Overview of Source and Destination Fine Grain Permission Option for Personal Data

for

CI Synchronizer (Enterprise Edition)

Last Updated: 19 March 2024

Table of Contents

Disclaimer

Nothing in this document represents any form or actual or implied guarantee or warranty by Syncfish. Furthermore, this document does not form any part of the terms and conditions of the service, or services offered by Syncfish.

Content in relation to CI Synchronizer

Material in this document that describes the working of CI Synchronizer is accurate as at the time of writing. Syncfish applies reasonable endeavors to maintain this content, however it is possible for the system behavior of CI Synchronizer to deviate from the content in this document. This also applies to the services provided by the providers who underpin CI Synchronizer (for example our Cloud Hosts).

Content in relation to Source and Destination Systems and Providers

Syncfish do not possess intimate details of the inner workings or the entire data structure of the source and destination systems. The information contained in the following pages should not be taken as any form of guarantee or warranty about the presence or storage location of Personal Data in those systems. Instead, the following information is provided so that organizations and their technical SMEs understand this topic and can assess the ability to implement fine grain controls should they wish to. Customers should contact the relevant source or destination system vendor to obtain further confidence about the storage of Personal Data and the access afforded by the credentials customers allocate to the two CI Sync (EE) components (i.e. the CI Sync (EE) Agent and the CI Sync (EE) SaaS solution).

Overview

Intended Audience

This document is intended for the following roles within an organization.

Role	Explanation
Data Privacy Personnel	Any individual responsible for assessing the data privacy implications of a CI Sync (EE) implementation within their organization.
Source and Destination System Subject Matter Experts (SMEs)	Technical SMEs with detailed knowledge of the authentication and authorization setup of CI Sync (EE) for access to Source System/s (to read data) and Destination System/s (to write data).

Document Purpose and Scope

This document explains two design concepts about Personal Data within the context of a CI Synchronizer (Enterprise Edition) implementation.

Concept #	Design Concept (explained as a test question)
Concept #1	Does CI Sync (EE) process or persist Personal Data?
Concept #2	Do default permissions in Source and/or Destination Systems allow the two CI Sync (EE) components to access Personal Data beyond the scope of CI Sync (EE)?

The purpose for explaining the above concepts is so customers (or prospective customers) are fully informed about the following four configuration topics.

1. The default behavior of CI Sync (EE) which **does not** process (or store) any Personal Data.
2. Under what **circumstances the default behavior of CI Sync (EE) may be changed** to process a correlation attribute that **might** contain Personal Data. Furthermore, what specific data is transited and/or persisted within the customer specific SaaS component of the CI Sync (EE) solution.
3. The **specific access the CI Sync (EE) Agent component** has to the **source system** data (regardless of the default behavior or customer specific behaviors note above).
4. The **specific access the CI Sync (EE) SaaS component** has to the **destination system** data (regardless of the default behavior or customer specific behaviors note above).

By understanding the above information (the two design concepts and the four configuration topics) customers can make the following decisions:

1. Do they want to adopt the default configuration of CI Sync (EE) which does not process (or store) any Personal Data, or do they want to override the default configuration (and if so, what data is then being processed and/or stored)?
2. Do they want to implement fine grain permissions on the source and destination system to restrict the CI Sync (EE) components from having any potential access to Personal Data stored in the source and destination systems? This question should be assessed regardless of whether the default configuration or overridden configuration is being used.

Explanation of Key Concepts and Configuration Options

Explanation of Concept #1 – Does CI Sync (EE) process or persist Personal Data?

The primary purpose of CI Sync (EE) is to transit IT asset device data from a source system to a destination system. The attributes associated with IT asset devices are most commonly values such as serial numbers, MAC Addresses, installed software and so on.

The primary purpose of CI Sync (EE) is not to transit (or store) Personal Data.

Default Configuration of CI Sync (EE)

- By default, CI Sync (EE) does not read, process, or store any specific attributes known to contain Personal Data. This applies to both the source systems and the destination systems. This is a privacy by design and default position of CI Sync (EE).
- It is theoretically possible for an unintended attribute to contain Personal Data (or any other value for that matter) and CI Sync (EE) would have no context whatsoever of this situation. For example, in the unusual situation the name of an individual is included in the machine/host name of a given IT asset, or within the contents of a custom field or "Tag" on a device, etc. None of these attributes are intended to contain Personal Data, but clearly if data of a personal nature is stored in these attributes, then such data would be passing through CI Sync (EE).

Customer Specific Override Configuration of CI Sync (EE)

- Occasionally customers may want CI Sync (EE) to create a reference between an IT asset and the user of that IT asset. Such reference between the device and a user can be helpful if the reference is set in the destination system.
- For example, within a CMDB it can be helpful for a Service Desk team to see the "Assigned To" attribute set on a Configuration Item (CI)/IT Asset record.
- In the above circumstance, and only upon request by a customer to override the default configuration, CI Sync (EE) will need to read a **user related <u>correlation value</u> from the asset record** in the source system so **it can then set a <u>relationship</u>** (i.e. a foreign key) between the destination system CI/Asset record and the user related table in the destination system.

The **contents of the correlation attribute** used to achieve the intended outcome will vary on a customer-by-customer basis (and needs to be agreed in advance) before the default configuration of CI Sync (EE) can be amended. The selection of a suitable correlation attribute is subject to determining a common attribute/value between the source and destination systems. Syncfish can assist customers to determine a suitable correlation attribute but ultimately this comes down to each customer understanding their own data and what is stored in the source and destination systems.

