Splunk for Forefront Identity Manager App
Oxford Computer Group

Splunk for FIM App user guide

Author(s)	Wim van den Heijkant (Senior Consultant)
Version	1.0
Date	5 April 2013

1 Introduction

This document is meant as a quick start / user guide for using the "Splunk for Forefront Identity Manager" app by Oxford Computer Group.

This user guide includes some screenshots of what reports can look like after you have successfully installed and configured the app, and this guide explains what the aim is of the given report or dashboard.

This guide doesn't explain how to install the Splunk for FIM app, nor does it explain how you configure log collection. There are separate documents that explain both these topics. For more information please contact lab@oxfordcomputergroup.nl.

This guide focuses mostly on the current version 1.1 of the Splunk for FIM app which is now available on Splunk-base http://splunk-base.splunk.com/apps/79890/splunk-for-forefront-identity-manager. But since this app is constantly in development, we will also show some of the new reports that will be available in version 1.2.

For more information about the Splunk for FIM app - version 1.2 please contact lab@oxfordcomputergroup.nl

2 Features

After installing the Splunk for FIM app you will get the following welcome screen:

It contains a link to the *Install and Configure* section that will help you setup and configure log collection and it introduces the 3 main features of the app:

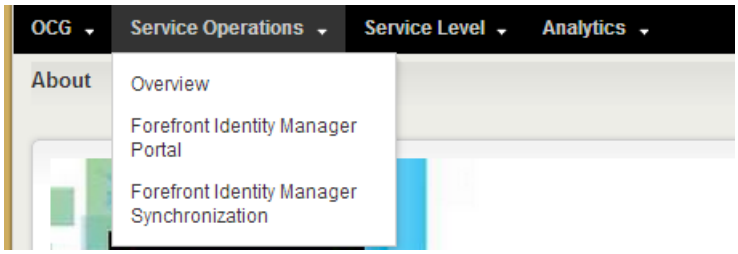
- Service Operations
- Service Level
- Analytics

This document will show example reports of all 3 of these features.

3 Service Operations

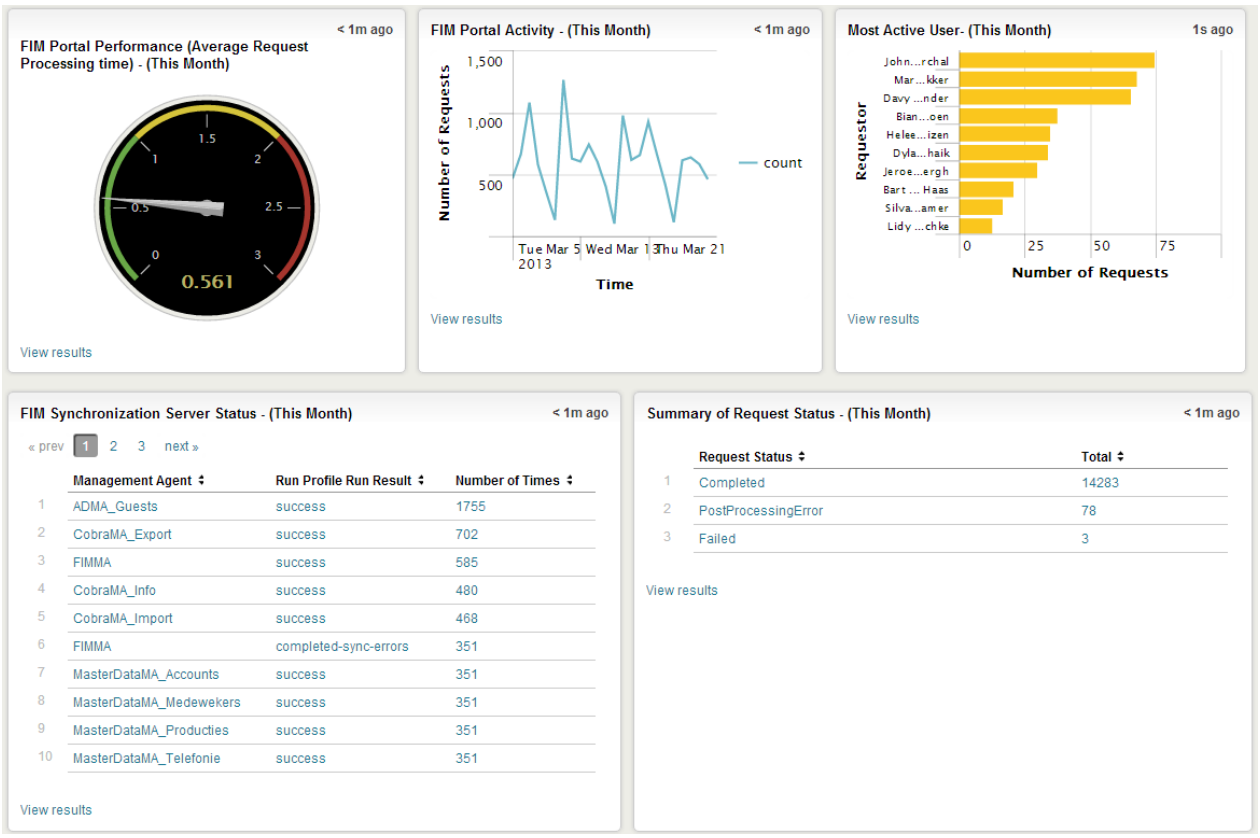
The dashboards in the *Service Operations* section of the Splunk for FIM app are targeted towards the IT operations team. It gives a quick insight in how the Forefront Identity Manager solution is functioning by showing error messages, activity and service response times.

