Installation and Configuration

Security Controls Connector 2023.1.1

Please note, from the 2021.3.1+ connector has changed extensively, and dashboards created in previous versions will fail. All OOTB Dashboards have been re-created for the new version and the default folder is now “Ivanti Security Controls”.

The Security Controls and ISeC connectors can both exist in the same datamodel.

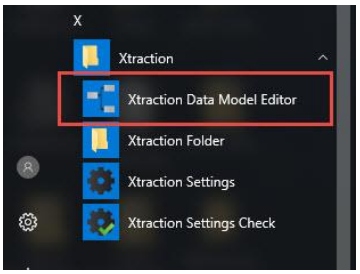
Xtraction only queries the Security Controls database, it has no direct interaction with the application itself. Be aware that the data returned in Xtraction may differ from what is represented in the Security Controls Console. The reason for this is that not all actions in Security Controls are immediately updated in the Security Controls database and data and values displayed may be calculated at runtime and not be the result of database queries.

To configure the Ivanti Security Controls connection

1. Create a read-only user to the Ivanti Security Controls database.

2. Copy the provided Ivanti Security Controls data model file to the Data\Configuration directory, located by default at:
   C:\Program Files (x86)\Xtraction Software\Xtraction\Data\Configuration

3. On the Xtraction server, open the **Xtraction Data Model Editor** program from the Start Menu

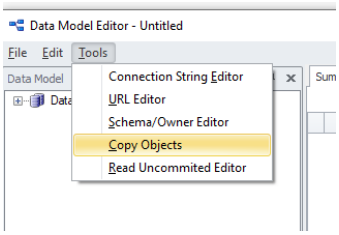


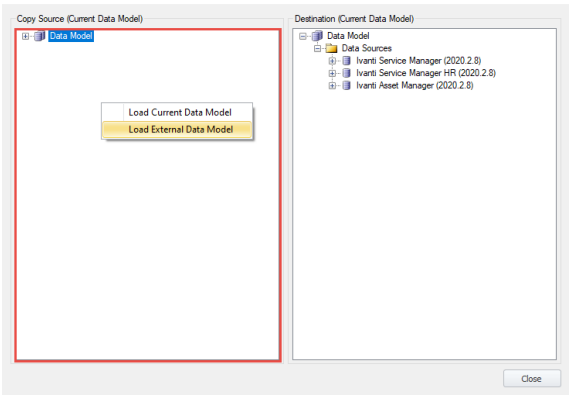
Click **File > Open** or **Ctrl-O** to open the file in the folder location mentioned above.

4. If you have an existing DataModel.dat file that you have already configured, and want to preserve the existing connections, you will need to merge the provided Ivanti Security Controls (ISeC) data model into DataModel.dat file using **Copy Objects.**

   Note: You will need an **Enterprise Server** license to complete this step:

a. Click **Tools > Copy Objects**.



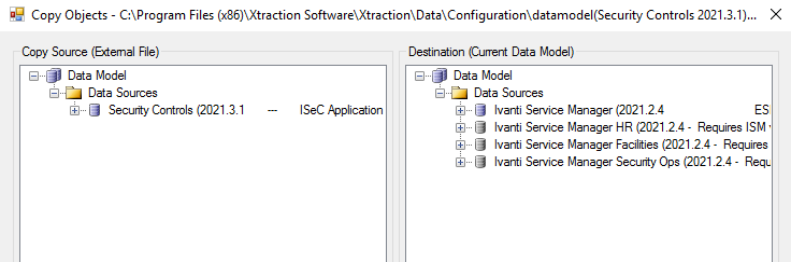


b. Right Click anywhere in the red outlined area and Select **Load External Data Model**.

c. Navigate to the Data\Configuration location and Select the provided Ivanti Security Controls data model file and Open

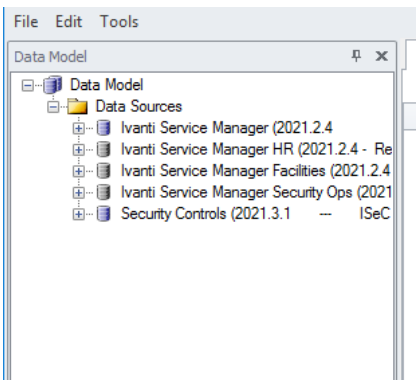
d. Expand the Data Model in the Copy Source (External File) screen to the Security Controls Datasource

e. Drag the Security Controls Datasource over to the Data Model in the Destination Screen



f. Click Yes to Confirm and then Close, the additional Security Controls Datasource is now visible

g. Click File > Save to complete the process



5. If you are not replacing an existing DataModel.dat file, just rename the existing file to be the DataModel.dat file using **File > Save As** or **Shift-Ctrl-S** once you are done configuring.

