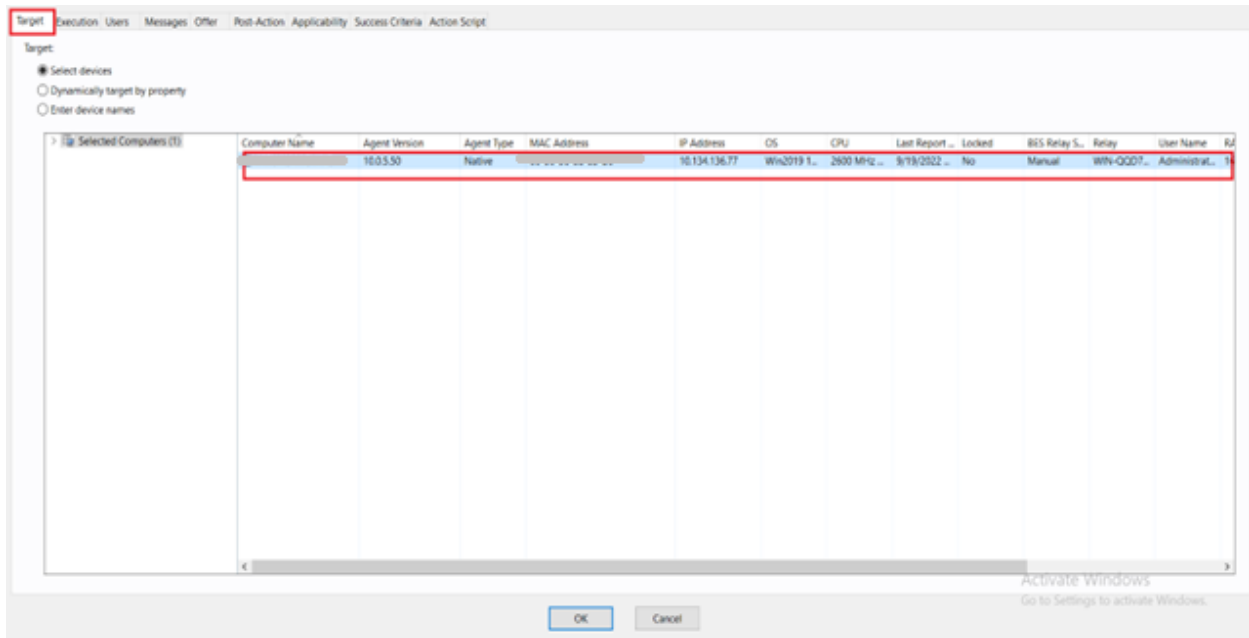
The changes are logged in the manage_dataflows.log file in the Dataflow folder.

Chapter 6. Working with basic functions

This module helps you update and validate configuration.

Updating the configuration

To update the configuration file, do the following steps:

1. Open the `Dataflowsconfig.xml` file in your preferred text editor.

   By default, the file is found at `C:\Program Files\HCL\IntegrationServices\src\Dataflowsconfig.xml`.
2. Edit the file and save the changes.
3. In the CLI, run the --ValidateConfiguration command.
4. Resolve issues found, if any.
5. Restart the service to import the new configuration.

Updating the credentials

If you need to change the credentials for a data source, access the Integration Service CLI with the ProvideCredentials command. You can supply an additional command line parameter to key in a specific data source to modify; otherwise, you are prompted to enter a user name and password.

To update the credentials, do the following steps:

1. Open the Integration Services CLI. By the default, the executable is found at `C:\Program Files\IntegrationServices\DataFlows.exe`.
2. Run the following command: --ProvideCredentials.
3. Enter the credentials for the data source:
     - Username
     - Password
4. Enter the BigFix REST API credentials:
     - Username
     - Password

Upon successful update, the following message appears at the command prompt: "The entered credentials are encrypted successfully".

Note: The password field appears blank even after you enter the password.

Initializing Schema

Purpose: This step initializes the analysis in BigFix.