The service operations menu consists of the following options:



3.1 Overview

The overview dashboard shows the following reports:



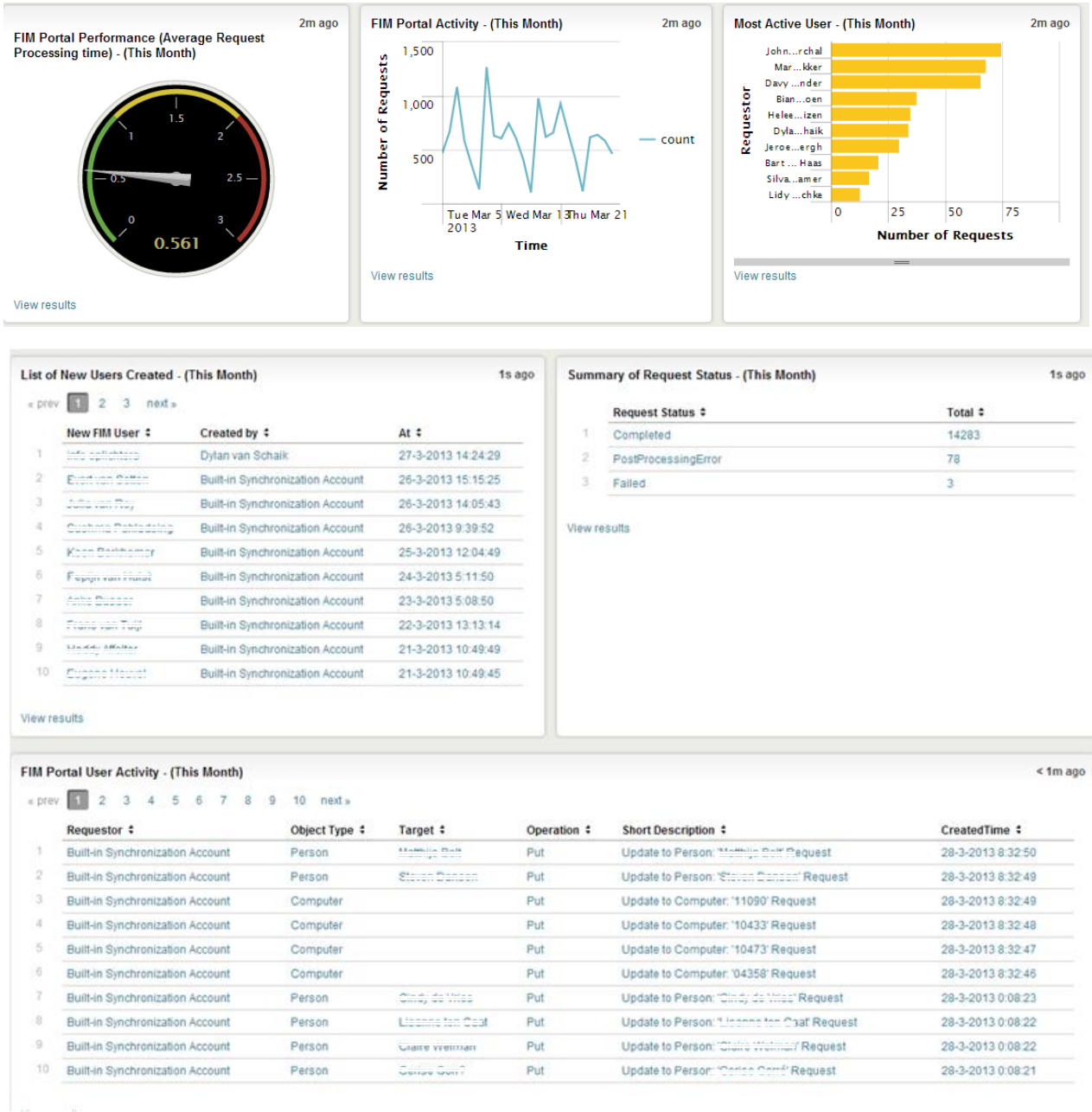
	Management Agent	Run Profile Run Result	Number of Times
1	ADMA_Guests	success	1755
2	CobraMA_Export	success	702
3	FIMMA	success	585
4	CobraMA_Info	success	480
5	CobraMA_Import	success	468
6	FIMMA	completed-sync-errors	351
7	MasterDataMA_Accounts	success	351
8	MasterDataMA_Medewekers	success	351
9	MasterDataMA_Producties	success	351
10	MasterDataMA_Telefonie	success	351