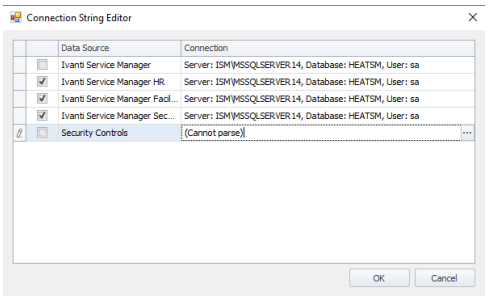
6. Enter the connection details for the Ivanti Security Controls data model database.

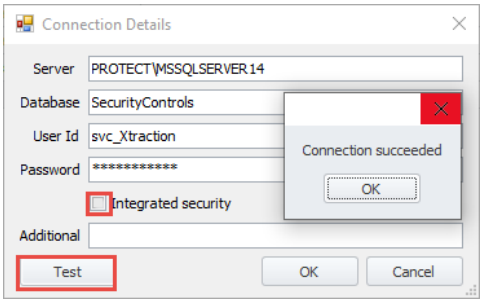
    a. Click **Tools > Connection String Editor**.

    b. Click the **Connection** column next to the Security Controls data source.

    c. Click the ellipsis (…) for the connection and enter the connection string properties for the Security Controls data source.
    Note: For SQL Authentication, enter User Id and Password. For Windows Authentication leave User Id and Password blank and check the Integrated Security checkbox.

    d. Click the **Test** button to validate that the connection can be made.



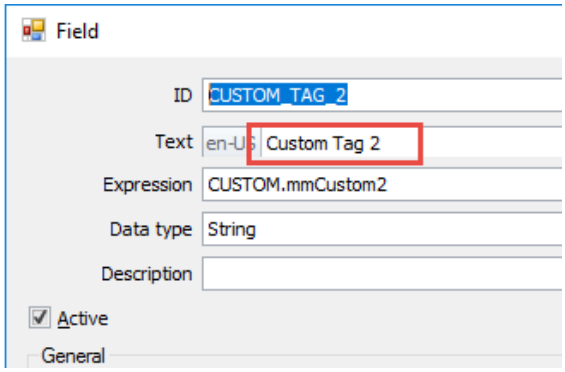


    e. Be sure to save your updated DataModel.dat file by selecting **File > Save** or **Ctrl-S**. The file must be named **DataModel.dat**. If renaming, use **Save As**.

7. Edit the Custom Fields if used:
    a. Custom Fields are available in the following views:
        - Machine
        - All Windows Patching Views
        - All Linux Patching Views
        - Deployments

    b. Open the Data Model Editor and File -> Open the DataModel.dat file in the Configuration Folder.

c. Expand the Security Controls datasource, Expand the Machine View
   - Double Click the Custom Table
   - Double Click Custom 1, 2, 3 fields in turn



   - Edit the Text field to the required value.
   - DO NOT change the ID or Expression.
   - Repeat with all other views in the datamodel
   - Once Finished – File Save

d. Start Xtraction from any terminal and using an Admin login reload the datamodel
   - The updated datamodel is available for all users.

8. The Security Controls Connector from 2021.3.1 onwards can show the current state of a machine as per all scans. To do this there are additional tables required in the database as well as a scheduled re-syncing of the data.
   a. ie. Required patches may have been scanned, detected and installed at different times in the machine's lifecycle. The machine may only have been scanned for other patches subsequently, these additional tables collate the last scan result for all detected patches, so the complete machine health can be determined rather than just the status of a sub-group of patches.

9. Run the "Script - Ivanti Security Controls Create Database Objects.sql" file against the Ivanti Security Controls database, this will create all the required Stored Procedures and Tables automatically.

10. Run the “Script - Ivanti Security Controls Cumulative Patches.sql” file against the Ivanti Security Controls database, this will insert details of all cumulative patch types.

11. If using any SQL Server edition apart from Express

(If using Express disregard and go to item 14.)

Run the “Script - Ivanti Security Controls Create Job Data Refresh.sql” on the Security Controls database server, it requires an account and the database name to be entered.

This creates a job using the SQL Server Agent that syncs the latest data on an hourly basis, the time period can be altered to suit individual needs.

12. The installation can be tested by executing the dbo. Xtr_UpdateData stored procedure, inserts, updates and deletions are recorded in the xtrEntityProcessLog table.
Test the job by running it manually in the SQL Server Agent.

Results | Messages

	EntityProcessLogId	BatchId	LogDate	ProcedureName	Description
1	1	1	2021-07-15 04:42:23.527	xtr_CurrentPatchStatus	Inserted 4916 records
2	2	1	2021-07-15 04:42:23.527	xtr_CurrentPatchStatus	Updated 0 records
3	3	1	2021-07-15 04:42:24.430	xtr_DeleteCPatches	Deleted 424 records
4	4	1	2021-07-15 04:42:24.473	xtr_DeleteObsPatches	Deleted 2 records
5	5	1	2021-07-15 04:42:24.487	xtr_DeleteODPatches	Deleted 64 records
6	6	2	2021-07-15 04:42:24.993	xtr_LinuxCurrentPatchStatus	Inserted 0 records
7	7	2	2021-07-15 04:42:24.993	xtr_LinuxCurrentPatchStatus	Updated 0 records
8	8	2	2021-07-15 04:42:25.007	xtr_LinuxDeleteCPatches	Deleted 0 records

Installation complete

13. If using SQL Server Express

(Not required for any other edition)

SQL Express does not have the SQL Server Agent enable so it cannot be used to schedule the sync.