In summary for Concept #1

- CI Sync (EE)'s primary intent is to synchronize IT Asset related data. The primary purpose is not to synchronize person/people related data. The default configuration of CI Sync (EE), which applied by default to all customer instances of CI Sync (EE) aligns to this intent.
- A customer may request the default configuration is overridden within the customer specific instance of CI Sync (EE) to cause CI Sync (EE) to correlate a given user related attribute in the source system against a given user related attribute in the destination system.
- Important points follow when considering an override of the default:
  - Analysis will be required by the customer and Syncfish to determine a suitable user related attribute for this purpose.
  - Determining whether the content of a user-related correlation attribute contains Personal Data or PII data is the customer's responsibility. This determination is not the responsibility of Syncfish because for CI Sync (EE) any given attribute can in theory contain any value whatsoever.
  - The customer specific instance of CI Sync (EE) will both transit and persist the user related correlation attribute values once it is included in a customer specific configuration.
  - It is the customer's responsibility to trigger any data privacy related contractual obligations when requesting Syncfish to override the default configuration of the customers CI Sync (EE) instance.

Diagrams showing the two concepts

The diagrams on the subsequent pages show how this works in practice.

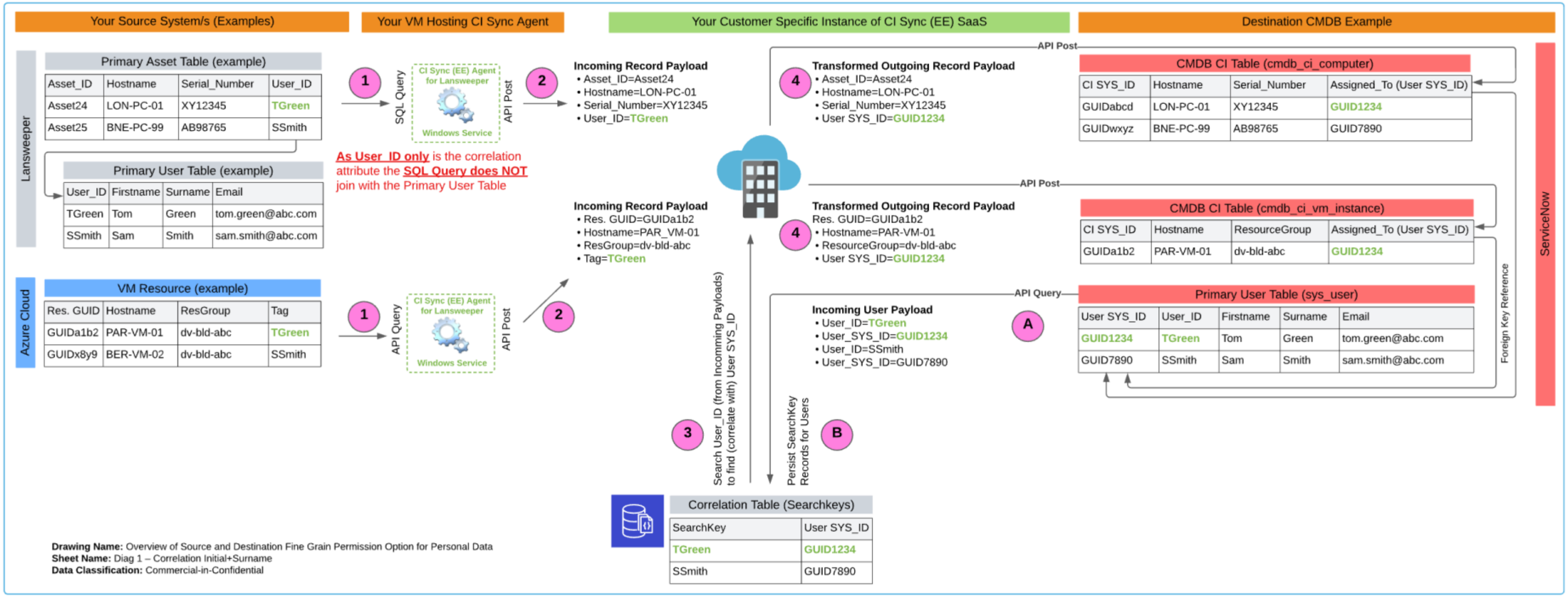
These diagrams are **only applicable if a customer has decided to override the default behavior** of CI Sync (EE). CI Sync (EE) does NOT read user related attributes from the source or destination systems if the default configuration is being used.

The two diagrams demonstrate how the content of the correlation value can differ on a customer-by-customer basis.

The two diagrams also demonstrate how in one situation a pseudonym style of value is used for correlation and in another situation a clearly personally identifiable value is used. In both examples the exact same correlation attribute is used, but in each case the content (values) held with the correlation attribute are very different.

The ideal data protection situation is for customers to locate a correlation attribute in the source and destination that only contains pseudonym values (e.g. a short form User ID value) rather than personally identifiable values (email address containing first name and surname).