From left to right from, top to bottom we see:

- FIM Portal Performance (Average Request Processing time) - (This Month)
  This is meant to show how your FIM Portal is performing by showing how long a request takes to get processed.
- FIM Portal Activity - (This Month)
  This shows how much activity there is on the FIM portal, what have been the busy days.
- Most Active User- (This Month)
  This shows the top 10 most active users in of the FIM portal
- FIM Synchronization Server Status - (This Month)
  This report shows the number of runs the FIM synchronisation service has made including how many runs were successful and how many runs contained errors.
- Summary of Request Status - (This Month)
  This shows the number of FIM portal requests including how may were successful and how many failed.

3.2 Forefront Identity Manager Portal

The Forefront Identity Manager Portal dashboard shows the following reports:



We see a number of the same reports, but also a couple of new ones:

- List of New Users Created - (This Month)
  Gives an overview of the new users that where created in FIM last month.
- FIM Portal User Activity - (This Month)
  Gives an overview of what happened in the FIM portal, we see users and computer objects that are managed in this portal and we see the name of the user that was updated.

3.3 Forefront Identity Manager Synchronization

The Forefront Identity Manager Synchronization dashboard shows the following reports:

Synchronization Performance Statistics - (This Month) < 1m ago

« prev 1 2 next »

	Management Agent	Number of Runs	Averarage run time	Fastests Run Time	Longest Run time
1	ADMA	702	13.18	0.08	386.48
2	ADMA_Guests	1755	0.49	0.03	23.28
3	Avaya_Info1	234	10.51	5.97	65.63
4	Avaya_Info2	234	1.88	1.06	12.02
5	CobraMA_Export	702	72.82	0.16	252.31
6	CobraMA_Import	468	60.80	13.37	148.80
7	CobraMA_Info	481	75.06	14.25	191.19
8	FIMMA	936	11.62	0.11	397.59
9	LastLogonMA	234	58.61	11.20	135.47
10	MasterDataMA_Accounts	351	11.42	0.09	137.91

View results

Synchronization Error Statistics - (This Month) < 1m ago

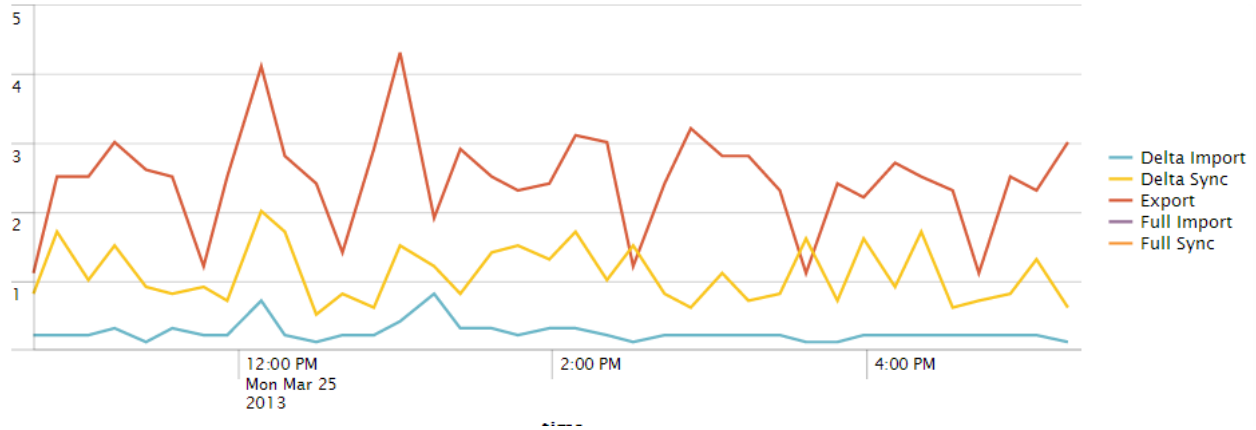
	Management Agent	Run Profile Run Result	Number of Times
1	ADMA	completed-export-errors	119
2	ADMA	completed-sync-errors	234
3	ADMA	completed-transient-objects	234
4	ADMA	extension-dll-timeout	13
5	CobraMA_Info	in-progress	1
6	FIMMA	completed-sync-errors	351
7	RuimteImportMA	completed-discovery-errors	117
8	ToegangspassenImportMA	completed-sync-errors	117