This will guide you in creating a scheduled job to run in Task Manager

- Copy the “Task - Ivanti Security Controls Sync Scheduler vxxxx.zip” file to a folder on the Server which hosts the Security Controls database.
- Unzip the file to a C:\TEMP folder, create one if not already there
  You will have the following files
  - RefreshSecurityControlsSync.bat (Only one that needs to be edited)

- RefreshSecurityControls.sql
- CreateISeCSyncTask.ps1
- Script – Ivanti Security Controls Account Persmissions v202x.x.x.sql

- Open RefreshSecurityControlsSync.bat in a text editor such as notepad, adjacent are the areas that will need some input.
- There are 2 lines that begin with sqlcmd, only one needs to be used. The top is used if Windows Authentication is preferred option, the 2nd if SQL Authentication is to be used.

```
@echo off

set isodt=%date:~10,4%-%date:~7,2%-%date:~4,2% %time:~0,2%.%time:~3,2%.%time:~6,2%

rem sqlcmd -S YourSQLServerName -e -d SecurityControlsDatabase -E -i "C:\Program Files\Ivanti\Security Controls\Xtr

sqlcmd -S YourSQLServerName -e -U UserAccount -P Password -d SecurityControlsDatabase -i "C:\Program Files\Ivanti\S
-o "C:\Program Files\Ivanti\Security Controls\XtractionSync\Log\Log_%isodt%.txt"
```

Items to be edited: (Note: Inputs are in plain text, no commas or quotation marks are used)

- Rem - Insert rem in front of the “sqlcmd” NOT to be used, this is short for remark and anything on that line will be disregarded.
- YourSQLServerName – name of the SQL Server instance
- SecurityControlsDatabase – name of the Security Controls database, default is SecurityControls but maybe anything
- If using Windows Authentication, un rem line 1, rem out line 2, save file and that is all that is required.
- If using SQL Authentication insert a UserAccount that has at least read access to the Security Controls database and the corresponding Password.
  Leave line 1 rem in place and save file.

Note: If this account, (regardless of whether it is a domain account or SQL Account) has less than full dbo rights to the Security Controls database, the

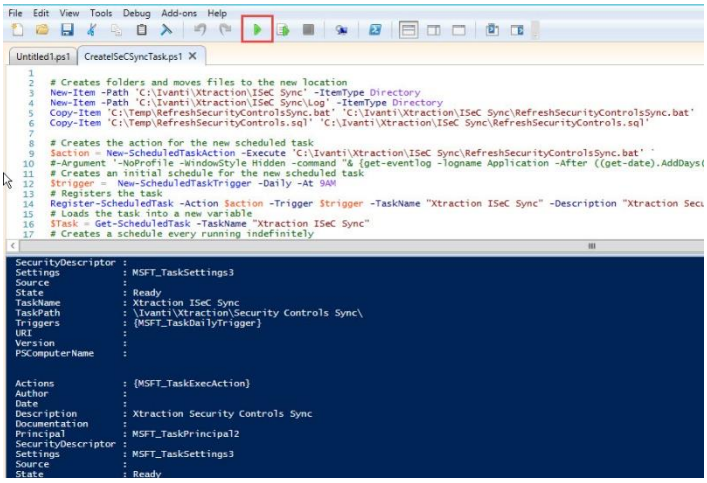
- Script – Ivanti Security Controls Account Persmissions v202x.x.x.sql

Script will need to be run against it. The script gives the account dbo rights to only the Tables and Stored Procedures required by the Xtraction Sync process leaving the reduced permissions to all Core Security Controls objects. Change the account name as required before running.

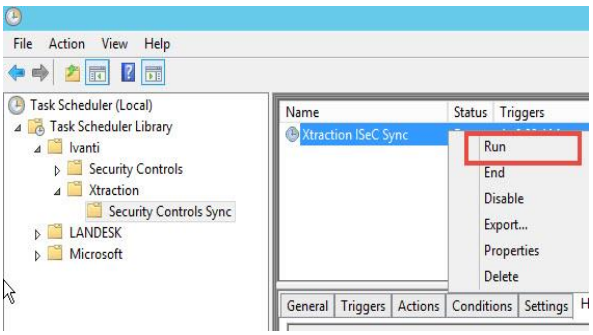
```
/*
**  Security Controls V2021.4.6 Connector - Permissions Script
**
**  1. Edit the "SET" line below, replacing the
**     default user (xtraction) with whatever SQL or Windows
**     account Xtraction will use to report against the Xtraction
**     database.  For example, 'xtraction_ro' or '[domain\svc_xtraction]'
**
**  2. Run this script to set the necessary permissions
**
*/

DECLARE @XtractionUsername VARCHAR(100)

--------- CHANGE THE FOLLOWING LINE AS REQUIRED ---------

SET @XtractionUsername = 'svc_Xtraction'

---------------------------------------------------------

exec('GRANT ALTER ON dbo.xtrCumulativePatches TO ' + @XtractionUsername)
exec('GRANT CONTROL ON dbo.xtrCumulativePatches TO ' + @XtractionUsername)
exec('GRANT DELETE ON dbo.xtrCumulativePatches TO ' + @XtractionUsername)
```

