Set groups managedBy (user and groups) as SecurityIQ data owners

This guide contains 3 steps:

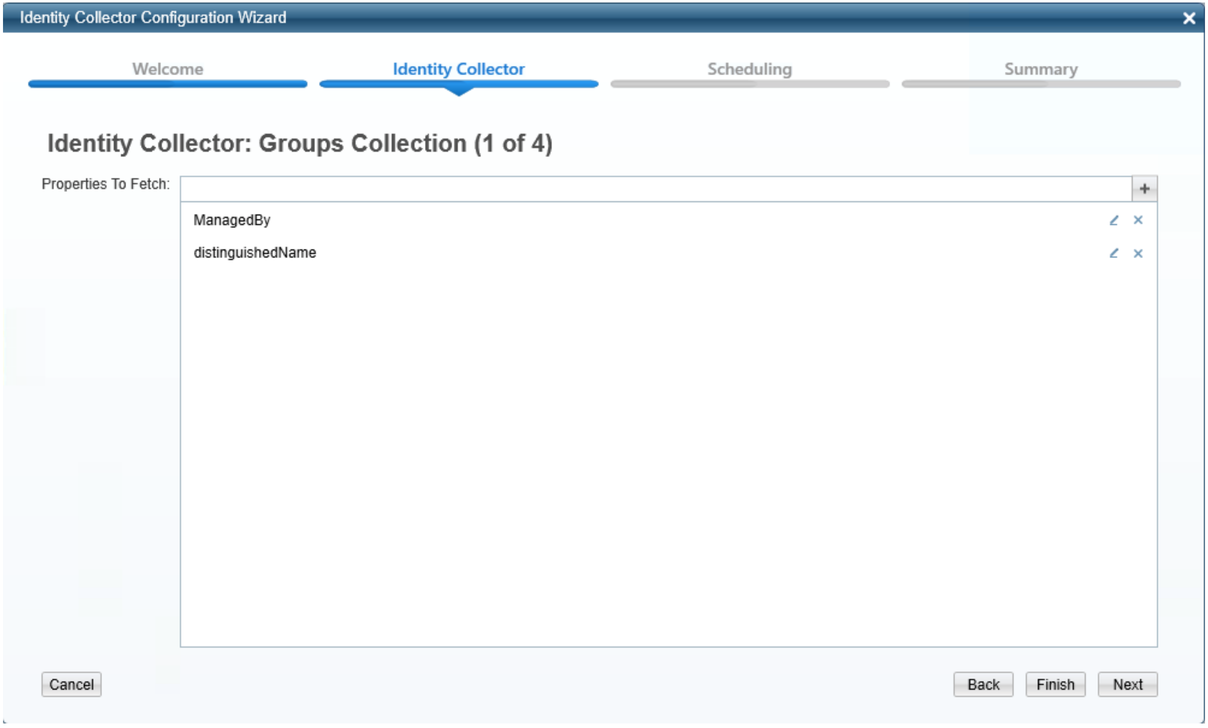
1. Extend Identity Collector to collect managedBy attribute
2. Create Store procedure that set the managedBy as SecurityIq data owners
3. Schedule a job that runs the above store procedure
4. test

1. Extend Identity Collector

a. Go to System -> Applications -> Permissions Management -> Identity Collectors -> Edit your Identity Collector that is connected to AD

b. Go to Identity Collector: Groups Collection (1 of4)

c. Add “ManagedBy” and “distinguishedName” (case sensitive)



Identity Collector: Groups Collection (1 of 4)