View results

We see the following:

- Synchronization Performance Statistics - (This Month)
  Shows the fastest, shortest and average synchronization times by management agent name. This report gives insight into which management agent is the slowest and which one is fastest.
- Synchronization Error Statistics - (This Month)
  Gives an overview which management agent gave which and how many errors.

Note; The next version of the Splunk for FIM app (version 1.2) we will add a historic overview of the performance by MA and Run profile:

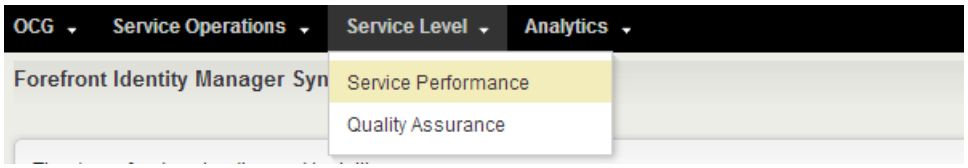


For more information about the Splunk for FIM app version 1.2, please contact lab@oxfordcomputergroup.nl.

4 Service Level

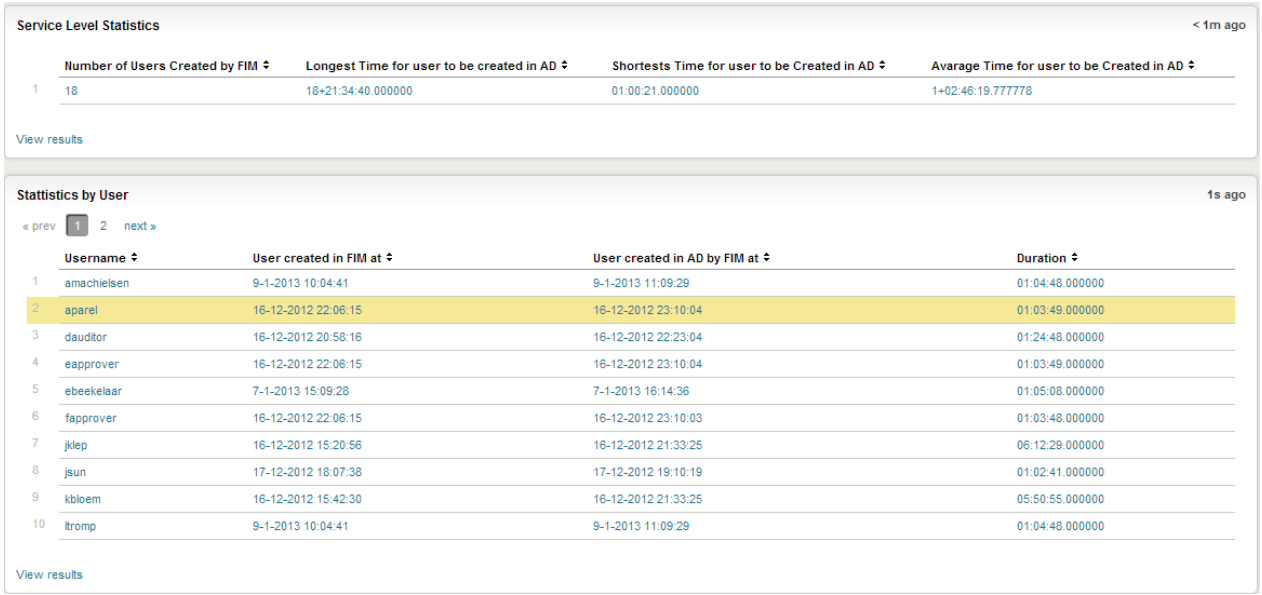
The dashboards in the Service Level section of the Splunk for FIM app are targeted towards IT service management. The reports attempt to give insights into the level of service that Forefront Identity Manager is currently delivering. If you have a Service Level Agreement where is mentioned that "users should be provisioned with an account within one hour" these reports may help you. The reports show the time it took for a user to get from Forefront Identity Manager to Active Directory. Additionally we try to supply insights into the quality of service Forefront Identity Manager is delivering by showing how many of your Active Directory users are managed by Forefront Identity Manager.