Diagram 1 – Username/User ID correlation attribute containing First Initial & Surname


Your Source System/s (Examples)
Your VM Hosting CI Sync Agent
Your Customer Specific Instance of CI Sync (EE) SaaS
Destination CMDB Example
Lansweeper
Azure Cloud
ServiceNow
1
SQL Query
CI Sync (EE) Agent for Lansweeper
Windows Service
API Post
2
1
API Query
CI Sync (EE) Agent for Lansweeper
Windows Service
API Post
2
API Post
4
API Post
4
API Query
A
Foreign Key Reference
3
Search User_ID (from Incomming Payloads) to find (correlate with) User SYS_ID
Persist SearchKey Records for Users
B

Primary Asset Table (example)

Asset_ID	Hostname	Serial_Number	User_ID
Asset24	LON-PC-01	XY12345	TGreen
Asset25	BNE-PC-99	AB98765	SSmith

Primary User Table (example)

User_ID	Firstname	Surname	Email
TGreen	Tom	Green	tom.green@abc.com
SSmith	Sam	Smith	sam.smith@abc.com

VM Resource (example)

Res. GUID	Hostname	ResGroup	Tag
GUIDa1b2	PAR-VM-01	dv-bld-abc	TGreen
GUIDx8y9	BER-VM-02	dv-bld-abc	SSmith

As User_ID only is the correlation attribute the **SQL Query does NOT** join with the Primary User Table

Incoming Record Payload
- Asset_ID=Asset24
- Hostname=LON-PC-01
- Serial_Number=XY12345
- User_ID=TGreen

Incoming Record Payload
- Res. GUID=GUIDa1b2
- Hostname=PAR_VM-01
- ResGroup=dv-bld-abc
- Tag=TGreen

Transformed Outgoing Record Payload
- Asset_ID=Asset24
- Hostname=LON-PC-01
- Serial_Number=XY12345
- User SYS_ID=GUID1234

Transformed Outgoing Record Payload
Res. GUID=GUIDa1b2
- Hostname=PAR-VM-01
- ResourceGroup=dv-bld-abc
- User SYS_ID=GUID1234

Incoming User Payload
- User_ID=TGreen
- User_SYS_ID=GUID1234
- User_ID=SSmith
- User_SYS_ID=GUID7890

CMDB CI Table (cmdb_ci_computer)

CI SYS_ID	Hostname	Serial_Number	Assigned_To (User SYS_ID)
GUIDabcd	LON-PC-01	XY12345	GUID1234
GUIDwxyz	BNE-PC-99	AB98765	GUID7890

CMDB CI Table (cmdb_ci_vm_instance)

CI SYS_ID	Hostname	ResourceGroup	Assigned_To (User SYS_ID)
GUIDa1b2	PAR-VM-01	dv-bld-abc	GUID1234

Primary User Table (sys_user)

User SYS_ID	User_ID	Firstname	Surname	Email
GUID1234	TGreen	Tom	Green	tom.green@abc.com
GUID7890	SSmith	Sam	Smith	sam.smith@abc.com

Correlation Table (Searchkeys)

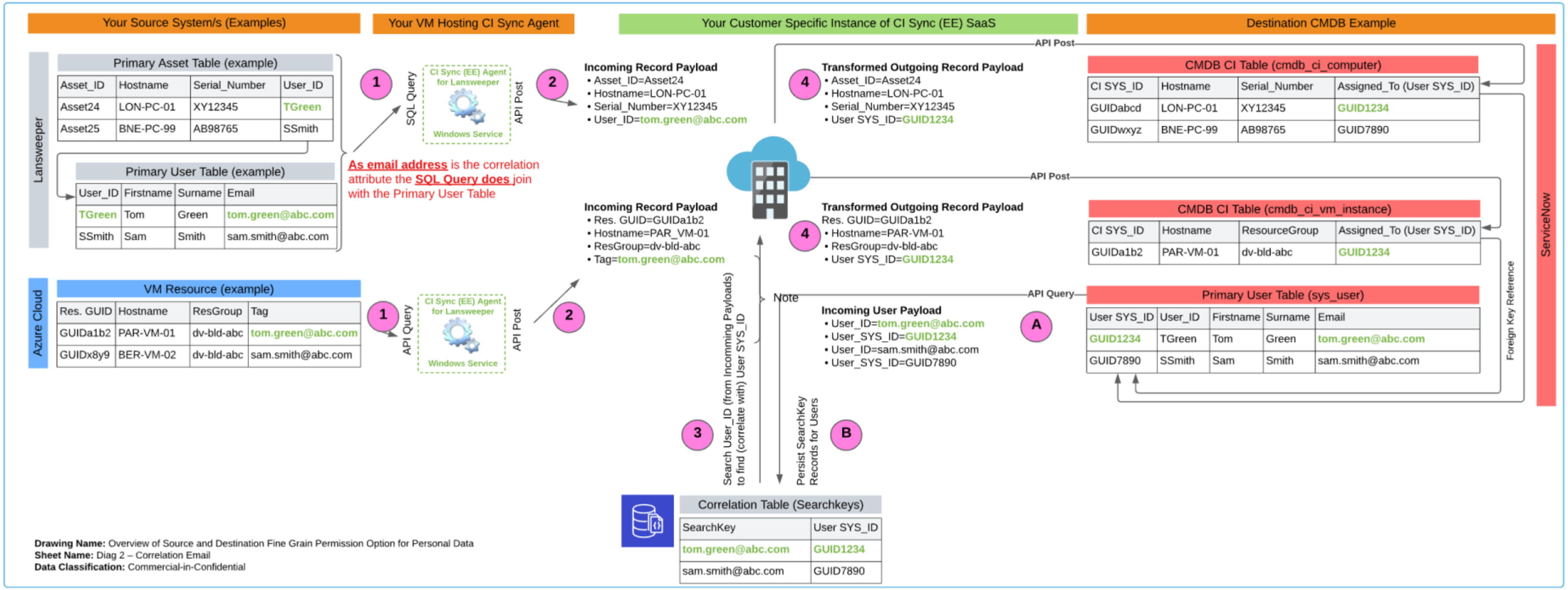
SearchKey	User SYS_ID
TGreen	GUID1234
SSmith	GUID7890

Drawing Name: Overview of Source and Destination Fine Grain Permission Option for Personal Data
Sheet Name: Diag 1 – Correlation Initial+Surname
Data Classification: Commercial-in-Confidential

Suggestion: Trace the bold/green TGreen value (and subsequently it's GUID1234 SYS_ID value) on the above diagram to see how it is processed by CI Sync.