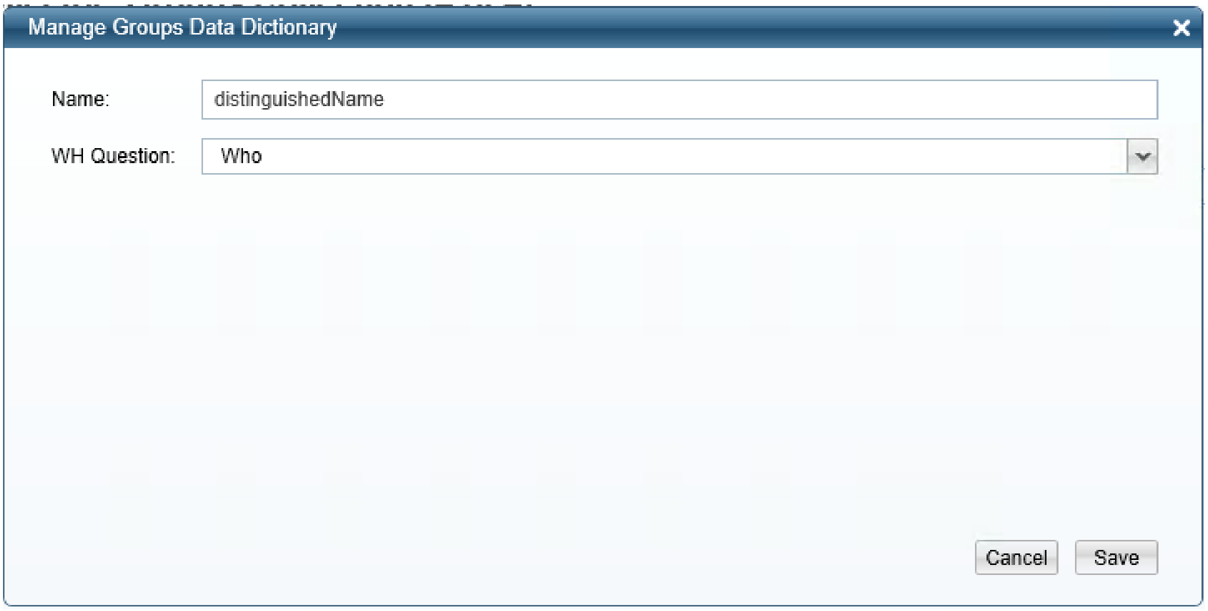
Properties To Fetch:

ManagedBy

distinguishedName

d. Click Next to page (4 of 4)