1. Navigate to the installation directory and run `\Dataflow.exe --InitializeSchemas` command.

   When successful, the message 'Schema Initialized Successfully!' appears in the command prompt.

Validating the configuration

Validating the configuration involves validating the credentials, data flows, duplicate column names and properties of the configuration. In the CLI, run the --ValidateConfiguration command. Upon successful completion, the following message appears: "Configuration verified successfully".

Configuring the solution

The default configuration file provides for bi-directional configuration, which synchronizes common properties across both the systems. The default mapping of properties could be customized to meet the unique needs of each environment.

- Configure the connection string of each data source in the default configuration file.
- Use the CLI to provide credentials and validate the document. For details, click link.
- Use the CLI to start the service. For details, click link.

Note: The base configuration is set to Preview Mode by default.

Chapter 7. Reference

The following topics contain information on how you can work with the configuration file and settings, the CLI that comes with the package. They also describe how to use the log files for troubleshooting purposes.

Configuration file

The name of the configuration file that Data Flow service uses is called `Dataflowsconfig.xml` and is located in the default installation path. The file contains three sections: Data Sources, Data Flows, and Settings. All tags and attribute names in the file must be in lower case. There is also an XSD file that you can use to validate the configuration file on startup.

\<DataSources\>

The `<DataSources>` tag of the Configuration File represents a collection of the different data sources that the solution is configured to interact with. For a configuration to be valid, two datasources are required at the minimum. The `<datasourcename>` attribute should be unique.

\<DataSource\>

The `<datasource>` tag is a child node of the `<datasources>` tag in the configuration document and represents the configuration information for a single datasource.

Attribute name	De-fault value	Required	Description
data-source-name		Yes	This attribute is used to uniquely identify the datasource. With this attribute, data-sources can be mapped to specific adapters within each data flow
connec-tion-string		Yes	This is the URL of the respective data sources. For example: `https://<ipad-dress/hostname>:{Port}/api` (BigFix) `https://<InstanceID>.Service-Now.com/api/now/table` (ServiceNow)
user-name		System generat-ed	This attribute is managed through the ProvideCredentials command. The data is en-crypted prior to being persisted in the configuration file
pass-word		System generat-ed	This attribute is managed through the ProvideCredentials command. The data is en-crypted prior to being persisted in the configuration file
verifyc-ert	True	No	This attribute enables or disables SSL certificate validation with this data source

Attribute name	De- fault value	Required	Description
proxy_- host	N/A	Yes	This attribute provides the proxy server host along with a port number (format: HTTP:// or HTTPS://proxy_host:proxy_port).
prox- y_user- name	N/A	Optional	This attribute is managed through the configureproxy command. The data is encrypt- ed prior to being persisted in the configuration file.
proxy_- pass- word	N/A	Optional	This attribute is managed through the configureproxy command. The data is encrypt- ed prior to being persisted in the configuration file.

Note: If the verify cert is set to True in case of proxy, ensure the proxy machine certificate is added to the client of the machine.

<DataFlows>

The `<DataFlows>` tag of the configuration file represents a collection of the different data flows that the solution is configured to execute.

<DataFlow>

Each `<DataFlow>` tag represents an instance of the flow of data from one system to another and consists of a Source Adapter tag and a Target Adapter tag.

Attribute name	Re- quired	Description
displayname	Yes	This attribute is used to describe the individual data flow
datatype	Yes	By default it is set to asset
schedule*	Yes	Find more information about schedule here

Schedule*

Cron Time String Format: The Cron time string format consists of five fields that Cron converts into a time interval. Cron then uses this interval to determine how often to schedule the DataFlow. 5 place values specifies Minute, Hour, Day of the Month, Month, Day of the week respectively.

Table 2.