Ref #	**Explanation** *(these only apply if a customer has decided to override the default behavior of CI Sync)*
A	At the start of each synchronization job, your customer specific CI Sync SaaS instance queries the sys_user table in ServiceNow. CI Sync only queries two values: (1) The agreed correlation attribute (in the above diagram this is the value in the User_ID field), and (2) the SYS_ID value.
B	CI Sync persists the two values in your customer specific SearchKey database (a MongoDB database which is a part of your customer specific CI Sync SaaS instance).
1	The CI Sync (EE) Agent (windows service) queries the **primary asset/resource table** from the Source System. The **query does not extend into any other tables if the agreed correlation attribute is entirely contained in the primary asset/resource table** (as per the example in the diagram which shows that "TGreen" is all that is required to correlate against the values held in the SearchKey database thanks to steps (A) and (B) above).
2	The CI Sync (EE) Agent sends the record payload to your CI Sync SaaS instance. The payload contains the asset/resource attributes/values and the user correlation attribute/value (i.e. "TGreen").
3	Logic in your CI Sync SaaS instance checks your MongoDB SearchKey table and finds a match on "TGreen"). CI Sync (EE) now knows the ServiceNow SYS_ID for the user "TGreen" (the pretend SYS_ID in the above example is "GUID1234").
4	The CI Sync SaaS code creates an ongoing record payload which now only contains the SYS_ID (i.e. "GUID1234"). CI Sync updates the relevant CMDB_CI table with the asset/record attributes/values in addition it sets the Assigned_To field with the SYS_ID of the user (i.e. "GUID1234") as the foreign key reference to the SYS_USER table.

Diagram 2 – Username/User ID correlation attribute containing a First Name & Surname style of Email Address



Your Source System/s (Examples)
Your VM Hosting CI Sync Agent
Your Customer Specific Instance of CI Sync (EE) SaaS
Destination CMDB Example
Lansweeper
Azure Cloud
1
SQL Query
CI Sync (EE) Agent for Lansweeper
Windows Service
API Post
2
1
API Query
CI Sync (EE) Agent for Lansweeper
Windows Service
API Post
2
4
4
API Post
API Post
API Query
Note
A
B
3
Search User_ID (from Incomming Payloads) to find (correlate with) User SYS_ID
Persist SearchKey Records for Users
Foreign Key Reference
ServiceNow

Primary Asset Table (example)

Asset_ID	Hostname	Serial_Number	User_ID
Asset24	LON-PC-01	XY12345	TGreen
Asset25	BNE-PC-99	AB98765	SSmith

Primary User Table (example)

User_ID	Firstname	Surname	Email
TGreen	Tom	Green	tom.green@abc.com
SSmith	Sam	Smith	sam.smith@abc.com

As email address is the correlation attribute the **SQL Query does** join with the Primary User Table

VM Resource (example)

Res. GUID	Hostname	ResGroup	Tag
GUIDa1b2	PAR-VM-01	dv-bld-abc	tom.green@abc.com
GUIDx8y9	BER-VM-02	dv-bld-abc	sam.smith@abc.com

Incoming Record Payload
- Asset_ID=Asset24
- Hostname=LON-PC-01
- Serial_Number=XY12345
- User_ID=tom.green@abc.com

Incoming Record Payload
- Res. GUID=GUIDa1b2
- Hostname=PAR_VM-01
- ResGroup=dv-bld-abc
- Tag=tom.green@abc.com

Transformed Outgoing Record Payload
- Asset_ID=Asset24
- Hostname=LON-PC-01
- Serial_Number=XY12345
- User SYS_ID=GUID1234

Transformed Outgoing Record Payload
Res. GUID=GUIDa1b2
- Hostname=PAR-VM-01
- ResGroup=dv-bld-abc
- User SYS_ID=GUID1234

Incoming User Payload
- User_ID=tom.green@abc.com
- User_SYS_ID=GUID1234
- User_ID=sam.smith@abc.com
- User_SYS_ID=GUID7890

CMDB CI Table (cmdb_ci_computer)

CI SYS_ID	Hostname	Serial_Number	Assigned_To (User SYS_ID)
GUIDabcd	LON-PC-01	XY12345	GUID1234
GUIDwxyz	BNE-PC-99	AB98765	GUID7890

CMDB CI Table (cmdb_ci_vm_instance)

CI SYS_ID	Hostname	ResourceGroup	Assigned_To (User SYS_ID)
GUIDa1b2	PAR-VM-01	dv-bld-abc	GUID1234

Primary User Table (sys_user)

User SYS_ID	User_ID	Firstname	Surname	Email
GUID1234	TGreen	Tom	Green	tom.green@abc.com
GUID7890	SSmith	Sam	Smith	sam.smith@abc.com

Correlation Table (Searchkeys)

SearchKey	User SYS_ID
tom.green@abc.com	GUID1234
sam.smith@abc.com	GUID7890

Drawing Name: Overview of Source and Destination Fine Grain Permission Option for Personal Data
Sheet Name: Diag 2 – Correlation Email
Data Classification: Commercial-in-Confidential

Suggestion: Trace the bold/green **tom.green@abc.com** value (and subsequently it's **GUID1234** SYS_ID value) on the above diagram to see how it is processed by CI Sync.