e. Create two new fields

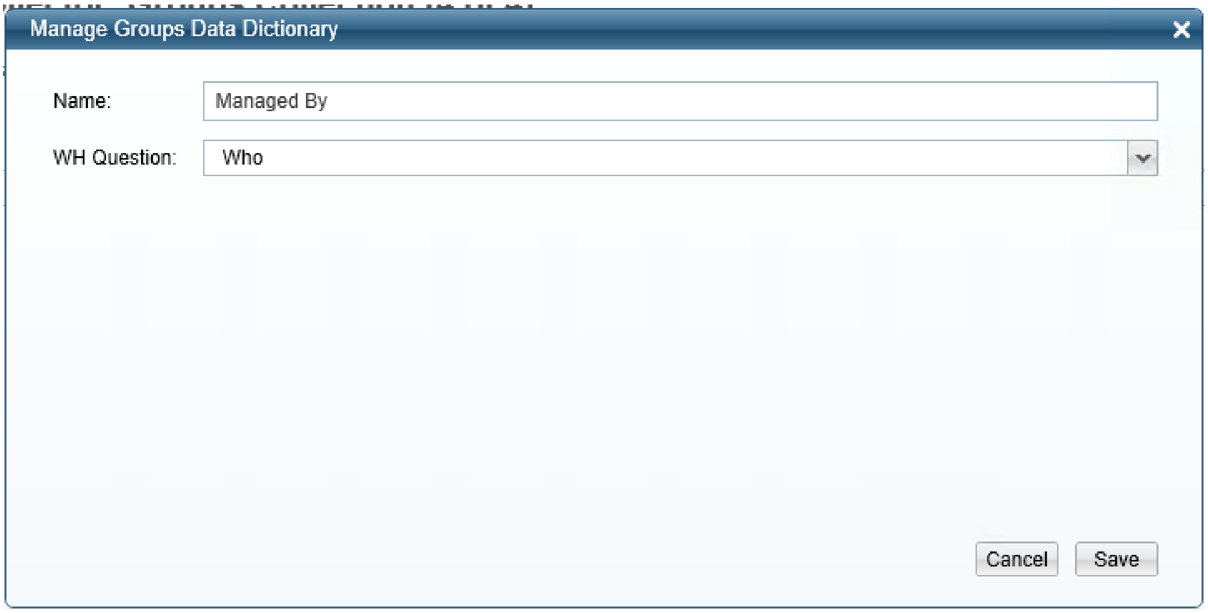


Manage Groups Data Dictionary

Name: distinguishedName

WH Question: Who

f. Click Save

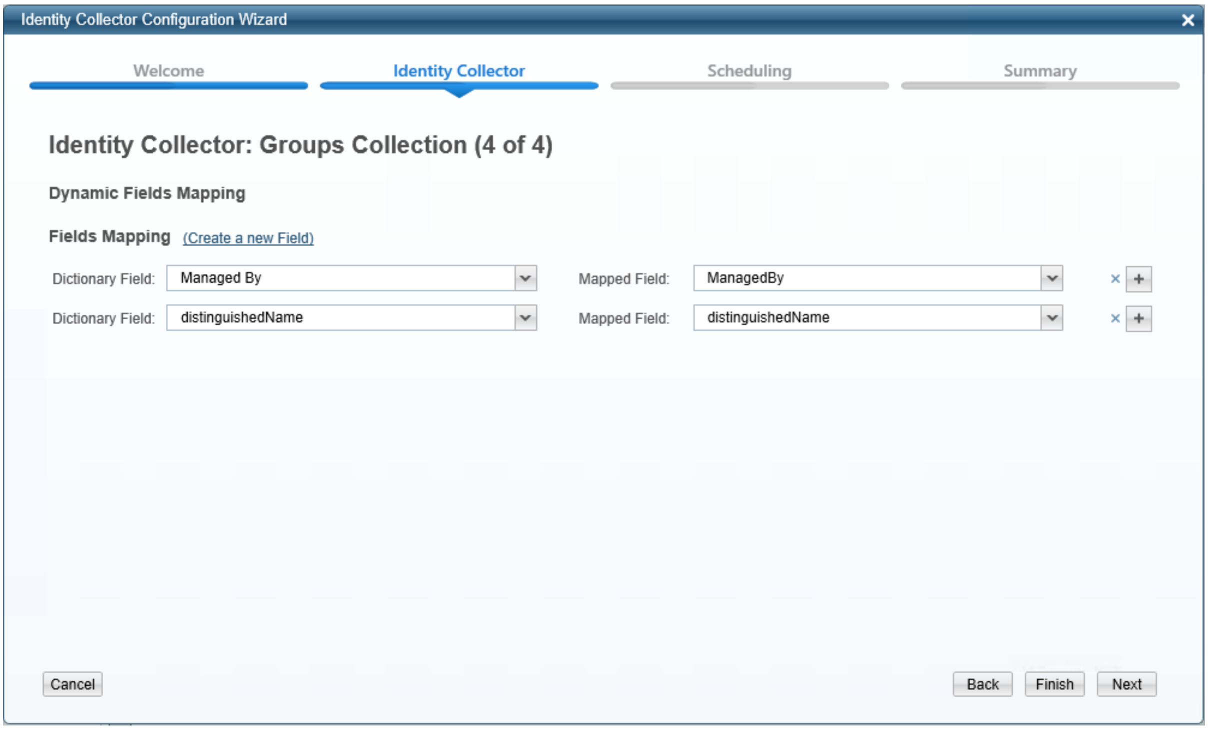


Manage Groups Data Dictionary

Name: Managed By

WH Question: Who

g. Map these two fields with the field that the Identity Collector will collect from AD:



Identity Collector: Groups Collection (4 of 4)

Dynamic Fields Mapping

Fields Mapping (Create a new Field)