The *Service Level* menu consists the following options:



4.1 Service Performance

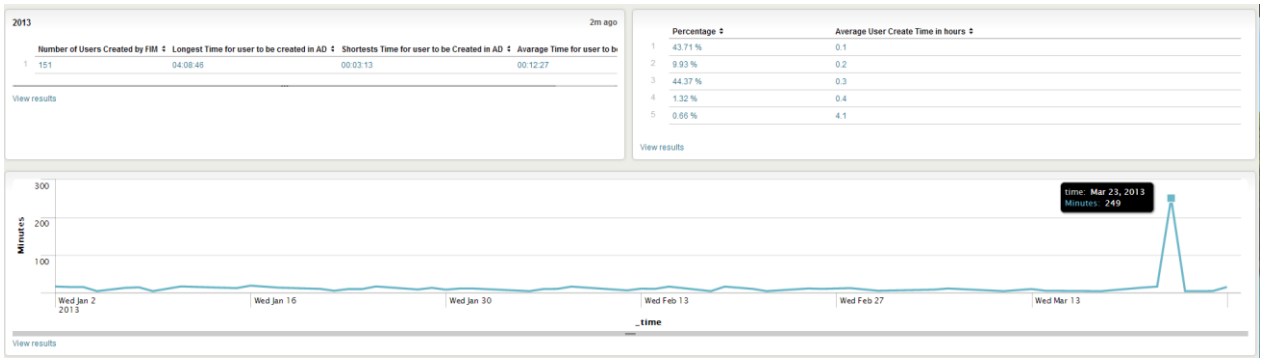
The *Service Performance* dashboard shows the following reports:



We see the following:

- Service Level Statistics
  This shows how many users where created by Forefront Identity Manager including the shortest, longest and average time for the user to get created in Active Directory.
- Statistics by User
  Gives an overview of the user and the time it took for them to get created in AD.

Note: For the next version of the Splunk for FIM app (version 1.2) we will add more context to these statistics by adding historic graphs:



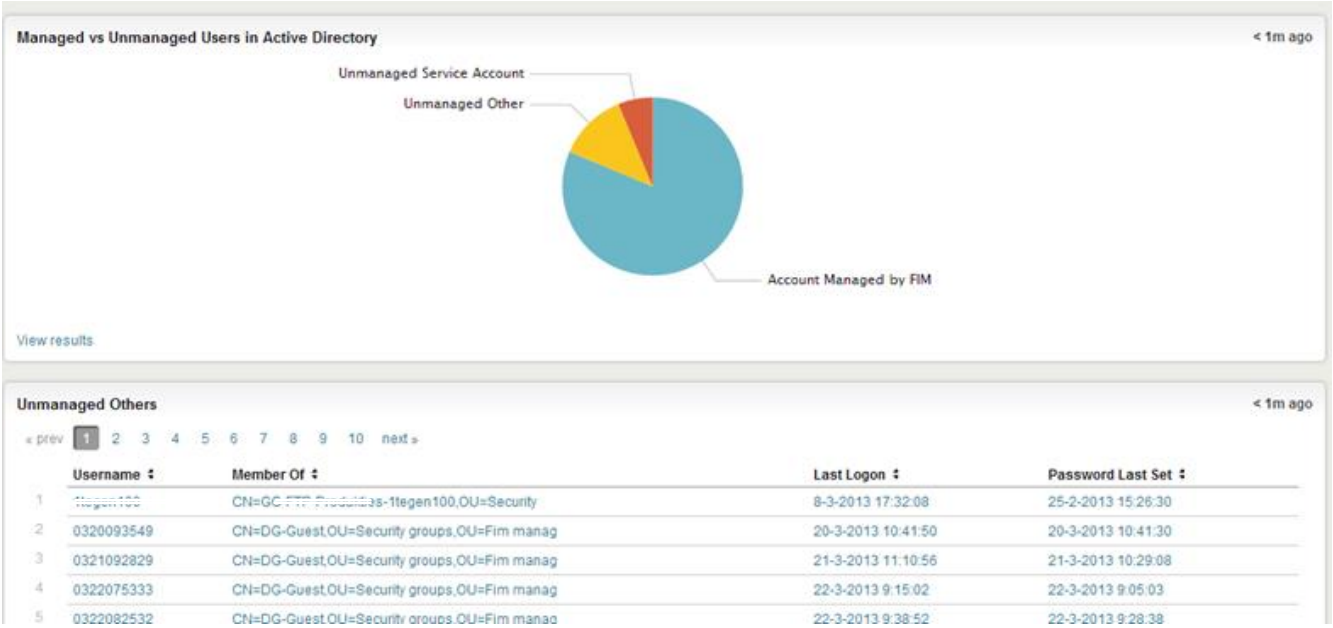
This helps to show when the service level was met and when there was a significantly longer creation time.