Ref #	**Explanation** *(these only apply if a customer has decided to override the default behavior of CI Sync)*
A	At the start of each synchronization job, your customer specific CI Sync SaaS instance queries the sys_user table in ServiceNow. CI Sync only queries two values: (1) The agreed correlation attribute (in the above diagram this is the value in the Email Address field), and (2) the SYS_ID value.
B	CI Sync persists the two values in your customer specific SearchKey database (a MongoDB database which is a part of your customer specific CI Sync SaaS instance).
1	The CI Sync (EE) Agent (windows service) queries the **primary asset/resource table** from the Source System. The **query needs to join/extend into the primary user table as the agreed correlation attribute is not contained in the primary asset/resource table.** The diagram shows the CI Sync query joins the tables on the common key ("User_ID") to it can return value "**tom.green@abc.com**") which what will ultimately be needed to correlate against the values held in the SearchKey database thanks to steps (A) and (B) above).
2	The CI Sync (EE) Agent sends the record payload to your CI Sync SaaS instance. The payload contains the asset/resource attributes/values and the user correlation attribute/value (i.e. "**tom.green@abc.com**").
3	Logic in your CI Sync SaaS instance checks your MongoDB SearchKey table and finds a match on "**tom.green@abc.com**"). CI Sync (EE) now knows the ServiceNow SYS_ID for the user "**tom.green@abc.com**" (the pretend SYS_ID in the above example is "**GUID1234**").
4	The CI Sync SaaS code creates an ongoing record payload which now only contains the SYS_ID (i.e. "**GUID1234**"). CI Sync updates the relevant CMDB_CI table with the asset/record attributes/values in addition it sets the Assigned_To field with the SYS_ID of the user (i.e. "**GUID1234**") as the foreign key reference to the SYS_USER table.

Explanation of Concept #2 – Do default permissions in Source and/or Destination Systems allow the two CI Sync (EE) components to potentially access Personal Data which is beyond the scope of CI Sync (EE)?

Yes. This is due to the behavior/permission model of many (if not most) source and destination systems. There are two reasonably obvious follow-on questions:

1. Is it possible for a customer to implement fine-grain permissions to restrict the two CI Sync (EE) components from having any access at all to the Personal Data related data/tables?
2. Which Personal Data related data/tables do the two CI Sync (EE) have access to (even when the CI Sync (EE) default configuration is being used and therefore CI Sync (EE) is not actually reading from such Personal Data related data/tables)?
3. How does an SME go about implementing fine-grain permissions on a given source and destination system?

As a reminder, the two CI Sync (EE) components are as follows:

1. The CI Sync (EE) Agent (the Windows Service responsible for reading data from one/more source systems and sending to the CI Sync (EE) SaaS instance).
2. The CI Sync (EE) SaaS (the per-customer SaaS instance responsible for processing the source system data (as received from the CI Sync (EE) Agent), transforming the source data and persisting it into one/more destination systems.

Each of the three questions noted above are responded to in the subsequent pages.

Question 1 - Is it possible for a customer to implement fine-grain permissions to restrict the two CI Sync (EE) components from having any access at all to the Personal Data related data/tables?

It may be possible to implement fine-grain permissions providing your SMEs understand the following topics (relative to the above question):

1. The **authentication** credential/s you created when implementing one or more **source system** connections via the CI Sync (EE) Agent Configuration Utility.
2. The **authentication** credential/s you created when implementing one or more **destination system** connections via the CI Sync (EE) SaaS User Interface.
3. The **authorization** type/level (e.g. roles and associated permissions) you have provided t**o the authentication credentials** noted above.

The extent to which fine-grain permissions can be implemented is entirely dependent upon permission model of the underlying technology within individual source and destination system. Not all systems (source and/or destination) support fine-grain access controls.

See the tables on the next page for an overview of the above topics (default authentication and authorization details).

Table showing the default authentication and authorization details for the CI Sync (EE) Agent component across several source systems.

Source System	**Default CI Sync Authentication Credential/s**	**Standard Authorization Type** *(for the authentication credential/s)*	**Default Authorization Level** *(for the authentication credential/s)*
Lansweeper	• **Windows Integrated Security** *Windows User Account used as the Windows Service Login Account associated with the CI Sync (EE) Agent.* • **Native SQL Login** Native SQL Login entered into the CI Sync (EE) Agent Config Utility UI.	SQL database role	**db_datareader role** assigned to the **entire the Lansweeperdb SQL database.**
SCCM	• **Windows Integrated Security** *Windows User Account used as the Windows Service Login Account associated with the CI Sync (EE) Agent.* • **Native SQL Login** Native SQL Login entered into the CI Sync (EE) Agent Config Utility UI.	SQL database role	**db_datareader role** assigned to the **entire the SCCM SQL database.**
Intune	• **Service Principal** create via an App Registration object for Intune within Azure AD.	Microsoft Graph API, Application Permissions	**DeviceManagementApps.ReadAll** (read Microsoft Intune apps) **DeviceManagementManagedDevices .ReadAll** (read Microsoft Intune devices). **User.ReadAll** (sign in read all users' full profiles).
Azure	• **Service Principal** create via an App Registration object for Azure within Azure AD.	AAD IAM User Roles	**Reader role** assigned to **each subscription in scope for CI Sync.**

Table showing the default authentication and authorization details for the CI Sync (EE) SaaS component within one destination system (ServiceNow).