Character	Descriptor	Acceptable values
1	Minute	**0** to **59**, or * (no specific value)

Table 2. (continued)

Character	Descriptor	Acceptable values
2	Hour	**0** to **23**, or * for any value. All times UTC
3	Day of month	**1** to **31**, or * (no specific value)
4	Month	**1** to **12**, or * (no specific value)
5	Day of the week	**0** to **7** (0 and 7 both represent Sunday), or * (no specific value)

Example usecases:

- Execute data flow after specific minutes past the hour, every hour.
- Execute data flow at specific time of UTC every Monday.
- Execute data flow every five minutes.
- Execute data flow every second hour, on the hour.

Example1: Cron time string of `0 10 15 * *` executes a command on the 15th of each month at 10:00 A.M. UTC.

Example2: Cron time string of `10/30 10 * * *` executes a command on the 10th minute of 10th hour of each day and for every 30 minutes there after.

> **Note:** The scheduler value should be configured one minute later to the current time if the dataflow needs to be executed immediately once the start of DataFlows service. For example, if the current time is 11:35:30 the scheduler can be configured to 36 11 * * *.

> **Note:** When initially testing the integration, "now" can be used in the scheduler and Dataflow execution can be tested manually. Once the configuration works, then configure the schedule as per convenience. Ex: schedule = "now".

<FilterQuery>

The `<FilterQuery>` tag is used to filter the records that are monitored by a particular adapter tag. This tag consists of a native query for the selected adapter type. For BigFixRest, this would be a session relevance, while in ServiceNowRest it would be a SysParam_Query value.

For details on session relevance, see The Relevance Language and on ServiceNow filters and queries, see Operators available for filters and queries.

> **Note:** The `<FilterQuery>` does not work when it is specified in the following format:

    <filterquery>

<![CDATA[*********]]>

</filterquery>

The `<FilterQuery>` should be specified in one line. Ex:

<filterquery><![CDATA[*********]]></filterquery>

<SourceAdapter>

The `<SourceAdapter>` tag identifies the source system from which the data is extracted. It must include a Properties collection, with a minimum of two properties being valid. Optionally, it may also consist of a `<FilterQuery>` that leverages the native querying syntax of the AdapterClass that is leveraged.

Attribute name	Re-quired	Description
display-name	Yes	This attribute is used to describe this adapter configuration
adapter-class	Yes	Options: bigfix or servicenow This attribute determines which adapter is used to extract data from the source data source
data-source-name	Yes	This attribute value must match the name of a data source defined in the data sources collection. It is used to provide connection information to the adapter

<TargetAdapter>

The `<TargetAdapter>` tag identifies the target system in to which the data is loaded. It must include a Properties collection, with a minimum of two properties being valid. Optionally, it may also consist of a `<FilterQuery>` that leverages the native querying syntax of the AdapterClass being leveraged.

Attribute name	Re-quired	Description
display-name	Yes	This attribute is used to describe this adapter configuration
adapter-class	Yes	Options: bigfix or servicenow This attribute determines which adapter is used to extract data from the source data source
data-source-name	Yes	This attribute value must match the name of a data source defined in the data sources collection. It is used to provide connection information to the adapter

<device_properties>

The `<device_properties>` tag represents a collection of properties in a specific adapter. Each property in this collection is mapped by position to the collection in the corresponding target or source adapter.

The `<sourcekey>` tag represents defines primary key of the adapter. Only one property in each collection must be designated as a Primary Key.

The `<targetkey>` tag represents defines foreign key of the adapter.

> **Note:** The source and the target column positions should not be changed as defined in the default configuration file.

<Property>

The `<Property>` tag represents a single column of data that is either extracted from or loaded in to a system. It may include simple transformation logic to facilitate the transformation of the data received.

Attribute name	Required	Description
displayname	Yes	This attribute is used to describe the property being configured
property-name	Yes	This attribute is used to identify the corresponding column using a notation specific to each adapter
datatype	Yes	The datatype which could be STRING, DATETIME, DATE, INT, DECIMAL, or BOOLEAN

> **Note:** BigFix Columns can be identified by using two patterns: Retrieved Property ID (int) or [SiteName]-[Analysis Name]-[PropertyNumber]

<IdentityProperty>

The `<IdentityProperty>` tag represents a single column of data that is either extracted from or loaded into a system. It may include simple transformation logic to facilitate the transformation of the data received.