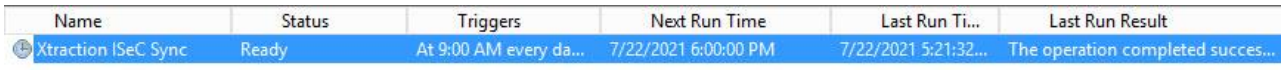
Option a. Automated Task Creation

- Run Powershell ISE as Administrator.
- File -> Open and navigate to “CreateISeCSyncTask.ps1” in the C:\Temp folder.
- Click on Run Arrow or Click shortcut key F5.
  The blue Powershell screen will populate while it creates folders, tasks and copies across files.



- To check that everything has been set-up correctly, go to Task Scheduler
  - Scroll down to the Ivanti / Security Controls / Reports folder and the “Xtraction ISeC Sync” task should be there.
  - Right click on the task and select Run
  - Status of the job will appear after a short time or by manually refreshing





Presumptions:

- Installer has the rights to run Powershell as an administrator

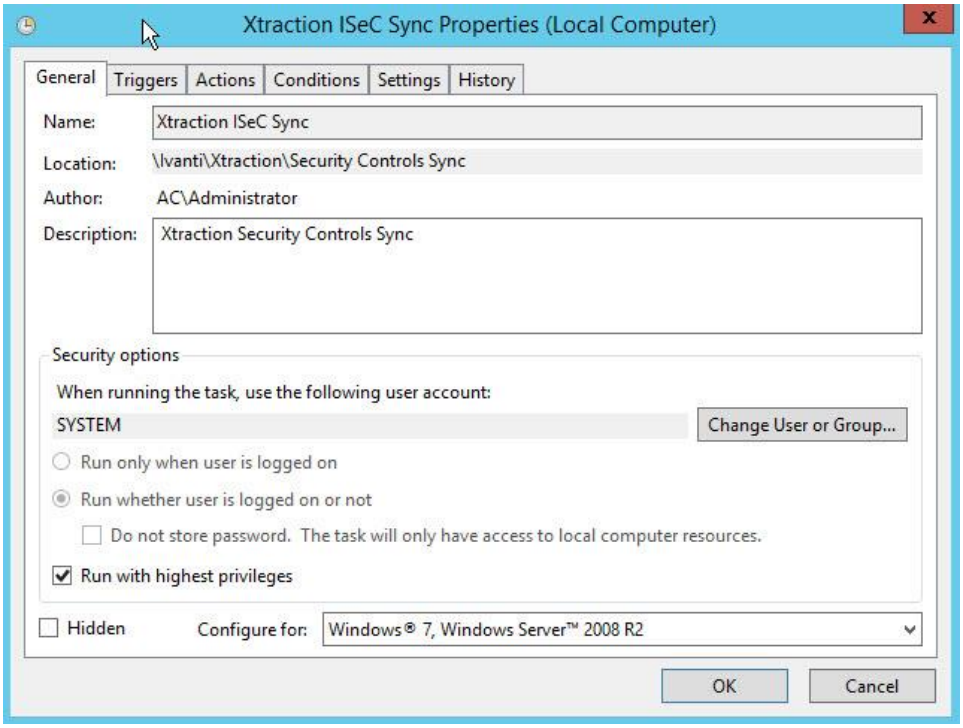
The account used in the script is **NT Authority\SYSTEM** and it relies on

- **NT Authority\SYSTEM** having retained its default full access to SQL Server
- **NT Authority\SYSTEM** having retained its default full access to all folders

Option b. Manual Task Creation

- Create the required folders to have the following tree:
  C:\Ivanti\Xtraction\ISeC Sync\Log
- Copy both "RefreshSecurityControlsSync.bat" and "RefreshSecurityControls.sql" into the "ISeC Sync" folder
- Give the account that will run the Task in the scheduler, full read/write access to the folder
- Create a new Task in the Windows Task Scheduler with the following requirements
  - Create a Folder Structure Ivanti / Xtraction / Security Controls Sync

Under the General Tab:



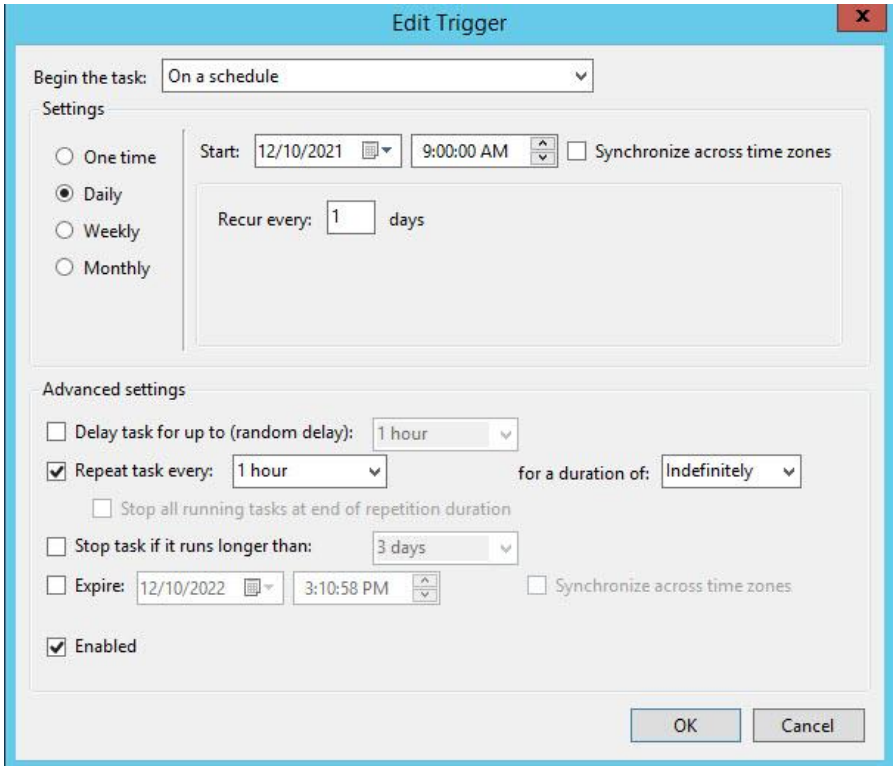
  - Name – Something self-explanatory
  - Description – Something self-explanatory
  - User Account – SYSTEM (recommended)
    - Run whether user is logged on or not – Checked
    - Run with highest privileges – Checked

Note: Can be any Windows Account however the account must have
"Log on as batch job rights" as specified in Local Security Policy. To check, look in

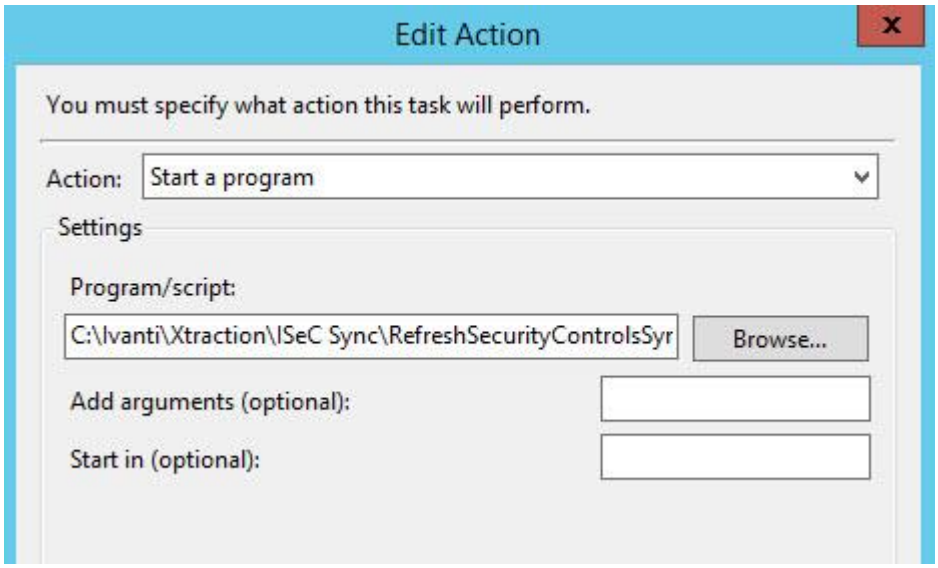
Local Security Policy -> Local Policies -> User Rights Assignment -> Log on as a batch job

- **Note:** this account is the account that will log on to the Security Controls database if Windows Authentication has been selected in the "RefreshSecurityControlsSync.bat file".
- Configure for: OS as required

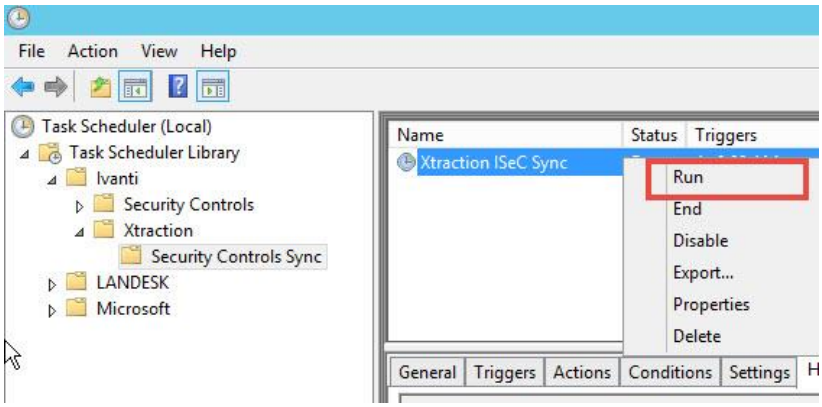
- Triggers – Recommended Hourly / Indefinitely