Destination System	**Default CI Sync Authentication Credential/s**	**Standard Authorization Type** *(for the authentication credential/s)*	**Default Authorization Level** *(for the authentication credential/s)*
ServiceNow	• **ServiceNow user account** *A ServiceNow user account (set as a Web service access only account with Basic Auth, OAuth or MFA) and configured within the CI Sync (EE) Settings Page of the CI Sync (EE) SaaS component UI.*	ServiceNow Roles	The following out of the box ServiceNow roles: • user_admin • personalize_choices • snc_platform_rest_api_access • cloud_admin • tracked_file_reader • asset • model_manager

Question 2 - Which Personal Data related data/tables do the two CI Sync (EE) components (i.e. the CI Sync (EE) Agent and the CI Sync (EE) SaaS solution) have access to (even when the CI Sync (EE) default configuration is being used and therefore CI Sync (EE) is not actually reading from such Personal Data related data/tables)?

It may be possible to implement fine-grain permissions providing your SMEs understand the following topics (relative to the above question):

1. The **source system/s database schema** (i.e. the database tables and database columns) that do store or might store Personal Data.
2. The **destination system/s database schema** (i.e. the database tables and database columns) that do store or might store Personal Data.

Below is an example of one source system (Lansweeper) and one destination system (ServiceNow). An SME with detailed knowledge of the database schema of other source/destination systems will likely be able to use these examples to develop a similar understanding.

Source System = Lansweeper

The following SQL tables/columns have been documented by Lansweeper as containing potential PII/Personal Data values (e.g. Firstname, Surname, Email Address, Phone Number, Login ID).

#	Table name potentially containing PII/PD data	Does CI Sync Query the Table?	Type of content potentially PII/PD	Does CI Sync Query the PII/PD related content by default?
1	tblAssets	**Yes** (by default)	Username	**No** (by default) **Yes** (Username **IF** the default is overridden for Last Logged On User mapping)
2	tblMacOSInfo	**Yes** (by default)	Username	**No** (by default)
3	tblMappedDrives	**Yes** (by default)	Username	**No** (by default)
4	tblOperatingsystem	**Yes** (by default)	Phone Number	**No** (by default)
5	tsysIPLocations	**Yes** (by default)	Username	**No** (by default)
6	tblADComputers	**Yes** (by default)	Description *NB: Description is a free-format text field (which could contain user names)*	**Yes** (by default)
7	tblAssetComments	**Yes** (by default)	Surname, Firstname	**No** (by default)
8	tblADusers	**No** (by default)	Username, Surname, Firstname, Email, Phone Number	**No** (by default) **Yes** (if the default is overridden for Last Logged On User mapping AND the tblAsset.username field is NOT being used for correlation)
9	tblCPlogoninfo	**No** (by default)	Username	**No** (by default) **Yes** (if the default is overridden for Last Logged On User mapping AND “most frequent user” mapping)
10	tblAirWatchDevice	**No** (by default)	Username, Email, User ID, Phone Number	**No** (by default) **Yes** (UserEMailAddress if the default is overridden for Last Logged On User mapping)
11	tblIntuneDevice	**No** (by default)	Username, Surname, Email, User ID, Phone Number	**No** (by default) **Yes** (EMailAddress if the default is overridden for Last Logged On User mapping)
12	tblCertificates	**No** (by default)	Not specified by Lansweeper	**No** (by default) **Case-by-Case Assessment** (i.e. customer will need assess content of the table for any values that may contain PII/PD)
13	tblAssetCustom	**No** (by default)	Contact	**No** (by default)
14	Htblemailaccountaliases	**No** (by default)	Username, email	**No** (by default)