Dictionary Field: Managed By — Mapped Field: ManagedBy

Dictionary Field: distinguishedName — Mapped Field: distinguishedName

h. Finish

Create Store procedure

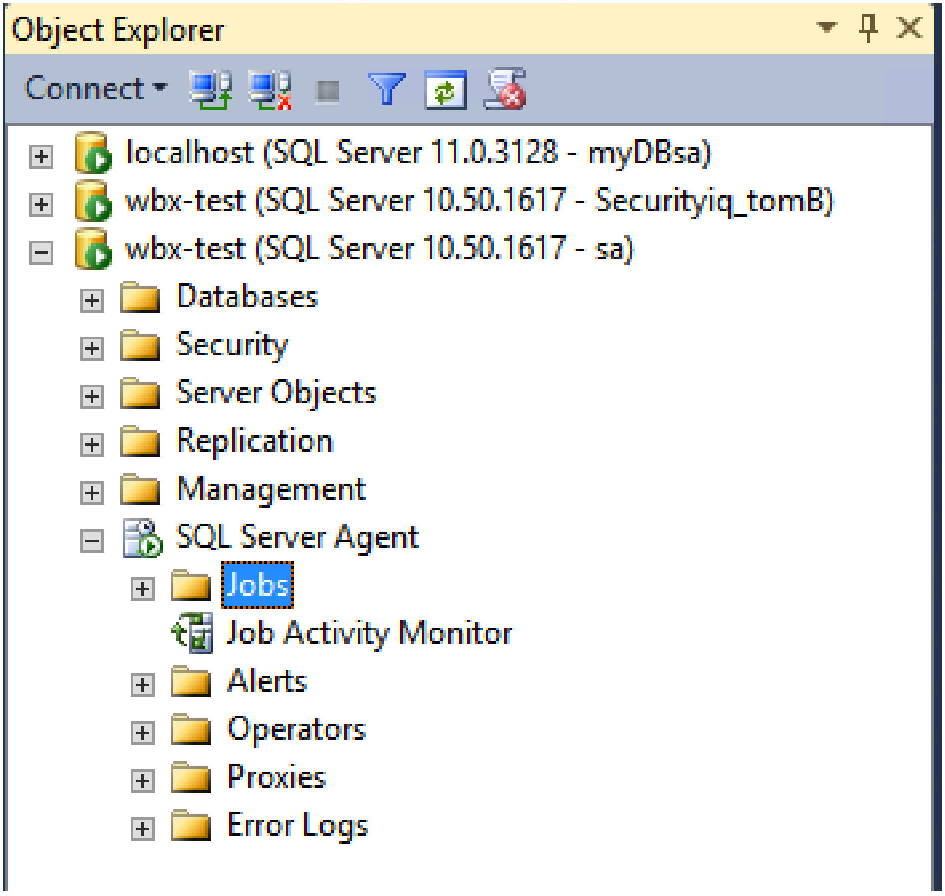
Run the following query to create Stored Procedure:

```
/****** Object:  StoredProcedure [whiteops].[sync_managedby_to_dataowner]
Script Date: 6/17/2018 3:02:07 PM
Created by tom.blinder@sailpoint.com******/
SET ANSI_NULLS ON
GO

SET QUOTED_IDENTIFIER ON
GO



CREATE PROCEDURE [whiteops].[sync_managedby_to_dataowner]
AS
BEGIN
          BEGIN TRY
          IF NOT EXISTS  (select * from sysobjects where name = 'managedby_to_data_owner_temp' and xtype='U')
    create table [whiteops].[managedby_to_data_owner_temp] (
        business_service_id BIGINT not null,
                   ra_user_id BIGINT not null
    )


          DELETE FROM [whiteops].[business_service_owner]
          WHERE EXISTS
            (SELECT *
            FROM [whiteops].[managedby_to_data_owner_temp]);

          TRUNCATE TABLE [whiteops].[managedby_to_data_owner_temp]

          INSERT INTO [whiteops].[managedby_to_data_owner_temp] (business_service_id,ra_user_id)(
                    SELECT bs.id AS 'resource_id',ru.id AS 'owner_id'
                             --bs.id 'resource_id',bs.br_name,ru.id AS 'role_id', ru.user_display_name
                             FROM whiteops.ra_role rr
                             LEFT JOIN whiteops.ra_user ru
                             ON rr.role_field1 = ru.user_full_name
                             LEFT JOIN whiteops.business_service bs
                             ON bs.name = rr.role_name
                             --Select only groups that the managedBy field is not empty
                             Where rr.role_field1 IS NOT NULL