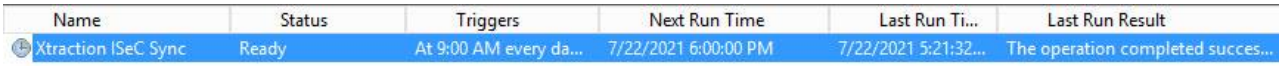


- Actions – Start a program
  - Navigate to the RefreshSecurityControlsSync.bat file
- Add Arguments – None Required
- Starts in – None Required



- To check that everything has been set-up correctly, go to Task Scheduler
    - Scroll down to the Ivanti / Xtraction / Security Controls Sync folder and the “Xtraction ISeC Sync” task should be there.
    - Right click on the task and select Run
    - Status of the job will appear after a short time or by manually refreshing

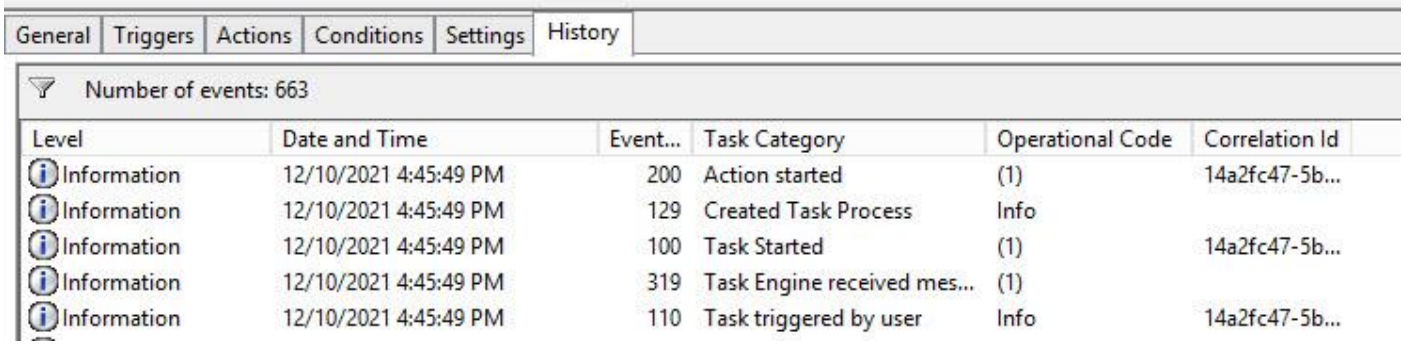




Installation complete

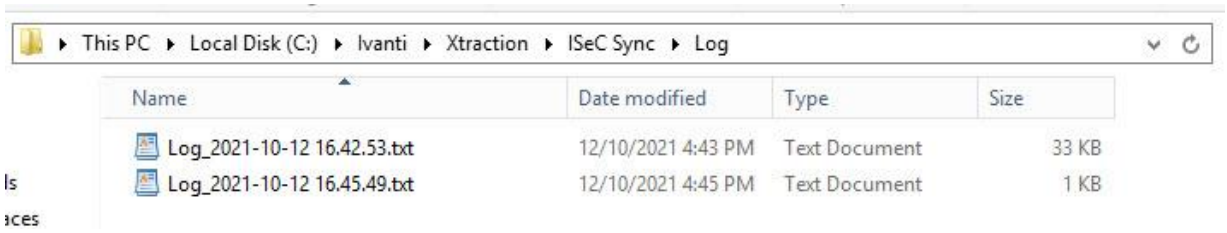
Troubleshooting:

- What should happen every time the task runs:
    - A history log is created in the Task Scheduler



Level	Date and Time	Event...	Task Category	Operational Code	Correlation Id
Information	12/10/2021 4:45:49 PM	200	Action started	(1)	14a2fc47-5b...
Information	12/10/2021 4:45:49 PM	129	Created Task Process	Info	
Information	12/10/2021 4:45:49 PM	100	Task Started	(1)	14a2fc47-5b...
Information	12/10/2021 4:45:49 PM	319	Task Engine received mes...	(1)	
Information	12/10/2021 4:45:49 PM	110	Task triggered by user	Info	14a2fc47-5b...