It shows that there was an issue on the 23 of March and it also shows that only 0.66% of users were created in more than 0.4 hours.

For more information about the Splunk for FIM app version 1.2 please contact lab@oxfordcomputergroup.nl

4.2 Quality Assurance

The quality assurance dashboard shows the following reports:



We see the following:

Managed vs Unmanaged Users in Active Directory

This shows how users in Active Directory are managed by your Forefront Identity Manager implementation.

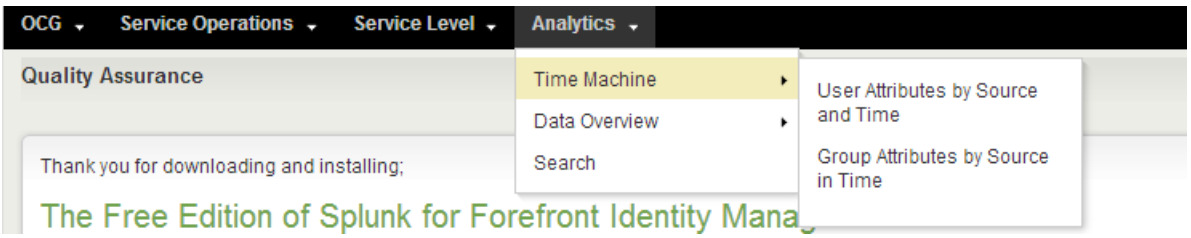
- Unmanaged Others

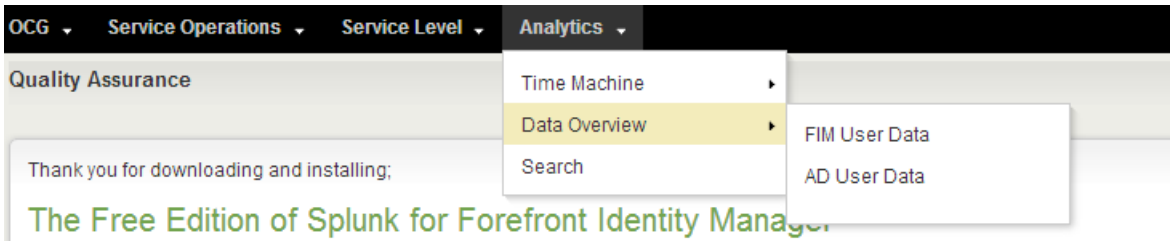
  Gives an overview of which accounts are currently not managed by Forefront Identity Manager.

5 Analytics

The dashboards in the analytics section of the Splunk for FIM app are targeted towards IT security or IT operations employees that need to do some analysis on identity data.

- Current data in the *Data Overview* section
- Historic data in the *Time Machine* Section
- Just a random search using the great Splunk *Search* functionality



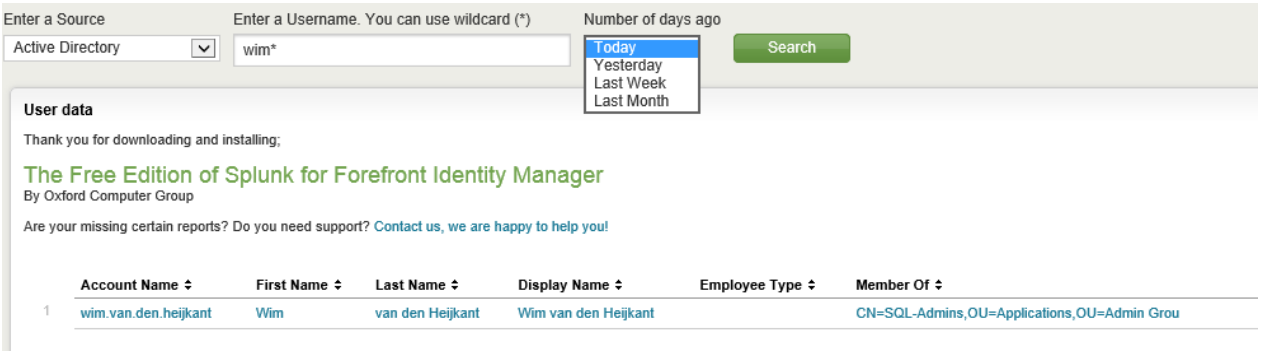


5.1 Time Machine

The *Time Machine* functionality is built to answer the question: What was the status of a user or group at a given moment in time in a given identity store. Answers to these questions can be interesting for IT security employees that need to know who had access to a certain resource at a given time. This information should also be interesting for IT operations.
These questions are really hard to answer with just Forefront Identity Manager.