Attribute name	Required	Description
display-name	Yes	This attribute is used to describe the property being configured
property-name	Yes	This attribute is used to identify the corresponding column using a notation specific to each adapter
datatype	Yes	The datatype which could be STRING, DATETIME, DATE, INT, DECIMAL, or BOOLEAN

Attribute name	Re-quired	Description
weight	Yes	This attribute assigns a weight to the property, which is used for the weighted confidence matching of records. Type: Int.
delimiter	No	This attribute transforms entry into multiple identity properties. To disable transformation, provide empty delimiter: "".

Note: Device Correlation is the mapping of machine records between two systems. The customer is able to configure "identity properties" for an adapter within a datasource, and facilitate the correlation of the records based upon a Weighted Confidence Algorithm.

<TransformationLogic>

The `<TransformationLogic>` tag can be used with a property tag to manipulate the value returned from a system. These transformations are simple python experiences, and typical use cases would be parsing maintenance windows or classification based upon a certain value.

Syntax for transformation logic: `<transformationlogic><![CDATA[str(this_value).lower()]]></transformationlogic></identityproperty>`

<Settings>

The `<Settings>` tag represents a collection of settings for the solution. For a detailed list of settings, see Configuration settings.

Attribute name	Re-quired	Description
key	Yes	This attribute is the name of the setting that is being config-ured
value		This attribute is the value of the setting that is being configured

Configuration settings

This module proides details for all available configuration settings.

Setting name	Data type	De-fault value	Description	Possible values
LogLevel	Enum	INFO	Sets the logging level for the service.	INFO, DEBUG, WARNING, CRITI-CAL, ERROR

Setting name	Data type	Default value	Description	Possible values
NumberOfConcurrentDataflows	Int	2	Sets the number of dataflow processors that can be run concurrently	User defined
PreviewOnly	Boolean	True	If set to true, writes any updates for a datasource into a file (rather than to the datasource)	True, False
DataFlow.QueueRefreshInterval	Int	120 (in seconds)	Number of seconds that a Data Flow Processing Thread sleeps, if there are no pending Tasks.	User defined
bigfixrest.QueueRefreshInterval	Int	120 (in seconds)	The number of seconds that the Adapter Updater waits after collecting the updates. It can be used to throttle output to data sources.	User defined
bigfixrest.UpdateBatchSize	Int	0	The number of updates that are allowed in a batch. If set to 0, there is no limit. An updater processes all the updates when detected.	User defined
servicenowrest.QueueRefreshInterval	Int	120 (in seconds)	The number of seconds that the Adapter Updater waits after updates. It can be used to throttle output to datasource	User defined
servicenowrest.UpdateBatchSize	Int	0	The number of updates that are allowed in a batch. If set to 0, there is no limitation and the updater processes all the updates when detected.	User defined
bigfixrest.MaxComputerAge	Int	2	Limits the computers that are returned by the BigFix Adapter to the number of hours configured by using the Last Report Time of the machine.	User defined
Bigfixrest.ContentSiteName	String	None	Provides a custom site for the service to create a custom analysis and inspect the data from ServiceNow.	User defined (alphanumeric)
servicenowrest.batch_size	Int	250	Limits the records that are returned by the Servicenow Adapter on each request.	default value=250, max value= 9999
LogRetentionPeriod	Int	5	Time for the process to wait before it deletes the log files in the log folder. The configured value is in days.	User defined

Command Line Interface

The Data Flow Service executable provides a Command Line Interface (CLI) that you can use to perform several different functions related to the setup and execution of the solution such as installing, uninstalling, starting and stopping the solution as a native system service, securely providing credentials for data sources, manually validating configuration before starting the service, and running the solution from the BigFix Console.

The Data Flow Service executable (`Dataflows.exe`) can be found in the default deployment folder. To view a list of all the commands supported, type --Help at the command prompt.