#	Table name potentially containing PII/PD data	Does CI Sync Query the Table?	Type of content potentially PII/PD	Does CI Sync Query the PII/PD related content by default?
15	htblemailaccounts	**No** (by default)	Username, email	**No** (by default)
16	htblslausers	**No** (by default)	User ID	**No** (by default)
17	Htblusers	**No** (by default)	Username, Email, User ID, Phone Number	**No** (by default)
18	tblAirWatchUser	**No** (by default)	Username, Surname, Firstname Email, User ID	**No** (by default)
19	tblAssetUserRelations	**No** (by default)	Username	**No** (by default)
20	tblAzureAdUser	**No** (by default)	Username, Surname, Firstname, Email, Phone Number	**No** (by default)
21	tblChromeOsRecentUser	**No** (by default)	Email	**No** (by default)
22	tblCitrixUser	**No** (by default)	Username, User ID	**No** (by default)
23	tblExchangeMailbox	**No** (by default)	Username, Surname, Email	**No** (by default)
24	tblExchangeMailboxAddress	**No** (by default)	Email	**No** (by default)
25	tblExchangeUser	**No** (by default)	Username, Surname, Firstname, Email, User ID, Phone Number	**No** (by default)
26	tblLinuxUser	**No** (by default)	Username, User ID	**No** (by default)
27	tblLoginLog	**No** (by default)	Username	**No** (by default)
28	tblNotificationUser	**No** (by default)	User Id	**No** (by default)
29	tblNtlogUser	**No** (by default)	Username	**No** (by default)
30	tblO365User	**No** (by default)	Surname, Firstname, Email, User ID, Phone Number	**No** (by default)
31	tblUsers	**No** (by default)	Username, Surname, Firstname, User ID	**No** (by default)
32	tblUsersHist	**No** (by default)	Username, Surname, Firstname	**No** (by default)
33	tblUsersInGroup	**No** (by default)	Username	**No** (by default)
34	tblUsersInGroupHist	**No** (by default)	Username	**No** (by default)
35	tsysCredentials	**No** (by default)	Username, Surname, Firstname, Email	**No** (by default)
36	tsysWebUsers	**No** (by default)	Username	**No** (by default)
37	tblChromeOS	**No** (by default)	Username	**No** (by default)
38	tblCitrixPhysicalBlockDevice	**No** (by default)	Username	**No** (by default)
39	tblCitrixPool	**No** (by default)	Username	**No** (by default)
40	tblEnvironment	**No** (by default)	Username	**No** (by default)
41	tblExchangeGroup	**No** (by default)	Email	**No** (by default)
42	tblExchangeMailboxStatistics	**No** (by default)	Email	**No** (by default)
43	tblO365Mailbox	**No** (by default)	Username, Surname, Email	**No** (by default)
44	tsysASServers	**No** (by default)	Username	**No** (by default)
45	TsysCloudConfiguration	**No** (by default)	Username	**No** (by default)
46	TsysConfig	**No** (by default)	Username	**No** (by default)
47	tsysMailConfig	**No** (by default)	Username, Email	**No** (by default)
48	Htblemailverification	**No** (by default)	Username, Email, User ID	**No** (by default)
49	Htblticket	**No** (by default)	User ID	**No** (by default)
50	tblADObjects	**No** (by default)	Username	**No** (by default)
51	tblAssetJournal	**No** (by default)	Username	**No** (by default)
52	tblAzureAdGroup	**No** (by default)	Email	**No** (by default)
53	tblAzureAdOrganization	**No** (by default)	Phone Number	**No** (by default)
54	tblDesktop	**No** (by default)	Name	**No** (by default)
55	tblExchangeActiveSyncDevice	**No** (by default)	Username, Surname, Email, Phone number	**No** (by default)

#	Table name potentially containing PII/PD data	Does CI Sync Query the Table?	Type of content potentially PII/PD	Does CI Sync Query the PII/PD related content by default?
56	tblLicenses	**No** (by default)	Username	**No** (by default)
57	tblLinuxFileInfo	**No** (by default)	Username	**No** (by default)
58	tblO365ActiveSyncDevice	**No** (by default)	Username, Surname, Email, Phone number	**No** (by default)
59	tblO365Contact	**No** (by default)	Email	**No** (by default)
60	tblO365Group	**No** (by default)	Username, Email	**No** (by default)
61	tblOsLicenses	**No** (by default)	Username	**No** (by default)
62	Tsysadmins	**No** (by default)	Username	**No** (by default)
63	tsysLapsResult	**No** (by default)	Username	**No** (by default)
64	tsysMailgroups	**No** (by default)	Email	**No** (by default)
65	tsysOTHubLink	**No** (by default)	Username	**No** (by default)
66	tsysPackages	**No** (by default)	Username	**No** (by default)
67	tsysPackageSchedule	**No** (by default)	Username	**No** (by default)
68	tsysRoleMembers	**No** (by default)	Username	**No** (by default)
69	htblagents	**No** (by default)	User ID	**No** (by default)
70	htblcalendarsettings	**No** (by default)	User ID	**No** (by default)
71	htblcustomticketfilters	**No** (by default)	User ID, Username, Surname, Firstname	**No** (by default)
72	htblemailtemplatesticketstates	**No** (by default)	User ID, Username, Email Address	**No** (by default)
73	htblfooterattachements	**No** (by default)	User ID	**No** (by default)
74	htblhistory	**No** (by default)	User ID	**No** (by default)
75	htblknowledgebase	**No** (by default)	User ID, Username	**No** (by default)
76	htblnotehistory	**No** (by default)	User ID	**No** (by default)
77	htblnotes	**No** (by default)	User ID	**No** (by default)
78	htblnotificationschecked	**No** (by default)	User ID	**No** (by default)
79	htbloldticketdata	**No** (by default)	User ID	**No** (by default)
80	htblsavedcustomfilters	**No** (by default)	User ID	**No** (by default)
81	htblschedule	**No** (by default)	User ID, Username	**No** (by default)
82	htblscheduleinfo	**No** (by default)	User ID	**No** (by default)
83	htblticketssummary	**No** (by default)	User ID, Username	**No** (by default)
84	htblticketuserrelation	**No** (by default)	User ID	**No** (by default)
85	htblwebroles	**No** (by default)	Username	**No** (by default)
86	tblAssetChangeLog	**No** (by default)	Username	**No** (by default)
87	tblAssetDocs	**No** (by default)	Surname, Firstname	**No** (by default)
88	tblAWSAmi	**No** (by default)	Username	**No** (by default)
89	tblCatalogBrand	**No** (by default)	Phone Number	**No** (by default)
90	tblCatalogOs	**No** (by default)	Phone Number	**No** (by default)
91	tblConfigLog	**No** (by default)	User ID	**No** (by default)
92	tblExchangeGroupMember	**No** (by default)	User ID	**No** (by default)
93	tblExchangeUserLicense	**No** (by default)	User ID	**No** (by default)
94	tblGroups	**No** (by default)	User ID	**No** (by default)
95	tblNotificationUser	**No** (by default)	User ID	**No** (by default)
96	tblO365AssignedLicense	**No** (by default)	User ID	**No** (by default)
97	tblO365AssignedPlan	**No** (by default)	User ID	**No** (by default)
98	tblO365GroupMember	**No** (by default)	User ID	**No** (by default)
99	tblO365Organization	**No** (by default)	Phone Number	**No** (by default)
100	tblPOTSModem	**No** (by default)	Phone Number	**No** (by default)
101	tblPOTSModemHist	**No** (by default)	Phone Number	**No** (by default)