    - A new log should be created in the “C:\Ivanti\Xtraction\ISeC Sync\Log” folder with a date and time
    - Each log should be around 33K in size



    - A corresponding log with a similar timestamp in UTC should be made in the database

```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP 1000 [ENTITYPROCESSLOGID]
      ,[BATCHID]
      ,[LOGDATE]
      ,[PROCEDURENAME]
      ,[DESCRIPTION]
  FROM [SecurityControls].[dbo].[xtrEntityProcessLog] order by batchid desc
```

Results | Messages

	ENTITYPROCESSLOGID	BATCHID	LOGDATE	PROCEDURENAME	DESCRIPTION
1	8944	255	2021-12-10 05:43:04.500	xtr_LinuxCurrentPatchStatus	Inserted 0 records
2	8945	255	2021-12-10 05:43:04.500	xtr_LinuxCurrentPatchStatus	Updated 0 records
3	8946	255	2021-12-10 05:43:04.500	xtr_LinuxDeleteCPatches	Deleted 0 records
4	8947	255	2021-12-10 05:43:04.503	xtr_LinuxCurrentPatchCount	Inserted 0 records
5	8948	255	2021-12-10 05:43:04.503	xtr_LinuxDistinctDeployed	Inserted 0 records
6	8935	254	2021-12-10 05:43:00.583	xtr_CurrentPatchStatus	Inserted 0 records
7	8936	254	2021-12-10 05:43:00.583	xtr_CurrentPatchStatus	Updated 0 records
8	8937	254	2021-12-10 05:43:00.647	xtr_DeleteCPatches	Deleted 0 records
9	8938	254	2021-12-10 05:43:00.657	xtr_DeleteObsPatches	Deleted 0 records
10	8939	254	2021-12-10 05:43:00.667	xtr_DeleteODPatches	Deleted 0 records
11	8940	254	2021-12-10 05:43:01.097	xtr_CurrentPatchCount	Inserted 154 records
12	8941	254	2021-12-10 05:43:01.110	xtr_DistinctAssessed	Inserted 233 records
13	8942	254	2021-12-10 05:43:01.163	xtr_DistinctDeployed	Inserted 135 records
14	8943	254	2021-12-10 05:43:04.500	xtr_DistinctPatched	Inserted 239 records

- In this example, there are logs in the Task History and Logs for 16.42.53 and 16.45.49 local time but no sync for 05:45 in the database, local time here is GMT +11, adjust for your local.
  The 16.42.53 sync ran as expected:
  - There was a record in the Task History.
  - A log was created at 16.43.
  - The database synced without error at 05:43 UTC
- The 16.45.49 did not
  - There was a record in the Task History at 16:45.
  - The log for 16.45.49 is only 1KB in size which would also indicate an issue.
  - There was no record in the database at 05.45 UTC.

Process

- Look for errors in the DB first
  The xtrEntityProcessLog table returns data from the sync process:
- If there are errors in the syncing of data, they will appear here:

```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP 1000 [ENTITYPROCESSLOGID]
      ,[BATCHID]
      ,[LOGDATE]
      ,[PROCEDURENAME]
      ,[DESCRIPTION]
  FROM [SecurityControls].[dbo].[xtrEntityProcessLog] order by batchid desc
```

Messages

ITYPROCESSLOGID	BATCHID	LOGDATE	PROCEDURENAME	DESCRIPTION
7	261	2021-12-10 06:06:26.500	xtr_LinuxCurrentPatchStatus	Inserted 0 records
8	261	2021-12-10 06:06:26.500	xtr_LinuxCurrentPatchStatus	Updated 0 records
9	261	2021-12-10 06:06:26.513	xtr_LinuxDeleteCPatches	Deleted 0 records
0	261	2021-12-10 06:06:26.573	xtr_LinuxCurrentPatchCount	Inserted 0 records
1	261	2021-12-10 06:06:26.573	xtr_LinuxDistinctDeployed	Inserted 0 records
5	260	2021-12-10 06:06:23.063	xtr_CurrentPatchStatus	Error(s) encountered. See more details in table ...
6	260	2021-12-10 06:06:23.067	NULL	Error(s) encountered. See more details in table ...
7	260	2021-12-10 06:06:23.070	NULL	Error(s) encountered. See more details in table ...
8	260	2021-12-10 06:06:23.070	NULL	Error(s) encountered. See more details in table ...
9	260	2021-12-10 06:06:23.073	NULL	Error(s) encountered. See more details in table ...

- Details of the error(s) can be seen in the xtrEntityProcessErrorLog table:

```
SELECT TOP 1000 [ENTITYPROCESSERRORLOGID]
      ,[BATCHID]
      ,[LOGDATE]
      ,[ENTITYNAME]
      ,[ERRORLINE]
      ,[ERRORMESSAGE]
  FROM [SecurityControls].[dbo].[xtrEntityProcessErrorLog] ORDER BY LOGDATE DESC
```