Command	Purpose	Additional information
--ProvideCredentials <Data-SourceName>	To securely capture credentials for the each of the datasources	The credentials are saved in configuration files for specific use in an encrypted format. An optional additional parameter may be provided to update credentials for a specific data source.
--ValidateConfiguration	To validate the configuration	
--Install	To install IntegrationServices as a native system service	
--Start	To start IntegrationServices after installing it as a native system service	
--Stop	To stop IntegrationServices that is started as a native system service	
--Uninstall	To remove IntegrationServices as a native system service	

Command	Purpose	Additional information
--initial-izeschemas	To initialize the schema	
--reset	To reset an application	
--configure-proxy	To configure proxy para-meters	

Logs

You can find log files in the `logs` folder in the installation path. They are organized by day. Configure the solution with INFO as the log level unless you intend to troubleshoot an issue.

Connections.[date].log

With DEBUG enabled, this log file contains detailed logging information related to the external connections to third-party datasources.

DataFlow.[date].log

With DEBUG enabled, this log file contains detailed logging information related to the execution of each dataflow. It is the primary interface used for debugging issues related to the ETL (Extract, Transform, Load)..

Main.[date]log

With DEBUG enabled, this log file contains detailed logging information related to the primary processes. It should show issues related to service start and configuration.

Chapter 8. Release Notes

The **release notes** outline the features, updates and patches that are included in each version of BigFix ServiceNow Dataflows, including the latest application updates.

09/30/2022

The BigFix team is very pleased to announce the release of version 1.2 of BigFix ServiceNow Data Flows! This integration enables organizations to harness the wealth of near real-time endpoint data that BigFix makes available to automatically enrich ServiceNow® CMDB. Conversely, it also provides BigFix with access to endpoint metadata and business contexts defined in ServiceNow® CMDB. This enables you to:

Better discover, track, and understand your assets with BigFix endpoint data available in ServiceNow®

Quickly identify, prioritize, and remediate issues by having the business context of your endpoints (such as Department, Location, and Environment) from ServiceNow® directly within BigFix. Even deploy actions targeting these attributes!

The main features of this release are:

- Simplified Deployment, Configuration, and Management of ServiceNow Data Flows through Fixlets
  - You can now deploy as well as configure ServiceNow Data Flows through a single Fixlet to get up and running that much more quickly and easily! For more information, please see the Deployment and configuration1 section of the documentation
  - Additional Tasks are available to simplify upgrades, as well as general management and configuration of ServiceNow Data Flows including data synchronization schedules, credentials, and service states. Please see the Fixlets and Tasks section of the documentation for more information.

- Improved logging

Resolved Defect Articles:

- KB0096631: Mailboxes are not created as expected
- KB0098267: ServiceNow Dataflow not working if Computer ID changes
- KB0098476: ServiceNow dataflow mismatch

Published site version: 5

Useful links:

For more information, please see the documentation.

The BigFix team is very pleased to announce the release of version 1.1 of BigFix ServiceNow Data Flows! This integration enables organizations to harness the wealth of near real-time endpoint data that BigFix makes available to automatically enrich ServiceNow® CMDB. Conversely, it also provides BigFix with access to endpoint metadata and business contexts defined in ServiceNow® CMDB. This enables you to:

- Better discover, track, and understand your assets with BigFix endpoint data available in ServiceNow®
- Quickly identify, prioritize, and remediate issues by having the business context of your endpoints (such as Department, Location, and Environment) from ServiceNow® directly within BigFix. Even deploy actions targeting these attributes!

The main features in this release are as follows:

- Improved Scalability
  - BigFix ServiceNow Data Flows now supports up to 300K devices!
- Better scheduling support
  - You can now define granular schedules for BigFix ServiceNow Data Flows to better control and manage when data will be synchronized and processed
- Proxy support
  - Communications from BigFix ServiceNow Data Flows can now be directed through a proxy for improved security
- Other minor enhancements and bug fixes

BigFix ServiceNow Data Flow is currently available with BigFix 10 Patch, Lifecycle, Compliance, or Inventory.