#	Table name potentially containing PII/PD data	Does CI Sync Query the Table?	Type of content potentially PII/PD	Does CI Sync Query the PII/PD related content by default?
102	tblQuickFixEngineeringInstalledBy	**No** (by default)	Username	**No** (by default)
103	tsysOIDlookup	**No** (by default)	Username	**No** (by default)
104	tsysreports	**No** (by default)	Username	**No** (by default)
105	tsysUsage	**No** (by default)	User ID	**No** (by default)
106	tsysWebRoles	**No** (by default)	Username	**No** (by default)

Other Source Systems

These source system attributes are known to contain or may contain potential PII/Personal Data values.

Source System	(Potential PII/PD) Attribute	Does CI Sync Query the Attribute/s?
Intune	userPrincipalName	**No** (by default) **Yes** (if the default is overridden for Last Logged On User mapping)
Azure	Tags (if populated by the customer with PII/PD)	**No** (by default) **Yes** (if the default is overridden for Last Logged On User mapping)
Nutanix	owner	**No** (by default) **Yes** (if the default is overridden for Last Logged On User mapping)

Destination System = ServiceNow

The following table has been documented by ServiceNow as containing potential PII/Personal Data values (e.g. Firstname, Surname, Email Address, Phone Number, Login ID).

#	(Potential PII/PD) Table	Does CI Sync Query the Table?	(Potential PII/PD) Column/s	Does CI Sync Query the Column/s?
1	SYS_USER	**No** (by default)	User_ID Firstname, Surname EmailAddress	**No** (by default) **Yes** (if the default is overridden for Last Logged On User mapping, then whichever field has been agreed as the correlation attribute)

Question 3 - How does an SME go about implementing fine-grain permissions on a given source and destination system?

If the CI Sync (EE) default configuration is being used, and therefore CI Sync (EE) is not actually reading from Personal Data related data/tables, an organization may still want to restrict CI Sync (EE) access (both Agent and SaaS component access) to such Personal Data related data/tables.

Alternatively, if the CI Sync (EE) default configuration has been overridden to include a user related correlation value, an organization may want to further restrict CI Sync (EE) access (both Agent and SaaS component access) at a column level within tables potentially storing Personal Data.

To do this, SME/s need to modify the default permissions on the CI Sync (EE) authentication credential to prevent access to entire tables and/or individual columns within the tables. When doing so:

1. SMEs must be careful not to restrict access to tables (and columns) used by the default configuration of CI Sync (EE).

2. The restrictions should be implemented on all source and all destination systems in scope for CI Sync (EE) within the organization.

Below is an example of one source system (Lansweeper) and one destination system (ServiceNow). An SME with detailed knowledge of the CI Sync (EE) authentication credentials, and the permission model of the source/destination system, and the database schema of other source/destination systems may be able to use these examples to implement fine-grain permissions on other systems in scope for CI Sync (EE).

General How-To: Implement fine-grain permissions on a Lansweeper Source SQL Database

1. Run a CI Sync (EE) Full Sync (not delta sync) sync job and ensure it completes error free. This proves the solution is working correctly before restricting CI Sync (EE) **Agent** permissions to the **source** data.
2. Open SQL Management Studio and connect to the Lansweeper SQL database.
3. Identify the CI Sync authentication credential (i.e. SQL user) that has been granted the db_datareader role at the database level of the Lansweeper SQL database.
4. Change the permissions to remove access as follows:
    a. Remove access to any Lansweeper **tables** identified as "**No** (by default)" in the documentation above (the large table in this document showing which tables and columns may contain PII/Personal Data).
    b. Consider also removing access to any **individual columns** with potential PII/PD within those Lansweeper tables listed as "**Yes** (by default)".
5. Re-run a CI Sync (EE) Full Sync (not delta sync) sync job and ensure it completes error free. This proves the solution is working correctly after restricting CI Sync (EE) **Agent** permissions to the **source** system.

General How-To: Implement fine-grain permissions on a ServiceNow Destination System

1. Run a CI Sync (EE) Full Sync (not delta sync) sync job and ensure it completes error free. This proves the solution is working correctly before restricting CI Sync (EE) **SaaS** permissions to the **destination** data.
2. Open ServiceNow and elevate to Security Admin.
3. Identify the CI Sync authentication credential being used by the CI Sync (EE) SaaS destination connection (if the setup instructions originally provided Syncfish have been followed the user account will likely be called cisync.integration).
4. Create ACL against the sys_user table that restricts access to the sys_user table for the CI Sync integration user account. Depending on whether CI Sync (EE) is using the default configuration vs an overridden configuration you may decide the ACL should restrict the CI Sync user account from the entire sys_user table or just those attributes not in scope for CI Sync (EE).
5. Re-run a CI Sync (EE) Full Sync (not delta sync) sync job and ensure it completes error free. This proves the solution is working correctly after restricting CI Sync (EE) **SaaS** permissions to the **destination** system.