5.1.1 User Attributes by Source in Time

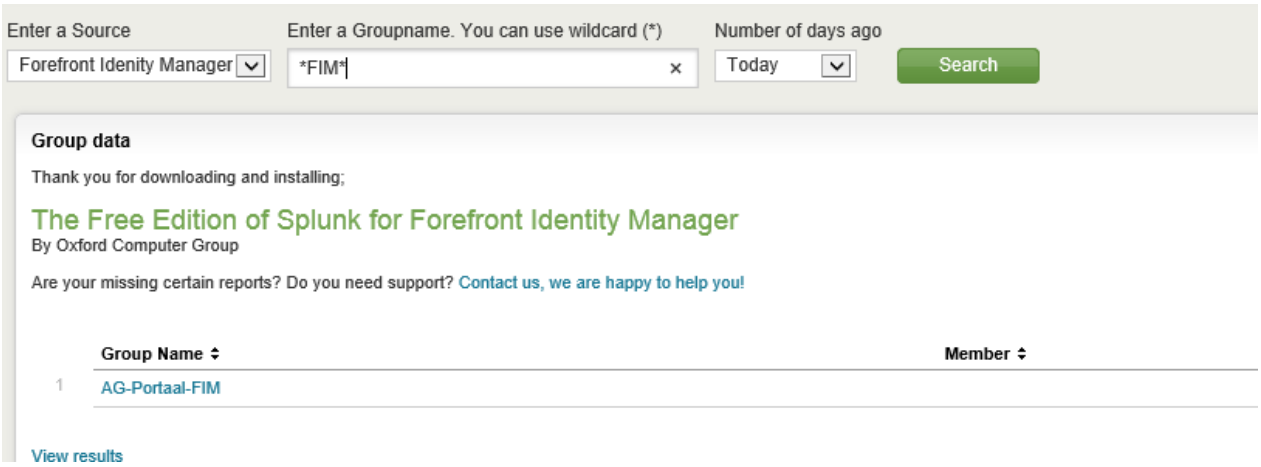
The user attributes by *Source in Time* feature contains the following search bar:



It allows you to search for user records within Active Directory or Forefront Identity Manager at any given time in history.

5.1.2 Group Attributes by Source in Time

The group attributes by *Source in Time* feature contains the following search bar:



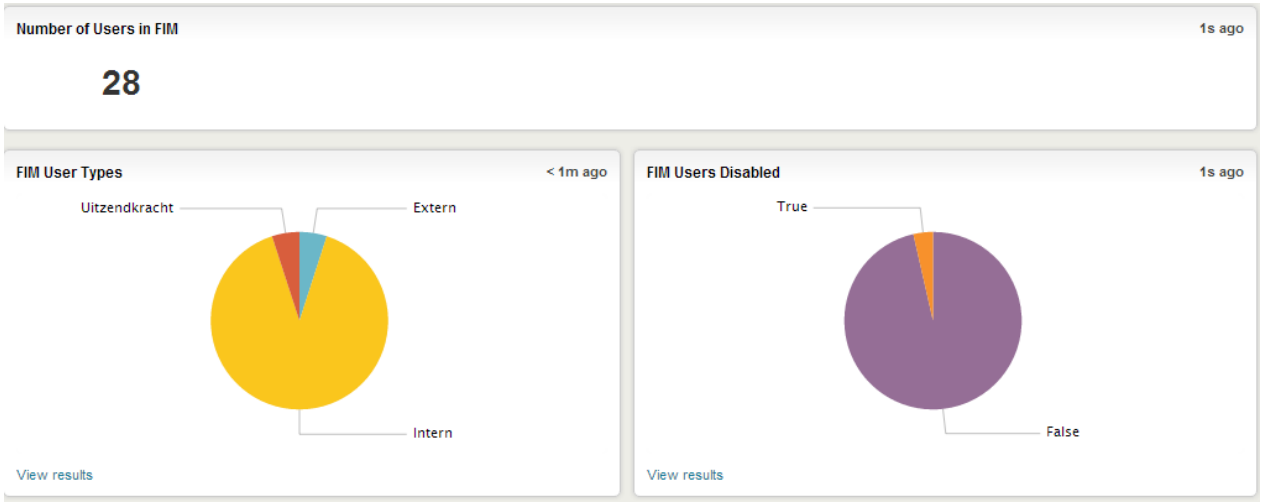
Andy basically gives you similar options but this time from the group perspective.

5.2 Data Overview

The *Data Overview* section is built to allow us to add some other interesting insights into the current state of the user and group data.