                             --verify it is managedBy user (not a group)
                             AND ru.id IS NOT NULL
                    UNION ALL
                    -- calculation groups that are set as managedBy, open them and set the members (users) as owners
                    SELECT --bs.id 'resource_id',ru.id AS 'role_id'
                             bs.id AS 'resource_id',rurv.user_id AS 'owner_id'
                             --bs.id 'resource_id',bs.br_name,rr.id AS 'role_id', rr.role_name
                             FROM whiteops.ra_role rr
                             LEFT JOIN whiteops.ra_role rr2
                             ON rr.role_field1 = rr2.role_field2
                             LEFT JOIN whiteops.business_service bs
                             ON bs.name = rr.role_name
                             LEFT JOIN whiteops.bam b
                             ON bs.parent_bam_id =b.id
                             LEFT JOIN [whiteops].[ra_user_role_view_no_everyone] rurv
                             ON rr2.id = rurv.role_id
                             --LEFT JOIN whiteops.ra_user ru
                             --ON rur.ra_user_id = ru.id
                             Where rr.role_field1 IS NOT NULL
                             --verify that the resource managedBY a group (not user)
                             AND rr2.id IS NOT NULL
                             --resource is from AD application
                             AND b.bam_type_id=9
          )


          INSERT INTO [whiteops].[business_service_owner] (business_service_id,ra_user_id)
          SELECT *
          FROM [whiteops].[managedby_to_data_owner_temp]

          END TRY
          BEGIN CATCH

          END CATCH
END
GO
```