Useful links:

For more information, please see the https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Install_Config/integrations_imp_guide.html

Appendix A. Support

For more information about this product, see the following resources:

- BigFix Support Portal
- BigFix Developer
- BigFix Playlist on YouTube
- BigFix Tech Advisors channel on YouTube
- BigFix Forum

Appendix B. Glossary

This glossary provides terms and definitions for the Modern Client Management for BigFix software and products.

The following cross-references are used in this glossary:

- *See* refers you from a non-preferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

A B C D E F G L M N O P R S T U V W

A

action

1. See Fixlet.
2. A set of Action Script commands that perform an operation or administrative task, such as installing a patch or rebooting a device.

Action Script

Language used to perform an action on an endpoint.

agent

See BigFix agent.

ambiguous software

Software that has an executable file that looks like another executable file, or that exists in more than one place in a catalog (Microsoft Word as a standalone product or bundled with Microsoft Office).

audit patch

A patch used to detect conditions that cannot be remediated and require the attention of an administrator. Audit patches contain no actions and cannot be deployed.

automatic computer group

A computer group for which membership is determined at run time by comparing the properties of a given device against the criteria set for group membership. The set of devices in an automatic group is dynamic, meaning that the group can and does change. See also computer group.

B

baseline

A collection of actions that are deployed together. A baseline is typically used to simplify a deployment or to control the order in which a set of actions are applied. See also deployment group.

BigFix agent

The BigFix code on an endpoint that enables management and monitoring by BigFix.

BigFix client

See BigFix agent.

BigFix console

The primary BigFix administrative interface. The console provides a full set of capabilities to BigFix administrators.

BYOD

Bring Your Own Device (BYOD) refers to employees using personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data.

C

client

A software program or computer that requests services from a server. See also server.

client time

The local time on a BigFix client device.

Cloud

A set of compute and storage instances or services that are running in containers or on virtual machines.

Common Vulnerabilities and Exposures Identification Number (CVE ID)

A number that identifies a specific entry in the National Vulnerability Database. A vendor's patch document often includes the CVE ID, when it is available. See also National Vulnerability Database.

Common Vulnerabilities and Exposures system (CVE)

A reference of officially known network vulnerabilities, which is part of the National Vulnerabilities Database (NVD), maintained by the US National Institute of Standards and Technology (NIST).

component

An individual action within a deployment that has more than one action. See also deployment group.

computer group

A group of related computers. An administrator can create computer groups to organize systems into meaningful categories, and to facilitate deployment of content to multiple computers. See also automatic computer group and manual computer group.

console

See BigFix console.

content

Digitally-signed files that contain data, rules, queries, criteria, and other instructions, packaged for deployment across a network. BigFix agents use the detection criteria (Relevance statements) and action instructions (Action Script statements) in content to detect vulnerabilities and enforce network policies.

content relevance

A determination of whether a patch or piece of software is eligible for deployment to one or more devices. See also device relevance.

Coordinated Universal Time (UTC)

The international standard of time that is kept by atomic clocks around the world.

corrupt patch

A patch that flags an operator when corrections made by an earlier patch have been changed or compromised. This situation can occur when an earlier service pack or application overwrites later files, which results in patched files that are not current. The corrupt patch flags the situation and can be used to re-apply the later patch.

custom content

BigFix code that is created by a customer for use on their own network, for example, a custom patch or baseline.

CVE

See Common Vulnerabilities and Exposures system.

CVE ID

See Common Vulnerabilities and Exposures Identification Number.