5.2.1 FIM User Data

FIM User Data contains the following reports:

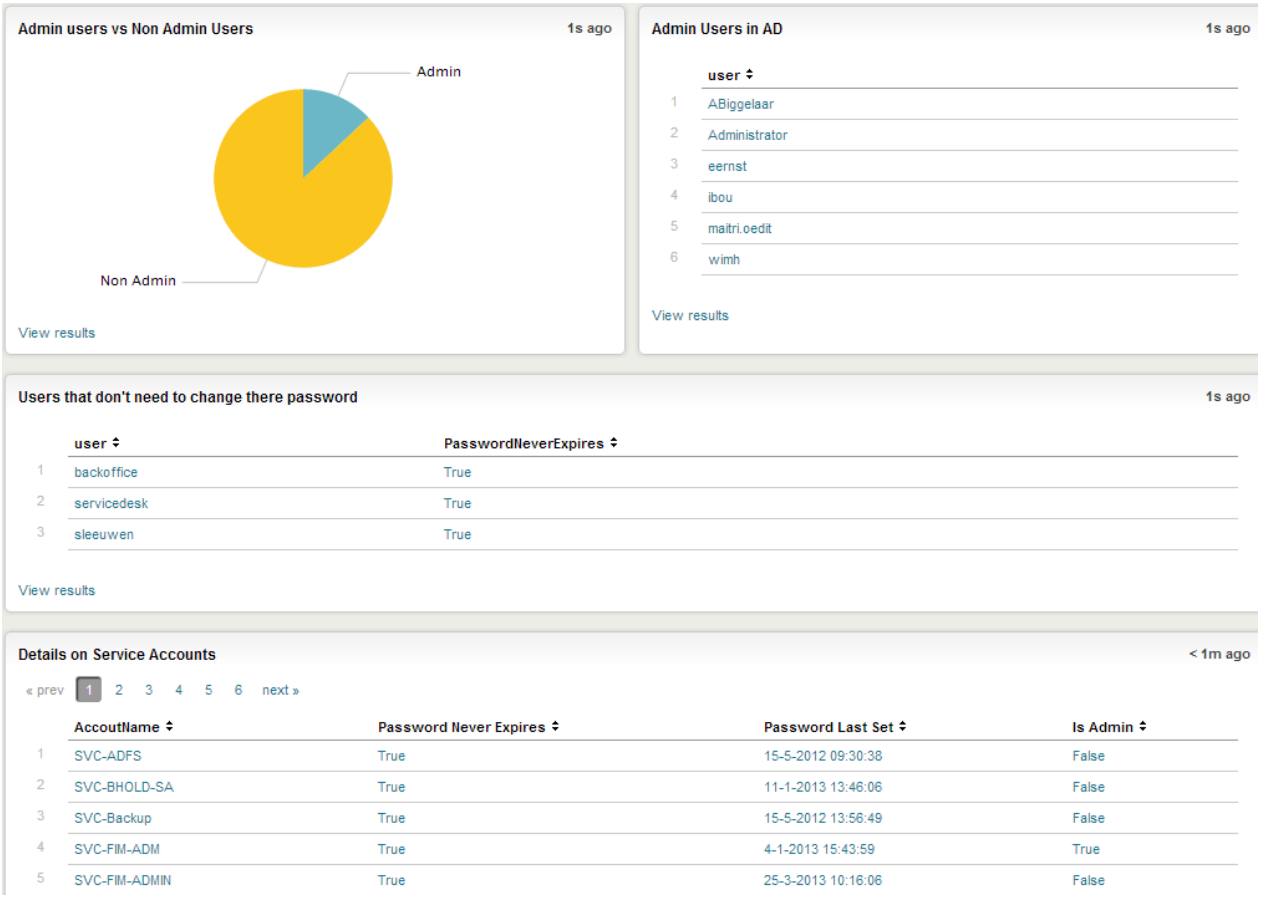


We see the following:

- Number of Users in FIM
  Counts of the number of FIM users.
- FIM User types
  A pie chart of the different employee types within FIM.
- FIM Users Disabled
  Insight into how many FIM users are disabled.

5.2.2 AD User Data

AD User Data contains the following reports:



We see the following:

- Admin users vs Non Admin Users
  Shows how many users in Active Directory have admin user privileges.
- Admin users in AD
  Shows a list of the Admin users, these can easily be exported to CSV or XML.
- Users that don't need to change their password
  Shows which users in Active Directory don't need to change their password.
- Details on Service Accounts
  Shows a list of service accounts in use in your environment, when the password was last set, if they have admin privileges etc.

5.3 Search

The *Search* feature lets you use the powerful built in search functionality of Splunk to find anything that isn't in any of the default reports.