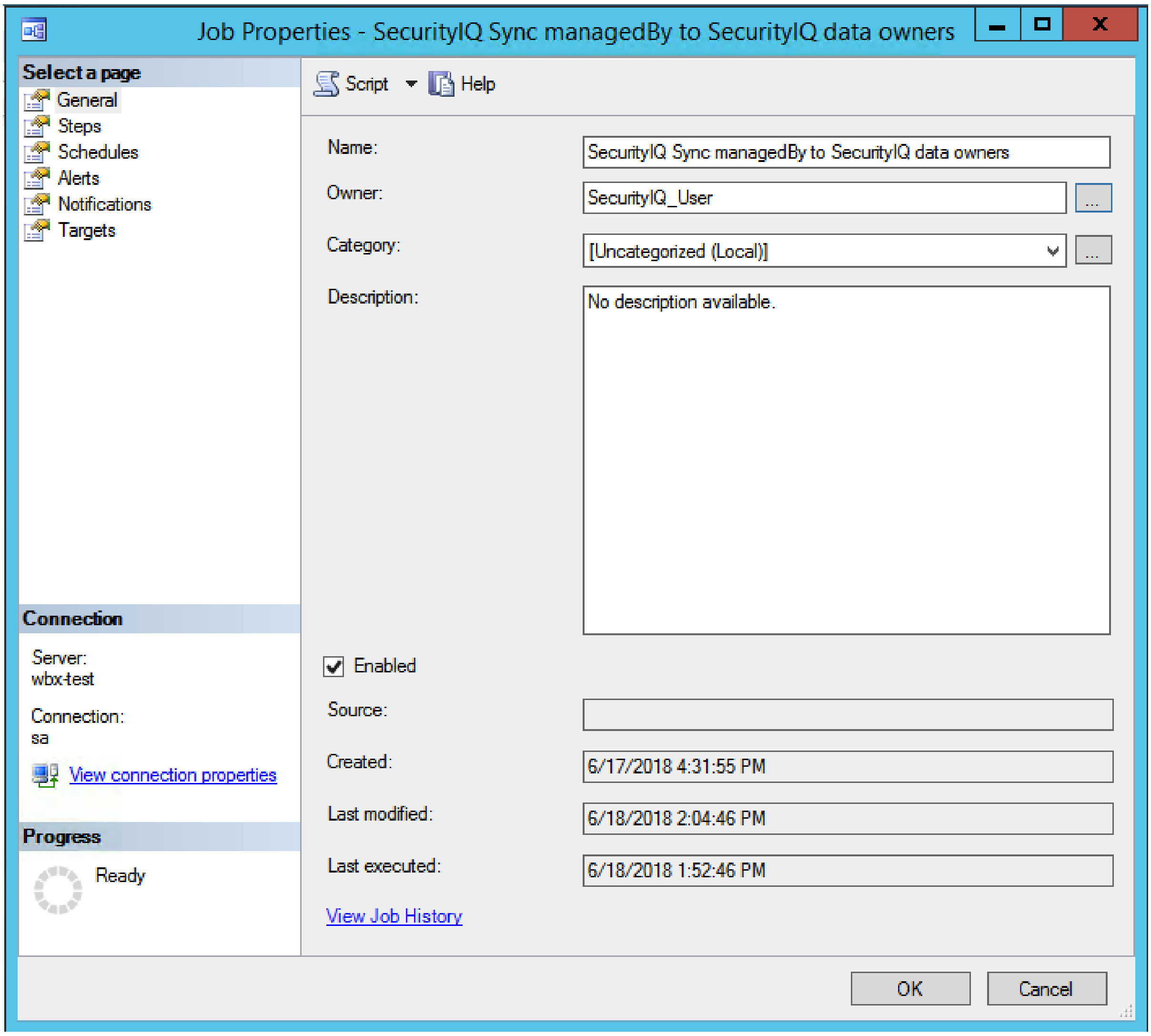
Schedule a job

Create a job and schedule the above stored procedure to run nightly

1. Choose SecurityIQ database
2. Go to SQL Server Agent -> Jobs -> Right click -> New Job...



3. Name it: SecurityIQ Sync managedBy to SecurityIQ data owners
4. Owner: choose SecurityIQ user



Server:
wbx-test

Connection:
sa

View connection properties

Name: SecurityIQ Sync managedBy to SecurityIQ data owners

Owner: SecurityIQ_User

Category: [Uncategorized (Local)]

Description: No description available.

☑ Enabled

Source:

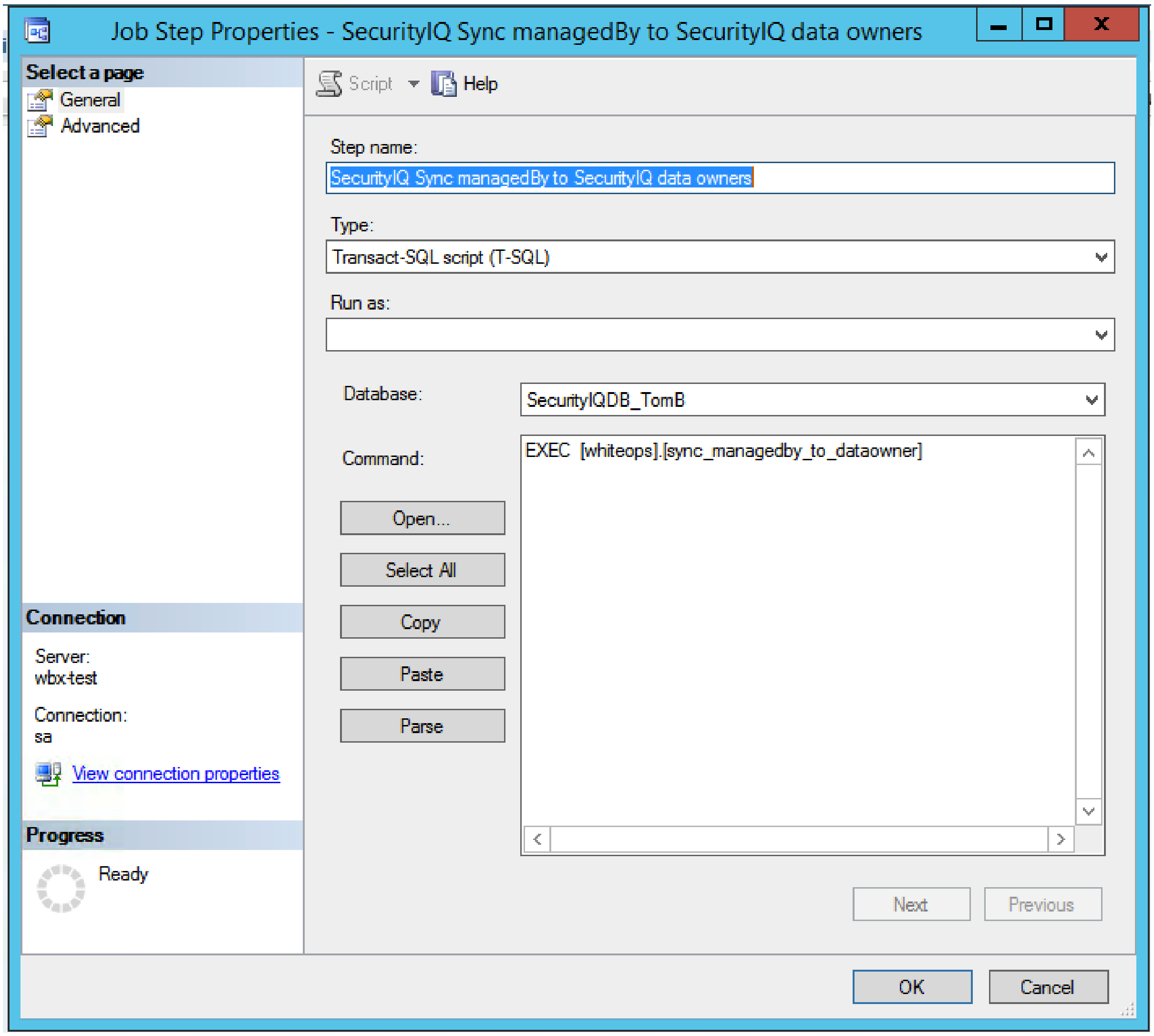
Created: 6/17/2018 4:31:55 PM

Last modified: 6/18/2018 2:04:46 PM

Last executed: 6/18/2018 1:52:46 PM

View Job History

5. Go to Steps -> New…
   a. Give this step a name
   b. Set the database to SecurityIQ database
   c. In the command field type:
      EXEC [whiteops].[sync_managedby_to_dataowner]



Job Step Properties - SecurityIQ Sync managedBy to SecurityIQ data owners

Step name: SecurityIQ Sync managedBy to SecurityIQ data owners

Type: Transact-SQL script (T-SQL)

Run as:

Database: SecurityIQDB_TomB

Command:

```
EXEC  [whiteops].[sync_managedby_to_dataowner]
```

Connection

Server: wbx-test

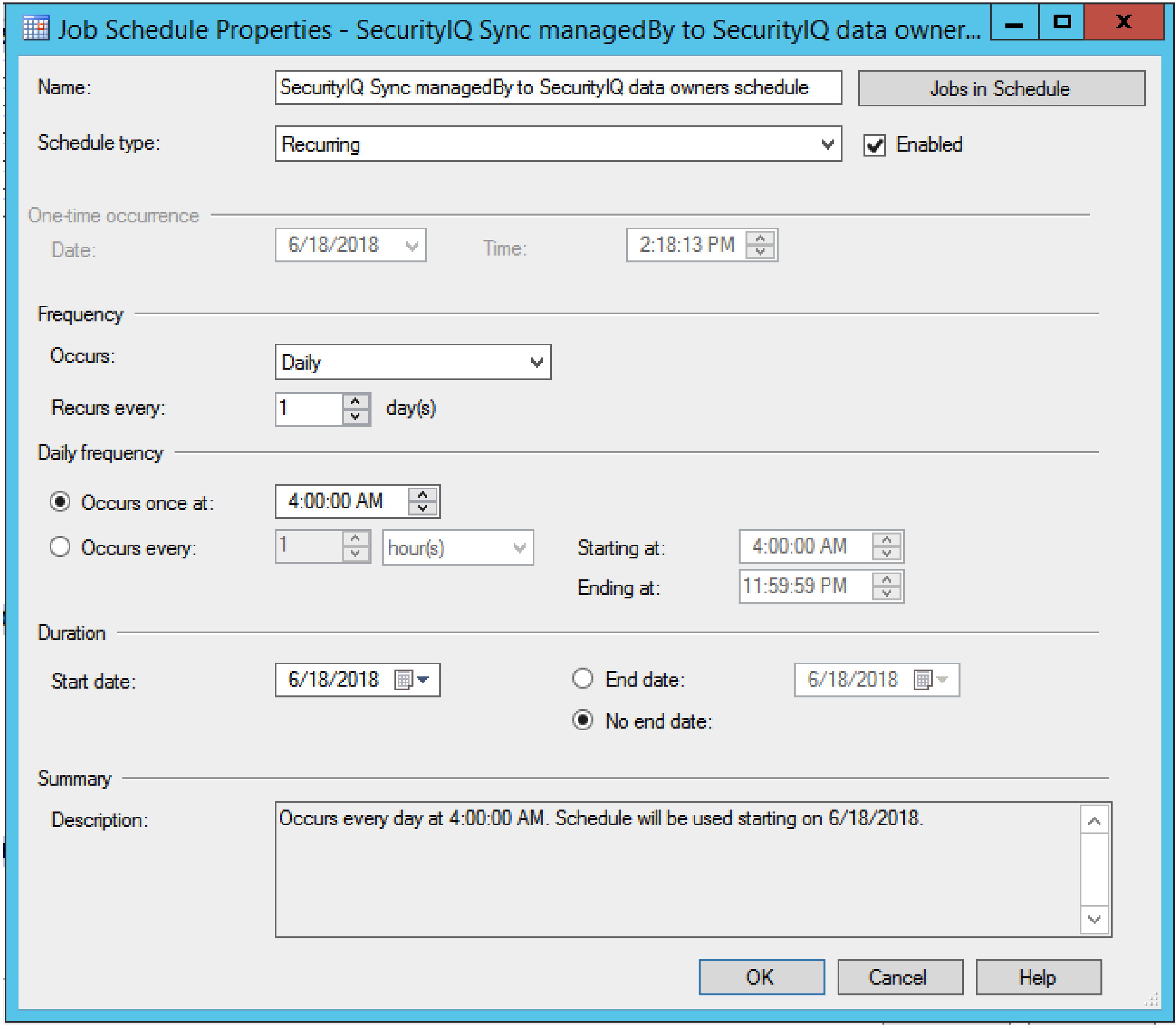
Connection: sa

Progress

Ready

6. Click the OK button
7. Go to Schedules -> New…
8. Give the schedule a name:
    a. SecurityIQ Sync managedBy to SecurityIQ data owners schedule
    b. Schedule it to run daily (recommended to run after the Identity Collector completes its run)

c. Example:



Job Schedule Properties - SecurityIQ Sync managedBy to SecurityIQ data owner...

Name: SecurityIQ Sync managedBy to SecurityIQ data owners schedule

Schedule type: Recurring ☑ Enabled

One-time occurrence

Date: 6/18/2018 Time: 2:18:13 PM

Frequency

Occurs: Daily

Recurs every: 1 day(s)

Daily frequency

● Occurs once at: 4:00:00 AM

○ Occurs every: 1 hour(s) Starting at: 4:00:00 AM Ending at: 11:59:59 PM

Duration

Start date: 6/18/2018 ○ End date: 6/18/2018

● No end date:

Summary

Description: Occurs every day at 4:00:00 AM. Schedule will be used starting on 6/18/2018.

d. Click OK and close the wizard.

9. To run this job new without waiting for the schedule, Right Click the job that we have just created -> Start Job at Step…

Test

Open SecurityIQ Admin Console

1. go to System -> Application -> in the Business Resource Tree, Choose the relevant AD application and double click it.
2. Click the Data Owners button to verify that the data owners were set.