D

data stream

A string of information that serves as a source of package data.

default action

The action designated to run when a Fixlet is deployed. When no default action is defined, the operator is prompted to choose between several actions or to make an informed decision about a single action.

definitive package

A string of data that serves as the primary method for identifying the presence of software on a computer.

deploy

To dispatch content to one or more endpoints for execution to accomplish an operation or task, for example, to install software or update a patch.

deployment

Information about content that is dispatched to one or more endpoints, a specific instance of dispatched content.

deployment group

The collection of actions created when an operator selects more than one action for a deployment, or a baseline is deployed. See also baseline, component, deployment window, and multiple action group.

deployment state

The eligibility of a deployment to run on endpoints. The state includes parameters that the operator sets, such as 'Start at 1AM, end at 3AM.'

deployment status

Cumulative results of all targeted devices, expressed as a percentage of deployment success.

deployment type

An indication of whether a deployment involved one action or multiple actions.

deployment window

The period during which a deployment's actions are eligible to run. For example, if a Fixlet has a deployment window of 3 days and an eligible device that has been offline reports in to BigFix within the 3-day window, it gets the Fixlet. If the device comes back online after the 3-day window expires, it does not get the Fixlet. See also deployment group.

device

An endpoint, for example, a laptop, desktop, server, or virtual machine that BigFix manages; an endpoint running the BigFix Agent.

device holder

The person using a BigFix-managed computer.

device property

Information about a device collected by BigFix, including details about its hardware, operating system, network status, settings, and BigFix client. Custom properties can also be assigned to a device.

device relevance

A determination of whether a piece of BigFix content applies to applies to a device, for example, where a patch should be applied, software installed, or a baseline run. See also content relevance.

device result

The state of a deployment, including the result, on a particular endpoint.

Disaster Server Architecture (DSA)

An architecture that links multiple servers to provide full redundancy in case of failure.

DSA

See Disaster Server Architecture.

dynamically targeted

Pertaining to using a computer group to target a deployment.

E

endpoint

A networked device running the BigFix agent.

F

filter

To reduce a list of items to those that share specific attributes.

Fixlet

A piece of BigFix content that contains Relevance and Action Script statements bundled together to perform an operation or task. Fixlets are the basic building blocks of BigFix content. A Fixlet provides instructions to the BigFix agent to perform a network management or reporting action.

Full Disk Encryption

To reduce a list of items to those that share specific attributes.

G

group deployment

A type of deployment in which multiple actions were deployed to one or more devices.

L

locked

An endpoint state that prevents most of the BigFix actions from running until the device is unlocked.

M

MAG

See multiple action group.

management rights

The limitation of console operators to a specified group of computers. Only a site administrator or a master operator can assign management rights.

manual computer group

A computer group for which membership is determined through selection by an operator. The set of devices in a manual group is static, meaning they do not change. See also computer group.

master operator

A console operator with administrative rights. A master operator can do everything that a site administrator can do, except creating operators.

masthead

A collection of files that contain the parameters of the BigFix process, including URLs to Fixlet content. The BigFix agent brings content into the enterprise based on subscribed mastheads.

MCM and BigFix Mobile

Refers to the offering by Bigfix that is common for both Modern Client Management to manage laptops (Windows and macOS) and BigFix Mobile to manage mobile devices (Android, iOS, and iPadOS).

mirror server

A BigFix server required if the enterprise does not allow direct web access but instead uses a proxy server that requires password-level authentication.

Multicloud

The utilization of distinct sets of cloud services, typically from multiple vendors, where specific applications are confined to a single cloud instance.

multiple action group (MAG)

A BigFix object that is created when multiple actions are deployed together, as in a baseline. A MAG contains multiple Fixlets or tasks. See also deployment group.

N

National Vulnerability Database (NVD)

A catalog of officially known information security vulnerabilities and exposures, which is maintained by the National Institute of Standards and Technology (NIST). See also Common Vulnerabilities and Exposures Identification Number.

NVD

See National Vulnerability Database.

O

offer

A deployment option that allows a device holder to accept or decline a BigFix action and to exercise some control over when it runs. For example, a device holder can decide whether to install a software application, and whether to run the installation at night or during the day.

open-ended deployment

A deployment with no end or expiration date; one that runs continuously, checking whether the computers on a network comply.

operator

A person who uses the BigFix WebUI, or portions of the BigFix console.