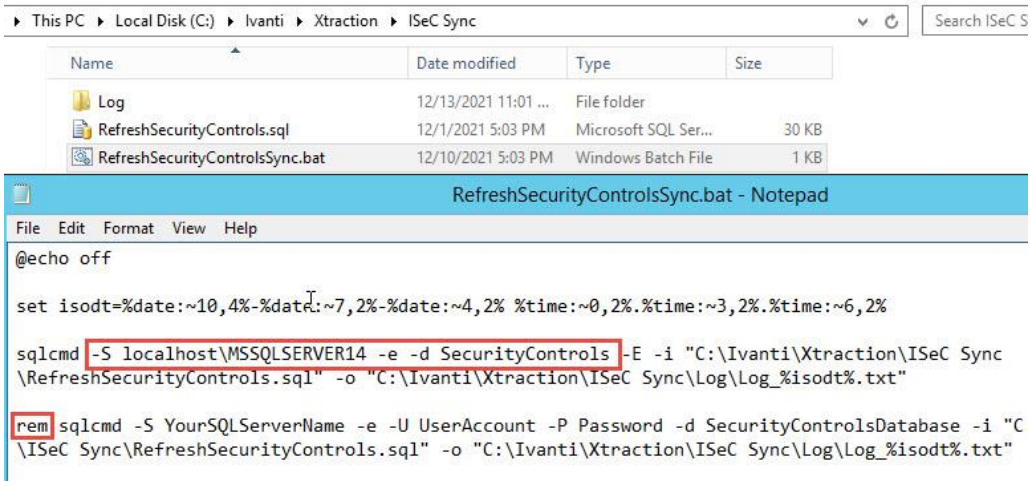
Messages

ITYPROCESSERRORLOGID	BATCHID	LOGDATE	ENTITYNAME	ERRORLINE	ERRORMESSAGE
	260	2021-12-10 17:06:23.080	xtr_UpdateData	14	Invalid object name 'xtrCurrentPatchStatus'.
	260	2021-12-10 17:06:23.077	xtr_DeleteODPatches	1	Invalid object name 'xtrCurrentPatchStatus'.
	260	2021-12-10 17:06:23.073	xtr_DeleteObsPatches	1	Invalid object name 'xtrCurrentPatchStatus'.
	260	2021-12-10 17:06:23.073	xtr_DeleteObsPatches	1	Invalid object name 'xtrCurrentPatchStatus'.
	260	2021-12-10 17:06:23.070	xtr_DeleteObsPatches	1	Invalid object name 'xtrCurrentPatchStatus'.

- if there is no record here, then the issue happened prior to the database sync being initiated and attention should be directed to the bat file the Scheduler is calling.

- Navigate to the location of the “RefreshSecurityControlsSync.bat” file.
  - “C:\Ivanti\Xtraction\ISeC Sync” folder by default

- Right Click to Edit in Notepad or another editor.
- Check the Server Name / Database / Creds (if using) are correct.
- Ensure the unused connection string has the work rem in front of it.



- Save any changes and Close the editor.
- If using SQL Authentication,
  - Double click the bat file to run.
- If using Windows Authentication
  - Holding down the SHIFT key, Right Click and Select Run as different user.
  - Insert the credentials of the account running the task in Task Scheduler, if that account is SYSTEM, use a different account that has at least dbo rights to the Security Controls DB.
    - This is just trouble shooting exercise to determine the script is running correctly.
- A command prompt window should open and stay open for the duration of the sync, it should not appear and disappear momentarily, this would indicate an error has occurred.
- Check the logs in the “C:\Ivanti\Xtraction\ISeC Sync\Log” folder, there should one there that corresponds to the current date and time and should be approx. 33KB in size.
- If there is an error, open the log to determine the cause, most common errors will be:
  - Cannot connect with the database
    - Usually, the log will be around 1K.
    - Check SQL Server service are running.
    - Recheck the connection string details in the “RefreshSecurityControlsSync.bat” file.
  - Permission issues
    - The log is usually around 31K and there is a message at the very end, similar to the one below.

```
Msg 229, Level 14, State 5, Server PROTECT\MSSQLSERVER14,
Procedure xtr_UpdateData, Line 1
The EXECUTE permission was denied on the object
'xtr_UpdateData', database 'SecurityControls', schema 'dbo'.
```

  - Confirm the permission script was run successfully against the Security Controls database, re-run if required for the account running the Task in the Windows Scheduler.

- Assuming the script ran correctly and there is still no data being synced, the next thing to check is Scheduled Task
  - Scroll down to the Ivanti / Security Controls / Reports folder and the “Xtraction ISeC Sync” task should be there.
  - Right click on the task and select Run.
  - Status of the job will appear after a short time or by manually refreshing.

- Potential Issues
  - Account running the Task does not have full control access to the folder containing the “RefreshSecurityControlsSync.bat” file.
  - Account in Task should be set to Run With Highest Privileges.
  - Task in some environments needs the following arguments added to the Action, copy lines below and paste into the arguments text box.

-NoProfile -WindowStyle Hidden -command "& {get-eventlog -logname Application -After ((get-date).AddDays(-1)) | Export-Csv -Path C:\Ivanti\Xtraction\ISeC Sync\Log\applog.csv -Force -NoTypeInformation}"