P

patch

A piece of code added to vendor software to fix a problem, as an immediate solution that is provided to users between two releases.

patch category

A description of a patch's type and general area of operation, for example, a bug fix or a service pack.

patch severity

The level of risk imposed by a network threat or vulnerability and, by extension, the importance of applying its patch.

R

relay

A client that is running special server software. Relays spare the server and the network by minimizing direct server-client downloads and by compressing upstream data.

Relevance

BigFix query language that is used to determine the applicability of a piece of content to a specified endpoint. Relevance asks yes or no questions and evaluates the results. The result of a Relevance query determines whether an action can or should be applied. Relevance is paired with Action Script in Fixlets.

S

SCAP

See Security Content Automation Protocol.

SCAP check

A specific configuration check within a Security Content Automation Protocol (SCAP) checklist. Checks are written in XCCDF and are required to include SCAP enumerations and mappings per the SCAP template.

SCAP checklist

A configuration checklist that is written in a machine-readable language (XCCDF). Security Content Automation Protocol (SCAP) checklists have been submitted to and accepted by the NIST National Checklist Program. They also conform to a SCAP template to ensure compatibility with SCAP products and services.

SCAP content

A repository that consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations.

SCAP enumeration

A list of all known security related software flaws (CVEs), known software configuration issues (CCEs), and standard vendor and product names (CPEs).

SCAP mapping

The interrelationship of enumerations that provides standards-based impact measurements for software flaws and configuration issues.

Security Content Automation Protocol (SCAP)

A set of standards that is used to automate, measure, and manage vulnerability and compliance by the National Institute of Standards and Technology (NIST).

server

A software program or a computer that provides services to other software programs or other computers. See also client.

signing password

A password that is used by a console operator to sign an action for deployment.

single deployment

A type of deployment where a single action was deployed to one or more devices.

site

A collection of BigFix content. A site organizes similar content together.

site administrator

The person who is in charge of installing BigFix and authorizing and creating new console operators.

software package

A collection of Fixlets that install a software product on a device. Software packages are uploaded to BigFix by an operator for distribution. A BigFix software package includes the installation files, Fixlets to install the files, and information about the package (metadata).

SQL Server

A full-scale database engine from Microsoft that can be acquired and installed into the BigFix system to satisfy more than the basic reporting and data storage needs.

standard deployment

A deployment of BigFix that applies to workgroups and to enterprises with a single administrative domain. It is intended for a setting in which all Client computers have direct access to a single internal server.

statistically targeted

Pertaining to the method used to target a deployment to a device or piece of content. Statically targeted devices are selected manually by an operator.

superseded patch

A type of patch that notifies an operator when an earlier version of a patch has been replaced by a later version. This occurs when a later patch updates the same files as an earlier one. Superseded patches flag vulnerabilities that can be remediated by a later patch. A superseded patch cannot be deployed.

system power state

A definition of the overall power consumption of a system. BigFix Power Management tracks four main power states Active, Idle, Standby or Hibernation, and Power Off.

T

target

To match content with devices in a deployment, either by selecting the content for deployment, or selecting the devices to receive content.

targeting

The method used to specify the endpoints in a deployment.

task

A type of Fixlet designed for re-use, for example, to perform an ongoing maintenance task.

U

UTC

See Coordinated Universal Time.

V

virtual private network (VPN)

An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure.

VPN

See virtual private network.

vulnerability

A security exposure in an operating system, system software, or application software component.

W

Wake-from-Standby

A mode that allows an application to turn a computer on from standby mode during predefined times, without the need for Wake on LAN.

Wake on LAN

A technology that enables a user to remotely turn on systems for off-hours maintenance. A result of the Intel-IBM Advanced Manageability Alliance and part of the Wired for Management Baseline Specification, users of this technology can remotely turn on a server and control it across the network, thus saving time on automated software installations, upgrades, disk backups, and virus scans.

WAN

See wide area network.

wide area network (WAN)

A network that provides communication services among devices in a geographic area larger than that served by a local area network (LAN) or a metropolitan area network (MAN).

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.